# Kartlegging av sektorlovgivning som regulerer virksomheters tiltak mot tilsiktede hendelser

## Innledning

Denne kartleggingen skal bidra med bakgrunnsstoff til følgende punkt i sikkerhetsutvalgets mandat: «Utvalget skal foreta gjennomgang av relevante sektorregelverk som regulerer beskyttelse av objekter og infrastruktur».

Utgangspunktet for å identifisere relevant regelverk er den forståelsen av begrepene samfunnskritiske funksjoner, samfunnskritisk infrastruktur og nødvendig funksjonsevne som er lagt til grunn i rapporten *Samfunnets kritiske funksjoner* («KIKS II»), som foreligger i høringsutgave pr. september 2015 fra Direktorat for samfunnssikkerhet og beredskap (DSB). Rapportens definisjon av samfunnskritisk bygger igjen på Infrastrukturutvalgets rapport, NOU 2006:6, *Når sikkerheten er viktigst*. Det er imidlertid bare i sjeldne tilfeller man finner disse begrepene direkte anvendt i rettskildene, og det er nokså varierende hvor tydelig ulike regelverk krever tiltak rettet mot tilsiktede uønskede hendelser.

Kartleggingen søker å identifisere hvilke regelverk som er rettet mot tilsiktede hendelser som kan ramme ulike offentlige eller private virksomheter på en slik måte at det får konsekvenser for samfunnskritiske funksjoner. Den omfatter både regelverk som har rendyrket krav til tiltak mot tilsiktede hendelser, og regelverk der kravene til tiltak er felles for tilsiktede og utilsiktede hendelser. Felles tiltak for tilsiktede og utilsiktede hendelser omtales tidvis som en «all hazards approach».

I utgangspunktet faller de regelverkene som kun omhandler utilsiktede hendelser, slik som ulykker og naturkatastrofer, utenfor denne kartleggingen. Enkelte innslag av regelverk som kun gjelder utilsiktede hendelser er nevnt i teksten, fordi de brukes til å illustrere forskjellene i ulike regelverk, eller til å drøfte om de reguleringer som gjelder for et virksomhetsområde kan sies å omfatte tilsiktede hendelser eller ikke. Det er bare de regelverk som er ført opp i tabellen over relevante lover og forskrifter som i denne kartleggingen anses å regulere virksomheters plikter til å etablere tiltak mot tilsiktede uønskede hendelser.

I denne kartleggingen, og i sikkerhetsutvalgets mandat, blir *tilsiktede* hendelser og handlinger satt opp som et motstykke til de utilsiktede hendelsene. Det er, som man kan se av dateringen av lover og forskrifter på området, en tendens til økende oppmerksomhet om behovet for at virksomheter håndterer tilsiktede hendelser på en systematisk og forberedt måte. I enkelte tilfeller vil også argumentasjonen i forarbeider til nyere lovendringer bekrefte en grad av faglig kursjustering i regelverkene. Likevel er det mange fellestrekk både i regelverket og i det konkrete sikkerhetsarbeidet, uavhengig av om det en skal gardere seg mot er en tilsiktet eller utilsiktet hendelse. I begge tilfeller vil det dreie seg om å ta stilling til hendelser som kanskje inntreffer, etablere hensiktsmessige og økonomisk forsvarlige tiltak, sørge for jevnlige nye vurderinger, og beslutte eventuelle endringer i sikkerhetsarbeidet dersom det er nødvendig osv. I en kartlegging som denne er det en viss fare for å vie forskjellene mellom tilsiktede og utilsiktede hendelser noe større plass enn de åpenbare likhetene.

Oversikten over regelverk som pålegger tiltak rettet mot tilsiktede hendelser er delt inn i ulike *områder*. Disse områdene følger en funksjonell systematikk, som i stor grad sammenfaller med det

man vanligvis betegner som sektorer, eksempelvis samferdsel, energi, helse, finans osv. Samtidig finnes det også funksjonelle områder som er mer sektorovergripende, som også hører hjemme i det samme bildet. Det gjelder særlig IKT og informasjonssikkerhet, med regelverk som praktisk talt alle virksomheter må forholde seg til. Farlige kjemiske, biologiske og radioaktive stoffer og eksplosiver (CBRNE) er også et område som involverer virksomheter og fagmyndigheter i flere sektorer.

Gjennomgangen av de enkelte områdene er hovedsakelig deskriptiv, men i enkelte tilfeller kan det være et vurderingstema hvorvidt de reguleringene som finnes på området bør regnes som rettet mot tilsiktede hendelser eller ikke. I slike tilfeller er det redegjort for vurderingen. Ellers er det, i tilknytning til de enkelte områdene, også omtale av eventuelt relevant overnasjonalt regelverk som den norske lovgivningen er knyttet opp til, selv om oversikten i tabellform er begrenset til norske lover og forskrifter.

Etter gjennomgangen av områdene/sektorene følger en gjennomgang av enkelte temaer som går på tvers områdene, og en vurdering av noen prinsipielle spørsmål som er forankret i litt videre teoretiske betraktninger enn de man kan lese direkte ut av de aktuelle regelverkene. I hovedtrekk dreier disse vurderingene seg om dilemmaer mellom samfunnskontroll og virksomhetenes handlingsrom, og mellom sammenhenger i sektorreguleringen og samordningen av truslene mot den enkelte virksomhet.

## Avgrensninger

Kartleggingen omfatter de plikter, oppgaver og tiltak som ulike virksomheter i samfunnet er pålagt for å avverge eller håndtere hendelser som kan ha konsekvenser for samfunnskritiske funksjoner eller samfunnskritisk infrastruktur. Disse pliktene kan på ulike vis bli påvirket av andre og mer generelle rettslige regelverk, for eksempel av forvaltningsrettslig, arbeidsrettslig eller selskapsrettslig art. Denne undersøkelsen er avgrenset til de plikter, oppgaver og tiltak som er direkte knyttet til et angitt samfunnssikkerhetshensyn, og går ikke nærmere inn på de ulike bredere rettslige sammenhengene virksomhetene står i.

Tilsiktede anslag mot en samfunnskritisk funksjon vil normalt være omfattet av straffebestemmelser, og i en del tilfeller også av prosessbestemmelser som kan innebære adgang til inngripende etterforskningsmetoder. Lovgivning som dreier seg om etterforskning og rettsforfølging av eventuelle gjerningspersoner er ikke omfattet av denne kartleggingen.

På visse områder har virksomheter plikt til å gjennomføre tiltak som reduserer faren for kriminelle handlinger, eksempelvis hvitvaskingslovens krav til rapportering av mistenkelige transaksjoner, eller helsepersonellovens plikt til å varsle politi og brannvesen dersom det er nødvendig for å avverge alvorlig skade på person eller eiendom. Situasjoner der virksomheter har en generell plikt til å avverge mulige kriminelle handlinger, uten at det primært dreier seg om tilsiktede handlinger rettet mot virksomheten eller mot infrastruktur som virksomheten har ansvar for, er heller ikke om fattet av denne kartleggingen.

## Metodebetraktninger

Kartleggingen skal finne frem til ulike virksomheters plikter til å vurdere trusler og treffe tiltak for å avverge eller håndtere tilsiktede handlinger som kan ramme nødvendige funksjoner i samfunnet.

Først og fremst er identifikasjon av relevant regelverk avgrenset til generelle normer, altså den rettskildefaktoren som kalles «lov». I hovedsak er det lagt vekt på å identifisere aktuelle regler i

norske lover og forskrifter, med en omtale av eventuelle overnasjonale regler som de norske reglene forholder seg direkte til. På en del områder finnes det veiledningsdokumenter fra tilsynsmyndigheter, som kan variere fra å være opplæringslitteratur til å være poengtert regelfortolkning. I praksis kan man nok tenke seg at veiledningsdokumenter fra tilsynsmyndigheter vil fungere som generelle normer uavhengig av stil og form, ettersom de antakelig ofte kan leses som «det som skal til for at tilsynsmyndigheten blir fornøyd». I enkelte av drøftingene er det trukket frem momenter fra veiledninger på enkelte områder, men det synes ikke formålstjenlig med en systematisk gjennomgang av alt som finnes. Det som ikke på noe vis er med i denne kartleggingen er eventuelle konkrete pålegg fra domstoler, tilsynsmyndigheter eller overordnede organer til enkeltvirksomheter.

Det er noe ulik begrepsbruk i ulike sektorer for den type plikter som er kartlagt, i tillegg til at det forekommer endringer i de sikkerhetsfaglige begrepene over tid. Det er ulikheter i sektorenes tradisjoner for hvordan de utformer regler, varierende grad av generelle eller spesifikke regler, og forskjellige tradisjoner for hvilken trinnhøyde i regelverket man velger å plassere detaljeringer og presiseringer på.

Kartleggingen er gjennomført i en vekseldrift mellom ulike faglige og politiske dokumenter som drøfter samfunnssikkerhet, og ulike tekstlige og systematiske søk i rettskilder på Lovdata. Man må gå litt dypere til verks enn rene ord- og frasesøk, blant annet fordi måten man ordlegger seg på både har variert over tid og er forskjellig fra sektor til sektor. Videre er det en del forskjeller i reguleringsmetodikken, som varierer fra sterke innslag av fagterminologier til noe som er nærmere dagligtale. Det er også en del forskjeller i hvor stort handlingsrom virksomhetene gis i de ulike regelverkene.

Utover disse søkestrategispørsmålene er det også et mer grunnleggende metodiske problem: En gjennomgang av rettskilder gir ikke i seg selv særlig god dekning for å beskrive negative funn, altså fravær av reguleringer på et område. Måten styring og tilsyn organiseres på kan være effektiv i praksis selv når pliktformuleringene i regelverket virker vage. Fraværet av en konkret plikt til å håndtere en uønsket tilsiktet hendelse er derfor ikke i seg selv et bevis for at slike hendelser ikke blir håndtert på en måte som gir tilstrekkelig sikkerhet og som overordnede myndigheter kan etterprøve.

# Regelverk på de enkelte områdene

De fleste av de enkelte områdene i kartleggingen er knyttet opp til en bestemt samfunnssektor, mens områdene objektsikkerhet, IKT og farlige stoffer er tverrsektorielle. I denne sammenhengen er det egentlig ikke særlig viktig å skille mellom de områdene som har en mer eller mindre entydig sektortilhørighet. Det som skiller det ene området fra det andre dreier seg i større grad om felles faglige perspektiver, felles type trusler, felles tilsynsmyndigheter og eventuelt felles overnasjonalt regelverk. Noen av områdene dekker flere forskjellige regelverk, det gjelder særlig energi og samferdsel, med ulike regelverk og tilsynsmyndigheter innenfor samme sektorer.

## Området generell objektsikring

I **sikkerhetsloven av 20. mars 1998 nr. 10** ble det vedtatt en del endringer i bestemmelsene om objektsikkerhet i 2008. Endringene er nærmere beskrevet og begrunnet i Ot.prp.nr. 21 (2007-2008), de dreide seg dels om å tilpasse kriteriene for hvilke objekter som er skjermingsverdige til infrastrukturutredningens (NOU 2006:6) avklaring av begrepene samfunnskritiske funksjoner og samfunnskritisk infrastruktur. Blant annet fikk § 17 inn som et kriterium at det skal «… tas hensyn til

akseptabel tidsperiode for funksjonssvikt, mulighet til å gjenopprette funksjonalitet, og hensynet til objektets betydning for andre objekter». Det ble også gitt en ny § 17a om klassifisering av skjermingsverdige objekter, og en ny § 17b om objekteiers plikt til å beskytte objektene. Innholdet i de to nye paragrafene var i tråd med tidligere utkast til forskrift om objektsikkerhet, men man hadde kommet frem til at det var hensiktsmessig å forankre hovedinnholdet direkte i loven. Sikkerhetslovens §§ 17, 17a og 17b peker på tre temaer som i varierende grad også finnes i sektorlovgivning om tiltak mot tilsiktede uønskede hendelser, henholdsvis hvordan pliktsubjekter pekes ut, eventuell klassifisering av de verdiene som skal sikres, og eventuelle krav til vandel eller skikkethet hos de som jobber med sikring. Disse tre temaene er også til stede i forholdsvis sammenlignbar form i sikkerhetslovens bestemmelser om informasjonssikkerhet.

