SINTEF

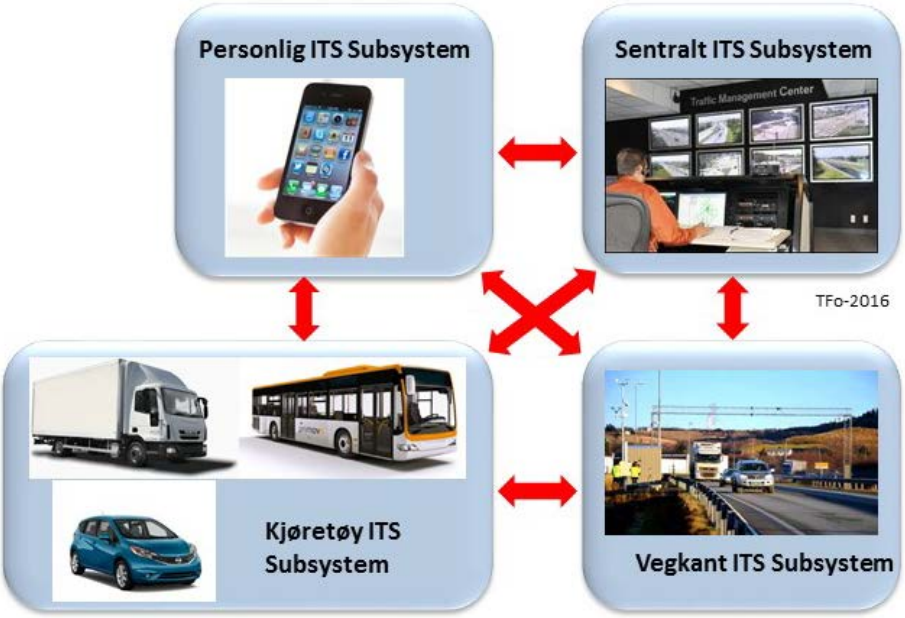
A27550 - Åpen

Rapport

Ikke-teknologiske aspekter ved kooperativ ITS

Bilen som sensor

Forfattere
Trond Foss
Kristin Ystmark Bjerkan
Marianne Elvsaas Nordtømme



2016-04-11

SINTEF

Postadresse:

Foretaksregister:

Rapport

Ikke-teknologiske aspekter ved kooperativ ITS

Bilen som sensor

EMNEORD:
ITS
Personvern
Brukeraksept
Forretningsmodeller
Transportdata
Eierskap

VERSJON
2.0

DATO
2016-04-11

FORFATTERE
Trond Foss
Kristin Ystmark Bjerkan
Marianne Elvsaas Nordtømme

OPPDRAGSGIVER
Statens vegvesen, Vegdirektoratet

OPPDRAGSGIVERS REF.
Tomas Levin

PROSJEKTNR
102010386

ANTALL SIDER OG VEDLEGG:
67

SAMMENDRAG

Dette prosjektet har hatt som mål å bidra til økt kunnskap om såkalte ikke-teknologiske aspekter rundt kooperativ ITS og håndteringen av data som genereres fra kooperativ ITS. Dette er viktig for å oppnå vellykket implementering av kooperative ITS-løsninger, i tråd med målene i Nasjonal transportplan.

Denne rapporten oppsummerer aktuell kunnskap fra de ovennevnte kunnskapstema, og foreslår ved hjelp av denne hvordan Statens vegvesen kan bidra til økt utbredelse av kooperativ ITS eksemplifisert ved RSI. Rapporten gir et verktøy til å systematisere hvilke roller og aktører som inngår i trafikkdata sitt livsløp, og diskuterer hvordan eierskap til data kan defineres og håndteres. Rapporten gir også en oppsummering av kunnskap om trafikanters aksept for å logge og dele transportdata, og viser hvordan forretningsmodeller kan brukes i fremme av ITS.

UTARBEIDET AV
Trond Foss

SIGNATUR

KONTROLLERT AV
Terje Reitaas

SIGNATUR

GODKJENT AV
Roar Norvik

SIGNATUR

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
A27550	9788214060300	Åpen	Åpen

SINTEF

Forord

Denne rapporten presenterer resultatene fra prosjektet *Vegvesenet, Data og Intelligent Transport (VDoIT)*. Prosjektet er gjennomført av SINTEF Teknologi og samfunn avd. Transportforskning på oppdrag av Statens Vegvesen Vegdirektoratet gjennom FoU-programmet *Smartere vegtrafikk med ITS* (SMITS).

Den overordnede målsettingen med prosjektet har vært å gi Statens vegvesen støtte og mer kunnskap rundt såkalte *ikke-teknologiske aspekter* rundt kooperativ ITS og håndteringen av data som genereres fra kooperativ ITS. Prosjektet har besvart problemstillinger knyttet til tre temaområder: i) personvern og aksept, ii) forretningsmodeller og iii) ansvar ved utlevering av data. Prosjektet *Road Status Information (RSI)* er benyttet som eksempel i besvarelse av problemstillingene.

Prosjektgruppen ved SINTEF har bestått av Trond Foss, Kristin Ystmark Bjerkan og Marianne Elvsaas Nordtømme. Forskningsleder Terje Reitaas har vært kvalitetssikrer.

Trondheim, april 2016

Roar Norvik

Forskningssjef

Sammendrag

Denne rapporten inneholder dokumentasjon fra prosjektet *VDoIT – Vegvesenet, Data og Intelligent Transport.* Den overordnede målsettingen med prosjektet har vært å gi Statens vegvesen støtte og mer kunnskap rundt såkalte *ikke-teknologiske aspekter* rundt kooperativ ITS og håndteringen av data som genereres fra kooperativ ITS. Prosjektet har besvart problemstillinger knyttet til tre temaområder: i) personvern og aksept, ii) forretningsmodeller og iii) ansvar ved utlevering av data. Prosjektet *Road Status Information (RSI)* er benyttet som eksempel i besvarelse av problemstillingene.

I løpet av de siste tiårene har transportsystemers sårbarhet fått mer og mer oppmerksomhet. Noen av de mest fremtredende *sikkerhets- og sårbarhetsutfordringene* finnes innen personvern og IKT-sikkerhet, og kan sees både fra et teknologisk og administrativt synspunkt. Som ryggmargen i intelligente transportsystemet samler IKT-systemer inn mye informasjon som kan true personvernet til brukerne. En viktig del av personvernet er brukeraksept, f.eks. tilfeller der brukeren må velge mellom en gitt ITS-applikasjon som gir større sikkerhet og innsamling av data som kan være en trussel mot brukerens personvern. Når det gjelder den teknologiske delen av personvernet er det et viktig prinsipp som heter *personvern gjennom design*. Dette betyr at personvern ivaretas fra dag 1 i utviklingen av ITS-applikasjonen eller –tjenesten og i utviklingen av IKT-systemer som støtter ITS-applikasjonen.

Sikkerhet i intelligente transportsystemer er ikke bare et spørsmål om teknologi, men også et spørsmål om bevissthet og krav blant myndigheter, operatører og brukere. Teknologi kan løse de fleste utfordringer knyttet til sikkerhet og sårbarhet, men i enkelte tilfeller for en langt høyere kostnad enn kostnaden ved den potensielle skaden en uønsket sikkerhetshendelse kan forårsake. Imidlertid bør implementering av teknologien være et resultat av administrative og politiske beslutninger basert på myndigheters, operatørers og brukeres kunnskap og bevissthet.

For å studere hvilket ansvar Statens vegvesen kan pådra seg ved å distribuere trafikkdata i form av rådata, som behandlede data og som ITS tjenester har prosjektet beskrevet *roller og grensesnitt involvert i trafikkdataenes livsløp*. I sine ulike former omtales slike data som trafikkdata, rådata, behandlede data, primærdata, sekundærdata og meldinger. Data kan berøre en rekke roller, som eier av infrastruktur for datainnsamling, kommunikasjonstjenesteyter, trafikkdatabehandler, sekundærdata tjenesteyter, trafikkdata tjenesteyter og trafikkdata bruker. Disse rollene kan ha en eller flere funksjoner, f.eks. å levere en tjeneste, bruke data eller levere data.

Med økende tilfang og bruk av data generert i transportsystemet vil problemstillinger knyttet til *eierskap av data* i stadig større grad også berøre offentlige transportmyndigheter. Dette prosjektet definerer eierskap til trafikkdata slik: *Eieren av trafikkdata er den fysiske personen, organisasjonen eller myndigheten som har skapt et gitt sett med trafikkdata og som kan verifisere at dette settet er sanne og pålitelige. Med trafikkdataeierskap menes retten til å bruke, leie ut, selge, gi bort og destruere trafikkdata.* Prosjektet presenterer et mulig avtaleverk for å regulere eierskap og bruksrett til trafikkdata, der en bilateral eller multilateral avtale primært beskriver rollene og ansvarsforholdene for de ulike typene aktører som slutter seg til verdikjeden for trafikkdata og hvilke rettigheter og plikter som er knyttet til de ulike rollene.

