Juridisk vurdering av deling av data fra maritime overvåkings- og meldingssystemer

Rapport fra arbeidsgruppe

11.01.2013

Innhold

Kapittel 1. Innledning og bakgrunn for arbeidsgruppen

Overvåkings- og meldingssystemer for sjøtransporten er viktige elementer i sjøsikkerhetspolitikken, både nasjonalt og internasjonalt. Internasjonalt samarbeid om overvåking av sjøtransport og forbedring av meldings- og rapporeringsrutiner er under rask utvikling. Det etableres også systemer for å bedre ressurskontroll, bekjempe miljøkriminalitet, styrke antiterrorarbeid og styrke grenseovervåking.

Fiskeri- og kystdepartementet har blant annet ansvar for sjøtransport, havnepolitikk og forebyggende sjøsikkerhet. Som fagetat under departementet har Kystverket som en av sine oppgaver å samle inn og tilrettelegge for bruk av data fra maritime overvåkings- og meldingssystemer. Fiskeri- og kystdepartementet har identifisert et behov for en juridisk vurdering av regelverk som eventuelt kan sette rammer for denne oppgaven. Vurderingen vil legges til grunn ved utarbeiding av retningslinjer for deling av maritime data.

Kapittel 2. Sammendrag

I kapittel 4 omtales juridisk eierskap til ulike maritime data. En ekstern utredning av problemstillingen følger som vedlegg 1 til rapporten.

I kapittel 5 omtales de aktuelle maritime overvåkings- og informasjonssystemene.

Kapittel 6 viser til de avtalene som per i dag er inngått om deling av data fra maritime overvåkings- og meldingssystemer. En liste over avtalene følger som vedlegg 2 til rapporten.

Kapittel 7 er å anse som rapportens hovedkapittel, og inneholder en vurdering av nasjonale regelverk og deres betydning for deling av data fra maritime overvåkings- og meldingssystemer. De regelverk som arbeidsgruppen har vurdert er følgende:

- Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)
- Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven)
- Lov 20. mars nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)
- Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument offentleg verksemd (offentleglova)
- Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven)

Arbeidsgruppen har i tillegg vurdert relevante internasjonale regelverk, og denne vurderingen fremkommer av kapittel 8.

I kapittel 9 er det foretatt en vurdering av økonomiske og administrative konsekvenser av arbeidsgruppens konklusjoner.

I kapittel 10 er arbeidsgruppens konklusjoner presentert.

Kapittel 3. Arbeidsgruppens mandat, sammensetning og arbeid

Fiskeri- og kystdepartementet besluttet ved brev datert 27. september 2011 å nedsette en arbeidsgruppe med representanter fra både Kystverket og departementet. På bakgrunn av tidligere innspill fra Kystverket, ble arbeidsgruppen gitt i mandat å gjennomføre en juridisk vurdering av regelverk som kan ha betydning for adgangen til å dele data fra ulike systemer for overvåking av skipstrafikk og maritime rapporterings- og meldingssystemer innenfor Kystverkets ansvarsområde. Det skulle i denne forbindelse ses hen til nasjonal lovgivning, internasjonale konvensjoner, EU-rett og EØS-avtalen. Arbeidsgruppen fikk videre i oppdrag å identifisere problemstillinger som ev. burde redegjøres for eksternt.

Arbeidsgruppen har bestått av:

- Seniorrådgiver Anita Christoffersen, Fiskeri- og kystdepartementet
- Rådgiver Øystein Haga Skånland, Fiskeri- og kystdepartementet
- Seniorrådgiver Bjørnar Kleppe, Kystverket
- Seniorrådgiver Jeanette Assev-Lindin, Kystverket
- Rådgiver Kjetil Borhaug, Kystverket

Arbeidsgruppen hadde sitt første møte 7. november 2011, og har til sammen hatt 9 møter.

Ulike deler av rapporten har vært forelagt berørte departementer og etater for innspill og kommentarer.

Kapittel 4. Eierskap til data

Arbeidsgruppen stilte tidlig i arbeidet spørsmål ved hvem som har juridisk eierskap til ulike maritime data, og i hvilken grad dette ville ha betydning for deling av slike data.

Arbeidsgruppen innhentet derfor en ekstern vurdering av følgende problemstillinger:

- Mange aktører, både offentlige og private, er involvert i produksjon, utsendelse, deteksjon/ innsamling, systematisering, bearbeiding og videredistribusjon av maritime data. Hvilke forhold er av betydning når eierskap til data skal vurderes?

- Hva innebærer det å ha eierskap til data? Hvilke generelle rettigheter og plikter medfører eierskap til de aktuelle maritime dataene, og hvilke begrensninger legger dette på andre aktørers bruk av dataene?
- Hvem eier de ulike maritime dataene som Kystverket i dag tilgjengeliggjør og distribuerer?

Bing Hodneland advokatselskap ved advokat/professor dr. juris Olav Torvund og advokat Magnus Ødegaard ble tildelt oppdraget. Utredningen følger rapporten som vedlegg 1.

Bing Hodneland slår fast at ingen kan ha eller oppnå eierskap til maritime data (enkeltopplysninger isolert sett) som Kystverket i dag tilgjengeliggjør og distribuerer. Aktører som har foretatt en vesentlig investering knyttet til innsamling og/ eller systematisering av data, kan imidlertid ha vern for sin samling av maritime data (databasen) i kraft av det særskilte databasevernet i lov 12. mai 1961 nr. 2 om opphavsrett til åndsverk mv. (åndsverkloven) § 43 og databasedirektivet.[1]

Åndsverkloven § 43 første ledd sier følgende om hvilke rettigheter dette vernet medfører:
"enerett til å råde over hele eller vesentlige deler av arbeidets innhold ved å fremstille eksemplar av det og ved å gjøre det tilgjengelig for allmennheten."

Utredningen konkluderer med at Kystverket har foretatt vesentlig investering knyttet til innsamling og systematisering av data i AIS-databasen og SafeSeaNet-databasen. Disse databasene er derfor vernet etter åndsverkloven § 43 og databasedirektivet. Etter arbeidsgruppens vurdering, innebærer dette at Kystverket har enerett på å gi tilgang til disse databasene. Andre kan ikke uten avtale fremstille kopi av vesentlige deler av disse basenes innhold, videreformidle tilgang til data, eller systematisk hente ut deler av databasenes innhold. Offentleglova og andre relevante regelverk som gir krav på innsyn vil imidlertid komme til anvendelse på de enkelte dataene.

LRIT-databasene som Kystverket har tilgang til, er per i dag ikke vernet av åndsverkloven § 43 og databasedirektivet. Bing Hodneland begrunner dette med at systemet er lukket, at data produseres innenfor systemet og at Kystverket ikke har foretatt investeringer knyttet til innsamling og systematisering av dataene.

Utredningens konklusjoner er lagt til grunn for arbeidsgruppens vurderinger.

[1] Eu-direktiv 96/9 av 11.mars 1996 om rettslig vern av datbaser

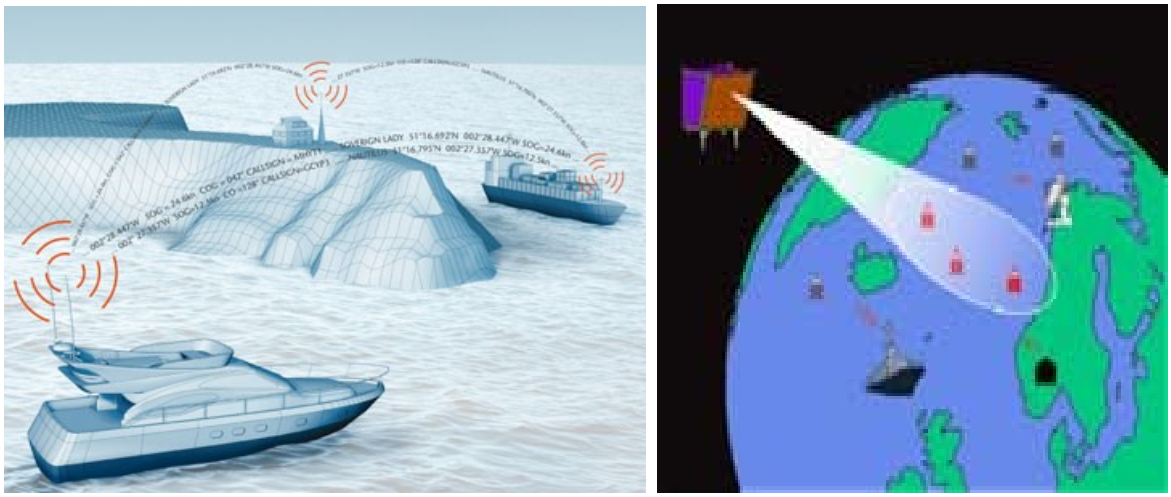
Kapittel 5. Bakgrunnsinformasjon

Som et bakteppe for studien, har arbeidsgruppen sett behov for å klargjøre nøkkelbegreper og gi kortfattet informasjon om de i denne sammenheng sentrale maritime overvåkings- og informasjonssystemene.

5.1 Hva er AIS-data?

AIS er et automatisk identifikasjonssystem som er innført av FNs sjøfartsorganisasjon IMO for å øke sikkerheten for skip og miljø, samt forbedre trafikkovervåking og sjøtrafikktjenester. Systemet innebærer at fartøy utveksler informasjon om blant annet hverandres posisjon, kurs og fart, slik at kollisjonsfaren reduseres. AIS-data fanges opp ved hjelp av basestasjoner på land, og dataene kan dermed gi oversikt over skipstrafikken.

AIS-data er i sin natur åpen informasjon og kringkastes ut fra det enkelte fartøy på åpen kommunikasjonskanal. Kystverket mottar AIS-data som sendes fra fartøy langs norskekysten ut til ca. 40 nautiske mil, organiserer disse i en database, gjør dataene søkbare, distribuerer data til brukere i Norge og maritime myndigheter i flere andre land og lagrer historiske data. I tillegg mottar Kystverket AIS-data som sendes ut fra skip på global basis og som detekteres av den norske nasjonale AIS-satellitten, AISSat-1. AIS-data oppfanget ved hjelp av AIS-satellitten kan behandles og distribueres sammen med data innsamlet ved hjelp av de landbaserte basestasjonene.