Lovendringene som gjelder objektsikkerhet trådte i kraft fra 1. januar 2011, samtidig med **forskrift om objektsikkerhet av 22. oktober 2010 nr. 1362**. Forskriften gir en del nærmere regler, blant annet om utpeking av objekter, klassifisering i nivåene MEGET KRITISK, KRITISK og VIKTIG, og regler om objekteiers, altså den ansvarlige virksomhetens, plikt til å etablere og vedlikeholde permanent grunnsikring for objektene. Autorisering og sikkerhetsklarering av personer er ikke et absolutt krav, men et spørsmål vedkommende departement kan ta stilling til for objekter i de to øverste klassene.

Forskriftens § 1-3 første ledd sier følgende om forholdet mellom den generelle objektsikringsplikten i sikkerhetsloven og sektorlovgivning på området: «Der det finnes relevante og tilstrekkelige bestemmelser innenfor sektorlovgivningen, og det er etablert tilsynsorgan, går disse foran bestemmelsene i denne forskriften». Det er verdt å merke seg at høringsutkastet til forskriften, sendt ut 3. november 2009, ikke inneholdt noen slik bestemmelse. Høringsinstanser påpekte et behov for at forholdet mellom objektsikkerhetsforskriften og sektorlovgivning skulle tydeliggjøres. Vilkårets første del, at det finnes relevante bestemmelser i sektorlovgivningen, er formodentlig greit å ta stilling til. Vilkårets andre del, at slike bestemmelser også må være tilstrekkelige, må vel innebære en mulighet for å vurdere det slik at objektsikkerhetsforskriften likevel vil gå foran dersom sektorlovgivningen er for perifer for objektsikringens mål og metoder. Det er vanskelig å se at § 1-3 i seg selv gir klare nok føringer til å bedømme om sektorlovgivningen på et område skal gå foran objektsikkerhetsforskriften eller ikke. Et nærliggende alternativ blir da en form for saksbehandling for å bestemme konkret hvordan forholdet mellom objektsikkerhetsforskriften og sektorlovgivningen på et område skal være.

Forskrift om objektsikkerhet henviser til forskrift om sikkerhetsadministrasjon, som er en annen forskrift i medhold av sikkerhetsloven. Forskrift om sikkerhetsadministrasjon gir anvisninger om et styringssystem basert på risikovurderinger, iverksetting av forholdsmessige tiltak, etterprøving, avvikshåndtering og eskalering, i stor grad beslektet med den generelle HMS-forskriften og andre tilsvarende internkontrollbestemmelser. Henvisningen mellom objektsikkerhetsforskriften og forskrift om sikkerhetsadministrasjon kan se noe haltende ut, ettersom man ikke finner objektsikkerhet blant de fagområdene forskriften sier den gjelder for, og heller ikke i forskriftens definisjoner og regler ellers. I denne kartleggingen er forskrift om sikkerhetsadministrasjon ikke tatt med her i forbindelse med objektsikkerhet, den er derimot tatt med lenger ned i kartleggingen sammen med forskrift om informasjonssikkerhet under området IKT.

## Området CBRNE

CBRNE står for kjemisk, biologisk, radioaktivt, kjerne- og eksplosiv, som også omtales som masseødeleggelsesmidler. Det inngår som et sentralt element i *protect*-søylen i EUs anti-terrorstrategi fra 2005. Lovgivningsarbeidet på dette området er under utvikling fra EUs side, og det

er grunn til å anta at det blir omfattende institusjoner og oppfølgingssystemer på europeisk nivå etter hvert. Det er mange innslag av CBRNE regler og tiltak i regelverk i ulike sektorer, for eksempel innen miljø og helse. Det er flere ulike sektorer og tilsynsorganer som har oppgaver innenfor ulike deler av CBRNE-feltet.

På området nukleært materiale har vi en **forskrift om fysisk beskyttelse av nukleært materiale og nukleære anlegg av 2. november 1984 nr. 1809**, der det angitte formålet er å «legge forholdene til rette for å minimalisere mulighetene for tyveri av nukleært materiale og sabotasje mot nukleære anlegg.» Forskriften er gitt i medhold av **atomenergiloven av 12. mai 1972 nr. 28**.

Norge har to anlegg som er omfattet av forskriften, reaktorene i Halden og Kjeller. Etter forskriftens § 1 tredje ledd er disse anleggene også å anse som skjermingsobjekter etter sikkerhetsloven. Ved en forskriftsendring som trådte i kraft 1. januar 2008 ble begrepet *designbasistrussel* innført i dette regelverket som et faglig og metodisk rammeverk for å håndtere tilsiktede trusler. Metodikken Design basis threat (DBT) er et opplegg som det internasjonale atomenergibyrået IAEA har innført på dette området, og dreier seg om å definere hva et anlegg skal tåle, basert på profiler av skadevolderes mulige intensjoner og gjennomføringsevne. Designbasistrussel skal utarbeides av anleggsinnehaveren på bakgrunn av nasjonale trusselvurderinger. I norsk sammenheng betyr dette PSTs trusselvurdering, i henhold til forskriften.

Den generelle strålevernforskriften, **forskrift om strålevern og bruk av stråling av 29. oktober 2010 nr. 1380**, hører også inn under Statens strålevern. Forskriften er gitt i medhold av **lov om strålevern og bruk av stråling av 12. mai 2000 nr. 36.** I utgangspunktet omfatter forskriften «enhver tilvirkning, import, eksport, overdragelse, besittelse, installasjon, bruk, håndtering og utvinning av strålekilder», også dagligdagse forbrukerartikler som laserpekere og visse typer røykvarslere med mer. Det er gjort unntak fra deler av forskriftens bestemmelser for en del typer produkter, noe som blant annet innebærer at en del godkjente forbrukerartikler ikke er omfattet av kravene til risikovurdering og forebyggende tiltak i § 17. For de strålekildene som ikke er unntatt fra sikringskravene stiller § 17 krav til risikovurdering og forebyggende tiltak som både omfatter utilsiktede og tilsiktede hendelser, «sikre strålekildene mot tyveri, sabotasje, skade, herunder brann- og vannskade». Strålevernforskriften bruker uttrykket klassifisering, men da som en teknisk typebetegnelse som henviser til vedtatte faglige standarder og ikke som en skjønnsmessig vurdering av verdi eller beskyttelsesbehov.

Et annet og noe nyere innslag på CBRNE-feltet er kontroll med eksplosiver. Ny forskrift i medhold av **brann- og eksplosjonsvernloven av 14. juni 2002 nr. 20, forskrift om håndtering av utgangsstoffer for eksplosiver av 2. juni 2015 nr. 588,** gjennomfører EU-forordning 98/2013 om markedsføring og bruk av utgangsstoffer for eksplosiver. (Dette er en del av et omfattende program i EU for kontroll med ulike samfunns-, miljø- og helseskadelige varer, REACH). Forskriftens formål, § 1, har to ledd. Første ledd gjelder å hindre tilsiktet skade eller at sprengstoff kommer på avveie, andre ledd gjelder å beskytte mot uhell og ulykker (HMS).

**Forskrift om håndtering av farlig stoff, 8. juni 2009 nr. 602**, i medhold av samme lov, inneholder også en bestemmelse, § 14, om risiko og risikovurdering, der det heter at «Vurderingen skal inkludere interne og eksterne forhold samt uønskede tilsiktede handlinger».

## Området energi

Energi er en sektor der det i liten grad henvises til internasjonal regulering av sikkerheten i de norske rettskildene. Samfunnssikkerhetsmeldingen St.meld.nr. 17 (2001-2002), s. 47, pekte på at det er

grunn til å anta at større internasjonalisering av energimarkeder, der også andre land i økende grad vil være sårbare for hendelser som rammer norsk energisektor, vil kunne bidra til større behov for internasjonalt samarbeid og overnasjonal sikkerhetsregulering etter hvert.

En av sikkerhetsbestemmelsene i **petroleumsloven av 29. november 1996 nr. 72,** § 9-3, dreier seg om tilsiktede hendelser: «Rettighetshaver skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger samt til enhver tid ha beredskapsplaner for slike anslag.»

Petroleumssektoren har imidlertid hatt et gjennomgående HMS og «safety»-perspektiv, som er dekket opp av andre paragrafer i petroleumsloven. Det finnes foreløpig ikke forskriftsbestemmelser som utdyper plikten til å hindre bevisste anslag, men det er kanskje grunn til å regne med at dette vil komme etter hvert; ved et delegeringsvedtak 14. februar 2013, ble ansvaret for § 9-3 delegert fra Arbeidsdepartementet til Petroleumstilsynet.

Selv om lovfestede krav til sikkerhet innen petroleumsvirksomheten har vært HMS- og interkontrollbaserte, med all hovedvekt på å håndtere fare for liv og helse ved ulykker, er det ikke slik at man har unnlatt sikring mot tilsiktede handlinger. Det har vært oppmerksomhet om terrorfaren helt tilbake til 1970-tallet. Dette har imidlertid vært håndtert i et annet spor, med innsats fra politiets beredskapstropper og ved behov også fra Forsvarets spesialkommando. Dette er sparsommelig omtalt i den forrige sårbarhetsutredningen, NOU 2000:24, s. 124: «Ved spesielle situasjoner kan politiet støttes av Forsvaret. På sokkelen vil det primært være aktuelt å sette inn Forsvarets spesialkommando (FSK) med bistand fra alle forsvarsgrener og med støtte fra kommando- og kontrollapparatet i Forsvaret. FSK er den eneste militære enheten som er trenet for operasjoner på offshoreanlegg. FSK skal være klar til å bli satt inn i innsats som bistandsenhet til politiet. FSK er i utgangspunktet dimensjonert for å settes inn som en enhet mot kun ett objekt om gangen. Gjennomføringen skal skje som en ren militær operasjon ledet av forsvarskommandoen for Sør-Norge eller Nord-Norge». Bistand fra militære til politi i særskilt krevende situasjoner har vært formalisert i instrukser og etter hvert også i lovgivning, men det dreier seg primært om å løse akutte kriser og ikke om forebyggende sikkerhet i virksomhetene.

Man må kunne gå ut fra at den nødvendige treningen for slike operasjoner i praksis har involvert operatørvirksomhetene noe, i det minste for å legge til rette for hensiktsmessige øvinger, men det er likevel ikke godt synliggjort som en del av virksomhetens plikter, og dermed er det heller ikke opplagt at ansatte i virksomhetene har vært særlig godt kjent med terrorsikringen. Petroleumsloven § 9-3 åpner imidlertid for å gi regler også om virksomhetenes arbeid med å beskytte mot tilsiktede hendelser.

Innen elektrisk kraft er det mer omfattende regler som dreier seg om tilsiktede hendelser:

For beredskapsbestemmelsene i **energiloven av 29. juni 1990 nr. 50** har det vært klart helt fra denne lovens forarbeid (ot.prp. nr. 43 1989-90) at disse også skal omfatte terrorhandlinger i fredstid. Det legges blant annet opp til en robust organisering, kalt kraftforsyningens beredskapsorganisasjon (KBO), som er et samvirke av alle virksomhetene og skal håndtere kriser og blant annet sørge for samordnet forsyning i krisesituasjoner. Det er imidlertid ikke et opplegg som er avgrenset til å håndtere tilsiktede hendelser, det dreier seg vel så mye om naturlige hendelser og ulykker.