Ett mulig produkt av økende innsamling og bruk av data er prediksjoner både mot det offentlig og mot allmennheten. I dag finnes allerede praksis og erfaringer med deling av prediksjoner basert på offentlige data det er mulig å lære av. I tillegg til vurderinger av *juridisk ansvar* vil det være viktig å vurdere eventuelle *utilsiktede konsekvenser* slike prediksjoner kan gi. Utlevering av prediksjoner og data som grunnlag for

prediksjoner kan endre premissene for trafikanters, transportørers, entreprenørers og andres beslutningstaking og adferd. I forberedelse av utlevering av slik informasjon (og eventuelle data som kan produsere slik informasjon) er det viktig å gjennomgå mulige konsekvenser og særlig eventuelle uønskede hendelser det kan gi. Det finnes en rekke metoder for å vurdere risiko og uønskede hendelser, og i en forenklet versjon av grovanalyse beskriver en matrise sannsynlighet for at en uønsket hendelse oppstår og konsekvensen dersom den skulle oppstå.

Deling av data mellom de involverte aktørene er en grunnleggende faktor i kooperative ITS-løsninger. Det medfører behov for å studere en rekke problemstillinger knyttet til personers *villighet til å dele* og *aksept for å dele data* om blant annet egen reise- eller kjøreadferd. Noen studier rapporterer brukeraksept av innsamling av GPS-baserte reisedata. Et norsk prosjekt om kollektivreisende deling av egne reisedata, SMiO-prosjektet, viser at 60 % er positive til å dele egne reisedata gjennom en mobilapplikasjon. Det fremgår også at kollektivreisende har stor tillit til programmer som registrerer deres reisemønster, og at personvern ikke er en fremtredende bekymring ved deling av reisedata. I prosjektet Non-stop angir yrkessjåfører hvor villig de er til å dele ulike data om seg selv og kjøretøyet automatisk dersom det medfører at de kan passere kontrollstasjon uten å stanse. Mellom 58-74 % av sjåførene ønsker å dele de ulike data. Med bakgrunn i kjente akseptstudier innen transport generelt og for ITS-tiltak spesielt, kan man skissere en teoretisk forklaringsmodell for hva som vil påvirke holdninger til å dele data, der formålet med deling av data er økt trafikksikkerhet. Hovedessensen i modellen er at bakenforliggende variabler som kjønn, alder og utdanning mv. påvirker holdninger til personvern (*vil mitt behov for personvern bli ivaretatt på en måte som er tilfredsstillende for meg?)* og holdninger til trafikksikkerhet (*er glatte veger et problem for trafikksikkerheten og er dette noe jeg er opptatt av?).*

Fordi kooperative ITS–løsninger antas å ha stort potensiale for å løse utfordringer i transportsystemet er det viktig å synliggjøre for aktører i posisjon til å beslutte og/eller påvirke virkemiddelbruk verdier (gevinster) kooperative ITS løsninger kan gi og hvordan disse kan innhentes. For å synliggjøre verdier (gevinster) og forutsetninger for å realisere disse er det hensiktsmessige å definere à priori forretningsmodeller. En forretningsmodell beskriver begrunnelsen for hvordan en organisasjon skaper, leverer, og fanger verdi, og Osterwalder og Pigneurs anerkjente modell definerer ni byggesteiner. Generering, håndtering og bruk av data kjent som PSI (Public Sector Information) er et omfattende temaområde som de siste årene har sett økende interesse fra både praksisfelt og forskning, og som til en viss grad er forsøkt knyttet til særskilte forretningsmodeller for slik data. Disse fokuserer i stor grad på å kvantifisere verdien av offentlige data og å identifisere hvordan organisasjoner kan gjøre forretning av denne type data. Verdien av data er uløselig knyttet til den informasjonen den kan skape og attributter ved informasjonen som bidrar til å skape verdi.

Summary

This report includes documentation from the project VDoIT. The overall objective has been to provide the National Public Roads Administration (NPRA) support and knowledge about non-technological aspects of cooperative ITS and handling data from cooperative ITS. The project has addressed three issues: i) privacy and acceptability, ii) business models and iii) responsibility related to sharing data. The project Road Status Information (RSI) is used as an example in addressing these issues.

Over the past decades, transport system vulnerability has gained more and more attention. Some of the most prominent security and vulnerability challenges are found in *privacy and ICT security*, and can be seen both from a technological and administrative point of view. As the spinal cord in intelligent transportation system, ICT systems collect a lot of information that could endanger user privacy. An important aspect of privacy is user acceptability, eg. instances where the user must using an ITS application which provides greater safety against allowing access to data that can threaten his or her user privacy. An important principle related to technological privacy is privacy by design. This means that privacy is protected from day one in the development of ITS application or services, and in the development of ICT systems that support the ITS application.

Security in intelligent transport systems is not just a matter of technology, but also a matter of awareness and requirements from authorities, operators and users. Technology can solve most challenges related to security and vulnerability, but in some cases with a far higher cost than the cost of potential damage by an unwanted security incident. However, implementation of technology should result from administrative and political decisions based on authorities, operators and users' knowledge and awareness.

To study what responsibilities the NPRA may incur by distributing raw traffic data, processed data and ITS services, the project has described *roles and interfaces involved in the life cycle of traffic data*. In its various forms, such traffic data are referred to as raw data, processed data, primary data, secondary data and messages. Data can engage with a variety of roles; data capture infrastructure owner, communication service provider, traffic data processor, secondary data service provider, traffic data service provider and traffic data user. These roles may have one or more functions, for example to deliver a service, to use the data or to supply data.

With an increasing amount and use of data generated in the transportation system, issues related to ownership of data will increasingly also affect transport authorities. This project defines ownership of traffic data as follows: The owner of traffic data is the physical individual, organisation or authority that has created a given set of traffic data and can verify that these are true and reliable. Traffic data ownership means the right to use, rent, sell, give away and destroy traffic data. The project presents a possible agreement to regulate the ownership and use of traffic data, where a bilateral or multilateral agreement describes the roles and responsibilities of the different actors in the value chain of traffic data, as well as the rights and obligations that relate to the different roles.

One possible result of increasing collection and use of data are predictions, and there are several examples that can provide practices and experiences with sharing predictions based on public data. In addition to assessing legal responsibility, it will be important to consider possible unintended consequences such predictions can produce. Publishing predictions and data as a basis for predictions can change the preconditions under which road users, carriers, contractors and others make decisions. In preparing publication of such information (and any data that can produce such information), it is important to review possible consequences and in particular any unwanted incidents. There are a variety of methods to assess

risks and unwanted incidents, and simplified preliminary hazard analysis uses a matrix to describe the probability of an incident occurring and the consequences that might occur.

Data sharing is a fundamental factor in cooperative ITS solutions. It implies the need to study issues relating to people's willingness to and acceptability of sharing data about for instance travel or driving behaviour. Some studies report user acceptability of collecting GPS-based travel data. A Norwegian project on public travellers who report own travel data, the SMIO project, shows that 60% are positive to share their own travel data through a mobile application. It also shows that public transport travellers have great confidence in mobile applications that register their travel patterns, and that privacy is not a prominent concern in sharing travel data. In the NonStop project, professional drivers indicate how willing they are to share various data about themselves and the vehicle automatically if it means that they can pass control stations without stopping. Between 58 and 74% of the drivers wish to share different types of data. Based on the known acceptability studies in transport and ITS one can outline a theoretical explanation model with factors that influence attitudes toward sharing data when doing so increases traffic safety. The essence of the model is that underlying variables such as gender, age and education, etc. affects attitudes towards privacy (will my need for privacy be addressed in a way that is satisfactory to me?) and attitudes to road safety (slippery roads are a problem for road safety and this is something I am concerned about?).

Because cooperative ITS solutions are believed to have great potential for solving challenges in the transport system, it is important to demonstrate the values (gains) of cooperative ITS applications and how these can be obtained. To visualize value (gains) and prerequisites for realizing these it is appropriate to define an à priori business models. A business model describes the rationale of how an organisation creates, delivers, and captures value, and Osterwalder and Pigneurs highly acknowledged model defines nine building blocks. Generation, handling and use of data known as PSI (Public Sector Information) is a complex subject area which in recent years has seen increasing interest from both professional practice and research, and is to some extent associated with specific business models for such data. These focus largely on quantifying the value of public data and identifying how organizations can make business out of this type of data. The value of data is inextricably linked to the information it can create and valuable attributes of the information.

SINTEF

Innholdsfortegnelse

TABELLISTE

FIGURLISTE

1 Innledning

Denne rapporten inneholder dokumentasjon fra prosjektet *VDoIT – Vegvesenet, Data og Intelligent Transport*. VDoIT har som mål å bidra til vellykket implementering av kooperative ITS-løsninger, i tråd med målene i Nasjonal transportplan. Dette er søkt oppnådd gjennom å gi Statens vegvesen støtte og mer kunnskap rundt såkalte *ikke-teknologiske aspekter* rundt kooperativ ITS og håndteringen av data som genereres fra kooperativ ITS.