AIS- signaler sendes mellom skip og til landstasjoner og satellitt

Forskrift 15. september 1992 nr. 701 om navigasjonshjelpemidler og bro-, styrehus-, radioarrangementer for skip kapittel 4 og forskrift 13. juni 2000 nr.660 om konstruksjon, utstyr, drift og besiktelser for fiske- og fangstfartøy med største lengde på 15 meter og derover kapittel 10 regulerer bærekrav til AIS- utstyr om bord på norske skip. I tillegg er det mange fartøy som utstyrer seg med AIS, selv om de faller utenfor bærekravet til AIS-utstyr. Ut fra disse dataene vil skipet identifiseres entydig og skipets posisjon, kurs

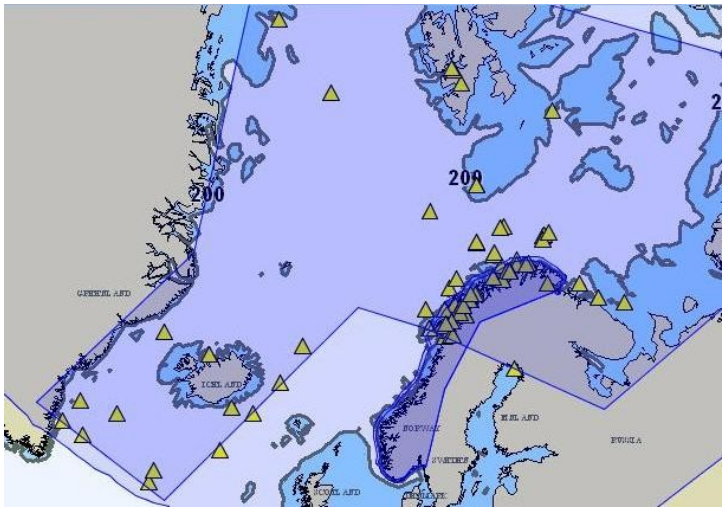
og fart vil være tilgjengelig i tilnærmet sann tid. Informasjon om skipets destinasjon, type, dimensjoner og farlig eller forurensende last er også inkludert i AIS-dataene. For en fullstendig oversikt over meldingsinnhold, se vedlegg 3.

AIS-data brukes i forbindelse med trafikkovervåking, kontroll og inngrep overfor fartøy som utgjør en fare for sjøsikkerheten. Dataene brukes videre til å lokalisere forulykkede og omkringliggende fartøy i forbindelse med redningsaksjoner, og til overvåking av fartøy involvert i ulovlig, urapportert eller uregistrert fiske eller andre ulovlige aktiviteter. Kystverket bruker også historiske AIS-data til å utarbeide statistikk over sjøtrafikken langs kysten. Statistikken gir Kystverket mulighet til bedre planlegging og tilrettelegging for rask, sikker og effektiv sjøtransport.

5.2 Hva er LRIT-data?

Long Range Identification and Tracking (LRIT) er et globalt satellittbasert system for identifisering og sporing av fartøy. Forskrift 15. september 1992 nr. 701 om navigasjonshjelpemidler og bro-, styrehus-, radioarrangementer for skip kapittel 4 regulerer hvilke skip som har bærekrav til LRIT- utstyr. Forskriften implementerer en beslutning av FNs sjøfartsorganisasjon IMO om at LRIT er obligatorisk for passasjerskip, lasteskip over 300 bruttotonn og flyttbare offshore boreenheter i internasjonal fart. Systemet er laget slik at det geografiske dekningsområdet er globalt og inkluderer havområder og polare områder. Normalt sendes posisjonsrapporter fra skip hver sjette time, men dette kan justeres ved behov.

LRIT-data kommuniseres på lukket kommunikasjonskanal, og kun IMOs medlemsstater kan motta data fra LRIT- systemet. I motsetning til AIS-systemet så inneholder LRIT-systemet databaser over fartøy som har plikt til å sende data og tidspunkter for når data skal sendes. Dette danner grunnlag for kontroll med at fartøyene sender data i tråd med sine forpliktelser. LRIT-data har i utgangspunktet et sikkerhetsformål (security), men kan til dels benyttes på liknende måte som AIS-data.



Øyeblikksbilde av skipsposisjoner rapportert gjennom LRIT- systemet i et avgrenset område

5.3 Hva er SafeSeaNet-data?

SafeSeaNet (SSN) Norway er et nasjonalt meldingssystem for skip som ankommer eller forlater norske havner. Systemet bidrar til økt sjøsikkerhet, havnesikring og effektiv sjøtransport ved å lagre, hente og utveksle fartøysopplysninger.

Gjennom SSN rapporterer skip melding om anløp til havn, melding om farlig og forurensende last[2] og ISPS- anløpsmelding[3] til Kystverket. Disse meldingene inneholder blant annet skipets identitet, anløpssted, anløps- og avgangstid, detaljer om type og mengde farlig eller forurensende last samt passasjerliste og mannskapsliste. For fullstendig liste over meldingsinnholdet i ISPS-anløpsmeldinger, se vedlegg 5.

SSN-data kan kombineres med for eksempel AIS- eller LRIT-data for å gi detaljert informasjon om skipstrafikk og aktuelle fartøy. Dette er viktig informasjon for blant annet Kystverkets sjøtrafikksentraler og oljevernberedskap. SSN gir også informasjon om passasjerer og besetning, noe som er viktig ved søk og redningsaksjoner.

SSN Norway er basert på det europeiske Single Window konseptet som innebærer at det utvikles en nasjonal portal hvor fartøy, rederier og operatører kan sende inn rapporteringspliktig informasjon til nasjonale myndigheter kun én gang. Denne informasjonen blir videreformidlet automatisk til nasjonale myndigheter for å forenkle og øke kvaliteten på offentlig saksbehandling overfor maritime brukere. Informasjon om farlig eller forurensende last blir videreformidlet til det sentrale europeiske SSN systemet.

SSN Norway benyttes også som rapporteringsportal for meldinger til flere offentlige etater, herunder Sjøfartsdirektoratet og Forsvaret, i tillegg til Kystverket. Arbeidsgruppen vil kun se på SSN- data som Kystverket mottar og har ansvar for.

Kapittel 6. Eksisterende avtaler om deling av data

Fiskeri- og kystdepartementet og Kystverket har inngått avtaler om gjensidig deling av maritime data både på nasjonalt nivå og med andre stater og internasjonale organisasjoner. Arbeidsgruppen har vurdert at en gjennomgang av de eksisterende avtalene faller utenfor gruppens mandat.

Stortinget har gitt Kystverket nasjonalt ansvar for innsamling av AIS- data fra landbaserte mottakere og satellitt, distribusjon av data nasjonalt, samt internasjonalt samarbeid om utveksling av slike data[4]. På denne bakgrunn anbefaler arbeidsgruppen at Kystverket gis i oppdrag å gjennomgå avtalene på bakgrunn av konklusjonene i

[2] Forskrift 17.desember 2009 nr. 1633 om krav til melding for fartøy over 300 bruttotonn og fartøy som transporterer farlig eller forurensende last.
[3] ISPS: The International Ship and Port Facility Security Code
[4] Kapittel 1062 i Prop.1 S (2011-2012) Fiskeri- og kystdepartementet

denne rapporten. En oversikt over eksisterende avtaler om gjensidig deling av maritime data følger i vedlegg 2.

I tillegg til avtalene om gjensidig deling av maritime data som vist til i vedlegg 2, har flere private og offentlige aktører tilgang til AIS-data, LRIT-data og SSN-data gjennom tilganger til Kystverkets systemer.

Kapittel 7. Vurdering av nasjonalt regelverk

Arbeidsgruppen har identifisert enkelte regelverk som kan ha betydning for adgangen til å dele data fra systemer for overvåking av skipstrafikk og maritime rapporterings- og meldingssystemer. En juridisk vurdering av disse regelverkene fremkommer under. Dette er å anse som rapportens hoveddel.

7.1 Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)

Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger. Loven er generell og gjelder i utgangspunktet for all slags behandling av personopplysninger.

Personopplysningsloven bygger på EU-direktiv nr. 95/46 av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet). Direktivet har som siktemål å etablere felles reguleringsprinsipper og et ensartet vern for behandling av personopplysninger i hele EU-området.

7.1.1 Lovens saklige virkeområde

Det følger av personopplysningsloven § 3(1) at loven gjelder ved behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler og ved annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister. Behandling av data kan være innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter. Loven skiller ikke mellom privat eller offentlig virksomhet.

Begrepet personopplysning defineres i lovens § 2 (1) punkt 1 som "*opplysninger og vurderinger som kan knyttes til en enkeltperson*". Opplysninger og vurderinger om juridiske personer faller utenfor definisjonen.

Det følger av forarbeidene i Ot.prp nr. 92 (1998-1999) kapittel 16 merknad til § 2 at "*med uttrykket «enkeltperson» menes en person som direkte eller indirekte kan identifiseres, f. eks*

ved hjelp av navn, identifikasjonsnummer eller et annet kjennetegn." Det kreves således ikke at personens navn må fremgå direkte i forbindelse med opplysningen for at det skal dreie seg om en personopplysning, så lenge man kan identifisere vedkommende på annen måte. I forhold til spørsmålet om en person lar seg identifisere, "*skal det tas i betraktning alle hjelpemidler som det er rimelig å tro at noen kan komme til å anvende for identifiseringsformål*." Forarbeidene uttaler at "*det vil dreie seg om en personopplysning selv om det må benyttes en nøkkel - f eks i form av en tallkode - for å knytte forbindelsen mellom opplysningen og den bestemte personen*". Det fremgår videre at en i tvilstilfeller kan legge vekt på formålsbestemmelsen i personopplysningsloven ved avgjørelsen av hvor langt personopplysningsbegrepet rekker, og at "*det kan tenkes tilfeller der ordlyden i nr. 1 isolert sett trekker i retning av at en opplysning er «personopplysning», men hvor personvernhensyn ikke kan begrunne at opplysningen vernes*." Vi konkluderer derfor med at personopplysningsbegrepet bør tolkes relativ vidt, men at formålsbestemmelsen kan tilsi en innskrenkende tolkning.

Kystverket mottar LRIT- og AIS- data fra fartøy. Bærekravet for LRIT gjelder i hovedsak fartøy som går i internasjonal fart og som er passasjerskip eller lasteskip med BT på 300 eller over. Bærekrav for AIS er i hovedsak lagt på passasjerskip, lasteskip, fiskefartøy og fritidsfartøy over 300 BT eller 45 meter. Etter en nærmere innfasingsplan skal bærekravet innføres også for fiskefartøy fra 15 til 45 meter.

LRIT- og AIS- data gir informasjon om hvor et fartøy befinner seg og annen informasjon relatert til fartøyet selv. Informasjon om fartøyets IMO nummer, MMSI[5] eller kallesignal gjør det mulig å finne eieren av fartøyet ved å knytte informasjonen fra AIS/LRIT til informasjon som er tilgjengelig i diverse åpne register, blant annet Norsk internasjonalt skipsregister og Norsk ordinært skipsregister (her kan man registrere fartøy ned til 7 meter). Mindre privateide fartøyer har ofte eieren om bord, og man vil dermed ved hjelp av skipsopplysningene kunne finne ut hvor eieren av fartøyet befinner seg. Det vil imidlertid ikke være mulig å finne mannskapslister og passasjerlister i slike skipsregister som nevnt her. Informasjon om hvilke personer som faktisk er om bord vil dermed ikke være like tilgjengelig som informasjon om eieren. Slike opplysninger vil uansett være personopplysninger etter personopplysningsloven, og må vernes av den som er behandlingsansvarlig etter lovens definisjoner.

