RAPPORT SIITS

Arbeidspakke 5

Utfordringer med datadeling, ansvar, personvern og hendelser i fremtidens IITS

SIITS

proactima

Arbeidspakke/tema:	**Kontaktperson:**
Arbeidspakke 5	Malena Kyvik Martens

Bakgrunn for rapport:

Denne rapporten er utarbeidet i forbindelse med arbeidspakke 5 i SIITS-prosjektet. Arbeidspakke 5 dekker temaer som eierskap til og ansvar for data, og nye forsikringsløsninger i fremtidens intelligente integrerte transportsystemer. Denne rapporten er utarbeidet i samarbeid med partnere, underleverandører og andre samarbeidspartnere til SIITS, gjennom to forskjellige arbeidsmøter hvor tematikken i rapporten ble drøftet.

I denne rapporten har vi undersøkt noen utfordringer som oppstår med hensyn til datadeling, ansvar og personvern ved hendelser i fremtidens IITS. Dette er en overordnet problemstilling som danner grunnlag for en rekke underproblemstillinger. Blant annet undersøker rapporten hvordan fremtidens intelligente integrerte transportsystemer kan se ut med hensyn til deling av data, og dermed hvilke nye ansvarsstrukturer som blir etablert. Deretter belyses utfordringer med hensyn til innsamling av data, deling av data og konsekvenser dersom datadeling av ulike årsaker ikke er mulig.

Proactima vil takke alle som har bidratt til rapporten, og særskilt takk til Norsk Romsenter og Kartverket som har deltatt i workshop og gitt skriftlige innspill til rapporten.

Nøkkelord	Ansvar, datadeling, IITS, GNSS, system, risiko og sårbarhet, forsikring, risikostyring
Rapportnr.	1073996-RE-12
Forfatter(e)	Malena Kyvik Martens
Konfidensialitet	Åpen
Revisjonsnr.	01
Revidert dato	18.12.2023
Antall sider	20

Rev.nr.	Dato	Årsak til revisjon
00	07.09.2023	Utkast
01	18.12.2023	Endelig rapport

Utarbeidet av	Verifisert av	For SIITS
Malena Kyvik Martens	Hermann Steen Wiencke	Anne-Kari Valdal

Innhold

1 Sammendrag

Utviklingen innenfor intelligente integrerte transportsystemer (IITS) skjer raskt, og flere nasjonale myndigheter ser på integrering og automatisering av transportsektoren som en nøkkel til å nå FNs bærekraftsmål. Som med all utvikling, oppstår det ulike utfordringer som må håndteres for å optimalisere resultatet av teknologiutviklingen for samfunnet som helhet, for private aktører og for den enkelte forbruker. I arbeidspakke 5 i SIITS-prosjektet er hensikten å belyse utfordringer ved ansvar og eierskap til data i fremtidens IITS, og å identifisere nye ansvarsstrukturer og utvikle markedsriktige og bærekraftige forsikringsprodukter.

I denne rapporten har vi undersøkt noen utfordringer som oppstår med hensyn til datadeling, ansvar og personvern ved hendelser i fremtidens IITS. Dette er en overordnet problemstilling som danner grunnlag for en rekke underproblemstillinger. Blant annet undersøker rapporten hvordan fremtidens intelligente integrerte transportsystemer kan se ut med hensyn til deling av data, og dermed hvilke nye ansvarsstrukturer som da blir etablert. Deretter belyses utfordringer med hensyn til innsamling av data, deling av data og konsekvenser dersom datadeling av ulike årsaker ikke er mulig. I denne rapporten er sistnevnte illustrert ved GNSS (Global Navigation Satellite Systems).

I arbeidet med rapporten har det fremkommet en rekke utfordringer knyttet til ansvar og eierskap ved dataproduksjon- og deling, samt når sentral infrastruktur for ITS ikke fungerer. Det skaper for eksempel flere utfordringer at det er mange aktører som både utvikler teknologi, deler data og er avhengig av datadeling, samtidig som det foreløpig ikke er noen helhetlig styring av teknologiutvikling eller hvilke regulatoriske krav som stilles. Videre er det per i dag problematisk å dele data over landegrenser, noe som blant annet kan illustreres med kartdata. Til slutt ser vi flere juridiske utfordringer med hensyn til ansvar og eierskap til data, som ikke enkelt lar seg løse i en verden stadig preget av enorme mengder data og lange, digitale verdikjeder.

Konsekvenser dersom datadeling ikke er mulig, kan illustreres ved avhengigheten til GNSS (satellittdata). Satellitter utgjør en sentral grunninfrastruktur for datadeling i samfunnet, og ikke minst i utviklingen av IITS. Faller GNSS-signaler ut, vil det få enorme konsekvenser for både trafikksystemer og andre kritiske samfunnsfunksjoner som samfunnet er avhengig av. En sentral utfordring her er at ansvar og beslutningsmyndighet knyttet til satellittsystemene ligger hos andre aktører enn norske myndigheter.

Hva kan så gjøres med utfordringene som er identifisert her? Noen forslag tiltak og løsninger skisseres i rapporten under. Et eksempel er å styrke samarbeidet mellom offentlig og privat sektor, mellom private aktører og ikke minst mellom nasjoner. I dette ligger det både å sørge for at datadeling er mulig og ønsket, at det er incentivordninger fra myndighetssiden som støtter opp om- og tilrettelegger for bruk og deling samtidig som det etableres gode avtaler, men også at alle aktører jobber mot å tilpasse slik at det er mulig å motta og dele data. Det er også styrke kunnskap og bevissthet rundt avhengigheter, og hvilke avhengigheter som oppstår når samfunnet i økende grad blir datadrevet.

For å sikre god deling og ikke minst klare ansvarsstrukturer er det nødvendig å ha gode avtaler mellom aktørene som nettopp avklarer eierskap til data og ansvar for dataene. Ved økt bruk av stordata, kunstig intelligens og stordataanalyser, kan det være behov for strukturer for datadelings- og samarbeidsavtaler. Tillit mellom aktører og forbrukere er også en vesentlig faktor, som ikke kan tas for gitt.

2 Introduksjon

2.1 Formål med arbeidet

Arbeidspakke 5 i SIITS-prosjektet har blant annet som formål å belyse utfordringer ved ansvar og eierskap til data i framtidens IITS. Mer konkret skal arbeidspakken undersøke følgende utfordringer:

1) Hvilke nye utfordringer ser de ulike aktørene relatert til eierskap av data, personvern, ansvar og grensesnitt i fremtidens IITS?
2) Hvordan endres ansvarsstrukturer i fremtidens IITS, og hvordan påvirker det hvem som blir forsikringstakere og objekteiere?
3) Hvilke nye faktorer påvirker risikomodell og prising av forsikringsprodukter?
4) Hvordan må en ny risikomodell for prising av forsikringer være?

Denne rapporten har som formål å blant annet belyse spørsmål 1 og 2. I tillegg belyser rapporten hvordan ansvarsstrukturer kan endres i fremtidens IITS ut ifra ulike typer systemforståelser og når nye avhengigheter oppstår.

3 Metode

10. november 2022 og 9. januar 2023 ble det gjennomført to workshoper om datadeling og eierskap i SIITS-prosjektet. Her deltok Statens vegvesen, ITS Norway, Disruptive Engineering, Advokat Arve Føyen, Proactima, Tryg, Kartverket og Norsk Romsenter. Rapporten er en oppsummering av diskusjonene fra disse to dagene, supplert med betraktninger, innspill og undersøkelser gjort i etterkant.

I workshopene ble det fokusert på tre ulike temaer:

1) Systemdiskusjon: Proactima hadde på forhånd etablert fire mulige systembeskrivelser av et IITS-system basert på produksjon og deling av data. Systembeskrivelsene var sett ut ifra ulike perspektiver, og skulle gi deltakerne en felles forståelse og utgangspunkt for diskusjon rundt de ulike systembeskrivelsene, og fordeler og utfordringer med disse.
2) Hvordan samler de ulike aktørene inn data? Og hvilke utfordringer oppstår vedrørende ansvar og eierskap? Alle deltakerne hadde forberedt egne presentasjoner om innsamling av data, ansvar og eierskap.
3) Hvilke konsekvenser kan bortfall av data gi? Diskusjonen var rettet både mot konsekvenser ved bortfall av data og påfølgende bortfall av kritisk infrastruktur, samt ansvarsfordelingen ved slike hendelser.