Følgende problemstillinger ligger til grunn for VDoIT:

- *Personvern og aksept:*
  - Hvilke krav må man stille til systemer som skal motta og prosessere data fra kjøretøy dersom data er å oppfatte som personopplysninger?
  - Hvor villig er befolkningen til å dele data med andre trafikanter og med Statens vegvesen?
- *Forretningsmodeller:*
  - Hvordan kan forretningsmodeller for kooperative ITS-løsninger og implementering av disse se ut?
  - Finnes det gode verktøy for å utvikle/vurdere alternative forretningsmodeller?
- *Ansvar ved utlevering av data:*
  - Hvilket ansvar kan Statens vegvesen pådra seg ved å gi ut prediksjoner til trafikanter?
  - Hvem er til enhver tid eier av trafikkdata som genereres, samles inn og behandles?
  - Finnes det rammeverk som kan benyttes for å i størst mulig grad avdekke uintenderte konsekvenser?

For å belyse problemstillingene i VDoIT på en måte som er mest mulig relevant for Statens vegvesen, er et av etatens pågående prosjekter valgt som case. Dette er FoU-prosjektet *Road Status Information (RSI)*, hvor Statens vegvesen, NTNU og SINTEF ønsker å samarbeide med kjøretøyprodusenter for å hente data om vegens friksjonsforhold fra bilen (V2X). I det pågående RSI-prosjektet etableres en demonstrasjon hvor man benytter kjøretøy solgt av Volvo i Norge, men fordi problemstillingene i prosjektet er relevante uansett hvilken kjøretøyprodusent det er snakk om, er presentasjoner i rapporten ikke knyttet til en bestemt kjøretøyprodusent.

Denne rapporten består av syv kapitler. Det første kapittelet løfter frem relevante og aktuelle problemstillinger knyttet til sårbarhet, personvern og sikkerhet i IKT systemer. Kapittel 3 og 4 viser trafikkdatas livsløp og eierskap. Hensikten med disse kapitlene er å beskrive roller og grensesnitt involvert i trafikkdataenes livsløp, samt å vurdere hvordan eierskap til data endres underveis i livsløpet. Kapittel 4 avsluttes med bemerkninger rundt ansvar ved deling av data fra Statens vegvesen.

Kapittel 5 gjør rede for foreliggende kunnskap om personers villighet til og aksept for å dele eller logge egne reise- og trafikkdata.

Kapittel 6 gir en innføring i rammeverk for utvikling av forretningsmodeller, med særlig fokus på modeller for gjenbruk av åpne, offentlige data. I tillegg beskriver kapittelet arbeidet med å utvikle en forretningsmodell for RSI-prosjektet.

Rapporten avsluttes med oppsummering og konklusjon.

2 Personvern, data og ITS

2.1 Økt sårbarhet

I løpet av de siste tiårene har transportsystemers sårbarhet fått mer og mer oppmerksomhet. Transportsystemer blir mer integrerte og hendelser eller brudd i et transportsystem kan ha en innvirkning på andre transportsystemer. For eksempel kan sammenbrudd i metrosystemet forårsake sammenbrudd i byens vegnett. Endringer i klima kan også forårsake hendelser og gir nye utfordringer for transportsystemer, for eksempel flom og jordskred. Sist, men ikke minst, er terrorisme en ny trussel mot transportsystemer gjennom at angrep mot transportinfrastruktur og/eller transportmidler kan føre til store skader og tap av menneskeliv. Slike angrep kan i verste fall sette et eller flere transportsystemer helt ute av drift i lengre perioder. Med innføring av ITS vil ikke potensielle angriperes mål nødvendigvis endres, men heller angriperens evne til å angripe. Ufrivillige handlinger og svikt i ITS kan også forårsake alvorlige avbrudd og brukerfrustrasjon. Alle transportformer (luft, vei, jernbane og sjø) blir møtt med utfordringer knyttet til personvern og sikkerhet som ITS bringer med seg. Sikkerhetsperspektivet i ITS er fortsatt på et tidlig stadium (Whyte 2012), og mye må gjøres med tanke på design, standardisering, programvarearkitektur, tjenesteyting og sikkerhetsadministrasjon.

Intelligente transportsystemer (ITS) er transportsystemer der informasjon og kommunikasjonsteknologi (IKT) brukes for å oppnå mer trygg, sikker, effektiv og miljøvennlig transport av personer og gods. ITS-applikasjoner for sikkerhet og beredskap i vegtrafikken er ett av fire satsingsområder i det europeiske ITS-direktivet (EU 2010). Det er et paradoks at ITS-applikasjoner kan gjøre transportsystemer mindre trygge og sikre, f.eks. ved dårlig kvalitet på informasjon eller kommunikasjon, eller når nødvendig informasjon ikke er tilgjengelig på grunn av systemfeil eller angrep fra hackere eller terrorister. Sårbarheten i intelligente transportsystemer øker etter hvert som disse systemene blir mer integrerte og avanserte.

Økt kompleksitet og sårbarhet i kjølvannet av ITS krever nye retningslinjer og forvaltningsperspektiver. Det er viktig å skape bevissthet, innføre presise mål og oppdatere lovverket til å reflektere den nye virkeligheten. For eksempel er det et økende behov for å ta hensyn til nødvendig reservekapasitet i håndtering av feil i andre transportsystemer. Det er også viktig å være bedre forberedt på hendelser som sjelden eller aldri inntraff tidligere.

Noen av de mest fremtredende sikkerhets- og sårbarhetsutfordringene finnes innen personvern og IKT-sikkerhet, og kan sees både fra et teknologisk og administrativt synspunkt.

2.2 Personvern

Som ryggmargen i intelligente transportsystemet samler IKT-systemer inn mye informasjon som kan true personvernet til brukerne. Det europeiske ITS-direktivet (2010/40 / EU) slår fast at medlemsstatene skal sikre at behandlingen av personopplysninger i forbindelse med driften av ITS-applikasjoner og ITS-tjenester utføres i samsvar med unionens regler for å beskytte enkeltpersoners grunnleggende rettigheter og friheter. Videre skal medlemsstatene sikre at personopplysninger beskyttes mot misbruk, herunder ulovlig tilgang, endring eller tap av opplysninger. Det synes imidlertid å være et gap mellom lovgivning og implementering av ny teknologi og tjenester (Aquilina 2010). Teknologien utvikles i et høyt tempo og på en diffus måte uten å ta hensyn til personvernet. Lover og forskrifter om personvern er ikke tilstrekkelig detaljert og tar ikke tilstrekkelige skritt for å håndtere trusselscenarier i kjølvannet av raske teknologiske fremskritt(Aquilina 2010). En viktig del av personvernet er brukeraksept, f.eks. tilfeller der brukeren må velge mellom en gitt ITS-applikasjon som gir større sikkerhet og innsamling av data som kan være en trussel mot brukerens

personvern. En undersøkelse blant bilførere med ISA i Norge, Sverige og Danmark (Eriksson og Bjørnskau 2012) viste at bileiere hadde lite kunnskap om ITS applikasjoner, selv om aksepten for ITS applikasjonene var relativt høy. Det ble bemerket at hendelsesdataopptakeren (EDR) ble oppfattet å være en større trussel mot personvernet enn gjennomsnittlig hastighetskontroll og ISA-applikasjonen.

Når det gjelder den teknologiske delen av personvernet er det et viktig prinsipp som heter *personvern gjennom design*. Dette betyr at personvern ivaretas fra dag 1 i utviklingen av ITS-applikasjonen eller –tjenesten og i utviklingen av IKT-systemer som støtter ITS-applikasjonen. Det er begrenset kunnskap rundt hvordan slike prinsipper etterleves i fremtidige ITS-applikasjoner og -tjenester, og ett av målene for fremtidig forskning kan være å finne tiltak som støtter myndighetene i å sikre personvern gjennom design og lignende personvernfremmende tiltak. Noen eksempler på personvernfremmende tiltak er teknologiske og organisatoriske tiltak som begrenser uvedkommendes muligheter til å identifisere en person eller få tilgang til individuell informasjon. Andre tiltak er depersonalisering av informasjon, autentisering, autorisasjon (adgangskontroll) og krypteringsteknikker (Øvstedal m.fl. 2010).

2.3 IKT-sikkerhet

Det er mange forskningsartikler og bøker om sikkerhet i IKT-systemer, men svært få er knyttet til IKT-systemer i transportsektoren. Derfor synes det å være behov for mer kunnskap om hvorvidt generelle funn for IKT-systemer også gjelder ITS- applikasjoner og -tjenester. Ofte er sikkerhets- og sårbarhetsaspekter i vegtransport knyttet til kjøretøyets IKT-system og nettverket av samarbeidende elektroniske styringsenheter (eng. Electronic Control Unit (ECU)). Hoppe (2011) beskriver hvordan økende kompleksitet og ekstra funksjonalitet stadig kan friste angripere til å misbruke disse systemene og hvordan økt utveksling av informasjon mellom kjøretøy og kommunikasjonsinfrastruktur utenfor kjøretøyet kan misbrukes. For eksempel har en teknikk for å sende falsk trafikkinformasjon til kjøretøyets navigasjonssystem allerede blitt demonstrert. Det er også flere hjemmesider for hackere (og potensielle aktivister), for eksempel www.canbushack.com og www.hackaday.com, som gir detaljert informasjon om hvordan du får tilgang til ECUs og CANBUS nettverk innebygd i bilen og dermed får tilgang til kjøretøyets interne nettverk. Å utvikle tiltak for å imøtekomme disse truslene er også gjenstand for forskning. Raya, M. og kolleger (2005) fokuserer både på nettverk i kjøretøyet og kommunikasjon mellom kjøretøy og veg, og beskriver sikkerhetsmekanismer for å redusere trusler mot slike systemer. Innføringen av CALM-standarder for V2X kommunikasjon har åpnet for nye kommunikasjonskanaler mellom kjøretøy og infrastruktur (f.eks. vegkantinstallasjoner) i tillegg til den tradisjonelle Dedicated Short Range Communication (DSRC). Zelinka m.fl. (2011) fokuserer på sårbarhet ved å kombinere nettverk i kjøretøyet og nettverk med luftgrensesnitt , og foreslår en metode for gjensidig godkjenning mellom kjøretøy og vegkantutstyr.