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen **7. desember 2012 nr. 1157** utdyper beredskapsorganisasjonen, og angir plikter for den enkelte KBO-virksomhet til å vurdere risiko og iverksette tiltak, samt å rapportere ekstraordinære situasjoner til Norges vassdrags- og energidirektorat som er tilsynsmyndighet. Forskriften har også eget kapittel om informasjonssikkerhet. I disse informasjonssikkerhetsbestemmelsene er det egne kriterier for hva

som regnes som sensitivt, og krav til at virksomhetene skal identifisere den sensitive informasjonen, vite hvor den befinner seg, og vite hvem som har tilgang til den.

**Damsikkerhetsforskriften av 18. desember 2009 nr. 1600**, gitt i medhold av **vannressursloven av 24. november 2000 nr. 82**, har en bestemmelse om tilsiktede aksjoner i § 5-3. Kravet er at eier eller driver av demning skal sikre mot tilsiktede aksjoner hvis demningen er definert med konsekvensklasse 3 eller 4, som er de to øverste klassene. Det er nokså rigide kriterier for hva som inngår i kosekvensklassene (antall boenheter som kan rammes, fare for å ramme vei, jernbane, miljø, fremmed eiendom).

**Drivstoffanleggsloven, 31. mars 1949 nr. 3.** Loven gir regler om sikring mot sabotasje, og utpeking av anlegg. Loven angir ikke noe opplegg for vurdering av risiko eller plikt til å etablere forholdsmessige tiltak. Systemet er en plikt til å følge rådgjerder fra Oljeberedskapsrådet. Det er også en egen lov om beredskapslagring av petroleumsprodukter. Beredskapsloven angir ikke tiltak mot tilsiktede hendelser. Den dreier seg om å håndtere en krise dersom den har inntruffet, altså et rent forsyningsmessig anliggende.

## Området samferdsel

**Luftfartsloven 11. juni 1993 nr. 101** stiller krav til flysikringstjeneste, en betegnelse som dekker både kontrolltårn og tjenester på bakken.

Her er det egen **forskrift om forebyggelse av anslag mot sikkerheten i luftfarten mv., av 1. mars 2011 nr. 214**, altså mer spesifikt rettet mot tilsiktede anslag. Et slags halvoffisielt kortnavn på denne forskriften i Samferdselsdepartementet og Luftfartstilsynet er «securityforskriften», noe som tydeliggjør den faglige plasseringen. Forskriften omfatter blant annet krav til vedlikehold av beredskapsplaner, og til å avholde «beredskapsøvelse som omfatter anslag mot sikkerheten i luftfarten», minst annet hvert år. Forskriften inneholder også personkontrollbestemmelser, krav til vandel.

Bestemmelsene i forskriften er gjennomføring av en stor serie detaljerte EU-regler, med referanser til ulike tekniske standarder. Det har vært over 20 endringer i EUs rettsakter på denne forskriftens område etter 2008.

Skip og havner er også omfattet av sikkerhetskrav. Skip og havner er omfattet av ulike norske lover, med ulike tilsynsmyndigheter, og begge implementer EU-forordning 725/2004 om terrorsikring av skip og havner. Forordningen legger opp til at nasjonale myndigheter, eller virksomheter utpekt av nasjonale myndigheter, skal gjennomføre tilsynsoppgavene. Det er imidlertid også en mekanisme for samsvarskontroll i forordningen, medlemslandene skal utpeke et kontaktorgan som overvåker gjennomføringen av forordningen i medlemslandene.

**Skipssikkerhetsloven av 16. februar 2007 nr. 9**, § 39 første ledd: «Det skal treffes tiltak for å hindre og beskytte skipet mot terrorhandlinger, piratvirksomhet, blindpassasjerer og andre ulovlige handlinger». Det stilles krav om at de som arbeider om bord har identitetsbevis, videre gir paragrafen hjemmel for nærmere bestemmelser i forskrift. **Forskrift om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (sikkerhetsforskriften) av 22. juni 2004 nr. 972** oppstiller detaljerte krav, med henvisninger til både EU-regelverk og internasjonale konvensjoner. Tiltakene som kan iverksettes er svært omfattende, blant annet kan det brukes bevæpnede vakter og andre maktmidler innenfor visse rammer, dersom en trussel er direkte, umiddelbar, betydelig og uunngåelig.

**Havne- og farvannsloven av 17. april 2009 nr. 19,** § 43, pålegger «eiere og operatører av havner og havneterminaler … [å] treffe de tiltakene som er påkrevd for å forebygge og hindre terrorhandlinger og andre forsettlige, ulovlige handlinger rettet mot havnen, havneterminalen, eller fartøy som bruker havnen eller havneterminalen». Her er det to underliggende forskrifter som er praktisk talt likt bygget opp, en som gjelder havner og en som gjelder havneanlegg: **Forskrift om sikring av havner av 29. mai 2013 nr. 539** og **forskrift om sikring av havneanlegg av 29. mai 2013 nr. 538.**

Opplegget i disse forskriftene, og i EU-forordningen, er at det er et myndighetsorgan (Kystverket i Norge, eller en *Recognized Security Organization* godkjent av Kystverket) som vurderer trusselbildet og fastlegger et «maritimt sikringsnivå». Sikringsnivå 1 er der man kan holde seg til et minimumsnivå av relevante tiltak som skal opprettholdes til enhver tid, nivå 2 og 3 er forhøyede krav til sikring.

**Jernbaneloven av 11. juni 1993 nr. 100** fikk inn en lovendring 19. juni 2015, en ny § 6a som hjemler en forskrift om tilsiktete hendelser, pluss et nytt 6. ledd i taushetspliktbestemmelsene § 11, som lyder «Uten hinder av lovbestemt taushetsplikt kan tilsynsmyndigheten og politiet, Nasjonal sikkerhetsmyndighet, Direktoratet for samfunnssikkerhet og beredskap eller tilsvarende myndigheter gjensidig og etter forespørsel utveksle de opplysninger som er nødvendige for å sikre jernbanen mot tilsiktede uønskede handlinger.»

I medhold av den nye § 6a i jernbaneloven er det gitt en **forskrift om sikring på jernbane, av 1. juli 2015 nr. 848**. Dette er en rendyrking av regulering rettet mot tilsiktede hendelser. I forarbeid til endringene i jernbaneloven, prop.107 L (2014-2015), er det også henvist til standarden NS 5830, som etablerer det begrepsapparatet forskriften bygger på. Det kommer kanskje særlig til uttrykk i forskriftens definisjon av trusselvurdering, som omfatter «vurdering av trusselaktørenes intensjon og kapasitet», altså ikke rent kvantitative vurderinger av sannsynlighet.

En interessant side ved denne nye forskriften om sikring er at den står side om side med en annen eksisterende forskrift, sikkerhetsstyringsforskriften av 11. april 2011 nr. 389, om forebygging av jernbaneulykker, som skal fortsette å gjelde som før. På dette området har man altså truffet et valg om å gi forskjellige regler for tilsiktede og utilsiktede hendelser, i stedet for å legge opp til felles regler ut fra en «all hazards approach».

## Området IKT

På IKT-området er sikkerhet et område preget av regelverk, strategier og tiltak som favner bredt, med relativt beskjedne innslag av særskilt oppmerksomhet rettet mot samfunnskritiske funksjoner. Regelverk og standarder favner både sikring av IKT-infrastrukturen og informasjonsinnholdet, mot både utilsiktede og tilsiktede hendelser. Enkelte sektorspesifikke regelverk for informasjonssikkerhet finnes, for eksempel for elektrisk kraftforsyning og for finansinstitusjoner, men det regelverket som har størst nedslagsfelt ut fra hvor mange virksomheter som omfattes er sikkerhetsbestemmelsene hjemlet i **personopplysningsloven av 14. april 2000 nr. 31** § 13, som pålegger å «gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger». Nærmere krav til hvordan informasjonssikkerheten skal ivaretas følger av kapittel 2 i **personopplysningsforskriften av 15. desember 2000 nr. 1265**. Personopplysningsloven implementerer EUs personverndirektiv 96/46/EF, som i artikkel 17 stiller krav til forholdsmessige sikkerhetstiltak mot både tilfeldig og ulovlig ødeleggelse, og en dynamisk tilpasning til endringer i den teknologiske utviklingen. Innholdsmessig går kravene i personopplysningsforskriftens kapittel 2 ut på å etablere og etterleve et internt styringssystem, beslektet med det som er foreskrevet i de godt innarbeidede internasjonale «best practice»-standardene ISO 27001 og ISO 27002. Kriterier for akseptabel risiko besluttes i

utgangspunktet internt i virksomheten, men kan overprøves av Datatilsynet. Velbegrunnede akseptkriterier overprøves i praksis svært sjelden. Sikkerhetstiltakene omfatter både utilsiktede og tilsiktede hendelser. Det er ingen særskilte tiltak rettet mot å identifisere eller sikre samfunnskritiske funksjoner eller infrastruktur i dette regelverket, men utgangspunktet i § 2-1 er at det gjelder forholdsmessige krav om sikring av personopplysninger, «… tiltakene som treffes i medhold av forskriften, [skal] stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd». For virksomheter som forvalter samfunnskritisk infrastruktur, men som ikke behandler informasjon som er gradert etter sikkerhetsloven, vil det oftest være personopplysningsforskriftens bestemmelser som er det regelverket for informasjonssikkerhet de forholder seg til i praksis.

Personopplysningsforskriftens sikkerhetsbestemmelser har ikke særlig sterke virkemidler for å harmonisere sikkerhetstiltak og nivå for akseptabel risiko på tvers av virksomheter, det begrenser seg til kravet i § 2-15 om å sikre seg at de man samarbeider med om behandlingen av personopplysninger tilfredsstiller forskriftens krav. Noe mer harmonisering av sikkerhetsnivået på tvers av virksomheter oppnås i praksis gjennom strategier som *Nasjonal strategi for informasjonssikkerhet*, og gjennom ulike felles sikkerhetskomponenter, eksempelvis elektronisk signatur eller krav som stilles for å kunne tilknytte seg ID-porten for pålogging til offentlige tjenester.

For offentlig forvaltning som kommuniserer elektronisk med innbyggere, næringsliv eller andre forvaltningsorganer finnes bestemmelser om informasjonssikkerhet også i **eForvaltningsforskriften av 25. juni 2004 nr. 988**, gitt i medhold av **forvaltningsloven av 10. februar 1967** § 15a. Det er bestemmelser om informasjonssikkerhet som i all hovedsak bygger på samme best practice-grunnlag som personopplysningsforskriften. For de aller fleste forvaltningsorganer betyr dette at eForvaltningsforskriftens sikkerhetskrav oppfylles gjennom det samme styringssystemet som de følger etter personopplysningsforskriften. Med eForvaltningsforskriften vil tilsvarende krav også gjelde for forvaltningsorganer som ikke behandler personopplysninger. eForvaltningsforskriften har lagt opp til visse muligheter for å harmonisere sikkerhetsnivået på tvers av forvaltningsorganer, dels ved det veiledningsansvaret Direktorat for forvaltning og IKT (Difi) er tildelt i medhold av § 15, og dels ved det koordinerende organet som utpekes i medhold av § 36.

Ellers er det en bestemmelse i forvaltningsloven § 15a som har en viss selvstendig betydning for å sikre virksomheten mot tilsiktede sikkerhetshendelser, den hjemler forskriftsbestemmelser om «forvaltningens rett til å sperre for brukere som misbruker data ment for signering, autentisering, sikring av integritet eller konfidensialitet, og om hva som skal regnes som misbruk». Denne bestemmelsen blir detaljert nærmere i eForvaltningsforskriften § 14.