På bakgrunn av tolkningen over, vil alle LRIT- og AIS- data som gjelder posisjonen til fartøy som er registrert med en privatperson som eier være personopplysninger. Når et fartøy er registrert på en privatperson vil andre kunne sammenholde skipsregisteropplysninger og LRIT- og AIS- data for å få opplysninger om hvor en person befinner seg.

Kystverket har i dag ingen mulighet for å kontrollere om LRIT- og AIS- dataene kommer fra fartøy som er registrert på en privatperson eller en juridisk person før dataene eventuelt distribueres. For å oppfylle kravene personopplysningsloven stiller til

[5] Maritime Mobile Service Identity

håndtering av personopplysninger, er en praktisk mulighet å filtrere fartøyene etter skipstype og størrelse.

Når det gjelder LRIT er dette et system som ikke installeres av andre enn de som har bærekrav etter forskriften. Dette er større fartøy som er i kommersiell drift. Vi vurderer det som så lite sannsynlig at disse har eventuelle private eiere om bord, at informasjon om posisjonen til disse skipene ikke kan anses som en personopplysning sett i sammenheng med formålet med loven. De fleste av fartøyene med bærekrav til AIS er også over 300 BT og i kommersiell drift. Posisjonen til disse fartøyene anses heller ikke som en personopplysning. Når det gjelder fiskefartøy vil det etter hvert være et bærekrav for fiskefartøy ned til 15 meter. Så små fiskefartøy har ofte eieren av fartøyet om bord. I tillegg er det en del mindre fartøy som installerer AIS frivillig, og Kystverket vil også motta data fra disse fartøyene. I slike tilfeller vil det være stor sannsynlighet for at eieren faktisk befinner seg om bord.

Når det gjelder de maritime data som Kystverket krever inn i SafeSeaNet vil disse i stor grad knytte seg til informasjon om juridiske personer og personopplysningsloven vil ikke få anvendelse. Det er likevel noen tilfeller hvor det samles inn data som vil være å anse som personopplysninger. Det klareste tilfellet knytter seg til ISPS-anløpsmeldingen som i hovedsak gis av alle passasjerskip samt lasteskip (500 BT og over), som er i internasjonal fart. Denne meldingen gis i SafeSeaNet. Slike meldinger inneholder mannskapslister og passasjerlister som utvilsomt er å anse som personopplysninger etter personopplysningsloven. Andre meldinger som Kystverket krever inn i SafeSeaNet er melding om anløp og melding om farlig og forurensende last. Disse meldingene inneholder i seg selv ingen personopplysninger, men informasjon om skipet, lasten og destinasjonen. Men ved å ha opplysninger som identifiserer skipet vil man kunne identifisere en eier, slik som nevnt over for LRIT- og AIS- data. Anløpsmeldingen gis kun av fartøy over 300 BT, mens melding om farlig og forurensende last gis av alle fartøy som har slik last om bord, uavhengig av størrelse.

Spørsmålet blir dermed om det er mulig å sette en generell grense for størrelse på fartøy, evt. skille ut typer av fartøy, slik at man kan filtrere vekk data som vil være å anse som personopplysninger.

Arbeidsgruppen vurderer det slik at posisjonsdata fra fritidsfartøy alltid bør behandles som potensielle personopplysninger. Når det gjelder fiskefartøy og andre fartøy mener arbeidsgruppen det vil være mulig å sette en størrelsesgrense for når posisjonsdata vil være å anse som en personopplysning.

Det er en klar sammenheng mellom størrelsen på fartøyet og sannsynligheten for at eieren er om bord. På mindre fritidsfartøy og fiskefartøy vil det stort sett være slik at eieren alltid er om bord. På større kommersielle skip vil ikke dette være tilfelle. På slike skip vil det være svært lite sannsynlig at det er en privatperson som er eier, og dersom det er en privatperson som eier fartøyet, vil det være lite sannsynlig at en eier er om bord. Som nevnt peker forarbeidene på at det i noen tilfeller ikke foreligger personvernhensyn som taler for å verne opplysningene, selv om opplysningene strengt

tatt er personopplysninger. For disse større fartøyene vil lovens hovedformål om bevarelse av personlig integritet og privatlivets fred ikke gjøre seg gjeldende.

Arbeidsgruppen vurderer det slik at det vil være mulig å sette en grense for hvilke fartøy der posisjonsdata vil kunne være personopplysninger. Det presiseres først at arbeidsgruppen anser posisjonsdata fra fritidsfartøy til å være personopplysninger uavhengig av størrelse. Arbeidsgruppen foreslår at posisjonsdata fra fartøy under 300 BT eller 45 meter behandles som personopplysninger, jf. argumentasjonen i avsnittet over. Dersom fartøy over denne størrelsen eies av en privatperson, vurderer vi det som lite sannsynlig at eieren faktisk er om bord. Man er da også utenfor det som personvernhensynet skal verne, jf. uttalelsene i Ot.prp nr. 92 (1998-1999) kapittel 16 merknadene til § 2.

Størrelsesbegrensningen faller også sammen med virkeområdet for EU direktiv 2002/59 som blant annet regulerer bærekrav til AIS og ulike meldeforpliktelser for skip. Vi mener grensen vil være fornuftig i forhold til hva som kan være å anse som personopplysninger.

Det fremstår som klart at Kystverkets innsamling og senere eventuelle analyse av dataene som er omtalt her må være å anse som en behandling etter personopplysningsloven. Det er også en behandling som skjer med elektroniske hjelpemidler.

Loven får dermed anvendelse for Kystverkets behandling av de deler av ISPS-anløpsmeldingensom inneholder mannskapslister og passasjerlister, samt for de AIS-posisjonsdata og melding om farlig og forurensende last som avgis fra fartøy hvor det ikke er en juridisk person som eier og fartøyet er under 300 BT eller 45 meter.

7.1.2 Lovens geografiske virkeområde

Det følger av personopplysningsloven § 4(1) at "*Loven gjelder for behandlingsansvarlige som er etablert i Norge. Kongen kan i forskrift bestemme at loven helt eller delvis skal gjelde for Svalbard og Jan Mayen, og fastsette særlige regler om behandling av personopplysninger for disse områdene.*"

Det følger av forskrift 15.12.2000 nr. 1265 om behandling av personopplysninger § 1-4 og § 1-5 at personopplysningsloven gjelder for behandlingsansvarlige som er etablert på Svalbard og Jan Mayen.

For å være «etablert» kreves det at man har en forretningsmessig virksomhet. Her må tre kumulative vilkår være oppfylt: det må utøves en aktivitet i Norge, aktiviteten må skje gjennom en fast organisatorisk infrastruktur, og for et ubestemt tidsrom.

Det følger videre av § 4(2) at "*Loven gjelder også for behandlingsansvarlige som er etablert i stater utenfor EØS-området dersom den behandlingsansvarlige benytter hjelpemidler i Norge. Dette gjelder likevel ikke dersom hjelpemidlene bare brukes til å overføre personopplysninger via Norge.*"

7.1.3 Roller

Personopplysningsloven legger ansvar og plikter på den som har utpekte roller i behandlingen av personopplysninger. Loven skiller mellom å være behandlingsansvarlig eller å være databehandler. Spesielt den som er å anse som behandlingsansvarlig pålegges en rekke plikter i loven.

Den behandlingsansvarlige er den som alene eller sammen med andre har bestemmelsesrett over personopplysningene og den elektroniske behandlingen av disse. Dersom den behandlingsansvarlige er en juridisk person, vil den juridiske personen representert ved dens ledelse være behandlingsansvarlig. Ledelsen må sørge for at loven etterleves, og som ledd i dette foreta en intern arbeidsfordeling slik at det er klart hvilken stilling det ligger til å sørge for at loven etterleves i praksis.

Selv om den behandlingsansvarlige setter bort behandlingsoppdrag til andre (”outsourcing”), vil man fortsatt være behandlingsansvarlig. Den som utfører arbeid for den behandlingsansvarlige, vil være databehandler, jf lovens § 2 nr 5.

En og samme behandling kan i enkelte tilfeller ha flere behandlingsansvarlige. Et overordnet organ, f eks et departement, vil ofte ha en overordnet rolle i fastsettelse av formålene for personopplysningsbehandlingen, mens underordnete organer, f eks direktorater, vil detaljere formålene med behandlingen og velge praktiske hjelpemidler. I slike tilfeller vil begge organene kunne være ”behandlingsansvarlig” etter loven, og ha en selvstendig plikt til å oppfylle lovens krav. Ansvaret bør imidlertid plasseres, og i denne sammenheng vil det være naturlig å plassere behandlingsansvaret der man har den daglige og mest omfattende befatningen med personopplysningene, jf. ot.prp nr. 92 (1998-1999)kapittel 16 merknadene til § 2.

Lovens § 2 nr. 5 definerer begrepet ”databehandler” som den som behandler personopplysninger på vegne av den behandlingsansvarlige. Paragraf 15 setter krav til at behandlingsoppdraget skal være avtaleregulert. Videre er databehandlerens rådighet over opplysningene begrenset. I § 13 pålegges databehandleren et selvstendig ansvar for at informasjonssikkerheten er tilfredsstillende.

Kystverket vil være behandlingsansvarlig når det gjelder de personopplysninger som vi behandler og krever etter eget regelverk og databehandler når det gjelder de personopplysninger som vi behandler for andre etater via SafeSeaNet. Det er spesielt Tollvesenet og Politiet som krever personopplysninger. Disse opplysningene vil langt på vei være sammenfallende med de personopplysninger som kreves i ISPS-anløpsmeldingen.

7.1.4 Konsekvensen av at noe er en personopplysning

7.1.4.1 Krav til virksomheten

Det følger av personopplysningsloven at før en virksomhet kan behandle personopplysninger skal noen grunnleggende vilkår oppfylles.

Grunnvilkårene finner en i personopplysningsloven § 11. Bestemmelsen viser i første ledd bokstav a) til at personopplysninger bare kan behandles dersom dette er tillatt etter § 8 og § 9. Paragraf 9 omhandler sensitive personopplysninger, og omtales ikke videre. Det følger av § 8 at behandlingen enten skal ha grunnlag i samtykke fra den opplysningene gjelder, hjemmel i lov eller være nødvendig for visse nærmere angitte formål som er angitt i lovens § 8 bokstav a) til f).

Når det gjelder ISPS- anløpsmeldingen som Kystverket mottar, er denne hjemlet i forskrift 3. juli 2007 nr. 825 om sikring av havner og havneterminaler mot terrorhandlinger mv. Forskriften § 5 viser til at EØS- avtalen vedlegg XIII NR. 56bb forordning (EF) nr. 725/2004 av 31. mars 2004 gjelder som forskrift. Forordningen artikkel 6 viser til at det skal foretas en sikringskontroll i havnen. Artikkelen viser til SOLAS kapittel XI-2 regel 9.2, som igjen viser til ISPS-koden del B 4.39. Her kommer det frem at det skal kreves mannskapslister og passasjerlister fra skip som omfattes av ISPS regelverket og som skal til havn. Kystverkets adgang til å behandle disse personopplysningene har her hjemmel i lov.