Ruy og kolleger (2009) har vist hvordan sanntids industrielle prosesskontrollsystemer (ofte referert til som SCADA-systemer) kan redusere sårbarheten i kritiske infrastrukturer, inkludert offentlige transportsystemer. I kritiske infrastrukturer generelt, blir SCADA-systemer stadig basert på kommersielle hyllevarekomponenter (for eksempel Microsoft Windows) og åpne protokoller, og er koblet til andre systemer levert av operatør eller leverandør. Dette gjør det mulig for hackere eller aktivister å angripe SCADA-systemer. Nicholson m.fl.(2012) gir en oversikt over truslene mot SCADA-systemer.

2.4 Interessenter, sikkerhet og sikkerhetsbevissthet

Sikkerhet i intelligente transportsystemer er ikke bare et spørsmål om teknologi, men også et spørsmål om bevissthet og krav blant myndigheter, operatører og brukere. Teknologi kan løse de fleste utfordringer

knyttet til sikkerhet og sårbarhet, men i enkelte tilfeller for en langt høyere kostnad enn kostnaden ved den potensielle skaden en uønsket sikkerhetshendelse kan forårsake. Imidlertid bør implementering av teknologien være et resultat av administrative og politiske beslutninger basert på myndigheters, operatørers og brukeres kunnskap og bevissthet.

Innføringen av et nytt reisekort for kollektivtrafikanter og elektronisk avgiftsinnkreving for trafikanter i Nederland har vært en politisk sak i mange år, og vegen videre har hatt noen politiske hindringer. Jacobs (2010) diskuterer sammenhengen mellom IKT-arkitektur og politiske fora. IKT-arkitekturen styrer informasjonsflyt i et IKT-system og bestemmer hvem som kan se hva om hvem. Siden kunnskap om andre gir en sterkere posisjon og dermed mer makt, er IKT-arkitektur i høyeste grad et politisk anliggende. Dette innebefatter at makt gitt gjennom IKT arkitektur best diskuteres og avgjøres innen politiske fora, slik som parlamenter. Dessverre virker det å være lite bevissthet rundt følsomheten i disse sakene. I praksis tas beslutninger på forskjellige steder, for eksempel i styrerom, i departementene, via tjenestemenn, konsulenter og lobbyister. De som er i maktposisjoner vegrer seg mot å velge arkitekturer som reduserer deres makt. Så hvem forsvarer interessene til den enkelte borger og prøver borgernes selvråderett?

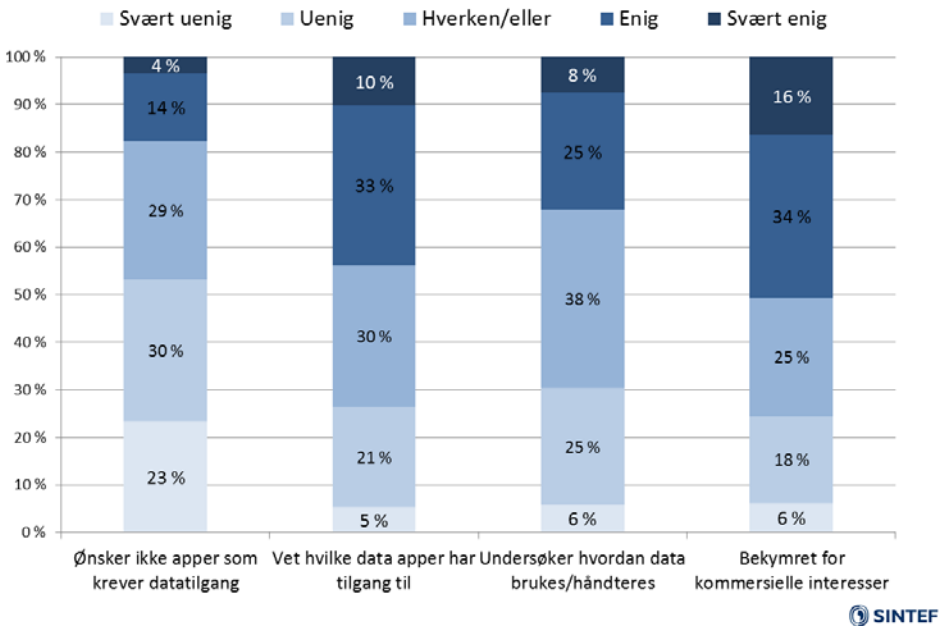
En undersøkelse blant norske transportoperatører (Øvstedal 2009) viste at de fleste kollektivtransportselskaper er bevisste mht. personvernproblematikk i egen drift. Hovedmotivasjonen bak dette er operatørens omdømme. Undersøkelsen viste også at ansatte var bevisst personvern, men at ikke alle av dem var fullt klar over hvordan eget arbeid og prosedyrer inngikk i personvernprofilen til operatøren.

Brukerbevissthet om sikkerhet og sårbarhet i IKT-systemer inngår i en rekke forskningsprosjekter. Disse prosjektene er imidlertid urovekkende få sammenlignet med det store antallet forskningsprosjekter som belyser sikkerhet og sårbarhet i transportsystemer. Potoglou og kolleger (2010) stiller et svært avgjørende spørsmål om balansen mellom sikkerhet, personvern og frihet i et case med UK Rail. Deres viktigste forskningsspørsmål var " i hvilken grad folk ville ofre sin rett til privatliv og frihet i bytte mot en tryggere og sikrere reise? "Analysen av den landsomfattende undersøkelsen viste viktigheten av forbedringer i sikkerhetsinfrastruktur og identifiserte områder av bekymring med hensyn til personvern og frihet, kontrollert for reiserelaterte faktorer. Analysen kvantifiserte også enkeltpersoners vilje til å betale ekstra for trygghet og sikkerhet på toppen av den gjennomsnittlige billettprisen.

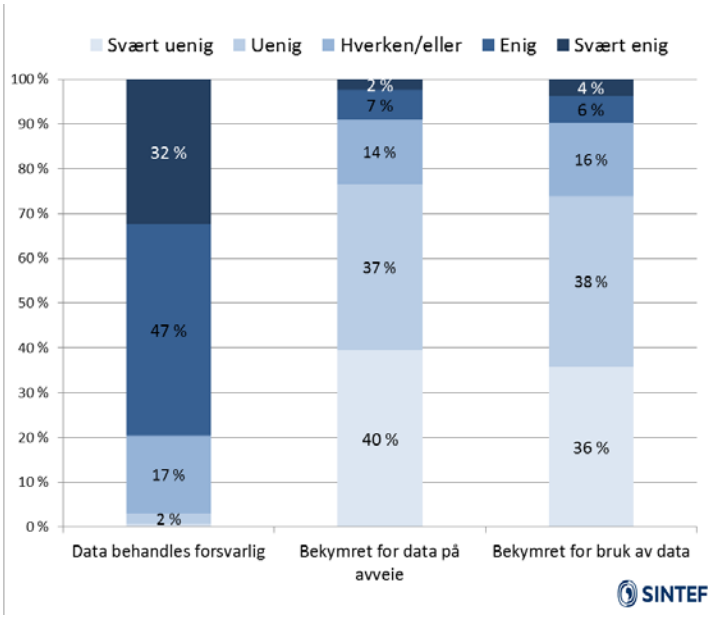
2.5 Erfaringer med personvern og deling av egne reisedata

I prosjektet Smidig Mobilitet i Oslo (SMiO) (også omtalt i kap. 5.2) kartlegges blant annet hvordan et utvalg kollektivreisende i Oslo og Akershus opplever personvern knyttet til å gi fra seg data om egne reiser i en GPS-basert mobilapplikasjon. Under gjengis deres opplevelse av og bekymringer knyttet til personvern ved deling av egne reisedata.

Figur 1 viser at 82 % er åpne for å laste ned programmer som krever tilgang til data på telefonen deres. Likevel vet under halvparten av de spurte hvilke data programmer faktisk har tilgang til, og enda færre undersøker hvordan data de deler skal brukes eller kommer til å håndteres. Halvparten er videre bekymret for at kommersielle interesser har adgang til data. På tross av denne bekymringen tyder resultatene på begrenset bevissthet rundt deling av egne data, og ikke nødvendigvis samsvar mellom den enkeltes bekymringer og aktiv undersøkelse rundt hvilke data som deles og hvordan de brukes.