I forkant av workshopen fikk hver deltaker tilsendt en rekke spørsmål som veiledning for utarbeidelse av presentasjoner, og som grunnlag for diskusjonene i etterkant av hver sesjon under workshopen. Disse varierte noe fra virksomhet til virksomhet, men var for eksempel knyttet til:

- Hvordan samler dere inn data, og hvilke typer data er dette?
- Hvor lagres data og hva blir de brukt til?
- Hvem har ansvaret for data som blir produsert?
- Hvilke utfordringer ser dere med hensyn til deling av data?
- Hvilke nye forretningsmodeller oppstår, og hvilke nye muligheter og utfordringer gir det med hensyn til dataproduksjon- og deling?
- Hvilke juridiske utfordringer oppstår ved deling av data mellom aktører?

I workshop 9. januar 2023 varfokuset spesielt rettet mot hvilke utfordringer forsikringsbransjen ser med hensyn til ansvarsstrukturer og eierskap til data.

4 Systembeskrivelse

Det er ikke enkelt å beskrive fremtidens integrerte intelligente transportsystemer (IITS) på en god måte. Dette er både fordi det er usikkert hvordan systemene faktisk vil se ut og hvor autonome og intelligente kjøretøy og infrastruktur blir, men også fordi systemene i økende grad blir komplekse, med mange ulike aktører og ulike teknologier som sammen og hver for seg skal fungere.

En tilnærming er å beskrive ett og samme system på mange forskjellige måter – der hver fremstilling forenkler bildet ved at bare utvalgte perspektiver og «lag» fremstilles. En slik tilnærming ble brukt som en innledning til workshopene, for å prøve å illustrere hvordan ulike aktører og perspektiver kan ha innvirkning på og få konsekvenser av hvordan systemene ser ut. Under er underlaget som ble brukt i diskusjonene kort oppsummert.

Først har vi sett på hva som kjennetegner komplekse systemer, og hvordan dette påvirker blant annet risikostyring. Deretter har vi skissert fire ulike systembeskrivelser (personvern, forretningsmodeller, forsikring og myndighetsperspektiv), for å illustrere hvordan ulike perspektiver på ett og samme system gir ulike aktører og dataflyt, og dermed også nye ansvarsstrukturer.

4.1 Systembeskrivelser

En forventet egenskap for fremtidens integrerte intelligente transportsystemer (IITS) er høy grad av kompleksitet. Leveson (2011) viser til fire forskjellige typer kompleksitet som er unikt for denne typen systemer:

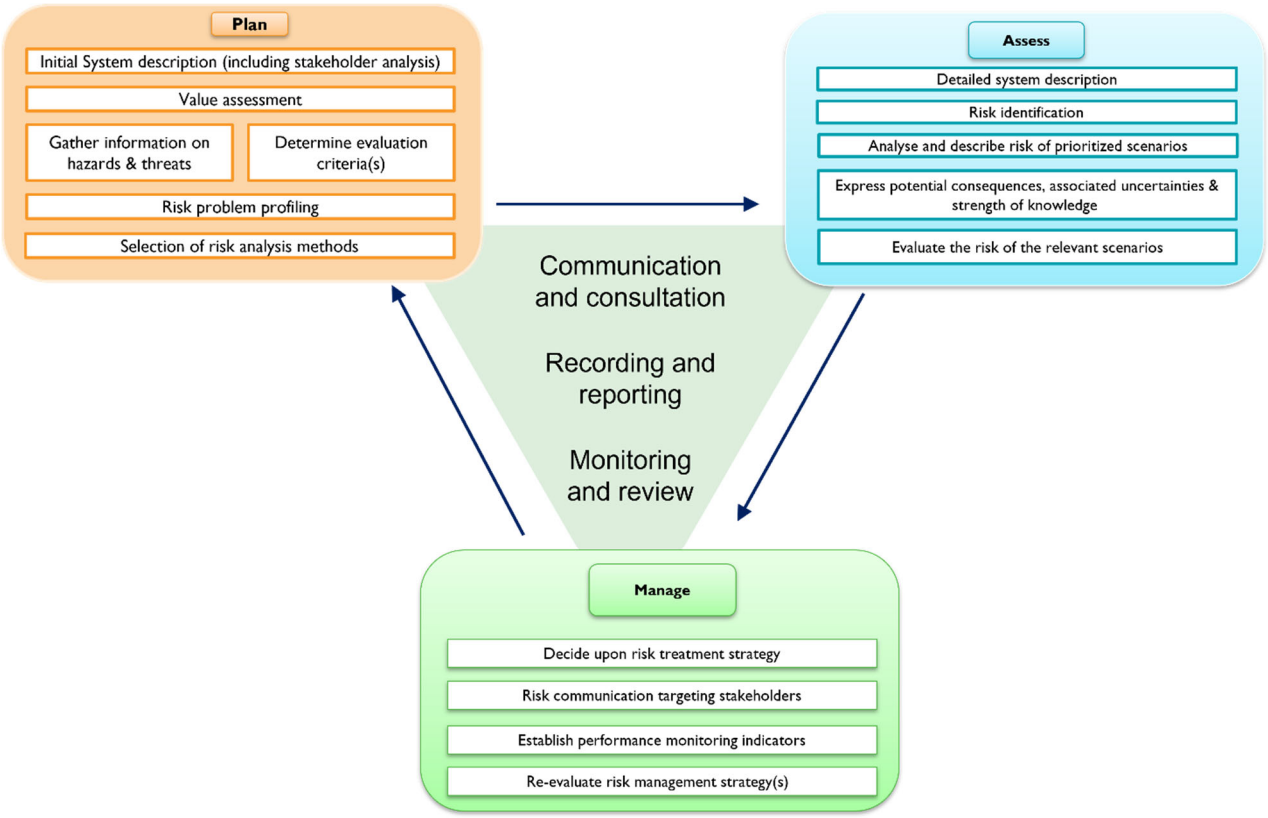
- *Decompositional complexity* betyr at det ofte er manglende konsistens mellom en systemmodell og den faktiske strukturen.
- *Interactive complexity* handler om de mange interaksjonene som er mellom systemkomponentene, som for eksempel fysiske komponenter, nettverk og interessenter.
- *Dynamic complexity* viser til at systemene endrer seg over tid på grunn av indre og ytre faktorer.
- *Non-linear complexity viser* til at det er mangel på åpenbare årsak-virkningsforhold som kan forklare hendelser og handlinger i systemet (Leveson, 2011).

Som et supplement til dette identifiserer Bansal et al (2022) ytterligere to faktorer som påvirker kompleksiteten i IITS-systemene.

- *Scalability* handler om systemets evne til å øke eller redusere systemets ytelse for å tilpasse seg endrede forventinger og behov (som endrede ressursbehov og funksjonalitetsbehov).
- *Novelty* handler om at systemene i seg selv er nye og unike, og man mangler erfaring om hvordan disse fungerer. I følge forfatterne er «Novelty […] about the uniqueness of the system due to a lack of previous experience. One-of-a-kind systems lack previous characterizations, suffer from poor problem framing and uncertain scope. Novelty often presents newer risks requiring non-traditional means of assessment and treatment. Analysts might make weak assumptions in the process» (Bansal, et al., 2022).

I arbeidspakke 2 i SIITS-prosjektet er målet å utvikle nye metoder og verktøy for å håndtere risiko og sårbarhet i slike komplekse systemer. Bansal et al (2022) har derfor utviklet et tilpasset

risikostyringsrammeverk for å bistå aktører i framtidens integrerte intelligente transportsystem. Se Figur 1 Risikorammeverk for IITS.