På sikkerhetslovens område er det gitt en **forskrift om informasjonssikkerhet, av 1. juli 2001 nr. 744.** Den gjelder for sikkerhetsgradert informasjon, og systemer der det behandles sikkerhetsgradert informasjon. Sammenliknet med personopplysningsforskriften og eForvaltningsforskriften er forskrift om informasjonssikkerhet mer detaljert, og legger en del større vekt på tilsiktede hendelser. Forskrift om informasjonssikkerhet henviser til **forskrift om sikkerhetsadministrasjon, av 29. juni 2001 nr. 723**, som anviser et risikobasert styringssystem for planlegging, iverksetting, kontroll med og forbedring av sikkerhetstiltakene.

Et annet tiltak innen informasjonssikkerhet, som mer spesifikt håndterer trusler rettet mot kritisk infrastruktur, er Varslingssystem for digital infrastruktur (VDI). Dette er en overvåknings- og responstjeneste som er frivillig, går på tvers av offentlig og privat sektor, og er delvis deltakerfinansiert. Det er foreløpig ikke noe særskilt rettslig grunnlag bak dette tiltaket, utover at det er nevnt som en del av det utøvende ansvaret Nasjonal sikkerhetsmyndighet (NSM) er tillagt i Instruks om sikkerhetstjeneste i Forsvaret av 29. april 2010 nr. 965. Etter instruksen skal NorCERT,

som er en del av NSM, også samarbeide med E-tjenesten og PST om å «produsere et oppdatert nasjonalt IKT-trusselbilde».

NSM har i relativt nylig avgitte sikkerhetsfaglige råd (pressemelding 10. september 2015) foreslått å endre den nåværende modellen med frivillig deltakelse til en lovhjemlet plikt til å delta i VDI for samfunnskritisk infrastruktur. Dersom det etableres en lovhjemmel om deltakelse i VDI vil et aktuelt spørsmål være hvordan den peker ut hvilke virksomheter som pålegges å delta, for eksempel om pålegget knyttes til definisjoner av kritisk infrastruktur eller blir utformet som en kompetanse til å peke ut deltakervirksomheter etter skjønn. Det er i denne forbindelse interessant å merke seg at de nevnte sikkerhetsfaglige rådene fra NSM går inn for statlig fullfinansiering av VDI i stedet for deltakerfinansiering. Det bygger vel på en antakelse om at det kan være vanskelig å pålegge økonomiske byrder for utvalgte virksomheter som ikke nødvendigvis deltar etter eget ønske.

Problematikken knyttet til harmonisert sikkerhetsnivå er et av de sentrale spørsmålene i utredningen NOU 2015:13 *Digital sårbarhet – sikkert samfunn*. Et begrep som vies en del plass i utredningen er de digitale verdikjedene. Virksomhetsinterne sikkerhetstiltak gir i prinsippet forskjellige svar på hvilke tap man kan leve med og hva det eventuelt koster å unngå dette på ulike punkter i verdikjeden. Tiltak som foreslås i utredningen er nasjonalt rammeverk for å vurdere verdier og fastsette akseptnivåer. Noe mer originalt, kanskje, er en anbefaling om at de ulike faglige tilsynsmyndighetene i større grad skal beskjeftige seg med å følge opp IKT-sikkerheten i virksomheter de har et faglig tilsynsansvar for, inkludert de digitale verdikjedene deres IKT-systemer inngår i. Summen av anbefalinger om tverrsektorielle tiltak for å redusere digital sårbarhet kan sies å være i tråd med den dreiningen mot security som man også ser på andre områder, for eksempel samferdsel og CBRNE, en styrking av systemer og strukturer som følger opp og eventuelt korrigerer bestemte elementer i virksomhetenes sikkerhetsarbeid.

## Området ekom

**Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 nr. 83**, § 2-10, setter et krav om forsvarlighet. Forsvarlighetsnivået kan fastsettes av Nasjonal kommunikasjonsmyndighet. Ekomloven er en sektorlov som retter seg mot tilbydere av internett og telefonitjenester. Reguleringen er forankret i en pakke av flere EU-direktiver. I ekompakkens rammedirektiv, 2002/21/EF er kommunikasjonsnettenes integritet og sikkerhet et område der nasjonale reguleringsmyndigheter i utgangspunktet har stor handlefrihet (artikkel 8, nr. 4). Et større innslag av felleseuropeiske regulering av sikkerhet på ekomområdet ser imidlertid ut til å være på vei inn med det foreliggende forslaget til nytt direktiv om nettsikkerhet, «Nis-direktivet», Kom(2013) 48. Forslaget var ikke merket som EØS-relevant, men det er nærliggende å regne med at det kommende direktivet kan bli omfattet av EØS blant annet på grunn av den tydelige koblingen mellom Nis-direktivet og ENISA-forordningen som Norge allerede har implementert.

Ekomvirksomhet er regulert nærmere i **ekomforskriften av 16. februar 2004 nr. 401**. Denne forskriften inneholder et stort spekter av bestemmelser. Blant annet implementerer § 8-7 i forskriften EU-forordning 526/2013, ENISA-forordningen. Det nye mandatet for ENISA i EU omfatter «cybercrime» som et av arbeidsfeltene, og et oppdrag om å samarbeide med nasjonale Cert (Critical Emergency Response Team). Slik sett er denne bestemmelsen i forskriftens § 8-7 et festepunkt for NorCert og NorSis.

Ellers har det vært en interessant endring i denne forskriften som, i hvert fall nominelt sett, har redusert noe av oppmerksomheten om samfunnskritisk infrastruktur. Kapittel 8 i forskriften, om sikkerhet og beredskap, ble endret fra juli 2013 slik at termen «brukere med samfunnskritiske

funksjoner» ikke lenger er med som innslagspunkt for skjerpede tiltak eller som rettesnor for prioriteringer. Bakgrunnen for endringen var et høringsnotat fra Samferdselsdepartementet sendt ut 23. juni 2010. Der ble det foreslått en rekke endringer i ekomloven og forskriften. En av endringene besto i å oppheve § 8-1, altså fjerne tilbydernes plikt til å «ha oversikt over egne brukere som innehar samfunnskritisk funksjon og elektronisk kommunikasjonstjeneste som er nødvendig for brukerens utførelse av slik funksjon». Videre ble etterfølgende paragrafer i forskriftens kapittel 8 endret slik at de ikke lenger henviste til brukere med samfunnskritiske funksjoner. På side 55 i høringsnotatet sies blant annet: «Det er meget få, om noen, brukere som har meldt seg som samfunnskritisk bruker til sin tilbyder, og meldt fra om hvilke ekomtjenester som er nødvendige for å utføre disse samfunnskritiske funksjonene. Bestemmelsen har derfor ikke fått den betydning man ønsket.»

Det som er tatt ut av forskriften er altså først og fremst begrepet «samfunnskritisk funksjon». Meningsinnholdet er kanskje til en viss grad bevart i de omformulerte begrepene, men det stilles ikke lenger krav til en tydelig identifikasjon av hvilke kunder som har slike funksjoner. Omformuleringen av øvrige bestemmelser i forskriftens kapittel 8 legger opp til å at tilbyderen skal prioritere de viktigste kundene, men uten at det er krav til en spesifikk oversikt over slike kunder. Et eksempel på omformuleringen fra § 8-4, før 1. juli 2013 begynte den slik: «Tilbyder etter § 8-1 første ledd skal i krise- og beredskapssituasjon gi prioritet til bruker med samfunnskritisk funksjon.» I någjeldende versjon av forskriften begynner § 8-4 slik: «Ved driftsstans skal tilbyder ved gjenoppretting prioritere hensynet til sluttbrukere med ansvar for borgernes liv og helse foran kommersielle hensyn».

Ekomloven hjemler også **forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskrifta), 10. september 2012 nr. 866.** Anlegg som er omfattet av sikkerhetskravene klassifisert med bokstavene A – D. Klasse A er anlegg som er omfattet av sikkerhetsloven. Klassene B og C er anlegg som er særs viktige for offentlige elektroniske kommunikasjonstjenester, på henholdsvis landsdelsnivå eller større og på fylkesnivå eller større. Klasse D er alle øvrige anlegg, de som ikke omfattes av klassene A, B eller C. Kravene til sikring omfatter både tilsiktede hendelser (eksempelvis innbrudd og angrep basert på elektromagnetisk puls eller høyfrekvente radiostråler), og utilsiktede hendelser (eksempelvis brann). Sikringskravene er gjennomgående utformet slik at anlegg i klasse A, B eller C skal gjennomføre og dokumentere tiltak tilpasset anleggets klasse og virksomhetens omfang.

## Området finans

Innen finanssektoren har Finanstilsynet gitt en egen **forskrift om IKT-systemer i banker mv, 21. mai 2003 nr. 630**, hjemlet i **lov om betalingssystemer mv. av 17. desember 1999 nr. 95** og **lov om tilsynet med finansinstitusjoner mv. av 7. desember 1956 nr. 1**. Hovedinnretningen i forskriften er å sikre at IKT-virksomheten leverer de tjenester som er avtalt, også der hele eller deler av IKT-virksomheten er utkontraktert til andre aktører. Forskriften er altså i hovedsak et krav til internkontroll, med særskilt vekt på å sikre vertikal kontroll med at tiltakene gir ønsket resultat. Det er imidlertid også verdt å merke seg en bestemmelse som dreier seg spesifikt om tilsiktede hendelser, i § 5: «Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk.»

Ellers er finanssektoren underlagt en rekke regler om soliditet og kapitalkrav med mer, basert på rammeverkene fra den internasjonale Baselkomiteen for banktilsyn. Både EU-lovgivning som er implementert i norsk regelverk og enkelte egne norske regelverk følger opp Baselkomiteens rammeverk. I all hovedsak dreier dette seg om finansiell soliditet, og ikke trusler eller konsekvenser

av tilsiktede uønskede hendelser. I Basel II ble det imidlertid innført et nytt begrep, «operasjonell risiko». Basel-definisjonen av operasjonell risiko lyder «the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events». Dette er en side ved rammeverket som dreier seg om å overvåke farene for feil, omgåelser og unnlatelser i den finansielle risikohåndteringen. Begrepet operasjonell risiko knyttes gjerne til «compliance» eller etterlevelse. I en del faglitteratur har operasjonell risiko blitt betegnet som meta-risk management (Ojo 2010, Power 2005) som vel kan oversettes til risikostyring av risikostyringen. I utgangspunktet kan håndtering av operasjonell risiko være rettet mot både utilsiktede og tilsiktede hendelser.

I norsk regelverk er denne siden ved Baselrammeverket prinsipielt dekket i forskrift om risikostyring og internkontroll av 22. september 2008 nr. 1080, og i underliggende rundskriv. I rundskrivet RFT-2015-9 henviser Finanstilsynet til Basel, og gir følgende forholdsvis åpne og vage omtale av operasjonell risiko: «Eksempler på slike risikoforhold kan være gjennomgående svakheter i foretakets IT-systemer, eller manglende etterlevelse av regelverk». Litteraturen om operasjonell risiko påpeker at begrepet er uklart, men det synes å være enighet om at både utro tjenere og eksterne svindlere som har kapasitet til å ramme en finansinstitusjon hardt vil ligge innenfor begrepet. I denne kartleggingen har jeg kommet til at pliktene til å håndtere ulike former for operasjonell risiko ikke er tilstrekkelig tydeliggjort i norsk regelverk til at de bør tas med i oversikten over plikter til å etablere tiltak mot tilsiktede uønskede hendelser i finanssektoren.