Figur 1. Hvor enig er du i følgende påstander: jeg ønsker ikke å laste ned applikasjoner som krever tilgang til data på telefonen min, jeg vet alltid hvilke data applikasjoner på min telefon har tilgang til, jeg undersøker alltid hvordan data fra applikasjoner på mobiltelefonen brukes og håndteres, jeg er bekymret for at kommersielle interesser har tilgang til ulike dataregistre (N=231)



Figur 2. Hvor enig eller uenig er du i at du er trygg på at data fra applikasjonen håndteres forsvarlig og i tråd med personvernlovgivningen, du er bekymret for at data skal komme på avveie, og du er bekymret for at data skal brukes til andre formål? (N=231)

Det samme prosjektet viser at kollektivreisende har stor tillit til programmer som registrerer deres reisemønster. Figur 2 viser hvordan de opplever den applikasjonen som ble brukt til registrering i SMiO-prosjektet. Et stort flertall føler seg trygge på at data behandles forsvarlig, og en liten andel (≤ 10 %) er bekymret for at data skal komme på avveie eller brukes til andre formål enn det spesifisert i prosjektet.

Dette viser at personvern ikke er en fremtredende bekymring blant personer som har eller er forespurt om å registrere egen reiseadferd.

3 Livsløp for trafikkdata

3.1 Innledning

Hensikten med dette kapitlet er å beskrive de ulike rollene og grensesnittene som er involvert i trafikkdataenes livsløp. Dette skal videre brukes for å studere hvilket ansvar Statens vegvesen kan pådra seg ved å distribuere trafikkdata i form av rådata, som behandlede data og som ITS tjenester, f.eks. i form av trafikkinformasjonsmeldinger om status og forventet status (prediksjon).

Kapittelet benytter rolle- og ansvarsmodellen som er beskrevet i Foss (2015b).

3.2 Begrepsavklaringer

Begrepet ***Trafikkdata*** slik det er brukt i denne rapporten dekker bl.a. følgende informasjon:

- Informasjon om objekter som benytter transportsystemet hvor informasjonen kan være knyttet til enkeltobjekter, f.eks. kjøretøy, eller til strømmer av objekter, f.eks. en strøm av fotgjengere. Informasjonen kan samles inn både ved hjelp av informasjon fra selve objektet eller fra sensorer tilknyttet den infrastrukturen som inngår i transportsystemet.
- Informasjon om selve transportinfrastrukturen, f.eks. temperatur i vegdekket/overbygning og status på overflate dekke, f.eks. våt, is- eller snødekket. Det kan også omfatte informasjon som sier noe om siktforhold i transportinfrastrukturen. Denne informasjonen kan samles inn ved hjelp av sensorer tilknyttet infrastrukturen, fra kjøretøyer som benytter infrastrukturen og som har sensorer som kan registrere informasjon om infrastrukturen og fra trafikanter som benytter infrastrukturen.

Begrepet ***Rådata*** i denne rapporten betyr informasjon slik det foreligger i sin opprinnelige form. Det vil f.eks. si informasjon om en observasjon eller registrering av objekter eller infrastrukturen før vi har begynt å sortere, gruppere og analysere de innsamlede dataene. Data som beskriver *ett* kjøretøys hastighet, vekt, antall akslinger og avstand til forankjørende kjøretøy er et eksempel på rådata.

Begrepet ***Behandlede data*** betyr i denne rapporten rådata som er sortert, gruppert og analysert. Dersom vi f.eks. samler rådata fra kjøretøy over en time for deretter å beregne gjennomsnittlig hastighet for alle kjøretøyer, antall kjøretøyer i hver vektklasse, antall akslinger i hver vektklasse og gjennomsnittlig avstand til forankjørende kjøretøy er dette Behandlede data.

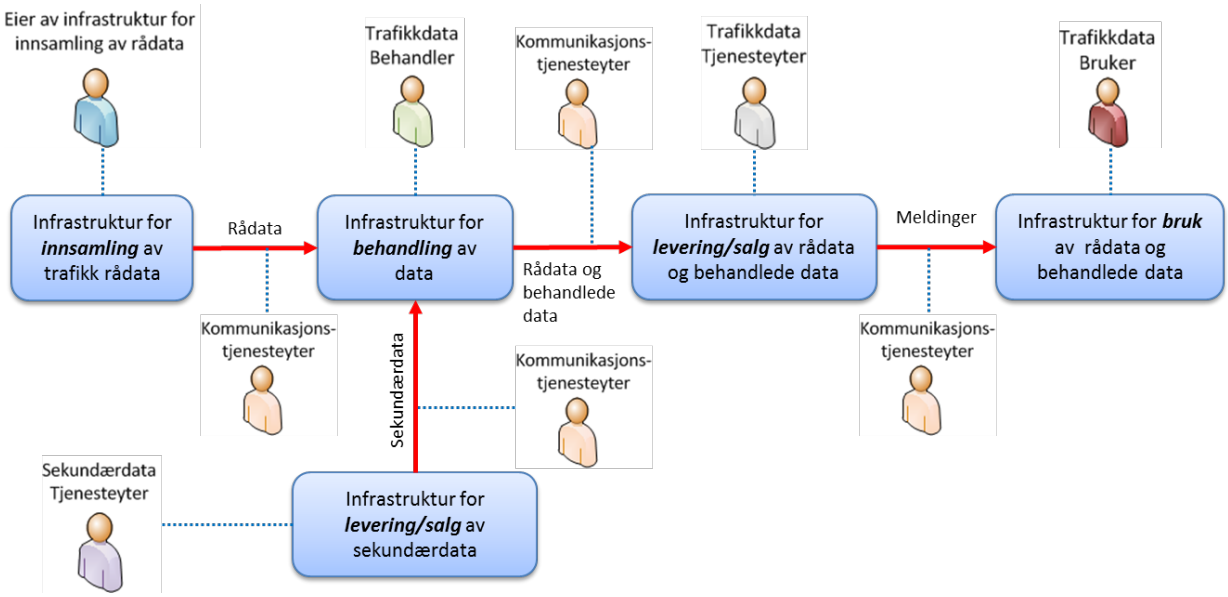
Begrepet ***Primærdata*** er all informasjon som kan regnes som Trafikkdata. ***Sekundærdata*** er all annen informasjon som ikke knyttes til objekter i transportsystemet eller til transportinfrastrukturen. Et eksempel på slike sekundærdata er meteorologiske data, f.eks. i form av værprognoser.

Begrepet ***Meldinger*** omfatter den informasjonen som sendes til sluttbrukeren, dvs. Trafikkdata bruker. Meldinger kan omfatte både Primærdata og Sekundærdata i form av behandlede data på et brukergrensesnitt tilpasset den enkelte bruker og den kan i enkelte tilfeller inneholde rådata. Meldingene kan gjerne deles inn i informasjonsmeldinger og styringsmeldinger. Et eksempel på det siste er en melding fra en VTS til alle bilførere om en pålagt omkjøring eller nedsatt fartsgrense pga. en hendelse.

3.3 Trafikkdatas livsløp

Figur *3* viser en overordnet beskrivelse av trafikkdatas livsløp som er delt inn i fire hovedprosesser som igjen er knyttet til den infrastrukturen som støtter utførelsen av hovedprosessene:

- Innsamling av Trafikk rådata
- Behandling av data, både Trafikk rådata og sekundærdata fra andre tjenesteytere
- Levering/salg av rådata og behandlede data
- Bruk av behandlede data i form av informasjons- og styringsmeldinger



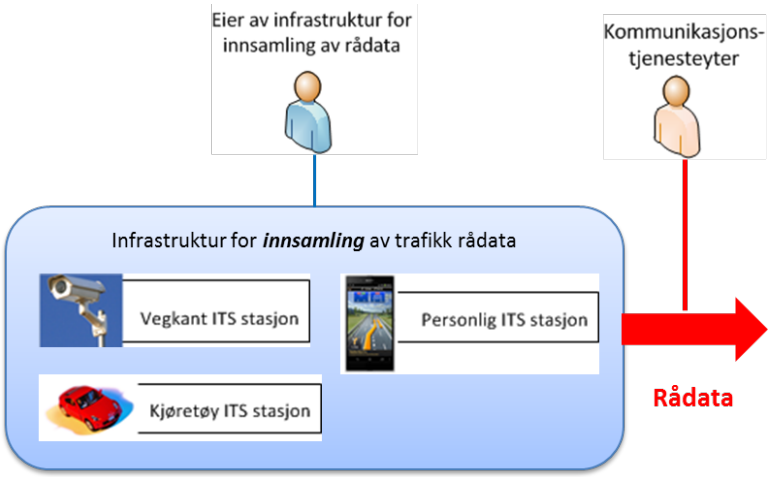
Figur 3: Oversikt over trafikkdata livsløp

Det vil være 6 ulike roller knyttet til livsløpet for trafikkdata:

Eier av infrastruktur for innsamling av rådata vil eie (og drive) den utrustningen som brukes til å observere og/eller registrere informasjon om objekter i transportsystemet og selve transportinfrastrukturen. Eksempler på slik infrastruktur er:

- Vegkant ITS stasjon. Her vil eier av infrastruktur gjerne være vegholder, f.eks. Statens vegvesen, fylkeskommuner og kommuner. Vegholders ansvarsområder vil omfatte planlegging, etablering og drift/vedlikehold av vegkantstasjonen. Vegkantstasjonen vil samle inn rådata gjennom egne sensorer og gjennom kommunikasjon med Kjøretøy ITS stasjon eller Personlig ITS stasjon som passerer eller oppholder seg i nærheten av vegkantstasjonen.
- Kjøretøy ITS stasjon med bileier som eier av infrastruktur. Rådata vil gjerne være informasjon fra kjøretøyets egne sensorer og interne IKT system via CAN-bus. Det er utvilsomt bileier som eier infrastrukturen, men det kan være mer uklart hvem som eier de rådataene som kjøretøyet produserer.
- Personlig ITS stasjon, f.eks. en smarttelefon hvor eieren (evt. brukeren) vil være eier av infrastruktur. Rådata vil gjerne være informasjon om ITS stasjonens bruker, f.eks. hvordan brukeren

har syklet eller gått en rute i transportsystemet. Også her er eierskapet til infrastrukturen hevet over enhver tvil, men eierskapet om rådata som genereres kan være mere uklart.