Innsamling eller øvrig behandling av AIS-data er ikke særskilt lovregulert. Det følger av personopplysningslovens § 8 første ledd bokstav d) at personopplysninger kan behandles dersom det er nødvendig for å utføre en oppgave av allmenn interesse. Om vilkåret er å anse som oppfylt krever en konkret vurdering i hvert enkelt tilfelle. Dette overlater et visst skjønn til den enkelte behandlingsansvarlige.

Kystverkets innsamling og registrering av AIS- data skjer som en del av Kystverkets arbeid med å ivareta sjøsikkerheten. Slike data er blant annet et viktig hjelpemiddel for sjøtrafikksentralene. AIS- data kringkastes fritt fra fartøyet, og det er ikke mulig for Kystverket å ikke motta data fra fartøy som frivillig installerer AIS eller som er i den kategorien som kan medføre at opplysningen om fartøyets navn og posisjon kan anses som en personopplysning. For å ivareta Kystverkets oppgaver er det derfor nødvendig å samle inn også disse opplysningene. Vurderingen er derfor at vilkårene for behandling av AIS- data som kan være å anse som personopplysninger er oppfylt.

Det foreligger dermed hjemmel til å behandle de personopplysningene som nevnt over. Paragraf 11 gir flere grunnkrav for behandling av personopplysninger. Noen av disse setter grenser for hva informasjonen kan benyttes til og disse omtales under.

7.1.4.2 Bruk av personopplysninger

Det følger av personopplysningsloven § 11 første ledd bokstav c) at en behandlingsansvarlig ikke kan bruke personopplysninger til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker. For det første må det nye formålet ha selvstendig hjemmel i ett av behandlingsvilkårene i § 8. Her vil ikke det forhold at opplysningene allerede er samlet inn ha betydning for vurderingen av om vilkårene i § 8 er oppfylt. I tillegg oppstilles det som et særskilt vilkår at det nye formålet ikke må være uforenlig med det eller de formålene som opprinnelig lå til grunn for innsamlingen av personopplysningene. Kravet om forenlighet innebærer at det til tross for at det nye formålet er hjemlet i § 8, kan være

slik at de innsamlede opplysningene likevel ikke kan brukes for dette formålet. I så fall må den behandlingsansvarlige innhente samtykke eller samle opplysningene inn på nytt. Hvor mye som skal til før det nye behandlingsformålet er uforenlig med det opprinnelige formålet for innsamlingen av opplysningene, kan ikke reguleres uttømmende i loven. Det følger av forarbeidene at spørsmålet må vurderes konkret og individuelt. Sentrale momenter i vurderingen vil være om bruk av opplysningene innebærer ulemper for den registrerte, om bruken skiller seg sterkt fra den som lå til grunn for innsamlingen, eller om bruken stiller strengere krav til datakvalitet enn det opprinnelige innsamlingsformålet. Et eksempel på formål som ofte vil være uforenlig med innsamlingsformålet, er bruk av opplysningene til kontrollformål, særlig når kontrollen ikke er en naturlig del av den virksomheten den behandlingsansvarlige driver, eller når ubehaget for den registrerte ikke står i et rimelig forhold til fordelene kontrolløren oppnår.

I kravet om at formålet skal være uttrykkelig angitt ligger at den behandlingsansvarlige forut for behandlingen må fastsette et formål som er tilstrekkelig konkret og avgrenset til at det skaper åpenhet og klarhet om hva behandlingen skal tjene til. Dette krever et visst presisjonsnivå – generelle og vage beskrivelser som "administrative oppgaver" eller "kommersiell bruk" vil ikke være tilstrekkelig presise, jf. Ot.prp nr. 92 (1998-1999) kapittel 16 merknad til § 11. Formålsbeskrivelsene må være mer presise enn de formål som angis i § 8 og § 9. Jo større fare behandlingen kan medføre for personvernet, desto viktigere er det at formålet er presist definert slik at den registrerte kan gjøre sine rettigheter gjeldende.

Formålet med innsamlingen av opplysninger om mannskapslister og passasjerlister må sees i sammenheng med formålet for innføring av regler om å forebygge og hindre terrorhandlinger og andre forsettlige ulovlige handlinger som kan skade havner, havneterminaler eller fartøy som anløper disse. Formålet med disse opplysningene er dermed klart avgrenset og vil betydelig begrense en senere bruk av dataene.

AIS- data er et viktig verktøy for flere av Kystverkets tjenesteområder. Sjøtrafikksentralene som overvåker og regulerer trafikken benytter AIS- data for å utføre sine oppgaver. Historiske AIS- data gir også grunnlag for en bedre planlegging av beredskapstiltak og trafikk. Dataene fungerer også som et viktig verktøy for analyse av risikoen knyttet til skipstrafikken. Hovedformålet med innsamling av AIS- data er å bedre sikkerhet for skip og miljø. [6]

7.1.4.3 Utlevering av opplysninger

Personopplysningsloven har ingen særlige regler om adgangen til å utlevere personopplysninger til andre enn den registrerte selv. Problemstillingen må derfor løses med utgangspunkt i samme vurdering som over. Dersom utlevering av opplysninger er uforenlig med det opprinnelige innsamlingsformålet, vil utlevering ikke være tillatt uten samtykke fra den registrerte, jf § 11 bokstav c).

[6] Formålet med AIS omtales i IMO resolusjon A.917 (22) og EU direktiv 2002/59

Distribusjon av dokumenter som inneholder personopplysninger vil være behandling av personopplysninger, og reglene i personopplysningsloven vil dermed få anvendelse dersom distribusjonen skjer eller innsyn gis ved bruk av elektroniske hjelpemidler. Dersom personopplysningene offentliggjøres eller det gis innsyn i dem uten hjelp av elektroniske hjelpemidler, gjelder personopplysningsloven bare dersom personopplysningene inngår i et personregister, jf § 3 første ledd bokstav b).

Overføring til utlandet er imidlertid regulert i personopplysningsloven §§ 29 og 30. Personopplysninger kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført personverndirektivet, oppfyller kravet til forsvarlig behandling. Bestemmelsen innebærer at det i slike tilfeller ikke kreves noen konkret vurdering av vernenivået, men at nivået automatisk aksepteres som tilstrekkelig. Uansett kan overføring skje dersom det foreligger en plikt etter folkerettslig avtale eller som følge av medlemskap i internasjonal organisasjon, jf. unntaksbestemmelsen i personopplysningsloven § 30 første ledd bokstav b.

7.1.4.4 Krav om innsyn

Det følger av personopplysningsloven § 6 at personopplysningsloven ikke innskrenker andre lovbestemte innsynsrettigheter. Dette innebærer at reglene i personopplysningsloven ikke kommer til anvendelse i den utstrekning offentleglova eller annen lovgivning gir rett til innsyn i personopplysninger. I slike tilfeller skal det med andre ord gis innsyn uavhengig av vilkårene i personopplysningsloven kapittel II.

Dokumenter som er omfattet av hovedregelen i offentleglova § 2 første ledd, men som samtidig dekkes av en unntaksbestemmelse som ikke medfører taushetsplikt, kan likevel offentliggjøres etter en merinnsynsvurdering, jf. offentleglova § 2 tredje ledd. Det foreligger dermed ingen innsynsrett i slike tilfeller. Personopplysningsloven § 6 første ledd er dermed ikke aktuell i den utstrekning det utøves merinnsyn. Dette innebærer at vilkårene i personopplysningsloven § 11, jf. §§ 8 og 9, må være oppfylt ved offentliggjøring av et dokument som kan unntas fra offentlighet, når dokumentet inneholder personopplysninger. Lovavdelingen har, i brev 16. juli 2004 til Datatilsynet, uttalt at dersom det er adgang til å gi innsyn i et dokument etter en slik vurdering, vil vilkåret for behandling av personopplysninger i personopplysningsloven § 8 første ledd andre alternativ og § 9 første ledd bokstav b være oppfylt. Vilkårene i personopplysningsloven § 11 vil da trolig ikke være til hinder for at det blir gitt merinnsyn.

Personopplysninger som lovgiver har ansett som sensitive, jf. personopplysningsloven § 2 nr. 8, vil normalt være omfattet av taushetsplikt, jf. blant annet forvaltningsloven § 13. Disse vil det ikke være adgang til å utlevere, jf. også offentleglova § 13. Dokumenter som kan, men ikke skal, unntas offentlighet vil sjelden inneholde personopplysninger. I den grad slike dokumenter inneholder personopplysninger, vil imidlertid personvernhensyn være et relevant moment ved vurderingen av om det skal utvises merinnsyn.

Det påpekes også at ved en vurdering av merinnsyn, må forholdet til personverndirektivet vurderes, se Lovavdelingens uttalelse (2001/04600) angående forholdet mellom personopplysningsloven og offentleglova. Her påpekes det at det kan tenkes tilfeller hvor det ikke er samsvar mellom direktivets vurdering av hva som er sensitive opplysninger og taushetsplikten i norsk rett. I slike tilfeller vil direktivet artikkel 8 kunne være til hinder for utøvelsen av merinnsyn.

Personopplysningsloven supplerer andre lovbestemmelser om innsynsrett. For den som ber om innsyn kan det være noe tilfeldig hvilken lov han eller hun har kjennskap til og ber om innsyn i medhold av. For å sikre at den som ber om innsyn blir kjent med sine lovbestemte innsynsrettigheter, pålegges den behandlingsansvarlige i annet ledd å informere den som ber om innsyn om annen lovfestet innsynsrett som rekker lenger enn personopplysningsloven. For offentlige behandlingsansvarlige følger en slik plikt allerede av forvaltningsloven § 11.

7.1.5 Konklusjoner

Det påpekes først at personopplysningsloven ikke vil få betydning for hoveddelen av de maritime data som Kystverket samler inn. Disse dataene omhandler juridiske personer og omfattes ikke av personopplysningslovens virkeområde.

Kystverket behandler personopplysninger i forbindelse med håndteringen av maritime data. Deler av ISPS- anløpsmeldingen som leveres i SafeSeaNet, mannskapslister og passasjerlister, er personopplysninger. Arbeidsgruppen mener at AIS- data og meldinger om farlig og forurensende last som mottas fra fartøy mindre enn 300 BT eller 45 meter kan inneholde personopplysninger, og ikke bør videreformidles uten nærmere vurdering. I tillegg bør AIS- data fra alle fritidsfartøy behandles som personopplysninger.

Det innebærer at det er begrensninger i forhold til videreformidling av disse opplysningene. De kan ikke leveres videre dersom formålet med den nye bruken er uforenlig med det opprinnelige innsamlingsformålet. I slike tilfeller vil utlevering ikke være tillatt uten samtykke fra den registrerte.

Ved krav om innsyn vil ikke personopplysningsloven være til hinder for å gi innsyn dersom det er *innsynsrett* i dokumentet. Ved innsyn etter en vurdering av merinnsyn, må det sees hen til personverndirektivet og personvernhensynet må vurderes som et moment i forhold til vurdering av merinnsyn.

7.2 Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven)

Ekomloven oppstiller en hovedregel om taushetsplikt i § 2-9. Kort fortalt gjelder plikten innhold av elektronisk kommunikasjon og den gjelder for de som er definert som tilbydere og installatører etter loven.