## Området helse

Et område innen helse der det er lagt opp til å se på tilsiktede hendelser, er overlagt spredning av smitte. I Norge er avdekking og rapportering av smittsomme sykdommer omfattet av **MSIS-forskriften av 20. juni 2003 nr. 740**. MSIS er et landsomfattende meldingssystem, etablert i 1975. Behovet for å hjemle registeret i en forskrift oppsto i og med hjemmelskravene for behandling av helseregistre som ble innført med den første helseregisterloven, i kraft fra 2002. MSIS-forskriften er nå hjemlet både i **helseregisterloven av 20. juni 2014 nr. 43** og i **smittevernloven av 5. mai 1994 nr. 55**.

I all hovedsak er innmeldt smitte noe som har ulike epidemiske årsaker, som normalt ikke er tilsiktede. Forskriften har imidlertid også en bestemmelse om overlagt spredning, § 3-5: «Leger som mistenker eller påviser tilfeller av smittsomme sykdommer som kan være forårsaket av overlagt spredning av smittestoffer, skal varsle kommunelegen, fylkesmannen og Nasjonalt folkehelseinstitutt.»

Denne bestemmelsen har vært med i MSIS-forskriften siden 2003. EU har imidlertid etablert tilsvarende bestemmelser senere. EU etablerte det europeiske smittevernbyrå ECDC i Stockholm i 2005. Ved rådsbeslutning 1082/2013/EU ble mandatet utvidet til også å følge opp smitte som kan være mulig bioterrorisme. Dette er nokså kryptisk formulert i rådsbeslutningen, ved en tilføyelse av kategorien «unknown origin». Det fremgår imidlertid av den tolkningen ECDC har gjort at dette skal omfatte mistanker om bioterrorisme. I et white paper, *Director's presentation* fra ECDC i 2013, beskrives to alternative risikomodeller for henholdsvis tilsiktet og utilsiktet spredning av smitte. Tilsiktet spredning vurderes i tre dimensjoner, threats – hazards – impacts, som kan sammenlignes med det som er etablert i de relativt nye norske standardene i NS 5830-serien. Modellen for å vurdere utilsiktet spredning har to dimensjoner, hazards – impacts.

Lovgivningen som regulerer primær- og spesialisthelsetjenesten, altså det store volumet av pasientbehandling, inneholder praktisk talt ikke i direkte forstand krav til å vurdere risiko for eller iverksette tiltak mot tilsiktede, uønskede handlinger. Det finnes enkelte særbestemmelser, som for

eksempel fastlegens rett til å få flyttet en pasient ut av fastlegelisten hvis han oppfører seg truende mot legen eller hans nærmeste, men slike bestemmelser har lite å si for helsetjenestens evne til å ivareta samfunnskritiske funksjoner. Å innfortolke tiltak mot tilsiktede handlinger i helselovgivningens forsvarlighetskrav vil også virke fremmed fra det som vanligvis legges i dette begrepet. Det har likevel blitt en økende oppmerksomhet om håndtering av tilsiktede handlinger blant de som arbeider med sikkerhet i sykehussektoren, der flere har arbeidet med å vurdere trusler i samfunnssikkerhetsperspektiv etter standarden NS 5830, uten at det er pålagt i sektorlovgivningen. Det kan kanskje sies å være et eksempel på at metodikken ikke er avhengig av lovpålagte plikter som anviser hva som kreves, men på den annen side vil fraværet av pålegg i lov innebære at det finnes lite grunnlag for tilsyn med de valg et sykehus treffer på dette området, og måten eventuelle tiltak gjennomføres på.

## Området samordning

Det kan være ulike behov for å samordne innsats og tiltak rettet mot uønskede hendelser. Flere virksomheter kan ha ansvar for ulike deler av en felles funksjon eller infrastruktur, eller det kan være behov for sikring innenfor geografiske områder der ulike virksomheter kan bli rammet av samme trussel.

På europeisk nivå stilles det krav til å utpeke kritiske objekter der sikkerhetshendelser kan skape alvorlige konsekvenser i to eller flere EU/EØS-land. Det er gitt et eget direktiv for slik samordning, 2008/114/EC, *European Programme for Critical Infrastructure Protection (EPCIP)*. Foreløpig er sektorene energi og transport omfattet av EPCIP, men IKT-infrastruktur er en varslet utvidelse. Det kan også tenkes at det vil bli utvidet til flere andre sektorer eller områder på sikt.

I Norge er dette direktivet implementert i **sivilbeskyttelsesloven av 25. juni 2010 nr. 45**, med et eget kapittel, og litt på siden av lovens øvrige systematikk. Plasseringen av direktivets regler i sivilbeskyttelsesloven, i stedet for i sikkerhetsloven, er i forarbeidet prop. L 129 (2011-2012) begrunnet med at direktivet har en «all hazards approach». Det vil si at det omfatter både tilsiktede og utilsiktede hendelser.

Den generelle beredskapsplikten på lokalt nivå følger av **forskrift om kommunal beredskapsplikt, 22. august 2011 nr. 894**. Forskriften er gitt i medhold av sivilbeskyttelsesloven, og omtaler et av arbeidsfeltene slik, i § 2 bokstav d: «særlige utfordringer knyttet til kritiske samfunnsfunksjoner og tap av kritisk infrastruktur». Likelydende bestemmelse finner man i **forskrift om sivilbeskyttelseslovens anvendelse på Svalbard og om beredskapsplikt for Longyearbyen lokalstyre, 18. desember 2012 nr. 1293**, § 3 bokstav d. Forskriftsteksten inneholder ikke egentlig noen veldig klar angivelse av at dette skal forstås som tilsiktede uønskede hendelser, men det er rimelig å forstå det slik ut fra den sammenhengen forskriften har blitt til i, og valget av begreper, at denne plikten inngår i en faglig dreining i retning av større oppmerksomhet om tilsiktede hendelser de senere år.

Regler om samordning på lokalt og regionalt nivå finnes først og fremst i **instruks for fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet, beredskap og krisehåndtering, fastsatt ved Kgl. res. 19. juni 2015, nr. 703.** Instruksen er hjemlet i Kongens instruksjonsmyndighet. Den nye instruksen som ble vedtatt i 2015 viderefører i hovedsak Fylkesmannens og sysselmannens strategiske samordningsfunksjon på regionalt nivå, slik den var utformet i forrige instruks fra 2008. En endring som likevel har en viss betydning i denne sammenhengen er plikten til å utarbeide en «fylkesROS», altså en risiko- og sårbarhetsvurdering, som skal tjene som felles plattform i samordningsarbeidet. I kommentarene som er publisert sammen med instruksen heter det at «[f]ylkesmannen skal utarbeide fylkesROS i tråd med DSBs veileder». I gjeldende veileder fra DSB er

utarbeiding av fylkesROS knyttet til samme begrepsapparat og metodikk som Nasjonalt risikobilde, med en tredeling mellom naturhendelser, storulykker og tilsiktede hendelser. I veilederen gis Fylkesmannen et visst skjønn i vurderingen av om fylkesROS også skal omfatte tilsiktede hendelser: «Fylket må vurdere nytteverdien av å analysere tilsiktede hendelser i fylkesROS. Det kan være spesielle terror- eller sabotasjemål i et fylke som aktualiserer økt kunnskap og bevissthet om disse regionalt. For tilsiktede hendelser angis ikke nødvendigvis en sannsynlighet, men en vurdering av om trusselen er til stede» (Veileder for fylkesROS, DSB 2014, s. 17).

Den plikten fylkesmannen og sysselmannen kan sies å ha til å vurdere tilsiktede hendelser som del av samordningen av samfunnssikkerhetsarbeidet er altså gjenstand for stor grad av skjønn, og hjemlet i rettskilder av forholdsvis lav trinnhøyde.

# Noen temaer i som går på tvers av områdene

De ulike regelverkene som er kartlagt har en god del til felles. De er i hovedsak basert på en plikt til å gjennomføre risikovurderinger, og til å treffe tiltak som er relevante og forholdsmessige til å håndtere de trusler eller den sannsynligheten for uønskede hendelser man har funnet behov for å gjøre noe med. Dernest er det en eller annen form for samfunnskontroll med at tiltakene etterleves og gir ønsket sikkerhetsnivå. Denne samfunnskontrollen utøves av ulike offentlige tilsynsorganer, eller i en viss beskjeden utstrekning av private aktører som tildeles bestemte kontrollfunksjoner.

Til tross for grunnleggende likhetstrekk mellom ulike sikkerhetsreguleringer er det også en del forhold som er forskjellige. En del av forskjellene dreier seg om ulike former for samfunnskontroll. På noen områder etterprøver tilsynsorganer først og fremst at sikkerhetssystemet blir etterlevd og fulgt opp i tråd med det virksomheten selv har vurdert som risiko, uten å overprøve virksomhetens autonome vurderinger. På andre områder består samfunnskontrollen av mer detaljerte pålegg, felles systemer og til dels rigide krav til detaljrapportering, som innebærer mindre autonomi for den enkelte virksomhet og i en del tilfeller også høyere kostnader forbundet med å etterleve reglene.

De første temaene i dette kapitlet er knyttet til tiltakstyper som finnes i sikkerhetsloven, og som i ulikt omfang finnes i deler av sektorlovgivningen. Deretter følger en mer åpen drøfting av noen mulige forskjeller mellom ulike trekk ved risikobasert regulering.

## Utpeking av virksomheter

I sikkerhetsloven § 17 er hovedprinsippet at hvert departement utpeker skjermingsverdige objekter, mens underordnet virksomhet foreslår hvilke av de objekter de eier eller bestemmer over som det kan være aktuelt å utpeke. Det er videre angitt noen kriterier for vurderingene, og en henvisning til lovens formål. Sikkerhetsloven kan gjøres gjeldende også for virksomheter som ikke er forvaltningsorgan, men som på annen måte har vesentlig betydning for sikringen av et objekt. Dersom et organ som ikke er forvaltningsorgan underlegges bestemmelser i forskrift om objektsikkerhet har de adgang til å klage på beslutningen, vanlige forvaltningsorganer har ikke en slik klageadgang.

I sektorlovgivningen er det i stor grad virksomhetens art, og en lovs virkeområde, som avgjør hvilke virksomheter eller hvilke objekter som blir omfattet av kravene til å sikring mot tilsiktede uønskede hendelser. For eksempel vil sikkerhetsbestemmelsene i personopplysningsforskriften kapittel 2 gjelde for alle virksomheter som behandler personopplysninger, mens kravene til fysisk sikring av

atomreaktorer vil gjelde for virksomheter som er definert som anleggsinnehavere i atomenergiloven. Generelle regler som angir typer virksomhet som omfattes kan sies å ha den fordelen at alle får de samme kostnadene til sikring. Det kan tenkes å redusere en mulig fare for et slags spill mellom sektorvirksomheter og sikkerhetsmyndigheter for å unngå å bli utpekt til å måtte følge et mer omfattende sikkerhetsregime. På den annen side kan helt generelle kriterier for hvilke virksomheter som skal omfattes av sikringskravene kanskje innebære en fare for at flere virksomheter blir omfattet, til en høyere totalkostnad for forvaltningen, enn å peke ut virksomheter etter mer konkrete vurderinger.

Det eneste sted i sektorlovgivningen der det lagt opp til samme form for konkrete vurderinger for å peke ut virksomheter er sivilbeskyttelsesloven § 24a, som gjelder identifisering av europeisk kritisk infrastruktur etter EPCIP-direktivet. Her ligger det imidlertid også kriterier til grunn for den vurderingen man skal bygge utpekingen på, nemlig hvorvidt driftsforstyrrelse eller ødeleggelse vil kunne få betydelige konsekvenser for to eller flere EØS stater.