Figur 4: Oversikt over infrastruktur for innsamling av rådata

Kommunikasjonstjenesteyter har følgende ansvarsområder:

- Flytte informasjon fra en avsender til en mottaker på en måte som sikrer at data:
  - bare kan aksesseres av autoriserte aktører
  - beholder sin integritet mellom avsender og mottaker
  - er tilgjengelige når mottaker trenger informasjonen

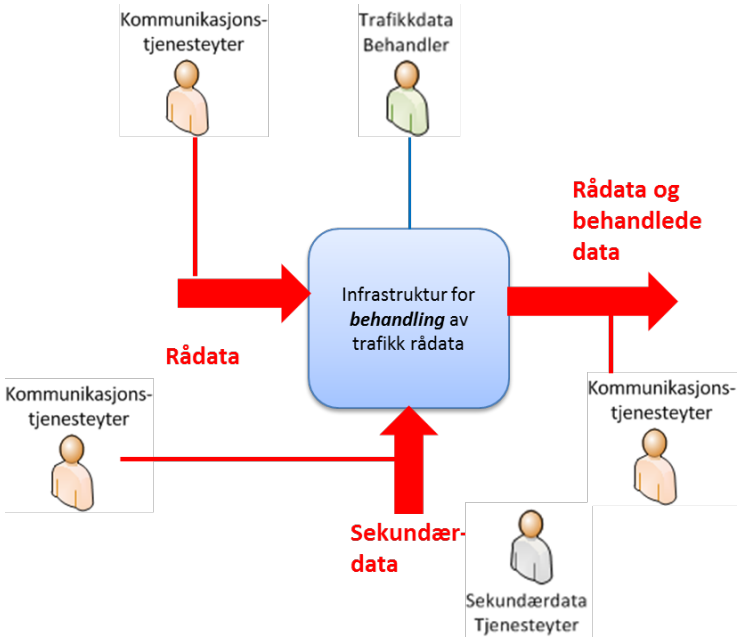
Det vil være flere grensesnitt i et system som samler inn data, behandler data og som tilbyr data/informasjon til sluttbruker. I alle disse grensesnittene vil det være tjenesteytere som transporterer informasjonen i sine egne kommunikasjonssystemer. Et typisk eksempel vil være en teleoperatør som transporter informasjon gjennom et trådløst nettverk, f.eks. GSM.

Trafikkdata behandler har følgende ansvarsområder:

- Planlegge og forberede gjennomføringen av innsamling av data som kan både være rådata og sekundærdata fra andre datatjenesteytere. Det er viktig å skille mellom Eier av infrastrukturen for innsamling av rådata og Trafikkdata Behandler. Den første rollen eier og driver infrastrukturen hvor rådata samles inn, mens den andre rollen er den som har ansvaret for selve innsamlingen av rådata. I mange tilfeller er dette en og samme aktør, f.eks. Statens vegvesen. I andre tilfeller er det forskjellige aktører, f.eks. en eier av en smarttelefon (eier av infrastruktur) med en applikasjon som samler inn data og en forskningsinstitusjon (trafikkdata behandler) som mottar dataene fra applikasjonen i smarttelefonen og lagrer data på sin egen server (infrastruktur for behandling av data).
- Gjennomføre og styre utførelsen av datainnsamlingen
- Kontrollere kvaliteten på dataene som er samlet inn
- Gjennomføre eventuell sortering, gruppering, sammenkopling med andre data og analysering av data
- Levere de behandlede data og/eller rådata til Trafikkdata tjenesteyter iht. det tjenesteyter har etterspurt enten selv eller via Trafikkdata bruker.

- Inngå avtale med Eier av infrastruktur for innsamling av rådata og eventuell betaling for rådata. Dette gjelder bare i de tilfellene Eier av infrastruktur og Trafikkdatabehandler er to ulike juridiske personer.
- Inngå avtale med Trafikkdata tjenesteytere om levering av trafikkdata og eventuell betaling for trafikkdata. Dette gjelder bare i de tilfellene Trafikkdatabehandler og Trafikkdata tjenesteyter er to ulike juridiske personer.

Typiske aktører som har denne rollen vil være Statens vegvesen, bykommuner, bilprodusenter, flåteoperatører og leverandører av mobilapplikasjoner hvor utvikleren både er Trafikkdata Behandler og Trafikkdata tjenesteyter.



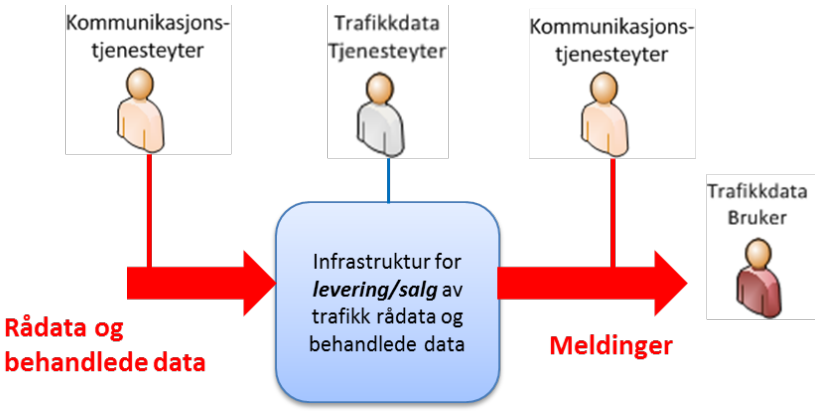
Figur 5: Oversikt over infrastruktur for behandling av rådata og sekundærdata

Sekundærdata tjenesteyter har følgende ansvarsområder:

- Utarbeide produktbeskrivelser for sekundærdata basert på brukerens krav. Et typisk eksempel på sekundærdata er værdata levert av et meteorologisk institutt.
- Definere og markedsføre tjenesten som skal tilbys brukerne, i dette tilfellet innsamlede og kontrollerte sekundærdata. Data kan gjerne leveres som generelle meldinger, f.eks. en værmelding.
- Inngå avtale med Trafikkdata behandler om levering av sekundærdata og eventuell betaling for sekundærdata
- Overvåke kvaliteten på innsamlingen og etterkontrollen av data slik at dataene har den kvaliteten som brukerne krever.

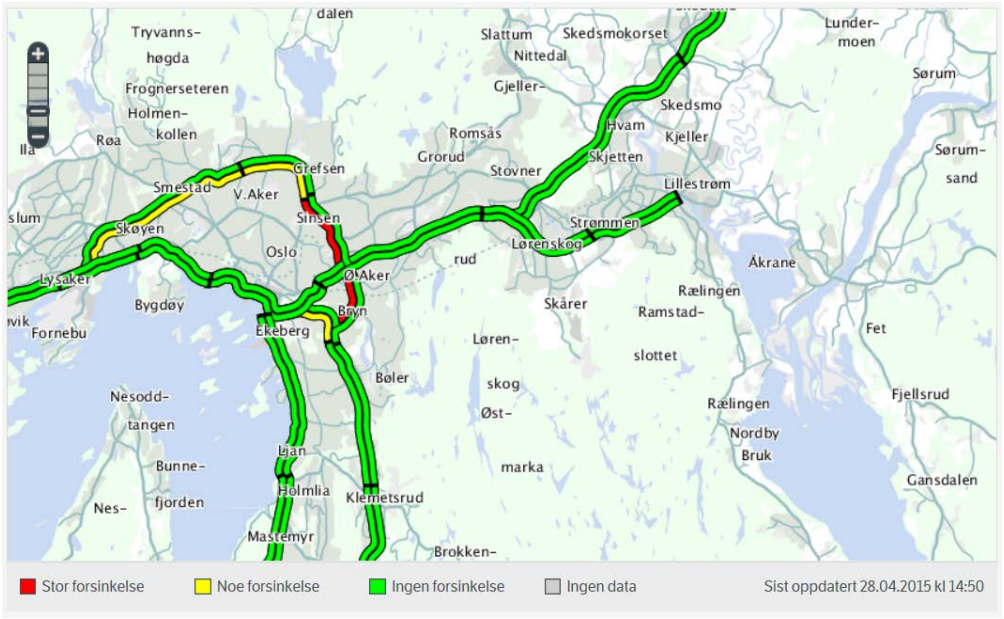
Trafikkdata tjenesteyter har følgende ansvarsområder, jfr. Figur 6:

- Utarbeide produktbeskrivelser for trafikkdata basert på brukerens krav, etterspørsel eller spesifikasjoner
- Definere og markedsføre tjenesten som skal tilbys brukerne, i dette tilfellet innsamlede og kontrollerte trafikkdata. Data kan gjerne leveres som trafikkinformasjonsmeldinger.
- Inngå avtale med Trafikkdata brukere om levering av trafikkdata (meldinger) og eventuell betaling for trafikkdata
- Inngå avtale med Trafikkdata Behandlerne som samler inn data om levering av trafikkdata og eventuell betaling for trafikkdataene.
- Overvåke kvaliteten på innsamlingen og etterkontrollen av data slik at dataene har den kvaliteten som brukerne krever.