7.2.1 Lovens virkeområde

Loven gjelder *"virksomhet knyttet til overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner"* jf. § 1-2. Den retter seg altså mot aktiviteter knyttet til installasjon av kommunikasjonssystemer og formidling av elektronisk kommunikasjon. Loven har definert nøkkelbegreper i § 1-5. Virkeområdet er svært vidt angitt, og maritime data som Kystverket fanger opp eller mottar på annen måte vil falle inn under loven.

7.2.2 Taushetsplikt etter ekomloven

Taushetspliktsbestemmelsen i § 2-9 fastslår at tilbydere og installatører har taushetsplikt om "innholdet av elektronisk kommunikasjon". Dette innebærer at den som må anses for tilbyder eller installatør etter loven ikke kan viderebringe informasjon fra andres kommunikasjon som vedkommende er blitt kjent med i rollen som tilbyder eller installatør.

I § 1-5 er det blant annet gitt definisjoner av "elektronisk kommunikasjon" (nr. 1), "elektronisk kommunikasjonsnett" (nr. 2), og "tilbyder" (nr. 16). Sett i sammenheng med disse definisjonene, pålegger § 2-9 taushetsplikt for den som tilbyr andre tilgang til et system for overføring av data ved hjelp av elektromagnetiske signaler og for den som kan anses som installatør av et slikt system.

All overføring av maritime data vil i praksis skje ved hjelp av elektromagnetiske signaler. Spørsmålet om ekomloven pålegger taushetsplikt for maritime data i Kystverkets besittelse vil dermed bero på om Kystverket må anses som "tilbyder" eller "installatør" etter loven. Bakgrunnen for å la loven gjelde for installatører er at den som får tilgang til informasjon i forbindelse med montering eller vedlikehold av kommunikasjonsnett også skal ha den samme plikten til å bevare taushet om informasjonen som den som driver nettet til daglig. For denne rapportens del er det tilstrekkelig å vurdere om Kystverket må anses som "tilbyder" ettersom det er i en slik funksjon Kystverket normalt vil kunne få tilgang til data og kjennskap til innholdet i disse.

7.2.2.1 AIS

AIS- data overføres åpent ved radiosignaler. Det er ingen begrensninger på hvem som kan installere en AIS- sender eller - mottaker. Kystverket har basestasjoner som mottar signalene, og har tilgang til AIS- data som er fanget opp via satellitt. Basestasjonene fanger opp AIS- data, som så overføres til Kystverkets server. Stasjonene er konfigurert for å motta signaler, men kan også settes opp til å sende visse AIS- dataelementer. Spørsmålet er om Kystverkets oppfanging og overføring av disse dataene er tilbydervirksomhet etter ekomloven. Forarbeidene gir ingen veiledning til problemstillingen.

I § 1-5 er en tilbyder definert som en som "tilbyr andre tilgang til" et elektronisk kommunikasjonsnett eller en elektronisk kommunikasjonstjeneste. I "tilbyr" ligger det normalt at man åpner opp for bruk av et nett eller en tjeneste, og i "tilgang" ligger det normalt at det er en viss styring med hvem som får benytte tjenesten. Ordlyden tilsier

at ansvarssubjektene etter § 2-9 skal begrenses til de som driver et kommunikasjonsnett eller en kommunikasjonstjeneste der det fysiske nettet, eller tjenesten i seg selv, er en forutsetning for at kommunikasjonen skal kunne finne sted, typisk et telefonnett, et bredbåndsanlegg eller et dataprogram som muliggjør kommunikasjon. AIS- nettverket vil eksistere uavhengig av Kystverkets basestasjoner, og basestasjonene tilfører ikke data til nettverket. Kystverket gir heller ikke tilgang til AIS- nettverket som sådan, men har satt opp et nettverk som kan motta signalene som for øvrig sendes åpent.

Kystverkets innhenting av AIS- data er hovedsakelig basert på et eget behov for dataene. Kystverket tilbyr imidlertid også andre tilgang til *informasjon* hentet ut fra det elektroniske kommunikasjonsnettet. Det er noe annet enn å gi tilgang til nettet, og en eventuell taushetsplikt må derfor løses etter annet regelverk. Etter arbeidsgruppens syn faller Kystverkets oppfanging og lagring av AIS- data dermed utenfor tilbyderdefinisjonen i ekomloven.

I alle tilfeller taler sterke reelle hensyn for at taushetsplikten etter § 2-9 må tolkes innskrenkende for kommunikasjon som er åpen og tilgjengelig for allmennheten slik som det er for AIS- data. Når man leser bestemmelsens første ledd første og andre punktum i sammenheng, gir også lovteksten et klart inntrykk av at taushetsplikten er ment rettet mot kommunikasjon som avsenderen og/eller mottakeren oppfatter som lukket.

7.2.2.2 LRIT- data

LRIT- data er krypterte data sendt fra skipet via satellitt til skipets flaggstat og til stater i nærheten av skipets posisjon. I Europa er det organisert et felles datasenter for mottak av LRIT-data. Dataene formidles til Kystverket gjennom en kontinuerlig datastrøm fra datasenteret. Kystverket tilbyr imidlertid ikke andre tilgang til kommunikasjonsnettet der disse dataene formidles, men til selve dataene. Ekomloven § 2-9 pålegger dermed ikke Kystverket taushetsplikt omkring disse dataene.

7.2.2.3 SafeSeaNet-data

SafeSeaNet-data er dataelementer som er samlet inn i via nettsiden SafeSeaNet Norway. I forbindelse med rapporten har Post- og teletilsynet kommentert tolkningen av tilbyderdefinisjonen i ekomloven. Tilsynet presiserer at den som tilbyr tilgang til en ren innholdstjeneste tilbudt over en underliggende elektronisk kommunikasjonstjeneste, som for eksempel internett, ikke vil anses som en tilbyder i ekomlovens forstand. SafeSeaNet blir vurdert som en slik type innholdstjeneste. SafeSeaNet-data er dermed ikke omfattet av taushetspliktsbestemmelsen i ekomloven § 2-9. Samferdselsdepartementet har i møte med Fiskeri- og kystdepartementet gitt sin tilslutning til Post- og teletilsynets uttalelse. Arbeidsgruppen legger denne uttalelsen til grunn.

7.2.3 Konklusjon

Kystverket har ikke taushetsplikt etter ekomloven § 2-9 for noen av de aktuelle maritime dataene.

7.3 Lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)

Formålet med sikkerhetsloven er å trygge rikets sikkerhet og vitale nasjonale sikkerhetsinteresser mot spionasje, sabotasje og terrorhandlinger ved forebyggende tiltak. Loven skal dessuten ivareta den enkeltes rettssikkerhet og trygge tilliten til og forenkle kontrollen med sikkerhetstjenesten. Tiltakene skal implementeres i stat, kommune og private virksomheter som loven gjelder for.

Sikkerhetsloven § 2 bestemmer at loven gjelder for forvaltningsorganer. Etter lovens § 11 andre ledd skal den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon sørge for at informasjonen merkes med aktuell sikkerhetsgrad. Etter § 12 plikter enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag eller verv for en virksomhet, å hindre at uvedkommende får kjennskap til informasjonen. Loven har videre bestemmelser for informasjon som klassifiseres som skjermingsverdig.

Det sentrale blir da om Kystverket er den som tilvirker maritim informasjon etter loven, og om maritim informasjon er skjermingsverdig. Nasjonal Sikkerhetsmyndighet har laget en veileding til hjelp for å avgjøre spørsmålet om skjermingsverdighet gjennom en verdivurdering.

Kystverket er å anse som forvaltningsorgan, og faller under virkeområdet. Kystverket tilvirker også maritim informasjon i den forstand at informasjonselementer fra skip samles inn og sammenstilles av Kystverket. Maritim informasjon er verdivurdert i tråd med Nasjonal Sikkerhetsmyndighets veiledning. Verdivurderingen følger som vedlegg 4 til rapporten. Den omfatter en vurdering av i hvilken grad en trusselaktør kan utnytte informasjonen, hvilken alvorlighet skaden kan ha for rikets sikkerhet eller vitale nasjonale sikkerhetsinteresser og tilgjengelighet av informasjon fra andre kilder. Konklusjonen er at de aktuelle maritime data ikke er skjermingsverdige etter sikkerhetsloven.

7.4 Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd (offentleglova)

Offentleglova har som formål å legge til rette for at offentlig virksomhet er åpen og gjennomsiktig, blant annet for å styrke rettssikkerheten for den enkelte, tilliten til det offentlige og publikums kontroll av den offentlige forvaltning.

Offentleglovas hovedregel er at forvaltningens saksdokumenter er offentlige så langt det ikke er gjort unntak i lov eller i medhold av lov. Det er altså unntak fra offentlighet som må ha særskilt hjemmel og begrunnes nærmere. Dersom det ikke kan påvises at et dokument faller utenfor lovens virkeområde eller går inn under et unntak fra offentlighet, må dokumentet på begjæring legges frem for den som spør etter det.

Offentleglova trådte i kraft 1. januar 2009. I forhold til tidligere lov utvider offentleglova på flere områder retten til innsyn ved at loven omfatter flere virksomheter, og dette innebærer en utvidelse av hva slags informasjon det kan kreves innsyn i. I tillegg har den som krever innsyn fått styrket sine rettigheter i forbindelse med saksbehandling av krav om innsyn. Det presiseres at innsynsretten også gjelder for utenlandske aktører på lik linje med norske.

7.4.1 Lovens virkeområde

For å sikre at allmennheten har muligheter til kontroll gjennom innsyn i offentlige virksomheter, har offentleglova et vidt virkeområde. Etter lovens (offl.) § 2 første ledd bokstav a), gjelder loven for staten, fylkeskommunene og kommunene. Etter første ledd bokstav b), omfattes andre rettssubjekter i saker der de treffer enkeltvedtak eller utferdiger forskrift. Bestemmelsens bokstav c) sier at loven gjelder for selvstendige rettssubjekt der stat, fylkeskommune eller kommune har en eierandel som gir mer enn halvparten av stemmene i "det øvste organet i rettssubjektet", mens bokstav d) sier at loven gjelder for selvstendige rettssubjekt der stat, fylkeskommune eller kommune *"har rett til å velje meir enn halvparten av medlemmene med røysterett i det øvste organet i rettssubjektet."*

Etter offl. § 2 første ledd bokstav a), er altså organ for staten omfattet av offentleglova sitt virkeområde. Et departement er et slikt organ for staten. Kystverket er en underliggende etat til Fiskeri- og kystdepartementet, og etatens virksomhet faller således inn under offentleglovas virkeområde.

7.4.2 Innsyn etter offentleglova

Ifølge offl. § 3 er som hovedregel alle saksdokumenter i offentlig virksomhet offentlige. Unntak fra dette foreligger kun hvis dette fremkommer av offentleglova selv, av andre lover eller av forskrifter gitt i medhold av lov. Dersom et dokument ikke er omfattet av et slikt lovforankret unntak, er dokumentet offentlig i samsvar med lovens hovedregel.