Den frivillige deltakelsen i varslingstjenesten VDI kan også betraktes som en form for utpeking, i den forstand at NSM neppe ville se seg forpliktet til å ta inn en virksomhet som de vurderer som uinteressant. På den annen side har også virksomheter som ikke ønsker å delta i VDI anledning til å takke nei etter den nåværende deltakermodellen.

Klassifiseringssystemet i ekom klassifiseringsforskriften kan kanskje ses som en mellomvariant av utpeking etter generelle kriterier og etter konkret beslutning. Å klassifisere et anlegg som klasse A er ensbetydende med at anlegget omfattes av sikkerhetsloven. Utpekingen av anlegget ligger da innkapslet i klassifiseringsbeslutningen. Det er likevel en vesentlig forskjell fra utpeking av objekter etter sikkerhetsloven § 17: Det er i utgangspunktet nettilbyderen selv som skal klassifisere anleggene, men klassifiseringen kan i særlige tilfeller overprøves av Nasjonal kommunikasjonsmyndighet.

## Klassifiseringer

Sikkerhetsloven § 17a gir kriterier for å velge mellom tre klassifiseringsgrader for objekter, MEGET KRITISK, KRITISK og VIKTIG. Kriteriene for de ulike gradene er knyttet til skadepotensial. Sikkerhetsloven angir også, i § 11, sikkerhetsgraderinger for informasjon.

Det er flere eksempler på klassifiseringer i sektorlovgivningen. Klassifiseringene er av litt ulik art. En form for klassifisering er tekniske klassifiseringer, som for eksempel «laserklasse» for produkter som omfattes av strålevern, eller klassifiseringer av farlige stoffer, der norske regler både forholder seg til et klassifiseringssystem fra EU og et system fra FN for merking av farlige stoffer. Slike former for teknisk klassifisering kan kanskje ikke sies å være direkte sammenlignbar med sikkerhetslovens klassifiseringsbegrep.

Meldinger om smittsomme sykdommer i MSIS er innrettet etter et klassifiseringssystem der ulike sykdommer er grupperes i A, B eller C etter hvor alvorlige de er. Gruppen er en del av meldingen, men den brukes ikke som kriterium for å avgrense hva som skal meldes inn dersom det dreier seg smitte som er spredt med overlegg.

Den formen for klassifisering som man har i sikkerhetsloven, og som det finnes noen paralleller til i sektorlovgivningen, forutsetter en mer sammensatt og skjønnsmessig vurdering. Slike klassifiseringskriterier i ulik sektorlovgivning brukes til å gruppere sammenlignbare nivåer av skadepotensial, eller til å definere terskelverdier for visse typer tiltak eller prioriteringer eller lignende.

Innen informasjonssikkerhet finnes det ulike former for implisitte eller eksplisitte klassifiseringskriterier. I personopplysningsforskriften, som de aller fleste virksomheter må forholde seg til, er ikke klassifisering brukt som begrep. Det er derimot et generelt prinsipp om forholdsmessige sikkerhetstiltak, og forskriften bruker vurderingsmarkørene «… personopplysninger hvor konfidensialitet er nødvendig», «… hvor integritet er nødvendig», og «… hvor tilgjengelighet er nødvendig». Dette forutsetter at virksomheten gjennomfører noen vurderinger av de opplysningene de behandler, men det vil normalt være opp til virksomheten selv å beslutte hva slags opplegg og systematikk de bruker for slike vurderinger. For noen typer virksomhet kan det kanskje være nærliggende å bruke personopplysningslovens definisjon av sensitive personopplysninger som klassifisering, men hvis man satte det som en generell norm ville man stå i fare for å undervurdere beskyttelsesbehovet i mange situasjoner der det behandles opplysninger som ikke kommer inn under den formelle definisjonen av sensitive personopplysninger. At det i utgangspunktet er opp til virksomheten selv hva slags klassifisering de velger å legge opp til er også i samsvar med best practice-standarden ISO 27001. Denne standarden bruker begrepet klassifisering, men det kravet standarden stiller er at virksomheten selv skal bestemme en policy for hvordan de klassifiserer informasjon.

Forskrift om IKT-systemer i banker mv. har i utgangspunktet omtrent samme innfallsvinkel som personopplysningsforskriften. Begrepet klassifisering brukes ikke, men det finnes implisitte krav til å vurdere informasjonen. De implisitte kravene legger noe klarere føringer her enn i personopplysningsforskriften, ettersom det kreves kontinuitetsplaner der man skal ha besluttet på forhånd hvilke IKT-systemer som skal dekkes, og en avvikshåndtering der de hendelsene virksomheten selv vurderer som «svært alvorlige» eller «kritiske» skal rapporteres til Finanstilsynet.

Eksplisitte krav til klassifisering i informasjonssikkerhetsregulering finner man først og fremst i forskriften om informasjonssikkerhet i medhold av sikkerhetsloven. Der er det fire angitte nivåer for sikkerhetsgradering. Et eksplisitt krav til klassifisering finnes også i kapittel 6 om informasjonssikkerhet i Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen. Det er for så vidt bare krav til å skille mellom sensitiv informasjon og annen informasjon, men kriteriene for hva som er sensitivt er definert så tydelig at man bør kunne forvente likeartet klassifiseringspraksis i alle virksomheter som er underlagt denne forskriften. Eksempler på «kraftsensitiv informasjon» i § 6-2 omfatter blant annet lokalisering av reservedriftsentraler, kart over jordkabler, oversikt over fordelingsnett til samfunnskritiske funksjoner med mer. Det følger av forskriften at kravene til sikkerhet er skjerpet for sensitiv informasjon. Forskriften angir relativt åpent formulerte sikkerhetsmål, og den enkelte virksomhet har forholdsvis stor handlefrihet til å beslutte hva de anser som hensiktsmessige tiltak.

Krav til klassifisering som del av et opplegg for å sikre objekter/anlegg finnes også i litt ulike former i noe av sektorlovgivningen.

Forskrift om sikring av havner, og forskrift om sikring av havneanlegg, bruker begrepet maritimt sikringsnivå, med tallene 1–3. Sikringsnivå 1 er det som skal gjelde til enhver tid, og kan vel sammenlignes med begrepet permanent grunnsikring i objektsikkerhetsforskriften. Sikringsnivåene 2 og 3 er midlertidige innskjerpinger av tiltak i situasjoner der myndighetene vurderer at risikoen befinner seg over normalnivå. Disse sikringsnivåene er en formell del av EU-regelverket for sikring av fartøy og havner, dette regelverket legger også opp til en samsvarskontroll mellom landene som sikrer at det etterleves. Tilsvarende system finnes også i sikkerhetsforskriften til skipssikkerhetsloven, der brukes betegnelsen beredskapsnivå i stedet for sikringsnivå.

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen har et opplegg for å klassifisere anlegg i klassene 1–3. Kriteriene for hvilken klasse et anlegg tilhører er knyttet til anleggets ytelse. Klasse 3 brukes der betydningen for energiforsyningen er størst. Både kriteriene for hva slags anlegg som inngår i en klasse, og hvilke sikringskrav som gjelder for hver klasse, er regulert forholdsvis detaljert i forskriften og i forskriftens vedlegg.

Ekom klassifiseringsforskriften klassifiserer anlegg i gruppene A–D. Disse klassene er nærmere omtalt under «område ekom» ovenfor.

Damsikkerhetsforskriften har et opplegg for klassifisering som deler anleggene inn i konsekvensklassene 1–4. Inndelingen av konsekvensklasser er basert på hvilke direkte følger en hendelse kan få, for eksempel hvor mange boliger eller hvilken infrastruktur som vil bli rammet. Det er bare i de to øverste konsekvensklassene det stilles krav til planlagte tiltak mot tilsiktede uønskede hendelser.

Det generelle bildet er at klassifisering er et virkemiddel som har en forholdsvis stor utbredelse i sektorlovgivning om sikring av objekter og infrastruktur. Det ser ut for at klassifiseringen er skarpere og tydeligere i formen på de områdene der det er relativt få eller ensartede virksomheter, mens det i større grad blir opp til virksomhetene selv å beslutte hvordan de vil klassifisere på områder der det er mange eller uensartede virksomheter som er underlagt samme regulering.

## Personkontroll

Sikkerhetslovens bestemmelser om personkontroll og sikkerhetsklarering er i første rekke knyttet til tilgangen til gradert informasjon. Det er imidlertid også mulig etter forskrift om objektsikkerhet, § 3-6, å stille krav til autorisasjon og sikkerhetsklarering for de som skal ha permanent adgang til objekt. Dersom det skal kreves sikkerhetsklarering for adgang til objekter sammenlignes nivåene slik at det kreves klarering for KONFIDENSIELT eller høyere for adgang til KRITISK objekt, og klarering for HEMMELIG eller høyere for adgang til et MEGET KRITISK objekt. Det er imidlertid verdt å merke seg at forskriften ikke legger opp til at det normalt skal være nødvendig med en sikkerhetsklarering for å få permanent adgang til et skjermingsverdig objekt. Det er et virkemiddel som bare skal brukes dersom objekteier kan begrunne behovet, og vedkommende departementet beslutter at det skal stilles krav til sikkerhetsklarering.

I sektorlovgivningen er det svært få eksempler på krav til klarering, vandelsdokumentasjon eller skikkethetsvurderinger for de som jobber med sikring av objekter og anlegg. Kravene til de som skal jobbe med sikkerhet er i de fleste tilfeller begrenset til krav om kunnskaper og ferdigheter, og i noen grad krav til helse.

De eksemplene man kan finne er på samferdselsområdet. I securityforskriften for luftfart er det en egen bestemmelse om vandelskontroll. Vandel kan kontrolleres på grunnlag av en uttømmende politiattest, men dersom man har en sikkerhetsklarering i henhold til sikkerhetsloven anses det som at kravet til vandelskontroll etter securityforskriften er oppfylt.

I de tilfeller der et skip har behov for bevæpnede vakter, stilles det i sikkerhetsforskriften krav til at vaktene har fylt 18 år, kan identifisere seg og fremlegge vandelsattest av nyere dato.

Jernbaneloven § 3d oppstiller i første punktum følgende omfattende liste: «Fører av rullende materiell og annet personell som skal utføre oppgaver knyttet til sikkerheten ved jernbane må oppfylle de vilkår som tilsynsmyndigheten fastsetter om kvalifikasjoner, alder, helse, fysisk og psykisk skikkethet, vandel, edruskap, utdanning, opplæring og trening m.m.» Kravene til kvalifikasjoner,

helse, edruskap og opplæring er omfattende og detaljerte i underliggende forskrifter, mens det ikke er gitt nærmere regler som spesifiserer hvordan vandel skal vurderes og eventuelt i hvilke tilfeller.

På andre områder er kravene i sektorlovgivningen til å dokumentere vandel eller pålitelighet eller tilsvarende egenskaper bortimot fraværende. Noen spredte krav til identifikasjonsbevis forekommer, og det kan man vel anta at er et innarbeidet tiltak svært mange steder uansett om det er nevnt i regelverket eller ikke.

På bakgrunn av § 3-6 i forskrift om objektsikkerhet kan det se ut til at den grunnleggende antakelsen har vært at personkontroll normalt ikke vil være et egnet og forholdsmessig virkemiddel for sikring av objekter og anlegg.