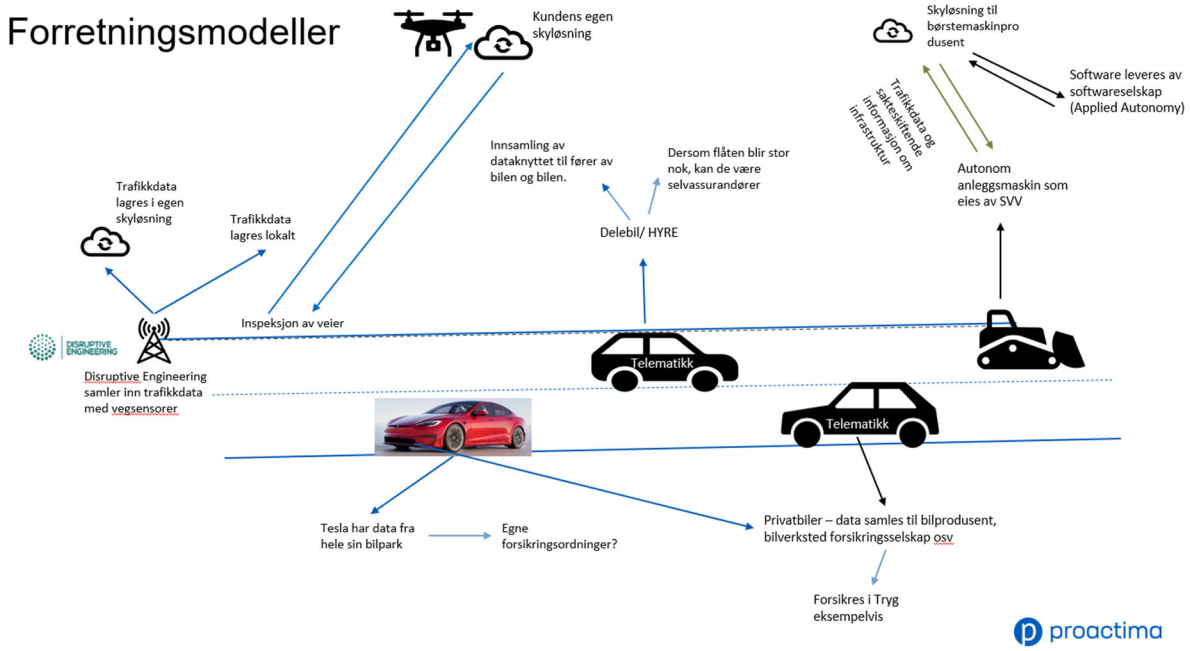
Figur 1 Risikorammeverk for IITS (Bansal et al, 2022)

Første punkt i denne modellen er planlegging, herunder kontekstuell forståelse og problemforståelse. Med andre ord hvordan systemet kan se ut, hvem de ulike interessentene er samt ulike synspunkt på systemet og kartlegging av risiko, farer og trusler.

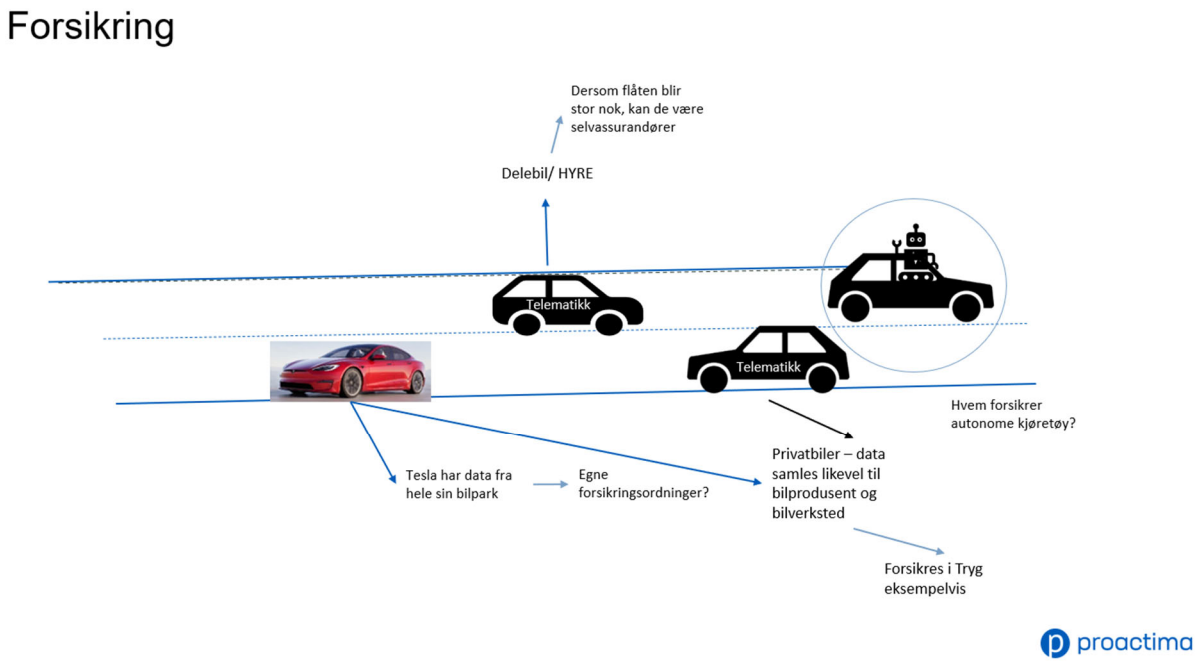
Med utgangspunkt i dette var det i forkant av workshopene hensiktsmessig å etablere noen prinsippskisser for å illustrere deling av data, sett fra ulike perspektiver. Dette fungerte som grunnlag for diskusjonen. De fire ulike perspektivene som var illustrert var:

- Nye forretningsmodeller
- Forsikring
- Myndigheter
- Personvern

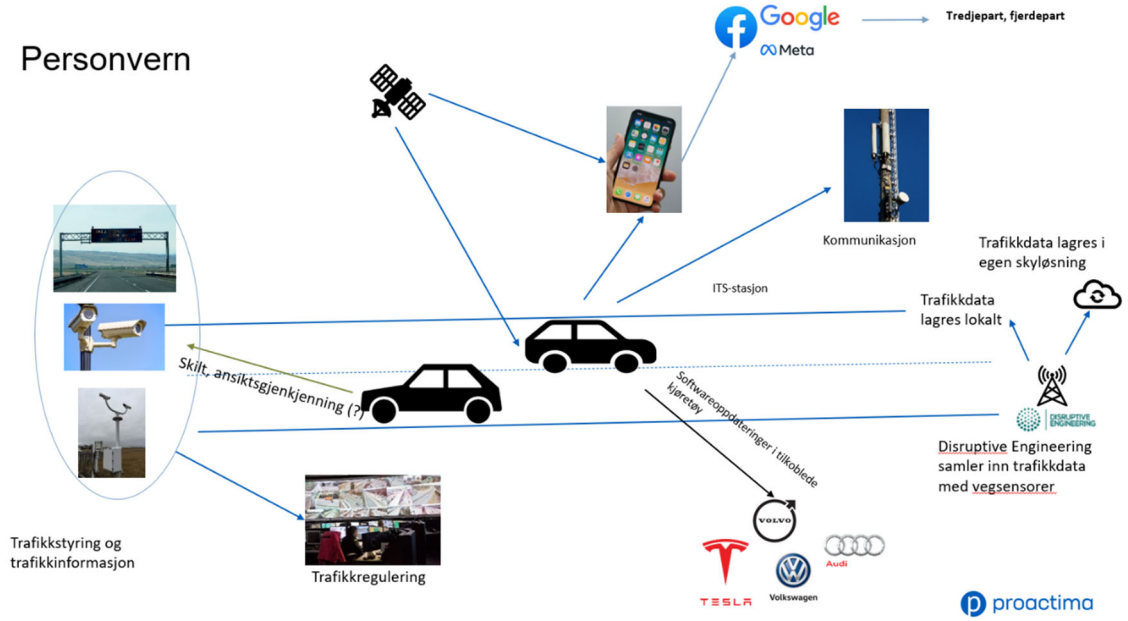
Skissene er gjengitt under.