Figur 6: Oversikt over infrastruktur for levering/salg av rådata og sekundærdata

En opplagt aktør her vil være Statens vegvesen som leverer tjenester som Reisetider og Visveg, se eksemplet i Figur 7 hentet fra vegvesen.no. I dette tilfellet er Statens vegvesen både Eier av infrastruktur for innsamling av rådata, Trafikkdata Behandler og Trafikkdata tjenesteyter. Andre aktører kan være bykommuner, bilprodusenter, utviklere av mobilapplikasjoner (f.eks. Ciber for applikasjonenen iTrafikken), leverandører av veginformasjonstjenester (f.eks. TomTom og Google).



Figur 7: ITS applikasjonen Reisetid på www.vegvesen.no

Trafikkdata bruker kan gjerne sees på som sluttbrukeren i verdikjeden og har følgende ansvarsområder:

- Beskrive hvilke trafikkdata som ønskes, f.eks. velge en ITS tjeneste som gir brukeren informasjon om status på vegnett og trafikkavvikling eller beskrive en vegstrekning hvor man ønsker å vite ÅDT
- Inngå en eksplisitt eller implisitt avtale med Trafikkdata tjenesteyter for levering av trafikkdatatjenesten.
- Kontrollere at tjenesten er levert
- Eventuelt betale for tjenesten

Her finnes det flere mulige aktører, for eksempel:

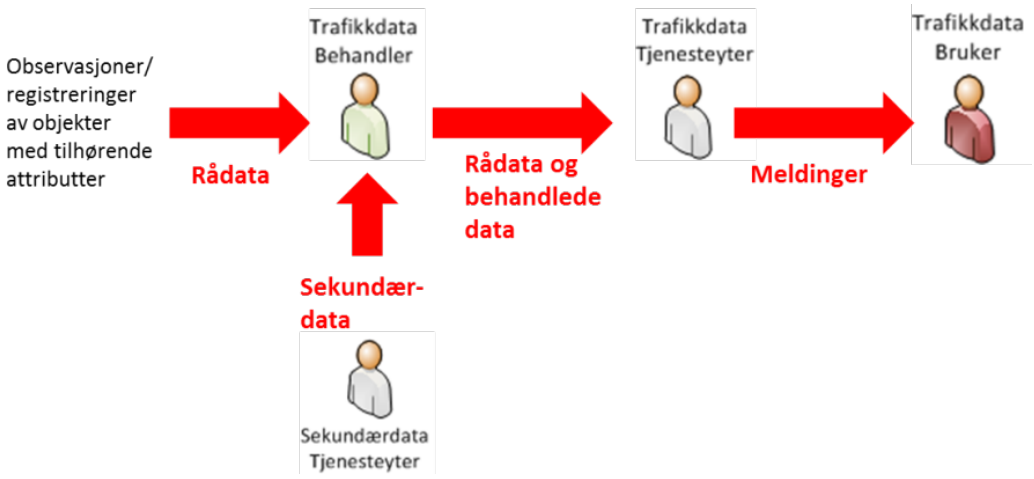
- En vegholder som skal vedlikeholde vegnettet og som bruker trafikkdata for et målrettet vedlikehold
- En Trafikkstyringsansvarlig, f.eks. en VTS, som skal styre trafikken slik at etterspørselen er mindre enn kapasiteten i et vegnett eller på en vegstrekning
- En bilfører som skal planlegge en reise i et vegnett eller på en vegstrekning

En aktør (en etat, organisasjon, selskap eller person) kan gjerne ha flere roller. Statens vegvesen kan f.eks. inneha rollene både som Eier av infrastruktur, Trafikkdata Behandler og Trafikkdata tjenesteyter. En Vegtrafikksentral kan være både Trafikkdata Behandler, Trafikkdata tjenesteyter og Trafikkdata bruker. En bilfører kan være både Eier av infrastruktur, Trafikkdata bruker og Sekundærdata tjenesteyter i de tilfellene bilføreren melder om forhold knyttet til veg og trafikkforhold, f.eks. glatt føre og dårlig sikt.

3.4 Oppsummering

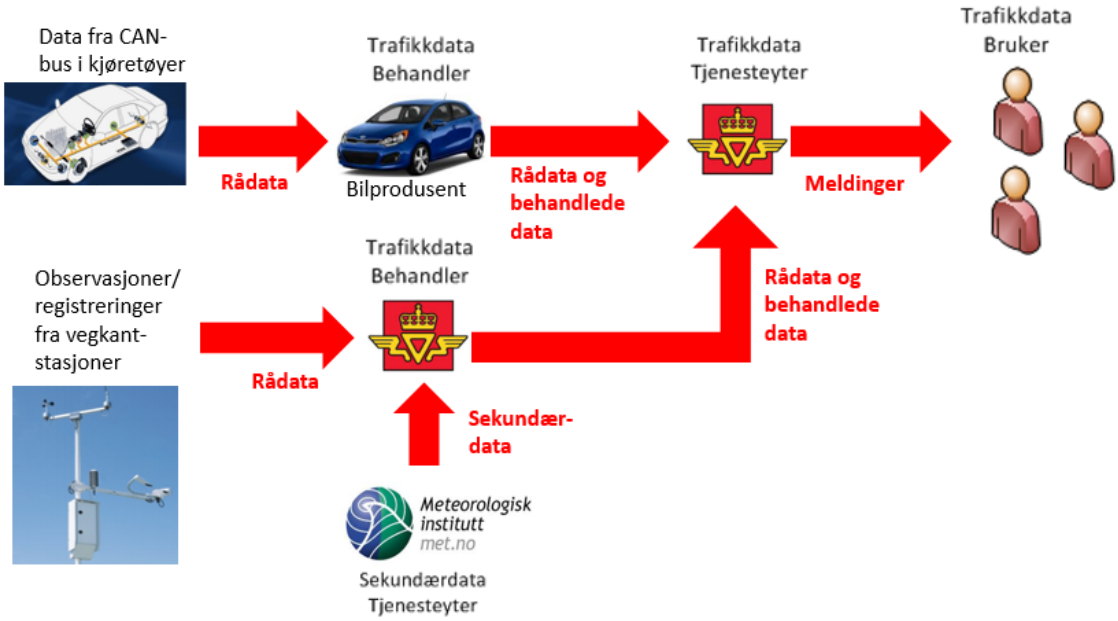
3.4.1 Trafikkdatas livsløp

Figur 8 viser en oversikt over livsløpet til trafikkdata fra de genereres gjennom observasjoner/registreringer av objekter til de ender opp hos sluttbruker, dvs. Trafikkdata bruker. Denne figuren viser den enkle teoretiske modellen for trafikkdatas livsløp.



Figur 8: Oversikt over livsløpet til trafikkdata

I praksis kan trafikkdatas livsløp være mere komplekst som vist i Figur 9. I dette eksemplet er det flere Trafikkdata behandlere som samler inn data fra ulike kilder og hvor data til slutt blir brukt av en Trafikkdata tjenesteyter som yter en informasjonstjeneste til ulike Trafikkdata brukere. I eksemplet nedenfor er kjøretøyprodusenten en Trafikkdata behandler ved at den samler inn data fra en flåte med sine kjøretøyer. Kjøretøyprodusenten sender så sine data, enten rådata eller behandlede data til Statens vegvesen som i dette eksemplet er Trafikkdata tjenesteyter. Statens vegvesen er også Trafikkdata behandler i dette eksemplet siden de samler inn data fra sine egne vegkantstasjoner og de mottar Sekundærdata fra Meteorologisk institutt om værforhold og værprognoser. Statens vegvesen bruker deretter dataene fra de to Trafikkdata behandlerne til å tilby ulike tjenester til ulike typer Trafikkdata brukere. Dersom dette var et system for å samle inn data om glatt kjørebane kan en se for seg at bilførere kunne få meldinger om glatt kjørebane på et "bilfører-vennlig" grensesnitt. Vegholder og entreprenører for vintervedlikehold kunne gjennom et annet grensesnitt få meldinger som initierer salting eller strøing på den strekningen hvor det er registrert eller forventes glatt kjørebane.



Figur 9: Eksempel på innsamling, behandling og levering av trafikkdata

3.4.2 Modell for roller og tjenester

Tabellen nedenfor viser en generell modell for roller og tjenester tilknyttet trafikkdatas livsløp.