## Angivelse av risikometodikk

I sikkerhetsloven og dens forskrifter er det krav til å gjennomføre og dokumentere risikovurderinger. Det gis i utgangspunktet ikke noen bestemte generelle føringer for hva slags metoder for vurdering som skal brukes. I forskrift om sikkerhetsadministrasjon, § 4-2 fjerde ledd, står det at «NSM kan pålegge en virksomhet å utarbeide skriftlig risikovurdering når særlige grunner foreligger, og bestemme hvilken vurderingsmetode som skal legges til grunn.» Det er altså en hjemmel for å gi anvisninger om risikometodikk i konkrete tilfeller, overfor enkeltvirksomheter. Som drøftet tidligere under gjennomgangen av området generell objektsikkerhet, kan det være noe usikkert hvordan henvisningen fra forskrift om objektsikkerhet til forskrift om sikkerhetsadministrasjon skal forstås. For risikovurderinger som gjelder informasjonssikkerhet på sikkerhetslovens område er det imidlertid ingen tvil om at NSMs kan gjøre bruk av denne adgangen til å pålegge en bestemt risikometodikk.

Risikovurderinger er et gjennomgående trekk ved praktisk talt alle generelle pålegg om å iverksette tiltak for samfunnssikkerhet. I de fleste tilfeller vil sektorlovgivningen, i likhet med sikkerhetslovens bestemmelser, ikke inneholde bestemte generelle føringer for risikometodikk. Noen få unntak finnes, men de er stort sett ganske forsiktig utformet. To eksempler man kan finne blant forskriftene er forskrift om sikring på jernbane, som definerer trusselvurdering som «vurdering av trusselaktørenes intensjon og kapasitet», og forskrift om fysisk beskyttelse av nukleært materiale og nukleære anlegg som anviser metodikken designbasistrussel for å håndtere tilsiktede trusler. At risikometodikken er anvist i forskrift er forankret og begrunnet i utenforliggende faglige standarder, henholdsvis NS 5830 for sikring på jernbane og Det internasjonale atomenergibyrå IAEAs sikkerhetsrammeverk for atomreaktorer. På disse områdene bidrar forskriftsfesting av risikometodikken til å markere vektleggingen av at det er risikoen for tilsiktede uønskede hendelser som skal vurderes, ettersom metodikken i disse tilfellene er tilpasset dette formålet.

I de fleste tilfeller vil en omtale av hvordan risiko skal vurderes være noe man finner i veiledninger fra relevante myndigheter. Eksempelvis har Datatilsynet en egen veiledning om risikovurderinger for informasjonssikkerhet, som beskriver en enkel modell for å vurdere kombinasjonen av sannsynlighet for og konsekvens av en uønsket hendelse. Det at risikometodikken i liten grad fastlegges i lov eller forskrift kan ses som et uttrykk for at dette først og fremst har vært sett som et faglig anliggende. Som ledd i veiledningsdokumenter er fremstillingsformen kanskje først og fremst ment å være en pedagogisk støtte, men de fungerer i praksis også normativt som et slags regelverk av lav trinnhøyde.

Det kan også være av en viss interesse å se at angivelse av risikometodikk kan være et element i overnasjonal regulering, som i praksis påvirker vurderingene av hendelser i Norge, selv om det ikke er direkte synlig i norske rettskilder. Meldingssystemet for smittsomme sykdommer som Norge har hatt siden 1975, og som fikk sin egen forskrift i 2003, har minst siden 2003 hatt smitte som spres med

hensikt som et av varslingskriteriene. Det er den legen eller helseinstitusjonen som oppdager smitten som rapporterer. I utgangspunktet er det bare fastslått smitte som rapporteres, den videre tolkningen og analysen av risiko for samfunnet vurderes av de som mottar og sammenstiller rapporteringene, i første instans Folkehelseinstituttet. Etter hvert har det norske meldingssystemet blitt del av den europeiske smitteovervåkningen, og i relativt nytt EU-regelverk har denne overvåkningen også blitt rettet mot bioterrorisme, altså smitte som spres med hensikt. Det europeiske organet for smitteovervåkning har utviklet separate risikomodeller for epidemisk smitte og bioterrorisme, som har betydning for hvordan hendelser som oppstår i Norge blir vurdert, men uten at det er synlig i norsk regelverk, og uten at det har betydning for hvordan norske leger og helseinstitusjoner rapporterer.

Ellers finnes lovfestet angivelse av risikometodikk også på enkelte områder som ikke dreier seg om tilsiktede hendelser, for eksempel i EUs regelverk om mathygiene, der metoden HACCP (Hazard Analysis and Critical Control Point) er lovfestet. HACCP oversettes til kritiske styringspunker i norsk regelverk. Det kan for eksempel dreie seg om kjernetemperatur i matvaren, pH-verdier, mugg, fare for fremmedlegemer i en matvare med mer. Risikometodikken HACCP er først og fremst anvendelig der de feil og skader man skal unngå er kjente og forutsigbare, og må avdekkes systematisk og håndteres på en bestemt måte.

Det forekommer altså, men i forholdsvis beskjeden utstrekning, at et rettslig regelverk anviser en bestemt risikometodikk for å treffe særskilte trekk ved de aktuelle sikringsbehovene så presist som mulig. Det kan formodentlig være hensiktsmessig i en del situasjoner, for å forenkle arbeidet eller for å gi god sammenheng mellom vurderinger og tiltak. På den annen side kan det også tenkes at en fastlagt metode innsnevrer det som ellers hadde vært et mer åpent blikk for nye og ukjente innfallsvinkler til en type risiko.

## Dilemmaer knyttet til harmonisering og samordning

Spørsmålet om hvem som bestemmer hva som er akseptabel risiko på et område, og hvordan man oppnår et harmonisert nivå av risikoaksept, er på et vis samme spørsmål sett fra to ulike vinkler.

I det som litt overflatisk kan kalles «tradisjonell internkontroll», er et grunnleggende premiss at virksomheten selv bestemmer hva som er et akseptabelt risikonivå, altså stor grad av autonomi for virksomheten. Med uttrykket tradisjonell internkontroll siktes det til den regelverksutviklingen som i Norge oppsto innen petroleumssektoren fra slutten av 1970-tallet, og fikk sin store utbredelse i HMS-reformen som trådte i kraft i 1992, med endringer i en rekke lover, blant annet arbeidsmiljøloven, og den generelle internkontrollforskriften. Oppskriften var, og er i en del tilfeller fortsatt, et risikobasert styringssystem internt i virksomheten. Tilsynsmyndigheter reviderer i hovedsak de systemene virksomheten har lagt opp til, fortrinnsvis uten å overprøve tiltakene eller virksomhetens aksept av risiko. De prinsippene som lå til grunn i den norske internkontrollreformen hadde paralleller i flere andre lands lovgivning, og i EUs «New Approach» reguleringsprinsipp. Internkontrollprinsippet er analysert i en rekke retts- og samfunnsvitenskapelige artikler. Noen av de begrepene som har vært brukt for å analysere denne måten å gi regler på er refleksiv rett, regulert selvregulering, meta-regulering, «lighter-touch regulations» og tilsvarende. Et av de store fortrinnene ved tradisjonell internkontroll er at reguleringen spiller på lag med virksomhetens egeninteresser. Dermed blir reglene forholdsvis lite inngripende for virksomhetene, og det gir ganske fleksible regler som lett kan tilpasses ulike typer virksomhet av forskjellig størrelse og med forskjellige sikringsbehov. Terskelen for at et tilsynsorgan skal overprøve virksomhetens egen fastlegging av akseptnivå vil gjerne være ganske høy. Kritikken fra et tilsynsorgan vil oftest være at internkontrollsystemet er mangelfullt, ikke

er vedlikeholdt, eller er fraværende. Velbegrunnede valg av tiltak eller vurderinger av hvilken risiko som aksepteres overprøves fortrinnsvis ikke.

Tradisjonell internkontroll har to grunnleggende ulemper: Den ene er at det er vanskelig å harmonisere et sikkerhetsnivå på tvers av virksomheter som skal samhandle, noe som særlig gjør seg gjeldende innen informasjonssikkerhet. To virksomheter som følger personopplysningsforskriften eller eforvaltningsforskriften – eller to virksomheter som er sertifisert etter standarden ISO 27001 for den saks skyld – kan likevel ha så ulikt reelt sikkerhetsnivå at de ikke uten videre kan samhandle med et kjent og opprettholdt sikkerhetsnivå som er godt nok for begge, selv om hver av virksomhetene for seg skulle etterleve sine regler på eksemplarisk vis. Slike regler overlater mye til virksomhetene, og fører i liten grad til harmonisert nivå. Det kan imidlertid bemerkes at det finnes ulike sektorstandarder med felles risikoakseptnivå på en del områder, nettopp for å sørge for at samhandling skal være forsvarlig. Noen eksempler er Norm for informasjonssikkerhet i helsesektoren i Norge, standarden PCI DSS for internasjonale betalingskort, og i mer begrenset forstand ID-porten for norsk forvaltning. Generelle forskrifter og standarder som overlater beslutninger om tiltak og aksept av risiko til den enkelte virksomhet gir imidlertid lav grad av harmonisering som resultat.

Den andre ulempen er at virksomhetens egen aksept av risiko gir lite kontroll med risiko som ligger på utsiden av virksomhetsgrensene. Et eksempel på dette fikk man med en tilspisset debatt (i 2008) mellom Petroleumstilsynet og DSB om sikring av eksplosiver i landbasert virksomhet. Petroleumstilsynets tilnærming var risikobasert internkontroll for å sikre mot ulykker og alvorlige konsekvenser av feilhåndtering innad i virksomheten, mens DSB var opptatt av oversikt over og sporing av sprengstoff på avveie, noe som forutsetter strukturer og systemer som når lenger enn den enkelte virksomhets grenser. En vesentlig del av problemstillingen med samfunnskritiske funksjoner og samfunnskritisk infrastruktur dreier seg om at sikkerhetsnivået må være kjent og etterprøvbart utover virksomhetenes grenser.

Motstykket til den tradisjonelle internkontrollen er eksternt fastlagte regler og rammer. Innen for eksempel havnesikring og flysikkerhet er det myndighetsorganer som fastlegger hva som er akseptabel risiko, og stiller med rapporteringskanaler og eventuell avvikshåndtering for hendelser som oppstår utenfor eller har konsekvenser utenfor den enkelte virksomhet. Fordelene med aksept av risiko som enten nedfelles konkret i et regelverk eller som fastlegges av et organ utenfor den enkelte virksomhet er at man oppnår et mer harmonisert sikkerhetsnivå, som også er etterprøvbart, og som ikke blir avveid mot virksomhetenes egeninteresser. Det gir også større mulighet for å bygge pålitelig sikring av infrastruktur som er felles for hele eller store deler av samfunnet, altså der visse aktører (for eksempel internettilbydere) kanskje må levere tjenester med et høyere sikkerhetsnivå enn det den enkelte kundes vurdering av risiko opp mot kostnader tilsier.

Ulempene med eksternt fastlagt akseptnivå kan være høye utgifter til å holde i gang de strukturer og systemer som myndighetsorganene trenger for å overvåke flere ledd i en verdikjede. Det er også en stor fare for høy kompleksitet og detaljeringsgrad i regelverket, og kanskje til en viss grad også slitasje i hvor legitime reglene blir oppfattet å være. Både utgiftene til å overvåke verdikjeden og høy detaljeringsgrad får man et visst bilde av ved å se på utviklingen i en del regelverk, særlig deler av EU-lovgivningen. På CBRNE-området for eksempel, er det hyppige endringer i en svært detaljert liste over kjemikalier som skal følges opp, og disse endringene blir gjennomført ved at stadig nye EU-forordninger føyes til forskriften. Flysikkerhet er også et område der endringer i regelverket fra EU er hyppige, og apparatet for å holde regelverket a jour og iverksette endringer blir omfattende. Slitasje i legitimiteten er ikke noe man kan finne belegg for i rettskilder som sådan, det er i utgangspunktet et empirisk spørsmål. Det er ikke gjennomført noen slike undersøkelser i forbindelse med denne kartleggingen, men det kan kanskje illustreres med et par anekdotiske indisier fra

hendelser som har hatt noe oppmerksomhet i mediene. Ved innføring av EU-forordning om havnesikkerhet (725/2004) var det en håndfull medieoppslag om at de nye reglene ville stenge norske havner, både i økonomisk forstand fordi det ville bli dyrt, og i fysisk forstand fordi noen av de sentralt fastlagte tiltakene gikk ut på inngjerding av soner i havnene. Et annet eksempel, som riktignok hører hjemme i kategorien utilsiktede hendelser, var vulkanasken fra Island i 2010 der flyforbud ble besluttet av ICAO og IATA, mens en del av flyselskapene som fikk regningen i stigende grad begynte å stille spørsmål ved de sentrale prosessene og kriteriene for å fastlegge akseptnivået.