Offentleglova § 3 gir enhver rett til å kreve dokumentinnsyn, og den stiller ikke opp begrensninger på dette punktet. Dette innebærer at hvem som helst kan kreve dokumentinnsyn hos norske forvaltningsorganer, og det er uten betydning hvilket formål man har med sin henvendelse.

7.4.2.1 Nærmere om hva det kan kreves innsyn i

Forvaltningens "saksdokument, journalar og liknande register" er gjenstand for regulering etter offentleglova, jf. offl. § 3. Loven definerer dokument som *"ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lytting, framsyning, overføring eller liknande"*, jf. offl. § 4 første ledd. Begrepet "dokument" er

teknologinøytralt, og det spiller ingen rolle på hvilken måte dokumentet er lagret eller kommer til uttrykk.

Ved vurderingen av hva som er et dokument, er det sentrale vilkåret at det må være "ei logisk avgrensa informasjonsmengd". Det avgjørende vil i denne sammenheng være hvilken informasjon som innholdsmessig[7] hører sammen. Hva som skal regnes som et dokument i en database[8], må på samme måte som ellers avgjøres ut fra hva som utgjør en logisk avgrenset informasjonsmengde.

Maritime data består samlet sett av en informasjonsstrøm, der nye data genereres og lagres i Kystverkets databaser fortløpende. Informasjonsstrømmen består av enkeltmeldinger som avgis på bakgrunn av forskrifter om meldeplikter og bærekrav til utstyr for posisjonsrapportering. Posisjonsrapporter fra AIS og LRIT gis enkeltvis med visse intervaller. Den mest nærliggende fellesnevneren for innholdet i databasene er at dette er samme type data, altså AIS-data, LRIT- data eller SSN-data. Det at det er samme type data vil ikke være tilstrekkelig til at det er en innholdsmessig sammenheng mellom dataene. Det er derfor arbeidsgruppens vurdering at det samlede innholdet i databasene ikke er en logisk avgrenset informasjonsmengde. Ettersom meldingene og posisjonsrapportene er gitt enkeltvis, vurderer arbeidsgruppen det slik at hver rapport eller melding vil være en logisk avgrenset informasjonsmengde, altså ett dokument i lovens forstand.

I § 4 andre ledd er saksdokument for organet definert. Dette innebærer at dokumentet må befinne seg i organets besittelse, og at det etter sitt innhold må gjelde ansvarsområdet eller virksomheten til organet generelt.

Meldinger gitt i SafeSeaNet og de enkelte posisjonsrapporter fra AIS og LRIT vil dermed være å anse som saksdokumenter etter offentleglova.

7.4.2.2 Sammenstilling av opplysninger

Offentleglova pålegger offentlige virksomheter også å gi innsyn i opplysninger som er elektronisk lagret i databaser, jf. offl. § 9 som lyder som følger:

> **§ 9.** *Rett til å krevje innsyn i ei samanstilling frå databasar*
>
> Alle kan krevje innsyn i ei samanstilling av opplysningar som er elektronisk lagra i databasane til organet dersom samanstillinga kan gjerast med enkle framgangsmåtar.

[7] Ot.prp nr. 102 (2004/2005) side 120

[8] Med database menes en samling selvstendige verk, data eller annet materiale ordnet på en systematisk og metodisk måte som det er individuell adgang til ved elektroniske eller andre midler, jf. direktiv 96/9/EF (databasedirektivet) artikkel 1, pkt. 2.

Dette innebærer at dersom vilkårene i § 9 er oppfylt, har forvaltningen en plikt til å opprette en sammenstilling dersom dette må til for å etterkomme innsynskravet. Kystverket lagrer for eksempel opplysninger om fartøys bevegelser langs norskekysten, og kan sammenstille slike opplysninger. Dersom opplysningene kan sammensettes med enkle fremgangsmåter, vil dette være et nytt dokument i lovens forstand.

Hvorvidt en sammenstilling kan gjøres på en enkel måte, vil bero på en konkret vurdering i hvert enkelt tilfelle, blant annet basert på de tekniske muligheter og begrensinger som til enhver tid ligger i Kystverkets datasystemer. Per dags dato kan Kystverket for eksempel sammenstille opplysninger om et fartøys posisjoner som kartinformasjon med enkle virkemidler og uten omfattende ressursbruk.

Sammenstilling av omfattende informasjonsmengder kan være mulig, men et slikt arbeid vil være både tidkrevende og kostbart. Selv om de andre vilkårene i § 9 hadde vært oppfylte, ligger dette utenfor det som kan kreves etter denne bestemmelsen.[9]

7.4.2.3 Behandling av innsynskrav

Offentleglova § 30 regulerer hvordan det skal gis innsyn i dokumentet, og etter første ledd første punktum er det opp til organet selv å bestemme ut fra hensynet til forsvarlig saksbehandling hvordan dokumentet skal gjøres kjent. Hovedregelen er likevel at den som ber om innsyn har krav på papirkopi eller elektronisk kopi av dokumentet, jf. første ledd andre punktum. Elektronisk kopi omfatter både at dokumentet blir sendt på e-post, og at det blir kopiert til et annet medium som for eksempel en minnepinne.

Etter offl. § 28 andre ledd må innsynskrav gjelde en bestemt sak eller i rimelig utstrekning saker av en bestemt art. Dette innebærer at det må gis en tilstrekkelig presis beskrivelse av hva vedkommende ønsker innsyn i. Det kan altså ikke kreves innsyn i hele databaser, for eksempel SafeSeaNet Norway. Det legges derfor til grunn at loven ikke åpner for at det kan kreves generell tilgang eller passord til Kystverkets interne databaser.

7.4.2.4 Unntak fra innsyn

Som nevnt innledningsvis under punkt 3, kan et forvaltningsorgan bare nekte innsyn i et dokument dersom det er hjemmel for dette i lov eller i medhold av lov, jf. offl. § 3 første punktum.

Unntaksreglene innebærer ikke at dokumentene er underlagt taushetsplikt. Tvert imot har forvaltningen plikt til å vurdere merinnsyn, jf. offl. § 11, og kan bare bruke unntaksadgangen hvor det i det konkrete tilfellet foreligger et reelt og saklig behov for å unnta dokumentet fra offentlighet. Arbeidsgruppen finner imidlertid grunn til å presisere at det i medhold av offl. § 13 første ledd foreligger en plikt til å gjøre unntak for opplysninger som er omfattet av taushetsplikt. Det er en forutsetning at opplysningene er omfattet av taushetsbestemmelser i annen lov eller i medhold av lov.

[9] Se JDLOV-2010-11023

Arbeidsgruppen har funnet grunn til å reise spørsmålet om hvorvidt de internasjonale avtalene som er inngått om deling og distribusjon av maritime data, jf. rapportens kapittel seks, faller inn under lovens regler om unntak av hensyn til Norges utenrikspolitiske interesser, jf. offl. § 20. Ifølge offl. § 20 første ledd kan det gjøres unntak fra innsyn for opplysninger dersom det er nødvendig av hensyn til Norges utenrikspolitiske interesser, og ett av vilkårene i bokstav a) - c) er oppfylt. Med utenrikspolitiske interesser forstår vi Norges forhold til andre stater eller organisasjoner hvor medlemmene er stater. I kravet om at unntak må være "påkravd", ligger det at det må være en viss fare for skade på Norges utenrikspolitiske interesser dersom det blir gitt innsyn.

Enkelte av avtalene inneholder bestemmelser om konfidensialitet om dataene som utveksles. Uten å vurdere innholdet i selve avtalene, har arbeidsgruppen sett på hvorvidt en slik bestemmelse om konfidensialitet i avtalen kan gi grunnlag for å unnta dataene fra offentlighet, jf. offl. § 20. Gruppen vurderer at grunnvilkåret i § 20 om at det må være en viss fare for skade på Norges utenrikspolitiske interesser dersom det gis innsyn i de aktuelle maritime data, under enhver omstendighet ikke er oppfylt. Etter arbeidsgruppens vurdering, vil ikke denne unntaksbestemmelsen komme til anvendelse når det gjelder krav om innsyn i maritime data som omfattes av denne rapporten.

7.4.3 Konklusjon

På bakgrunn av overnevnte, vurderer arbeidsgruppen at de aktuelle maritime data faller innenfor offentleglovas virkeområde. Ved en innsynsbegjæring må det gjøres en konkret vurdering i forhold til de enkelte unntaksbestemmelsene i loven. Det kan ikke kreves generell tilgang eller passord til Kystverkets interne databaser.

7.5 Lov 10. februar 1967 nr. 10 om behandlingsmåten i forvaltningssaker (forvaltningsloven)

Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (fvl.) er den generelle prosesslov for all saksbehandling som foregår i forvaltningen. Forvaltningsloven gir blant annet regler for hvilke betingelser som må foreligge med hensyn til habilitet, taushetsplikt, utredning av saker, begrunnelse, klage m.v.

Formålet med forvaltningsloven er i første omgang å legge forholdene til rette for en betryggende saksbehandling i forvaltningen. Loven gir prosessuelle regler, mens materiell forvaltningsrett finnes i spesiallovgivningen og i ulovfestede regler om forvaltningens skjønns- og regelbruk.

Lovens målsetting er å legge opp til en betryggende saksbehandling som kan sikre materielt riktige resultater. Materielt riktige avgjørelser i forvaltningen er viktig å oppnå for at den enkeltes *rettssikkerhet* skal tilgodeses best mulig.

Forvaltningsloven gir i seg selv ingen avveining av rettssikkerhetskravene mot andre krav som for eksempel effektivitet. Den legger derimot mulighetene til rette for at både rettssikkerhetskrav og andre hensyn blir tilgodesett. Avveiningen mellom hensynene foretas av forvaltningen under saksbehandlingen[10].

7.5.1 Lovens virkeområde

Ifølge fvl. § 1 gjelder loven "*den virksomhet som drives av forvaltningsorganet når ikke annet er bestemt i eller i medhold av lov. Som forvaltningsorgan reknes i denne lov et hvert organ for stat eller kommune. Privat rettssubjekt regnes som forvaltningsorgan i saker hvor det treffer enkeltvedtak eller utferdiger forskrift*."

Fvl. § 1 innebærer at dersom et organ faller inn under definisjonen av hva som er et forvaltningsorgan, så gjelder loven for all virksomhet som drives av dette organet, også den virksomhet som for eksempel er av privatrettslig karakter.

Kystverket er Fiskeri- og kystdepartementets etat for kystforvaltning, sjøsikkerhet og beredskap mot akutt forurensning, og etatens behandling av maritime data vil være underlagt de generelle reglene i forvaltningsloven.

7.5.2 Forvaltningslovens regler om taushetsplikt

Fvl. § 13 flg. gir regler om taushetsplikt. Den sentrale bestemmelsen er § 13, som lyder som følger:

> **§ 13.** *(taushetsplikt).*
>
> Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:
>
> 1) noens personlige forhold, eller
>
> 2) tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.
>
> Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal reknes som personlige, om hvilke organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes personlige status for øvrig, samt om vilkårene for å gi slike opplysninger.
>
> Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han kan heller ikke utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre.