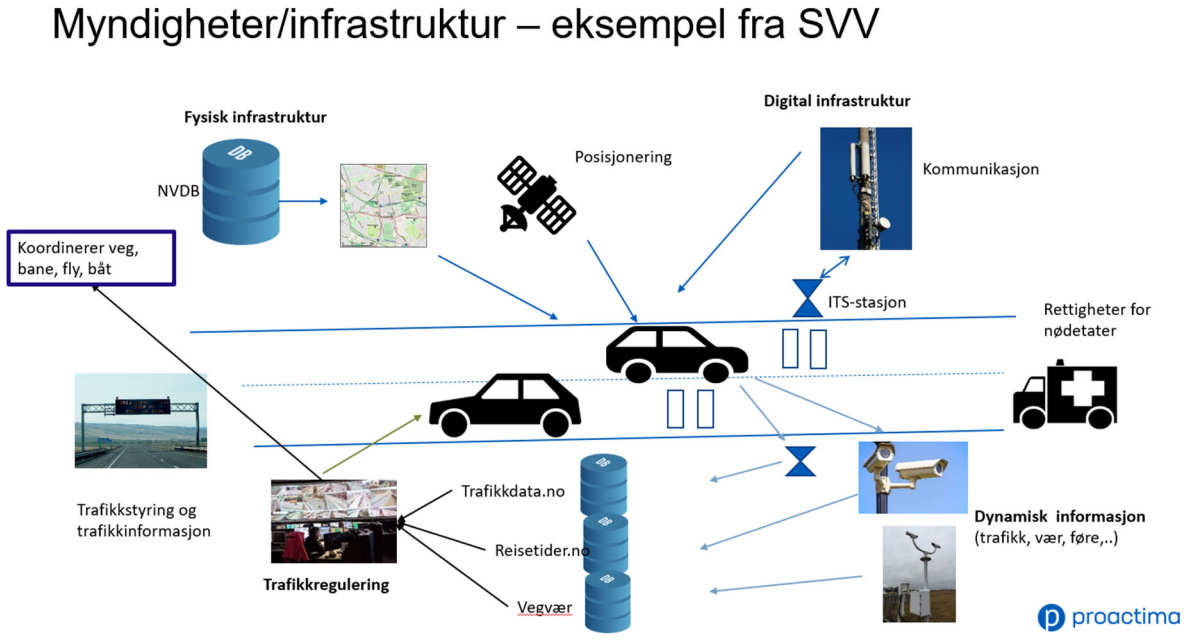
Figur 2 Systembeskrivelse forretningsmodeller



Figur 3 Systembeskrivelse forsikring



Figur 4 Systembeskrivelse personvern



Figur 5 Systembeskrivelse myndighetsperspektiv

Disse fire ulike perspektivene illustrerer hvordan et system for dataproduksjon- og deling vil kunne variere ut ifra hvilket utgangspunkt man har og hvilke interessenter og aktører som involveres, slik Bansal et al (2022) beskriver. Modellene er ikke fullstendige, men hensikten er likevel å synliggjøre hvordan ulike aktører og interessenter varierer ut ifra hvilket perspektiv man har, selv om utgangspunktet er det samme (trafikk på veg). For eksempel i et personvernperspektiv produseres det enorme mengder data fra kjøretøyet, som blir delt med en lang rekke aktører. Det er alt fra bilprodusenter til store aktører som Google og Meta. Også infrastruktur langs veiene samler data om kjøretøyene, og dette har i ulik grad personvernutfordringer avhengig av hvilken data det er snakk om, hvordan den samles inn og hva den brukes til. I et forsikringsperspektiv illustrerer modellen at basert på data som produseres og deles, kan det utvikles flere ulike nye forretningsmodeller innen forsikringsbransjen. For eksempel har bilprodusenter lettere tilgang på data som vil være interessant for forsikringsselskapene. Det kan åpne opp for nye forretningsmodeller der forsikringsselskapene kjøper data av bilprodusentene, eller at bilprodusentene etablerer egne forsikringsordninger.

Andre eksempler på nye forretningsmodeller som baserer seg på bruk av data er eksempelvis Google sine karttjenester som delvis baserer seg på offentlig tilgjengelig informasjon fra eksempelvis Nasjonal Vegdatabase (NVDB), og på data fra alle mobiltelefoner som sender stedsinformasjon til Google. Statens vegvesen innhenter også en rekke data fra veikantinfrastruktur og sammenstiller dette til trafikkdata og veidata som benyttes i vurderingen av trafikksituasjonen rundt på veiene som de har ansvaret for.

5 Ansvarsstrukturer for håndtering av data

De ulike systembeskrivelsene indikerer også nye ansvarsstrukturer. Med ansvarsstrukturer for håndtering av data menes hvilke aktører som har ansvaret for produksjon av data, deling av data, og ikke minst for kvaliteten av dataen, og ansvar ved hendelser knyttet til dataene. Dette er ulike områder hvor ansvaret kan variere, også avhengig av lengder på verdikjeder. Eksempelvis vil det fra et personvernperspektiv være strenge forordninger som regulerer produksjon, deling og bruk av personverndata. Personvernforordningen i EU retter ansvaret til databehandlere og behandlingsansvarlige, og det er store økonomiske konsekvenser dersom en virksomhet bryter med personvernforordningens bestemmelser.

Nye forretningsmodeller gir føringer for ansvarsstrukturene. Implikasjoner og krav relatert til personvern kan unngås dersom aktører som samler data, bygger sin teknologi slik at man unngår å behandle personsensitive data. Disruptive Engineering, en partner i SIITS, er en slik virksomhet. De bygger sin teknologi med *privacy by design*, eller innebygd personvern. Det betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning, og at man dermed unngår å samle inn persondata (Datatilsynet, 2023). Andre eksempler er datainnsamling hvor dataen går direkte til en kunde, uten å gå via datainnsamler først.

Generelt har datatilbyder behandlingsansvar for all behandling av opplysningene til og med deling. Dette inkluderer «transporten» av opplysninger, men ikke mottaket av dataen, ifølge Digitaliseringsdirektoratet (Digitaliseringsdirektoratet, 2023). Den som skal bruke dataen (konsumenten) har ansvaret for behandling fra og med mottaket av opplysningene. Usikkerhet rundt hvem som har ansvar dersom det oppstår hendelser med alvorlige konsekvenser fordi datakvalitet har vært dårlig eller feilaktig, er en utfordring som trekkes frem av deltakerne i den første workshopen. Spesielt gjelder dette når data som samles inn skal brukes som beslutningsstøtte i kritisk infrastruktur. Et eksempel på det kan være dersom dataen brukes til å styre vegtrafikken i et avgrenset område eller by eller i en tunell. Utfordringen blir fort forsterket i IITS, der kompleksiteten i systemet gjør det vanskelig å holde oversikt over nettopp datatilbyder og databehandler.

Et siste eksempel på mulig endring i ansvarsstrukturer i fremtidens intelligente integrerte transportsystemer, er konsekvenser av den økende bruken av kunstig intelligens (KI). Kunstig intelligens kan defineres slik: «kunstig intelligente systemer utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål. Enkelte KI-systemer kan også tilpasse seg gjennom å analysere og ta hensyn til hvordan tidligere handlinger har påvirket omgivelsene» (Kommunal- og moderniseringsdepartementet, 2020).Dersom KI «dekker» så mye av aktivitetene og handlingene i et system, vil det kreve nye avklaringer på hvor ansvaret for konsekvenser av aktivitetene og handlingen ligger.

For å regulere noe av ansvaret ved bruk av KI, utarbeider EU nå et forslag til risikobasert regelverk for kunstig intelligens. Forslaget har en inndeling i risikokategorier, som innebærer at jo høyere risiko bruken av kunstig intelligens utgjør, jo strengere skal bruken reguleres. De foreslåtte reglene regulerer derfor først og fremst «høyrisiko»-bruk av KI, som utgjør en potensiell trussel mot samfunnet og enkeltpersoner. Målet med forordningen er å gjøre EU best i verden når det gjelder utvikling og bruk av sikker, pålitelig og menneskesentrert kunstig intelligens, fordi tillit til KI-systemer er viktig og nødvendig for at det sosiale og økonomiske potensialet i KI skal kunne utnyttes fullt ut (Føyen, Ansvar når noe går galt, 2022).