En annen innvending som har vært fremmet mot securityregulering med eksternt fastlagt akseptnivå og detaljerte regler er at sikkerhetskompetansen kan forvitre dersom sikkerhetsarbeid forstås som å følge detaljerte regler i stedet for å arbeide med å utvikle virksomhetens sikkerhetsstyring. En slik innvending kommer blant annet til uttrykk i en masteravhandling om security i petroleumssektoren. Avhandlingens hovedkonklusjon er at det er behov for mer detaljert securityregulering i sektoren, mens innvendingene kommer frem i deler av informantintervjuene. En av bekymringene som ble fremmet av en informant var at «… detaljerte krav vil kunne føre til at selskapene nedprioriterer sin sikkerhetsadministrasjon med kompetente personer. Selskapene vil ikke stille krav til at security aktørene har en problemforståelse til å iverksette nødvendige og risikobaserte tiltak, men ta utgangspunkt i at standardiserte krav kan følges» (Stålesen 2011, s. 48).

Antakelig kan det variere mellom ulike sektorer hvordan forholdet er mellom behovene for kompetent sikkerhetsadministrasjon og ansatte operatører som overholder detaljerte krav. Securityforskriften innen luftfart er fylt med en rekke detaljer som først og fremst skal håndteres likt av et høyt antall operatører, mens arbeidet med å etterleve sikkerhetsregler forankret i IAEAs regime ved landets atomreaktorer kanskje forutsetter høyere kompetanse hos et lavt antall ansatte.

Et siste dilemma er at en rekke ulike sikkerhetsregelverk stablet ved siden av hverandre kan føre til unødvendig dobbeltarbeid og i verste fall motstridende krav for den enkelte virksomhet. I en situasjon der ett regelverk skal avverge bomber, et annet avverge tap av data og et tredje sørge for at personer blir evakuert raskt ved behov, kan sammenhengen mellom reguleringene ha en del å si for hvor byrdefullt dette blir for den enkelte virksomhet. Et internkontrollprinsipp som lar mest mulig være opp til den enkelte virksomhet vil kanskje gi mer fleksibilitet til å samordne kravene på en måte som passer for virksomheten. Når ulike sektorregler bindes opp i store strukturer og systemer for å overvåke og intervenere innen hvert sitt område, og de ulike sektorreglene kanskje også endres i høyst ulike tempo, er det en fare for at summen av sikkerhetsregler fremstår mer fragmentert og mer innsatskrevende for den enkelte virksomhet.

# Oppsummering

Kartleggingen har tatt for seg regulering av virksomheters plikter til å treffe tiltak mot tilsiktede, uønskede hendelser. Det omfatter både regulering som er spesifikt avgrenset til å omfatte tilsiktede hendelser, og regulering som er felles for tilsiktede og utilsiktede hendelser. Det finnes, slik kartleggingen viser, en del relevant sektorlovgivning av dette slaget.

De grunnleggende elementene i disse reglene er forholdsvis like, oftest en variant av et risikobasert styringssystem for planlegging, iverksetting, kontroll med og forbedring av sikkerhetstiltakene. Likevel er det også mange trekk ved reglene som viser at det er vanskelig å utlede noe klart mønster som kan brukes til å slå fast hva som er den beste, eller eventuelt den «mest typiske» måten å utforme slike regler på.

Klassifisering er kanskje det eneste av trekkene ved de kartlagte regelverkene som er forholdsvis utbredt. En eller annen form for klassifisering finner man i mange av regelverkene. Sektorlovgivningen har til sammenligning få innslag av regler om utpeking av virksomheter, eller om personellsikkerhet, eller som legger føringer for valg av risikovurderingsmetode.

Det er en bevegelse i regelverksutviklingen på en del områder i retning av mer eksternt fastlagte krav og mindre handlingsrom for den enkelte virksomhet. Det ligger noen dilemmaer i dette som både berører mulighetene for å oppnå et felles harmonisert sikkerhetsnivå i en verdikjede, og spørsmålet om hvordan sammenhengene mellom reglene, og kostnadene ved å følge dem, fortoner seg for virksomhetene.

En siste observasjon, som også kan være verdt å ta med i betraktningen når man skal ta stilling til hvordan nye regler skal utformes, er de store forskjellene i hvor hyppig og hvor omfattende ulike regelverk endres. Det dreier seg særlig om endringstakten i EU-lovgivningen på enkelte områder. Særlig innen sikkerhet i luftfarten og sikring av farlige stoffer er endringene i overnasjonale regler både hyppige og omfattende. På disse områdene kan det tenkes at norsk lovgivning bør la sektorene utvikle sine regler autonomt, for i det hele tatt å makte å henge med på endringene, i stedet for å prøve å se de norske implementeringene i sammenheng med sikkerhetsregulering på andre områder.

| Lov | Forskrift | Tilsynsmyndighet |
|---|---|---|
| *Område: Generell objektsikkerhet* | | |
| Sikkerhetsloven av 20. mars 1998 nr. 10 | Forskrift om objektsikkerhet av 22. oktober 2010 nr. 1362 | Nasjonal sikkerhetsmyndighet |
| *Område: CBRNE (Chemical, Biological, Radiological, Nuclear, and Explosives), kontroll med farlige stoffer* | | |
| Atomenergiloven av 12. mai 1972 nr. 28 | Forskrift om fysisk beskyttelse av nukleært materiale og nukleære anlegg av 2. november 1984 nr. 1809 | Statens strålevern |
| Lov om strålevern og bruk av stråling av 12. mai 2000 nr. 36 | Forskrift om strålevern og bruk av stråling av 29. oktober 2010 nr. 1380 | Statens strålevern |
| Brann- og eksplosjonsvernloven av 14. juni 2002 nr. 20 | Forskrift om håndtering av utgangsstoffer for eksplosiver av 2. juni 2015 nr. 588 | Direktoratet for samfunnssikkerhet og beredskap<br>(kan la andre føre tilsyn på deres vegne) |
| | Forskrift om håndtering av farlig stoff, 8. juni 2009 nr. 602 | I utgangspunktet den enkelte kommune<br>Direktoratet for samfunnssikkerhet og beredskap fører tilsyn med virksomheter som representerer en betydelig risiko eller der direktoratet har et særskilt behov for oversikt |
| *Område: Energi* | | |
| Petroleumsloven av 29. november 1996 nr. 72 | *(Forskriftshjemmel som ikke er benyttet, i lovens § 9-3 om tilsiktede anslag)* | Petroleumstilsynet<br>(myndighet delegert fra Arbeidsdepartementet 1.2.2013) |
| Energiloven av 29. juni 1990 nr. 50 | Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen av 7. desember 2012 nr. 1157 | Norges vassdrags- og energidirektorat |
| Vannressursloven av 24. november 2000 nr. 82 | Damsikkerhetsforskriften av 18. desember 2009 nr. 1600 | Norges vassdrags- og energidirektorat |
| Drivstoffanleggsloven, 31. mars 1949 nr. 3 | | Olje- og energidepartementet<br>(kompetanse etter loven kan overføres til en nemnd) |
| *Område: Samferdsel* | | |
| Luftfartsloven 11. juni 1993 nr. 101 | Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten mv. av 1. mars 2011 nr. 214 («securityforskriften») | Luftfartstilsynet |
| Skipssikkerhetsloven av 16. februar 2007 nr. 9 | Sikkerhetsforskriften (skip mv.) av 22. juni 2004 nr. 972 | Sjøfartsdirektoratet<br>(andre kan gis avgrenset tilsynsansvar basert på avtale) |
| Havne- og farvannsloven av 17. april 2009 nr. 19 | Forskrift om sikring av havner av 29. mai 2013 nr. 539 | Kystverket<br>(kan overlates til en *Recognized Security Organization*) |
| | Forskrift om sikring av havneanlegg av 29. mai 2013 nr. 538 | Kystverket<br>(kan overlates til en *Recognized Security Organization*) |
| Jernbaneloven av 11. juni 1993 nr. 100 | Forskrift om sikring på jernbane, av 1. juli 2015 nr. 848 | Jernbanetilsynet |

| Lov | Forskrift | Tilsynsmyndighet |
|---|---|---|
| *Område: IKT infrastruktur og informasjonssikkerhet* | | |
| Personopplysningsloven av 14. april 2000 nr. 31 | Personopplysningsforskriften av 15. desember 2000 nr. 1265 | Datatilsynet |
| Forvaltningsloven av 10. februar 1967 | eForvaltningsforskriften av 25. juni 2004 nr. 988 | Ikke tilsyn med kompetanse til å gi pålegg, men «Det organet departementet peker ut skal gi anbefalinger på området.» Difi er utpekt i brev fra KMD 12.3.2014 |
| Sikkerhetsloven av 20. mars 1998 nr. 10 | Forskrift om informasjonssikkerhet av 1. juli 2001 nr. 744 | Nasjonal sikkerhetsmyndighet |
| | Forskrift om sikkerhetsadministrasjon av 29. juni 2001 nr. 723 | |
| *Område: Ekom (Elektronisk kommunikasjon)* | | |
| Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 nr. 83 | Ekomforskriften av 16. februar 2004 nr. 401 | Nasjonal kommunikasjonsmyndighet |
| | Forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskrifta), 10. september 2012 nr. 866 | Nasjonal kommunikasjonsmyndighet |
| *Område: Finans* | | |
| Lov om betalingssystemer mv. av 17. desember 1999 nr. 95 | Forskrift om IKT-systemer i banker mv, 21. mai 2003 nr. 630 | Finanstilsynet |
| Lov om tilsynet med finansinstitusjoner mv. av 7. desember 1956 nr. 1 | | |
| *Område: Helse* | | |
| Helseregisterloven av 20. juni 2014 nr. 43 | MSIS-forskriften av 20. juni 2003 nr. 740 | Datatilsynet |
| Smittevernloven av 5. mai 1994 nr. 55 | | Helsetilsynet |
| *Område: Samordning (overnasjonalt/EPCIP, og samordning regionalt og lokalt)* | | |
| Sivilbeskyttelsesloven av 25. juni 2010 nr. 45 | Forskrift om kommunal beredskapsplikt, 22. august 2011 nr. 894 | Fylkesmannen |
| | Forskrift om sivilbeskyttelsesloven på Svalbard, 18. desember 2012 nr. 1293 | Sysselmannen |
| *(hjemlet i Kongens instruksjonsmyndighet)* | Instruks for fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet, beredskap og krisehåndtering, fastsatt ved Kgl. res. 19. juni 2015, nr. 703 | Fylkesmannen<br>(Direktorat for samfunnssikkerhet og beredskap «der det ikke er enighet om hvilke sivile tiltak som bør iverksettes») |

# Litteratur

Ojo, Marianne (2010). The growing importance of risk in financial regulation. *The Journal of Risk Finance, 11(3)*, s. 249-267.

Power, Michael (2005). The invention of operational risk. *Review of International Political Economy, 12(4)*, s. 577-599.

Stålesen, Jorun Stornes (2011). Security styring i petroleumssektoren. Mastergradsstudium i samfunnssikkerhet, Universitetet i Stavanger.