[10] Woxholth "Forvaltningsloven med kommentarer", 5. utgave 2011, s. 28-30

Paragraf 13 inneholder forvaltningslovens hovedregel om forvaltningsmessig taushetsplikt. Eckhoff/Smith definerer taushetsplikt som plikten *"til å sørge for at visse opplysninger ikke kommer ut, hverken ved å fortelle om dem eller ved å overlate dokumenter til andre"* (s 255)[11]. Et sentralt formål med regelen er opplysninger som en person normalt ønsker å holde for seg selv, ikke skal komme ut.

Taushetsplikten omfatter kun opplysninger som er fremkommet under utøvelse av arbeid eller tjeneste, og inneholder både et forbud mot å bringe videre bestemte opplysninger og en aktiv plikt til å hindre at andre får tilgang til dokumenter og notater.

7.5.2.1 Nærmere om fvl. § 13 første ledd nr. 1

I § 13 første ledd nr. 1 er det gitt regler om taushetsplikt på grunn av noens personlige forhold. Bestemmelsen tar sikte på å hindre offentliggjøring av opplysninger som man vanligvis ønsker å holde for seg selv. Alle slags forhold av denne art, herunder økonomiske, omfattes av uttrykket, for eksempel opplysninger om fysiske eller psykiske problemer eller sykdom. I bestemmelsens andre ledd er det gjort eksplisitt unntak for visse opplysninger. Forhold som er alminnelig kjent, anses derimot ikke som "personlige".[12]

Begrepet "noens personlige forhold" i fvl § 13 har et annet innhold enn begrepet "personopplysning" i personopplysningsloven § 2 første ledd nr. 1. Terskelen for at noe skal anses som "noens personlige forhold" er markert høyere enn terskelen for "personopplysning".

Posisjonsrapporter som Kystverket mottar inneholder opplysninger om hvor et bestemt fartøy befinner seg. Arbeidsgruppen vurderer dette til klart å falle utenfor bestemmelsens ordlyd, i tillegg til at opplysningene i stor utstrekning er allment kjent, se drøftelsen under kap. 5.1.

Meldinger som Kystverket har hjemmel til å innhente inneholder også informasjon om hvem som er om bord i visse fartøy. I § 13 andre ledd er det gjort visse avgrensninger av hvilke opplysninger som ikke skal regnes som "personlige" i forvaltningslovens forstand. Dette omfatter fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted. Opplysninger om hvem som er om bord i et skip ligger tett opp til disse kategoriene, og arbeidsgruppen mener derfor at disse opplysningene klart faller utenfor bestemmelsen.

På bakgrunn av informasjon om et skips posisjon og passasjerliste, kan man utlede hvor de omtalte personene befant seg på det aktuelle tidspunktet. Det samme gjelder informasjon om posisjon på mindre fartøy med personlige eiere (små fiskefartøy og

---

[11] Woxholth (2011) *Forvaltningsloven med kommentarer*, 5. utgave, Oslo: Gyldendal, s. 262

[12] Jf. fvl. § 13 a nr. 3 og Echoff, Torstein og Eivind Smith (2003) *Forvaltningsrett*, 7. utg. Oslo: Universitetsforlaget, s. 209

fritidsfartøy). Spørsmålet blir da om denne informasjonen skal anses som "noens personlige forhold". Arbeidsgruppen er av den oppfatning at ordlyden i § 13 første ledd, sett i sammenheng med eksemplene i andre ledd, angir en terskel for vilkåret som ligger høyere enn informasjon om hvor passasjerer på skip befinner seg. I helt spesielle situasjoner, for eksempel der personer er på flukt, kan informasjon om hvor personer oppholder seg være å regne som opplysninger om personlige forhold. Etter arbeidsgruppens vurdering, er dette snakk om rent hypotetiske situasjoner. Det er derfor lagt til grunn at bestemmelsen ikke kommer til anvendelse på de aktuelle maritime data.

7.5.2.2 Nærmere om fvl. § 13 første ledd nr. 2

Regelen i fvl. § 13 første ledd nr. 2 retter seg mot forretningsmessige forhold, dvs. informasjon som det kan være skadelig for en virksomhet at konkurrentene får rede på. Formålet med regelen er dels å hindre spredning av opplysninger som kan føre til økonomisk tap for et foretak, enten direkte eller ved at konkurrenter får tilgang til opplysningene. Dels er formålet å opprettholde et tillitsforhold mellom det offentlige og foretaket.

Spørsmålet blir etter dette om maritime data er av en slik karakter at de kan sies å inneholde næringsopplysninger som omfattes av § 13 første ledd punkt 2.

AIS- data identifiserer skipet, skipets posisjon, kurs og fart i sann tid. Med sann tid forstår vi at informasjonen blir oppdatert i samme hastighet som systemet mottar data. Det er også krav til at fartøyet skal legge inn informasjon, blant annet om skipets destinasjon, skipets type, dimensjoner og til dels last. AIS- data gir oversikt over hvor et fartøy befinner seg. Det er dermed mulig å utlede seilingsmønster for konkrete fartøy, for eksempel hvor og hvordan fiskefartøy fisker. Man kan også observere mønster for fraktefartøy som opererer i spotmarkedet. Arbeidsgruppen anser dermed AIS- data å være opplysninger om drifts- eller forretningsforhold i forvaltningslovens forstand.

På samme måte som for AIS- data gir LRIT- data oversikt over fartøys posisjon[13]. Som nevnt over, er arbeidsgruppen av den oppfatning at disse opplysningene faller inn under vilkåret om drifts- eller forretningsforhold. SSN- data inneholder opplysninger om anløp til havner, opplysninger om last og ISPS- informasjon. Disse opplysningene vil også gjelde fartøyenes drifts- eller forretningsforhold.

Videre må det være av "konkurransemessig betydning" å hemmeligholde opplysningene for at de skal omfattes av bestemmelsen. Vilkåret må forstås slik at den konkurransemessige betydningen må være konkret og av et visst omfang. Vi viser i denne sammenhengen til sivilombudsmannens årsmelding, 1993 s. 174:

"Det fremgår av forarbeidene til bestemmelsen, jf. Ot.prp.nr.3 (1976-77) 16 at det normalt ikke er tilstrekkelig for taushetsplikt at en offentliggjøring kan virke uheldig overfor vedkommende bedrift, så lenge opplysningen "ikke har karakter av

[13] Fiskefartøy har ikke bærekrav til LRIT

produksjonshemmeligheter o.l. som konkurrenter kan utnytte for egen drift". Tilsvarende gjelder for opplysninger som gjelder avtaler med forretningsforbindelser. Selv om disse uttalelsene knytter seg til den ordlyden bestemmelsen hadde før lovendringen i 1982, er det antatt at dette også vil gi en viss veiledning slik bestemmelsen lyder i dag, jf. Woxholth: Forvaltningsloven med kommentarer 122 og Frihagen: Forvaltningsloven I 279. Det er i denne sammenheng grunn til å peke på at formålet med reglene om taushetsplikt ikke har vært å beskytte næringsvirksomhet mot enhver form for konkurranse eller mot offentliggjøring av enhver ubehagelig opplysning for vedkommende bedrift. Mindre sensitive næringsopplysninger vil derfor ikke være underlagt taushetsplikt og vil kunne offentliggjøres i medhold av offentlighetsloven."

For at det skal være av "konkurransemessig betydning" å hemmeligholde informasjonen, må det være fare for et økonomisk tap eller en redusert gevinst av et visst omfang for fartøyene dersom opplysningene blir kjent[14].

Informasjon som kan fremskaffes fra åpne kilder vil ikke være underlagt taushetsplikt. Dette fremkommer av fvl. § 13a nr 3 som sier at taushetsplikt ikke er til hinder for *"at opplysningene brukes når ingen berettiget interesse tilsier at de holdes hemmelig, f.eks. når de er alminnelig kjent eller alminnelig tilgjengelig andre steder."*.

AIS- data kringkastes åpent, og fartøy som befinner seg innenfor dekningsområdet til senderen (40 nm) mottar disse automatisk. I tillegg kan enhver få tilgang til informasjonen både på åpne nettsider og via betalingstjenester[15]. Sanntids AIS- data er dermed ikke taushetspliktig etter § 13 første ledd nr. 2, jf. § 13a nr. 3.

Historiske data som er sammenstilt over lengre tid, vil kunne gi mer presis og omfattende informasjon enn hva som kan fremskaffes fra åpne kilder. Dette vil for eksempel innebære sammenhengende informasjon om fartøys seilingsmønster over tid. Med denne bakgrunnen, kan arbeidsgruppen ikke utelukke at historiske AIS- data i enkelte tilfeller vil kunne gi en konkurrerende virksomhet informasjon som medfører fare for økonomisk tap, eller redusert gevinst for fartøyet som sender signalene. Dette vil for eksempel kunne være informasjon om hvor fiskefartøy fisker eller hvor fraktefartøy i spotmarkedet trafikkerer.

Som nevnt ovenfor, kringkastes imidlertid AIS- data åpent, og fanges opp av alle nærliggende fartøy med AIS- mottaker. De tilgjengeliggjøres også av private aktører, både i form av øyeblikksbilder i sann tid og i form av tilgang til datastrøm. Den som ønsker informasjon om posisjonene til enkeltfartøyer kan dermed på en enkel måte skaffe seg kjennskap til dette. Arbeidsgruppen kan på denne bakgrunn ikke se at offentliggjøring av de AIS- data Kystverket besitter vil kunne medføre fare for et økonomisk tap av et slikt omfang at vilkåret vil kunne være oppfylt.

[14] Uttalelse fra Lovavdelingen, saksnummer 201004739 EO KG/OKL
[15] For eksempel www.marinetraffic.com, www.exactearth.com

LRIT- data er ikke like tilgjengelige som AIS- data, fordi de sendes over lukket samband. Og siden LRIT er basert på kommunikasjon via satellitt, vil LRIT- data være tilgjengelig fra skip i havområder utenfor dekningsområdet til AIS- basestasjonene langs kysten.

For seilaser i områder som ikke dekkes av private operatører av landbaserte AIS-mottakere, vil det derfor kunne stilles spørsmål ved hvorvidt LRIT- informasjon vil måtte anses som like tilgjengelig som AIS-data.

Informasjonen LRIT- systemet sender (fartøyets posisjon og identitet) inngår også i AIS-dataene. AIS- data kringkastes alltid åpent fra skip slik at informasjonen som utgjør LRIT- data vil være åpent tilgjengelig lokalt rundt skipet i alle områder. Informasjon som inngår i LRIT- data vil altså være noe mindre tilgjengelig i områder utenfor dekning fra operatører av landbaserte AIS- mottakere. LRIT- informasjon stammer ikke fra fiskefartøy, men bare fra lastefartøy på og over 300 BT og passasjerfartøy. Dette gjør at potensialet for at LRIT- dataene inneholder konkurransesensitiv informasjon er mindre enn om fiskefartøy hadde vært utstyrt med LRIT. Arbeidsgruppen går også ut fra at informasjon fra skip i havområder vil ha en lavere konkurransemessig verdi da skipet vil være lenger fra potensielle destinasjoner. Arbeidsgruppen kan derfor ikke se at det vil være av konkurransemessig betydning, etter fvl § § 13, å hemmeligholde LRIT- utstyrte fartøys posisjoner. Arbeidsgruppen er dermed av den oppfatning at heller ikke LRIT- data vil være omfattet av taushetsplikten etter § 13.