5.1 Ansvarsstrukturer og forsikring

Forsikringsaktørene har en sentral rolle som risikoavlaster innen de aller fleste områder. I et forsikringsperspektiv illustrerer Figur 3 Systembeskrivelse forsikring» hvordan nye aktører kommer til og kan etablere egne forsikringsordninger på bakgrunn av nye forretningsmodeller. I eksempelet er det tegnet inn aktører som har større flåter av kjøretøy som en konkurrent til privatbilismen. Slike aktører kan, dersom de blir store nok, være selvassurandører. Slik blir de konkurrenter til de eksisterende forsikringsaktørene. Kanskje forsvinner privatmarkedet for biler i fremtiden, samtidig som nye muligheter kan oppstå. Eksempler er økt «business to business»-marked, der enkeltselskaper eier større flåter og forsikrer seg hos dagens aktører. Andre eksempler er bildelingstjenester og bilprodusenter som kan tilby egne bilforsikringer som følger bilen (ikke sjåføren). Ved økende grad av autonomi i kjøretøyene kan det også bli behov for å tydeliggjøre ansvar for, og kostander ved, hendelser. Eksempelvis i tilfeller der de som sitter i kjøretøyet ikke har roller som sjåfører, men passasjerer. Ny teknologi og økt autonomi og integrasjon av kjøretøy kan også medføre økte utbetalinger i skadesaker, dersom feil eller digitale angrep fører til større ulykker (eksempelvis at et digitalt angrep gir feil på en hel flåte av kjøretøy). Per i dag likevel den største utfordringen for forsikringsselskaper at «digitale biler» som utsatt for selv mindre hendelser, er mye dyrere å reparere pga. elektronikken som ødelegges.

I arbeidet har det blitt identifisert en rekke risikoer for forsikringsbransjen med hensyn til uavklarte ansvarsstrukturer. Tre eksempler illustrerer disse risikoene.

- Den første risikoen er uavklart ansvarsforhold knyttet til inngåelse av ansvarsforsikring. Det kan være flere årsaker til en slik risiko. For eksempel usikkerhet knyttet til ansvar i en autonom fremtid ved kollisjon mellom to selvkjørende biler, ved overstyring av et autonomt system. Det kan også være usikkerhet knyttet til ansvar i en overgangsfase mellom vekslende bruk av selvkjøring, dersom trusselaktører skulle overstyre et autonomt system. For forsikringsbransjen kan konsekvensene være at de taper markedsandeler fordi selskapene ikke forstår ansvarsbildet eller at de selger «feil» forsikring til «feil» kunde. Grensesnittet mellom softwareleverandør og bilprodusent og øvrige leverandører kompliserer ansvarsstrukturene ved hendelser.

- Det kan også være risiko for uavklart regressansvar[1] i en skadesak. Årsakene til dette kan være flere. Blant annet at det er avvikende data fra ulike kilder. Som vi har sett produseres det enorme mengder data fra både kjøretøyet, sjåføren, sjåførens mobiltelefon og så videre. Alle disse datakildene kan gi usikkerhet med hensyn til hvem som har regressansvar. Er det bilprodusenten, bilprodusentens IT-leverandører, infrastruktureiere eller infrastruktureiernes IT-leverandører? Det kan også være usikkerhet knyttet til hvem som har ansvaret for kollisjoner mellom to autonome kjøretøy eller i en overgangsfase slik det er beskrevet over. Et annet eksempel er regressansvar dersom sikkerhetsoppdateringer ikke er gjennomført eller der de er utdaterte.
- Til sist er det en risiko ved uavklarte ansvarsforhold knyttet til eierskap av data. Lange, komplekse verdikjeder bestående av flere bilprodusenter, flåteeiere, sjåfører, utstyrsleverandører og IT-leverandører er et komplekst nettverk av datakilder. Hvilke forretningsmodeller som er gjeldende i fremtidens IITS vil også legge føringer for hvilke forsikringsprodukter selskapene vil tilby. Tilgang på stordata gir mange nye muligheter for forsikringsbransjen, i den grad andre aktører deler med hverandre. Ordninger der sjåfører kan få forsikringer basert på stordataanalyser av kjøremønster og atferd (pay as you go) kan gjøre at de som kjører bra, får billigere forsikring enn sjåfører med et annet kjøremønster.

Bruk av ny teknologi og nye forretningsmodeller gjør at ansvarsstrukturer i fremtidens intelligente integrerte transportsystemer kan endres. Kompleksiteten i systemene med hensyn til hvilke aktører som er involvert i den gitte konteksten, kan komplisere dette ansvarsbildet. Dette kan påvirke hvordan risiko styres i en virksomhet og i deler av systemet. Derfor er det en vanskelig, men viktig øvelse å kartlegge interessenter og øvrige aktører som et første steg i risikostyringen.

6 Diskusjon

Nye ansvarsstrukturer og komplekse systemer innenfor transport gjør at det oppstår en rekke utfordringer knyttet til dataproduksjon og deling. En måte å kategorisere utfordringene på, er i to overordnede grupper: utfordringer knyttet til datainnsamling- og deling, og konsekvenser dersom datadeling ikke er mulig. Innenfor disse to overordnede kategoriene finner vi en rekke utfordringer. Det er utfordringer for både de aktørene som skal operere og utvikle teknologi i fremtidens IITS, for myndigheter som ofte har et behov for data fordi de skal regulere og drive tilsyn. I det følgende beskrives kort noen av utfordringene som har fremkommet i arbeidet med denne rapporten.

6.1 Hvilke utfordringer er det med hensyn til innsamling og deling av data i et intelligent, integrert transportsystem?

Det er en rekke utfordringer som blir identifisert under spørsmålet «hvilke utfordringer er det med hensyn til innsamling og deling av data». Ulike aktører kan både produsere data og samle inn de samme dataene, men bruke dataene på ulike måter. For eksempel produserer Disruptive Engineering trafikkdata ved bruk av sensorer i vegbanen. Dette kan igjen brukes som informasjon om trafikkbildet for prioritering av tiltak på operativt eller politisk nivå. Det kan også fungere som underlag til reguleringsplaner fordi man får et oppdatert bilde av hvordan trafikksituasjonen faktisk er i et gitt geografisk område. Andre bruksområder er datadrevet drift og vedlikehold, effektmåling av tiltak, oppfølging av politiske vedtak, og evaluering- og kalibrering av trafikkmodeller.

Også vi som forbrukere produserer store mengder data som kan benyttes til mange svært ulike formål. Aktører som Google, Apple og Facebook samler inn og deler disse i varierende grad.

[1] Regress innebærer at man har krav på å få dekket et pengebeløp man har betalt på vegne av en annen.

6.1.1 Orkester uten dirigent

Fremtidens IITS handler nettopp om en mer eller mindre kjent fremtid. Dette er i seg selv en utfordring for de aktørene som skal produsere og samle inn data. Hvordan systemet vil se ut, hvilke aktører som er involvert og hvilke roller disse har (produsenter av data, forbrukere av data, forbrukere av tjenester mm) vil være dimensjonerende for hvilken data det er behov for i et IITS-system, og hva som eksempelvis skal tilbys av det offentlige. For noen produsenter av data vil deres teknologi være en premissleverandør for hvilke tjenester eksempelvis Statens vegvesen og Kartverket i neste omgang kan tilby.

Det er også en utfordring at offentlige myndigheters systemer ikke er harmonisert med hverandre, heller ikke innenfor egen virksomhet. Eksempelvis benytter de fem vegtrafikksentralene (VTSene) i Norge tre forskjellige tekniske systemer (SCADA-system). 2 VTSer bruker ett system. 2 VTSer bruker et annet, og den siste VTSen bruker et tredje system. De som har samme system, er ikke geografisk tilknyttet hverandre. Det kan bety at de som skal motta trafikkdata eller veidata ikke har systemer som kan motta akkurat den spesifikke type data. Dette vanskeliggjør situasjonen for tilbydere, og kan også svekke kvaliteten på dataen som tilbys. En annen utfordring er at VTSene ikke kan dele data imellom seg, og dermed være redundante installasjoner for hverandre og å få til en sømløs samhandling ved nasjonale kriser. En løsning på det tekniske aspektet ved dette, kan være at det blir satt koordinerte krav til standardiserte M2M-grensesnitt i anskaffelser[2].

Statens vegvesen jobber med å harmonisere systemene til vegtrafikksentralene, slik at trafikksentralene enklere kan samarbeide med hverandre. I prosjektet VTS Norge er ambisjonen til Statens vegvesen at alle VTSene skal være på det samme SCADA-systemet og kunne operere sammen, for å være mer robuste for fremtiden. Eksempelet med Statens vegvesen illustrerer også en mer helhetlig utfordring med anskaffelser. Ifølge enkelte av deltakerne i workshopen er det utfordrende at offentlige anskaffelser blir gjort uten hensyn eller kompetanse til ny teknologi og en helhetlig forståelse av hva samfunnet har behov for på sikt.

Store kommersielle aktører er ofte i front både på dataproduksjon og datadeling. Meta, Google og andre tilbydere av «gratis» tjenester som kart og sosiale plattformer, tar betalt i form av at personer gir i fra seg data. Dette gjør at disse aktørene kan utvikle sin teknologi og plattformer enda mer målrettet. For utvikling av karttjenester, benytter disse aktørene seg også ofte av offentlig tilgjengelig data, som Nasjonal Vegdatabank (NVDB). Aktører som Google og Tomtom er dermed konkurrenter til offentlige kartmyndigheter.

Foreløpig kan ikke norske myndigheter stille krav om deling av data til de som produserer og/eller samler inn data fra offentlige datakilder. Nye lovgivninger i EU kan endre på dette. For eksempel legger Open Data Directive, Data Act og Data Governance Act i større grad til rette for deling av data mellom private aktører og det offentlige nettopp for å øke innovasjon og deling av data i det indre markedet. Frem til disse trer i kraft er det ofte de store kommersielle aktørene som har de «beste» tjenestene for forbrukerne, uten at synergiene mot offentlige myndigheter blir utnyttet godt nok og ofte også uten at forbrukere er klar over hvilken data de gir i fra seg. Sistnevnte henger både sammen med bevissthet og tillit til tjenester og forutsetninger for å forstå teknologi. Teknologiske løsninger henger etter hvert så tett sammen at det er krevende å forstå hvordan løsningene virker og dermed hva man gir andre tilgang til.

En sentral utfordring er dermed at det er mange som produserer og benytter data innenfor IITS, men det mangler en koordinert samstyring eller dirigering for å få utnyttet all data og ny teknologi på en god måte som tjener forbrukeren.

[2] Maskin-til-maskin-nettverk (M2M) er nettverk av sensorer, styringer og maskiner som kommuniserer med hverandre uten menneskelig innblanding

6.1.2 Deling på tvers av landegrenser

Deling av data på tvers av landegrenser er også en utfordring. Det er ingen felles internasjonal standard for kart. Det betyr at kartdata er forskjellig fra land til land. Dette utfordrer både samarbeid og kryssing av landegrenser. Selv om karttjenestene til de store aktørene som Google og Apple fungerer overordnet, er ikke kartdataen nøyaktig nok til at den foreløpig kan benyttes i autonome kjøretøy eller i karttjenestene i moderne kjøretøy. Til dette trengs de offentlige kartmyndighetenes tjenester. Kartverket produserer for eksempel høydedata og punktskydata. Dette kan man lese mer om på Kartverkets nettsider.

Biler har i dag for eksempel Google Maps eller Tomtom i karttjenesten. Nasjonal Veidatabank (NVDB) eies av Statens vegvesen, men benytter kartløsninger som eies av Kartverket. NVDB har veidata som er åpent tilgjengelig for alle. Google bruker data fra NVDB sammen med matrikkelinformasjon. I Norge fungerer det fint for disse aktørene å bruke data fra NVDB, fordi disse dataene følger et sett med standarder som gjelder for hele landet. I andre land er ikke dette like utviklet, og det kan også være forskjeller fra fylke til fylke. Dette er derfor en stor utfordring for autonom kryssing av landegrenser, som MODI-prosjektet har fokus på (ITS Norway, 2022).

Kartdata er en viktig forutsetning for realisering av intelligente integrerte transportsystemer. Gode karttjenester er helt avhengig av nøyaktig posisjon og dermed også GNSS frem til det er etablert gode alternativer som kilde til nøyaktig tid i 5G-nettene. Fremtidens IITS trenger nøyaktig og redundant posisjonsbestemmelse. Det er en sterk kobling mellom kart og posisjon. En felles referanseramme for alle land betyr at man kan dra fra ett land til et annet, basert på det samme koordinatsystemet. En slik felles referanseramme for bruk av kart er viktig fordi jordskorpen er i konstant bevegelse. Enn så lenge opererer likevel hvert enkelt land og regioner med egne kartdata. Dette er en utfordring dersom man ønsker at autonome kjøretøy skal kunne krysse landegrenser.

6.1.3 Juridiske utfordringer

Det er også flere juridiske utfordringer. Det foregår diskusjoner i mange land rundt spørsmålet om det finnes eller bør etableres en eiendomsrett til data. Flere aktører i en verdikjede vil kunne hevde at de «eier» hele eller deler av et datasett, hvilket kan skape kompleksitet ved gjenbruk og anvendelse av datasettet for nye eller endrede formål.

Eksisterende lovverk vedrørende eierrettigheter til data synes ikke å være tilfredsstillende, og manglende avklaring rundt eierskap til data er, ifølge advokat Arve Føyen, en reell barriere for deling av data. Det kan være gode, forretningsmessige grunner til at en enkelt aktør er tilbakeholden med å dele data og delta i datadelingsinitiativ. Det er imidlertid flere viktige barrierer som gjør at aktørene er *for* forsiktige i forhold til deres egne interesser, for eksempel: uoversiktlig og vanskelig regelverk (GDPR, taushetsplikt, regler om offentlighet, regler om IPR), frykt for å gjøre noe galt, uoversiktlige ansvarsregler og frykt for å miste kontrollen. Aktørene kan ha flere ulike avtaler, som kan ha i seg større eller mindre grad av eierskap til data. På den ene siden kan kunden kreve fullt eierskap til dataene, slik at aktørene som leverer eksempelvis trafikkdata ikke lenger kan benytte dataene til å forbedre og videreutvikle tjenestene. På den andre siden kan aktørene inngå avtaler med kunder om bruksrett til data, men ikke fullt eierskap.

Det er ikke etablert noen klare regler om eiendomsrettigheter til data, og de eksisterende rettigheter relatert til data tilfredsstiller ikke behovene til aktørene i verdikjedene knyttet verken til genering eller utnyttelse av data. Eierskap til data styres av besittelse og av regler om beskyttelse av bedriftshemmeligheter. Hittil har den eneste fungerende løsningen vært å regulere mulige forhold mellom aktørene i avtaleform (Føyen, Eierskap og bruk av data, 2022).

Slike avtaler må i utgangspunktet baseres på at en eller flere relevante parter har kontroll med tilgangen på data, og at de regulerer videre tilgang til data gjennom avtaler med mottaker. Bruk av slike avtaler er langt fra ideelt, særlig i verdikjeder hvor mange aktører og datakilder er involvert i

forbindelse med innsamling, sammenstilling, berikelse, lagring og analyser, og hvor det derfor kan være et stort antall aktører som har eierinteresser i de aktuelle dataene. En videre komplikasjon er at stordata-analyse typisk involverer komplekse datastrømmer, datakilder og maskinlæringsalgoritmer trent på disse dataene. For slike formål må det tilrettelegges for tilgang til- og utveksling av data. Slik tilrettelegging kan fra et juridisk perspektiv først og fremst oppnås gjennom bruk av avtaler om deling av data. På grunn av kompleksiteten, kan det i forbindelse med stordata-analyser være nødvendig å etablere en innviklet struktur av datadelings- og samarbeidsavtaler. Det vil dessuten være slik at avtaler som er bindende mellom de aktuelle avtalepartnerne, ikke binder tredjeparter som ikke har forpliktet seg til vilkårene i avtalen (Føyen, Eierskap og bruk av data, 2022).

I EU er det nå en rekke initiativer for deling og tilgang på data, som nevnt over. Slike reguleringsinitiativer vil også kunne bidra til økt demokratisk kontroll av teknologisk utvikling som i stor grad er preget av kompleksitet, bedriftshemmeligheter og såkalte «black boxes» som det er vanskelig å få innsyn i.