SSN- data inneholder opplysninger om farlig eller forurensende last, avgangs- og anløpshavner, informasjon om skipet samt ISPS- informasjon. Arbeidsgruppen kan ikke se at disse opplysningene vil kunne være av konkurransemessig betydning for fartøyene å hemmeligholde. De er dermed ikke underlagt taushetsplikt etter § 13.

7.5.3 Konklusjon – forvaltningsloven § 13

Arbeidsgruppen konkluderer med at verken sanntids eller historiske AIS- data, LRIT-data eller SSN- data er omfattet av taushetsplikt etter forvaltningsloven § 13.

Kapittel 8. Vurdering av internasjonalt regelverk

I mandatet for arbeidsgruppen ligger det også å vurdere relevante internasjonale regelverk. Internasjonalt regelverk kan deles opp i regelverk som er ment å være bindende (traktater og EU- regelverk), og regelverk som har mer karakter av anbefalinger eller retningslinjer. De internasjonale reguleringene som er relevante for deling av maritime data er ikke av en slik karakter at de automatisk er gjeldende i Norge. Hvorvidt reguleringene påvirker deling av maritime data vil dermed avhenge av i hvilken grad de er implementert i norsk rett.

Generelt er det en presumsjon for at norsk rett samsvarer med de internasjonale forpliktelsene Norge har påtatt seg. I de tilfeller der relevante spørsmål for deling av

maritime data er regulert i en traktat, vil derfor traktaten ha sentral betydning i arbeidet med å utlede den norske rettsregelen. Ved en eventuell motstrid mellom en traktat og norsk lov eller forskrift, vil imidlertid de norske regelverkene være avgjørende. På den andre siden vil norske myndigheter etter traktattekstene normalt være forpliktet til å implementere traktatene i norsk rett. En situasjon der man konstaterer motstrid vil dermed normalt føre til at ansvarlig myndighet i Norge må endre norsk rett.

Arbeidsgruppen har identifisert to hovedgrupper av internasjonalt regelverk som er relevante i denne sammenhengen. Den første gruppen er regelverk som er gitt av FNs sjøsikkerhetsorganisasjon (International Maritime Organization - IMO). Den andre gruppen er regelverk gitt av EU. IMO- regelverk som pålegger statene forpliktelser, fører ofte til at det blir gitt bindende EU- regelverk som regulerer det samme. Dette gjøres for å sikre en ensartet og helhetlig innføring av regelverket innenfor unionens område. Gjennom EØS- avtalen vil Norge normalt være bundet til å implementere EU-regelverk.

8.1 IMO regelverk

Den internasjonale konvensjonen om sikkerhet for menneskeliv til sjøs (SOLAS) inneholder minimumskrav for konstruksjon, utstyr og drift av skip for dermed å bidra til å øke sjøsikkerheten. SOLAS kapittel V regel 19 (underpunkt 2.4) omhandler bærekrav til AIS på særskilte skip. Bestemmelsen sier ingenting om sensitivitet eller deling av data.

SOLAS kapittel V regel 19-1 omhandler bærekrav, innføringsplan og myndighetskrav for LRIT- utstyr. Videre følger det av kapittelets underpunkt 10 at:

"Contracting Governments shall, at all times:

1. *recognize the importance of LRIT- information,*
2. *recognize and respect the commercial confidentiality and sensitivity of any LRIT-information they may receive,*
3. *protect the information they may receive from unauthorized access or disclosure, and*
4. *use the information they may receive in a manner consistent with international law".*

SOLAS er gjennom lov 16. februar 2007 nr. 9 om skipsikkerhet med underliggende forskrifter gjort til norsk rett. Skipssikkerhetslovens formål er å trygge liv og helse, miljø og materielle verdier. Begrensninger i forhold til behandling og deling av maritime data faller ikke naturlig innunder dette formålet. Etter arbeidsgruppens vurdering vil forvaltningslovens regler om taushetsplikt, som omtalt i rapportens punkt 7.5, ivareta Norges forpliktelser etter SOLAS kapittel V regel 19-1 underpunkt 10. Dette underbygges også av uttalelser under utviklingen av LRIT i IMO[16].

[16] COMSAR 8/WP.5/rev. 1 punkt 41

8.2 EU/EØS regelverk

EU - direktiv 2002/59 (endret ved direktiv 2009/17) utvider grensene for bærekrav i forhold til SOLAS regel 19 underpunkt 2.4 når det gjelder AIS. Direktivet setter også bærekrav til LRIT- utstyr på lik linje med SOLAS kapittel V regel 19-1. Videre etablerer direktivet SafeSeaNet som system for å avgi meldinger fra skip, og utveksle meldinger mellom land. Et krav om utveksling av maritime data er også nedfelt i EU-direktiv 2010/65. Dette direktivet skal være gjennomført fullt ut innen 1. juni 2015.

I forhold til håndtering av maritime data (AIS, LRIT, melding om farlig eller forurensende last og anløpsmeldinger) inneholder direktiv 2002/59 artikkel 24 første avsnitt en bestemmelse om konfidensialitet:

"Member States shall, in accordance with Community or national legislation, take the necessary measures to ensure the confidentiality of information sent to them pursuant to this Directive, and shall only use such information in compliance with this Directive."

Etter arbeidsgruppens vurdering vil forvaltningslovens regler om taushetsplikt, som omtalt i rapportens punkt 7.5, ivareta Norges forpliktelser etter direktivets artikkel 24.

Direktiv 2002/59 pålegger kommisjonen å nedsette en styringsgruppe for å utarbeide retningslinjer for SafeSeaNet, herunder detaljerer kravene for tilgang til SafeSeaNet, se direktivets Annex 3 punkt 2.2. Slike retningslinjer er under utarbeidelse, og arbeidsgruppen anbefaler at Kystverket følger dette arbeidet og identifiserer eventuelle konflikter som kan oppstå i forhold til norsk regelverk.

Når det gjelder ISPS- anløpsmelding, følger det av artikkel 12 i EU-forordning 725/2004 at medlemsstatene skal beskytte og hindre uautorisert tilgang til taushetspliktige opplysninger, samt treffe tilstrekkelige tiltak i nasjonal lovgivning for å hindre dette. Etter arbeidsgruppens vurdering vil forvaltningslovens regler om taushetsplikt, samt offentleglova sine unntaksbestemmelser, sikre beskyttelse av denne type opplysninger.

Kapittel 9. Økonomiske og administrative konsekvenser

Hovedfokus for arbeidsgruppen har vært å trekke opp de juridiske rammene knyttet til Kystverkets oppgaver med å samle inn og tilrettelegge for bruk av data fra maritime overvåkings- og meldingssystemer.

Arbeidsgruppen anbefaler at Kystverket, på bakgrunn av den foreliggende rapporten, gjennomgår de avtaler som er inngått om deling av maritime data, både på nasjonalt nivå og med andre stater og internasjonale organisasjoner, jf. rapportens kapittel seks. Det vil også være aktuelt å utvikle nye retningslinjer for deling av slike data med utgangspunkt i denne rapportens konklusjoner. Avtalegjennomgang og utvikling av

retningslinjer vil påføre etaten en administrativ byrde, men det anslås at denne oppfølgingen er av begrenset omfang både tids- og ressursmessig og kan foretas innenfor gjeldende rammer. Utover dette antar arbeidsgruppen at rapportens konklusjoner ikke vil medføre økonomiske eller administrative konsekvenser, verken for det offentlige eller for private.

Kapittel 10. Konklusjoner

Arbeidsgruppens gjennomgang viser at de aktuelle regelverkene setter enkelte juridiske begrensninger for distribusjon og tilgjengeliggjøring av AIS-, LRIT- og SSN-data. Distribusjon av data innebærer i denne sammenheng å gi tilgang til databaser og presentasjonsverktøy. Tilgjengeliggjøring av data forstås i denne sammenheng som å gi innsyn i data etter en innsynsbegjæring etter offentleglova.

AIS-databasen og SafeSeaNet-databasen er vernet etter åndsverkloven § 43 og databasedirektivet. Dette innebærer at Kystverket har enerett til å gi tilgang til disse databasene.

AIS

Hovedregel

- Det er ikke juridiske begrensinger for distribusjon av data, men heller ikke plikt til å distribuere data til allmennheten.
- Det må gis innsyn i data etter innsynsbegjæring, i tråd med offentleglovas bestemmelser.

Unntak

- Mannskapslister og passasjerlister er personopplysninger, og det er begrensninger knyttet til distribusjon, jf. personopplysningsloven.
- Data fra fritidsfartøy kan inneholde personopplysninger, og det er begrensninger knyttet til distribusjon.
- Data som gjelder fartøy under 300 bruttotonn og 45 meter, kan inneholde personopplysninger, og det er begrensninger knyttet til distribusjon, jf. personopplysningsloven.
- Personopplysninger som nevnt i punktet over kan kun distribueres til stater som sikrer en forsvarlig behandling av opplysningene, jf. personopplysningsloven.

LRIT

Hovedregel

- Det er ikke juridiske begrensinger for distribusjon av data, men heller ikke plikt til å distribuere data til allmennheten.

- Det må gis innsyn i data etter innsynsbegjæring, i tråd med offentleglovas bestemmelser.

Unntak

- Arbeidsgruppen har ikke identifisert unntak.

Safe Sea Net (SSN)

Hovedregel

- Det er ikke juridiske begrensninger for distribusjon av data som Kystverket selv har hjemmel til å kreve inn, men heller ikke plikt til å distribuere data til allmennheten.
- Det må gis innsyn i data etter innsynsbegjæring, i tråd med offentleglovas bestemmelser.

Unntak

- Mannskapslister og passasjerlister som mottas som en del av ISPS-anløpsmeldingen er personopplysninger, og det er begrensninger knyttet til distribusjon, jf. personopplysningsloven.
- Melding om farlig eller forurensende last fra fartøy under 300 BT eller 45 meter, kan inneholde personopplysninger, og det er begrensninger knyttet til distribusjon, jf. personopplysningsloven.
- Personopplysninger som nevnt i punktet over kan kun distribueres til stater som sikrer en forsvarlig behandling av opplysningene, jf. personopplysningsloven.

Vedlegg

Vedlegg 1:
Rapport utredning av eierskap til maritime data - Bing Hodneland

Vedlegg 2:
Oversikt over internasjonale avtaler om deling av data fra maritime overvåkings- og meldingssystemer

Vedlegg 3:
Oversikt over meldingsinnhold i AIS-meldinger

Vedlegg 4:
Verdivurdering av maritime data

Vedlegg 5:
Fullstendig liste over meldingsinnholdet i ISPS-anløpsmeldinger