Til sist er en vesentlig utfordring for deling av data at det er svært mange aktører involvert, noe de ulike systembeskrivelsene skildrer. I et dataproduksjons/delingsperspektiv gjør det at mange aktører er gjensidig avhengig av hverandre for at dataen er av god kvalitet og kan benyttes. Ikke minst gjelder dette etter hvert som kunstig intelligens også i økende grad benyttes. Dette skaper utfordringer både med hensyn til avhengighetene som oppstår, men også hvordan ansvar skal plasseres ved hendelser.

6.2 Konsekvenser og ansvar ved manglende datadeling – eksempel fra GNSS

Som allerede er drøftet, er dataproduksjon- og deling helt sentralt for at fremtidens intelligente integrerte transportsystemer skal fungere. Vi har sett at ved å benytte ulike systembeskrivelser, får vi frem ulike aktører som alle produserer eller bruker data på ulike måter. Dette skaper nye ansvarsstrukturer og avhengigheter. Siste sesjon av workshopen omhandlet nettopp konsekvenser dersom datadeling av ulike årsaker ikke er mulig, eller kvaliteten på dataene ikke er god nok til det behovet som skal dekkes.

Det kan være en rekke årsaker til at datadeling ikke er mulig. Datadeling er et viktig grunnlag for realisering av IITS. Uten at det finnes kilder til nøyaktig tid og posisjonsdata, data om reisebehov, data om trafikksituasjoner, vær og vind (denne listen er ikke uttømmende), vil det være vanskelig å realisere fremtidens intelligente, integrerte transportsystemer. I et stadig mer digitalisert samfunn kan man forvente at trusselaktører ikke bare beveger seg i det fysiske rom, men i aller høyeste grad i det digitale rom. En overhengende menneskeskapt krise er også klimaendringer som vil påvirke hvordan kritisk infrastruktur (både veg, kraft og ekom) bygges og gjøres robust for å kunne tåle mer ekstremvær. Det er mange trusler mot og sårbarheter i fremtidens intelligente integrerte transportsystem, og disse kan forventes å bli forsterket når systemene blir komplekse og integrerte.

Hva er så konsekvensene dersom sentrale datakilder faller ut, eller der kvaliteten på dataen ikke er tilstrekkelig for det den skal brukes til, eller at kvaliteten svekkes over tid etter hvert som den følger en verdikjede? Et grunnleggende eksempel på dette er avhengigheten til satellittbaserte tjenester. Transport er en kritisk samfunnsfunksjon (Direktoratet for samfunnssikkerhet og beredskap, 2016). I dag deles denne kritiske samfunnsfunksjonen opp i fire ulike kapabiliteter: luftfartssystemet, vegtransportsystemet, jernbanesystemet og det maritime transportsystemet. I dag er disse separate sosiotekniske systemer, med egne systemer hver for seg. Alle disse systemene er i dag avhengig av nøyaktig tid og posisjon. I fremtiden kan man forvente at disse systemene er delvis eller helt integrert med hverandre, og da vil nøyaktig tid og posisjon bli enda viktigere.

Global Navigation Satellite Systems (GNSS) brukes i dag som kilde til nøyaktig tid og frekvens. Et GNSS deles ofte inn i tre segmenter: bakkesegmenter er for å kontrollere satellittene og dataen de

sender ut. Romsegmentet består av alle satellittene. Til sist er det brukersegmentet, som er summen av alle mottakerne innen alle anvendelsesområdene (Kapaasen, 2021). I forbindelse med GNSS, skilles det ofte på data og tjenester. GNSS tilbyr i utgangspunktet brukere tilgang til ulike tjenester. Vanlig bruk av Galileo (europeisk system for satellittnavigasjon) innebærer bruk av Open Service, som gir brukere gratis tilgang til global dekning av posisjon og tid. GNSS sender også noe data om nøyaktig tid (UTC). Ved posisjoner på bakken er det en GNSS-mottaker (for eksempel telefon eller bil) som regner ut sin posisjon på bakken basert på hvor langt unna den er satellitten.

I dag har nærmest alle smarttelefoner GNSS-mottakere og moderne biler har også egne mottakere. GNSS er med andre ord i økende grad den infrastrukturen som benyttes for både å få nøyaktig tid og nøyaktig posisjon for kjøretøy, mobiltelefoner, tog, mm. Kapaasen (2021) sier:

> «GNSS har gjort navigasjon på land svært aktuelt. Vi ser for eksempel GNSS-mottakere i treningsklokker, mobiltelefoner, kjøretøy og landbruksmaskiner. Hos nødetatene ser vi flåtestyring av utrykningskjøretøy og det brukes trygghetsalarmer som viser posisjon. Innen veitrafikk ser vi GNSS-basert nødvarsling (eCall), satellittbasert vegprising og intelligente trafikksystemer. Innen elkraft og tele-/data-kommunikasjon ser vi synkronisering av nett og datatrafikk» ((Kapaasen, 2021) s. 11).

GNSS er dermed en grunnleggende infrastruktur til dataproduksjon for dagens transportsystem. Autonome biler vil være helt avhengig av posisjonsdata for å kunne navigere på vei og forholde seg til andre kjøretøy og fotgjengere. Det vil også virksomheter med ansvar for trafikkstyring på tvers av modaliteter. Hvilke konsekvenser kan det ha dersom det ikke er mulig å få riktige posisjonsdata?

Det er mange hendelser som kan påvirke nøyaktigheten i, og tilgangen til GNSS-tjenestene. Dette er både tilsiktede og utilsiktede forhold, og menneskeskapte og naturlige hendelser: romskrot, romvær, forstyrrelser fra menneskeskapte systemer (som jamming, spoofing og meaconing). Fysiske hindringer kan også stoppe signaler, det samme kan feilbruk og skader eller feil på bakkesegmentene (Kapaasen 2021). Konsekvensene ved bortfall av signaler, kan være svært store. Først og fremst fordi GNSS fungerer som en verdensomspennende klokke som alle mulige systemer synkroniseres mot. Blir GNSS-signalet borte, blir også tidssignalet borte. Også 5G-teknologien er svært avhengig av korrekt tid og posisjon. 5G lar seg ikke realisere uten kontinuerlig tilgang på nøyaktig tid. Det er mulig å realisere 5G uten GNSS, men da må netteier kunne plassere egne atomklokker i nettet, eller kjøpe tidsinformasjon fra en leverandør som har atomklokker. I Sverige er det etablert en nasjonal abonnementstjeneste for tid. Dette har vi ikke i Norge enda, og enn så lenge vil derfor norske leverandører av 5G være avhengig av GNSS.

Både Statens vegvesen og Kartverket er hver for seg svært avhengige av både posisjonsdata og nøyaktig tid for at deres systemer skal fungere. Gode kartdata er avhengig av at posisjonstjenestene fungerer. Har man ikke nøyaktig posisjonsdata, så reduseres også kvaliteten på kartene som eksempelvis brukes i biler. Med en utvikling innen autonom transport, vil også posisjonsdata være sentralt for at trafikken skal flyte som ønskelig. En annen alvorlig konsekvens er at kommunikasjon generelt i samfunnet er utfordret ved fravær av GNSS, noe som vil være alvorlig for å sikre kontinuitet i alle de kritiske samfunnsfunksjonene i Norge inkludert finansielle transaksjoner og handel generelt.

Hvem har da ansvaret for sårbarhetene i disse avhengighetene? Norske myndigheter sitter langt unna de som eier satellittbasert infrastruktur. I dag er det fire GNSS systemer: amerikanske GPS, EUs Galileo, kinesiske BeiDou og russiske GLONASS. Alle kritiske samfunnsfunksjoner er i større eller mindre grad avhengig av satellittbaserte tjenester, men norske myndigheter har ingen mulighet til å påvirke i hvilken grad GNSS fungerer i Norge. Det som kan gjøres er å påvirke vår egen robusthet, ved at man åpner for muligheten til å benytte flere av systemene, ikke bare GPS slik som det er for mange i dag. Alternativt kan man regulere bruken, slik at for eksempel departement med hovedansvar for kritiske samfunnsfunksjoner pålegges å ha en beredskap for bortfall av GNSS.

Bruk av flere parallelle systemer har svært begrenset utbredelse i dag, selv om flere infrastrukturaktører etter hvert også benytter Galileo noe i tillegg til GPS. Fremdeles er det GPS som er rådende i droner, selvkjøringsnavigasjon i biler, mikromobilitet og flynavigasjon. Det er dermed en helt sentral utfordring at alle – og ingen har ansvar for en infrastruktur som er helt grunnleggende for å realisere IITS.

6.3 Konsekvenser for risikostyring

Hvordan vil da disse utfordringene som er skissert, kunne påvirke risikostyringen i fremtiden? Som vi ser av Figur 1 Risikorammeverk for IITS (Bansal et al, 2022) er den kontekstuelle forståelsen av systemet en vesentlig forutsetning for å gå videre med risikoidentifikasjon- og håndtering. For ulike aktører, både offentlige og private, vil systemstrukturen se ulik ut avhengig av hvor man er i en verdikjede/systemstruktur.

Alle de utfordringene vi har nevnt nå, kan plasseres i «planleggingsfasen» av risikostyringsmodellen. Utfordringene som er skissert, påvirker alle deler av problemforståelsen som er essensiell for å identifisere risiko og rammene for kompleksiteten. I dette notatet har vi bare fokusert på generelle utfordringer for systemforståelsen ved produksjon- og deling av data. En reell utfordring for den kontekstuelle forståelsen som danner første steg i risikostyringsrammeverket, er jo at systemet i varierende grad er komplekst (scalability). Eksemplet med GNSS synliggjør nettopp at det er nødvendig å trekke systemgrensene heilt ut til satellittene for å forstå avhengigheter som ligger langt utenfor tradisjonell systemavgrensing. Her har svært få aktører beslutningsmyndighet, mens alle andre aktører deriblant offentlige myndigheter, ikke har noe ansvar selv om infrastrukturen de skal beskytte er helt avhengig av satellitter.

Andre faktorer som også vil være viktig i denne fasen er å innhente informasjon om farer og trusler mot det systemet man har identifisert. Disse vil naturligvis også variere ut ifra hvilket systemutgangspunkt man har, og hvilke aktører som er involvert og hvilken type teknologi/infrastruktur som benyttes.

De utfordringene som er drøftet her, vil prege risikobildet til virksomheter som skal operere innenfor intelligente, integrerte transportsystemer. Systemforståelse og forståelse for at risikobildet vil variere ut ifra denne systemforståelsen, er et viktig utgangspunkt for risikostyringen i fremtidens intelligente, integrerte transportsystemer.

7 Konklusjon og tiltak

Denne rapporten har fokusert på noen utfordringer som oppstår med hensyn til datadeling, ansvar og personvern ved hendelser i fremtidens IITS. Vi har diskutert hvordan ulike perspektiv på et system kan synliggjøre ulike ansvarsstrukturer og hvordan dette igjen vil påvirke virksomheters arbeid med risikostyring. Videre har vi drøftet utfordringer knyttet til dataproduksjon- og deling samt konsekvenser dersom datadeling ikke er mulig eller sentrale datakilder faller bort. Spesielt er GNSS som kilde til nøyaktig tid- og posisjon en sentral datakilde med store konsekvenser dersom den type data faller bort.

Det er mange aktører på ulike nivå som både produserer data, deler data og videreforedler data til ulike behov. Offentlige aktører som skal benytte dataen opererer ofte med ulike system for å motta informasjon, noe som gjør det utfordrende for dataprodusenter å levere gode data. Videre er det også utfordrende for det offentlige at en rekke kommersielle aktører benytter seg av åpent tilgjengelige data, uten at det finnes insentiv om å «gi noe tilbake» for å styrke kvaliteten på offentlige data (som kartdata). Datadeling på tvers av landegrenser er også utfordrende, fordi land opererer med egne standarder. Ofte er standardene ulike fra region til region innad i et land også.

Det er også en rekke juridiske utfordringer som gjør at aktører kan vegre seg for å dele data, i frykt for å bryte med etablerte regelverk (personvern) eller av bedriftshensyn. Det handler med andre ord om å dele data som er riktig og nødvendig, men samtidig ikke dele data som kan avsløre eller øke sårbarheter i systemer.

Det kan både være større og mindre konsekvenser ved manglende datadeling eller bortfall av sentrale datakilder. I tilfelle med GNSS, er nøyaktig tid og posisjonsdata helt sentralt både for kjøretøy, utvikling av kart, navigasjonstjenester, ekom og strøm mm. Bortfall av GNSS som følge av for eksempel spoofing eller jamming, kan dermed ha store konsekvenser for muligheten til å dele gode data mellom aktørene i IITS (for eksempel mellom kjøretøy eller trafikkinfrastruktur).

For å håndtere disse utfordringene tilstrekkelig forskning, utredning og utprøving.

Det fremstår likevel tydelig at en styrking av samarbeidet mellom offentlig og privat sektor, mellom private aktører og ikke minst mellom land og over deres grenser, vil bidra til å senke utfordringene noe. I dette ligger det både å sørge for at datadeling er mulig og ønsket, at det er incentivordninger fra myndighetssiden som støtter opp om- og tilrettelegger for bruk og deling, men også at enhver sørger for at det er mulig å motta og dele data. Videre er det viktig at det er en bevissthet rundt avhengigheter og hvilke avhengigheter som oppstår når samfunnet i økende grad blir datadrevet.

For å sikre god deling og ikke minst klare ansvarsstrukturer er det også nødvendig å ha gode avtaler mellom aktørene som nettopp avklarer eierskap til data og ansvar for dataen. Ved økt bruk av stordata, kunstig intelligens og stordataanalyser, kan det være behov for strukturer av datadelings- og samarbeidsavtaler. Tillit mellom aktører og forbrukere er også en vesentlig faktor, som ikke kan tas for gitt

Denne rapporten har bare påpekt noen utfordringer og noen mulige løsninger, men fremdeles er det en rekke andre områder som ikke er belyst og som bør belyses for å bedre realisere IITS. Et eksempel på behov for videre forskning er hvordan myndigheter og privat næringsliv skal kunne forbedre samfunnssikkerheten når ansvarsstrukturene for datadeling er utydelige, i et stadig mer datadrevet samfunn. Som eksempelet med GNSS illustrere, er stadig flere kritiske samfunnsfunksjoner avhengig av nøyaktige data om tid og posisjon. Ansvarsprinsippet er et helt sentralt samfunnssikkerhetsprinsipp, men hva skjer med samfunnets sikkerhet og beredskap dersom ansvaret ikke er tydelig plassert?

8 Referanser

Bansal, S., Metcalfe, C., Flage, R., Bjelland, H., Jensen, A., & Røed, W. (2022). Outline of a risk management framework for future transport systems. *32nd European Safety and Reliability Conference (ESREL 2022).* Singapore.

Datatilsynet. (2023). *Hva er innebygd personvern (Privacy by design)?* . Hentet fra Spørsmål og svar: https://www.datatilsynet.no/regelverk-og-verktoy/sporsmal-svar/Innebygd-personvern/hva-er-innebygd-personvern/

Digitaliseringsdirektoratet. (2023). *Be om tilgang til data*. Hentet fra Datadeling: https://www.digdir.no/datadeling/be-om-tilgang-til-data/2257#roller_og_ansvar_skal_avklares

Direktoratet for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner - hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

Føyen, A. (2022). Ansvar når noe går galt. Presentasjon av Arve Føyen, 10. november 2022.

Føyen, A. (2022). Eierskap og bruk av data. Presentasjon ifbm SIITS, 10. november 2022.

ITS Norway. (2022, Oktober 1). *Pressemelding: Norske partnere sitter i førersetet for rekordstort og viktig Europeisk forsningsprosjekt innen automatisert godstransport*. Hentet fra https://www.kartverket.no/globalassets/til-lands/posisjon/pressemelding-om-modi-oppstart-20220930.pdf

Kapaasen, K. B. (2021). *Når tiden går i bane.* Trondheim: Masteroppgave ved NTNU - Institutt for sosiologi og statsvitenskap.

Kommunal- og moderniseringsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens.* Oslo. Hentet fra: https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf: Kommunal- og moderniseringsdepartementet.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety.* The MIT Press.

+47 4000 1933

POST@PROACTIMA.COM

PROACTIMA.COM