Rolle	Leverer tjenesten	Bruker data	Leverer data	Eksempel på aktør
Eier av infrastruktur for innsamling av rådata	Bruk av infrastrukturen for innsamling av rådata. Tjenesten leveres til Trafikkdata Behandler.	Bruker ikke trafikkrelaterte data, men kun data knyttet til overvåking og drift av infrastrukturen.	Leverer ikke trafikkdata, men kun egne data knyttet til overvåking og drift av infrastrukturen.	Statens vegvesen, kommune, bileier, eier av smarttelefon
Kommunikasjons-tjenesteyter	Transport av informasjon i linjebaserte og trådløse nettverk. Tjenesten leveres til alle andre roller.	Bruker ikke trafikkrelaterte data, men kun egne data knyttet til overvåking og drift av kommunikasjons-nettverket.	Leverer ikke trafikkrelaterte data, men kun egne data knyttet til overvåking og drift av kommunikasjons-nettverket.	Netcom, Telenor, Statens vegvesen (egne og leide kabel- og fibernett)
Trafikkdata behandler	Innsamling, kvalitetssikring, behandling av trafikk rådata og sekundærdata og levering av data. Tjenesten leveres til Trafikkdata tjenesteyter.	Rådata og sekundærdata	Rådata og Behandlede data	Statens vegvesen, kjøretøyprodusent, ITS apputvikler, kollektivselskap
Sekundærdata tjenesteyter	Levering av sekundærdata. Tjenesten leveres til Trafikkdata Behandler.	Sekundærdata innsamlet og behandlet av Sekundærdata Behandler	Sekundærdata	Meteorologisk Institutt
Trafikkdata tjenesteyter	Levering av trafikkdata i form av ulike typer meldinger. Tjenesten leveres til Trafikkdata bruker.	Rådata og Behandlede data	Meldinger	Statens vegvesen, NRK1, P4, ITS app leverandører, TomTom, Google
Trafikkdata bruker	Leverer ikke tjenester, - er kun bruker av tjenester levert av Trafikkdata tjenesteyter	Meldinger	Ikke relevant	Bilfører, VTS, Vegholder, vegvedlikeholds-entreprenører, SSB

4 Eierskap til trafikkdata

4.1 Bakgrunn

Dette kapittelet ser på begrepene trafikkdata og eierskap av trafikkdata, samt hvordan eierskap av data rent generelt er omtalt i en del litteratur som er gjennomgått.

Kapittelet ser primært på data som ikke inneholder personopplysninger, dvs. upersonlige data. I en del tilfeller vil selvfølgelig trafikkdata kunne inneholde data, f.eks. et kjøretøys registreringsnummer, som gjør det mulig å knytte de innsamlede dataene til eieren av det objektet som er benyttet til å samle inn dataene. De mest opplagte typer objekter er kjøretøyer, smarttelefoner og billettmedia. Personvern er behandlet i andre deler av dette prosjektet og er derfor ikke inkludert. Noen av de viktigste referansene mht. personvern er gitt i Tabell 1 på side 31.

4.2 Hva menes med trafikkdata, rådata og behandlede data

Begrepet ***trafikkdata*** er beskrevet i forrige kapittel og er definert som følgende:

- *Informasjon om objekter som benytter transportsystemet hvor informasjonen kan være knyttet til enkeltobjekter, f.eks. kjøretøy, eller til strømmer av objekter, f.eks. en strøm av fotgjengere. Informasjonen kan samles inn både ved hjelp av informasjon fra selve objektet eller fra sensorer tilknyttet den infrastrukturen som inngår i transportsystemet.*
- *Informasjon om selve transportinfrastrukturen, f.eks. temperatur i vegdekket/overbygning og status på overflate dekke, f.eks. våt, is- eller snødekket. Det kan også omfatte informasjon som sier noe om siktforhold i transportinfrastrukturen.*

*Begrepet **Rådata** betyr informasjon slik det foreligger i sin opprinnelige form. Det vil f.eks. si informasjon om en observasjon eller registrering av objekter eller infrastrukturen før man har begynt å sortere, gruppere og analysere de innsamlede dataene. Data som beskriver ett kjøretøys hastighet, vekt, antall akslinger og avstand til forankjørende kjøretøy er et eksempel på rådata.*

*Begrepet **Behandlede data** betyr her rådata som er sortert, gruppert og analysert. Dersom vi f.eks. samler rådata fra kjøretøy over en time for deretter å beregne gjennomsnittlig hastighet for alle kjøretøyer, antall kjøretøyer i hver vektklasse, antall akslinger i hver vektklasse og gjennomsnittlig avstand til forankjørende kjøretøy er dette Behandlede data.*

4.3 Hva menes med eierskap i tilknytning til trafikkdata

Eierskap er et sentralt begrep mht. trafikkdata. Begrepet eierskap (ownership) er definert i flere engelske ordbøker, men ikke tilsvarende definert i norske ordbøker. I Bokmålsordboka er eierskap definert som det å eie noe (helt eller delvis). Dette er en mindre presis definisjon sammenlignet med noen av de engelske definisjonene:

- Dictionary.com definerer eierskap som:
  - the state or fact of being an owner
  - legal right of possession; proprietorship
- MacMillan dictionary definerer eierskap som:

  - legal possession of something, usually something big and valuable
  - an attitude of accepting responsibility for something and taking control of how it develops
- Oxford Dictionary definerer eierskap som:
  - The act, state, or right of possessing something:
- Business Dictionary har kanskje den mest relevante definisjonen av eierskap:
  - The ultimate and exclusive right conferred by a lawful claim or title, and subject to certain restrictions to enjoy, occupy, possess, rent, sell, use, give away, or even destroy an item of property.
    Ownership may be corporeal (title to a tangible object such as a house) or incorporeal (title to an intangible object, such as a copyright, or a right to recover debt). Possession (as in tenancy) does not necessarily mean ownership because it does not automatically transfer title.

I Al-Khouri (2012) diskuterer forfatteren begrepet 'Ekte Eier' og hvem som er den ekte eieren av data. Svaret på dette ligger i *sannferdighet, pålitelighet og verifiserbarhet*. Den som til en hver tid kan verifisere at data er sannferdige og pålitelige er den ekte eieren av data.

Hvis man ser på den definisjonen som er gitt i Business Dictionary så sier den at eierskap er den ultimate og eksklusive retten, overdratt gjennom et lovmessig krav eller hjemmel, til å nyte, okkupere, besitte, leie ut, selge, bruke, gi bort og til og med ødelegge en eiendel. En kombinasjon av Al-Khouris begrep 'ekte eier' og Business Dictionary sin definisjon på eierskap kan danne grunnlag for en definisjon av trafikkdata eierskap:

Eieren av trafikkdata er den fysiske personen, organisasjonen eller myndigheten som har skapt et gitt sett med trafikkdata og som kan verifisere at dette settet er sanne og pålitelige. Med trafikkdataeierskap menes retten til å bruke, leie ut, selge, gi bort og destruere trafikkdata.

Denne definisjonen innebærer at alle leddene i den verdikjeden som er beskrevet for livsløpet til trafikkdata vil være eiere av trafikkdata. I hvert ledd i verdikjeden vil det skapes nye data og det er bare den som har skapt disse nye dataene som vil kunne verifisere de nye dataene mht. sannhet og pålitelighet. En Trafikkdata behandler kan f.eks. ikke verifisere at trafikkdata er sanne og pålitelige etter at trafikkdata er gitt bort til eller solgt til en Trafikkdata tjenesteyter som er neste ledd i verdikjeden. Han kan bare verifisere de dataene som Trafikkdata behandler selv har skapt. For at alle leddene i verdikjeden, og spesielt sluttbruker, skal kunne stole på trafikkdata, betinger det et avtaleverk mellom aktørene som sikrer konfidensialitet, integritet og tilgjengelighet gjennom hele verdikjeden i og med at trafikkdata hele tiden lagres, behandles og flyttes på. Et slikt avtaleverk vil også inkludere bestemmelser om hvem som eier hvilke data til enhver tid.

I noen tilfeller vil det være *delt eierskap*, dvs. at verifiseringen krever at to aktører i verdikjeden må verifisere at trafikkdata er sanne og pålitelige. Delt eierskap kan avtales gjennom en avtale mellom de to partene. Dette gjelder spesielt i de tilfellene hvor rådata er samlet inn fra en mobil enhet, f.eks. en smarttelefon. Den som har samlet inn rådata (trafikkdata behandler) vil kunne verifisere at de innsamlede dataene er de som virkelig kommer fra den mobile enheten, mens den som eier den mobile enheten (eier av infrastruktur for innsamling av trafikkdata) vil kunne verifisere at de rådataene som er samlet inn samsvarer med virkeligheten, f.eks. eierens reisemønster.

Det vil også kunne forekomme tilfeller *av overført eierskap*. I dette tilfellet overføres eierskapet av trafikkdata til en aktør som har samme mulighet som opprinnelig eier til å verifisere sannhet og pålitelighet. Dette kan skje på andre måter enn den metoden som opprinnelig eier kan benytte. Det kan også skje gjennom at den som har fått overført eierskapet får tilgang til opprinnelige data gjennom en transparent kanal hos

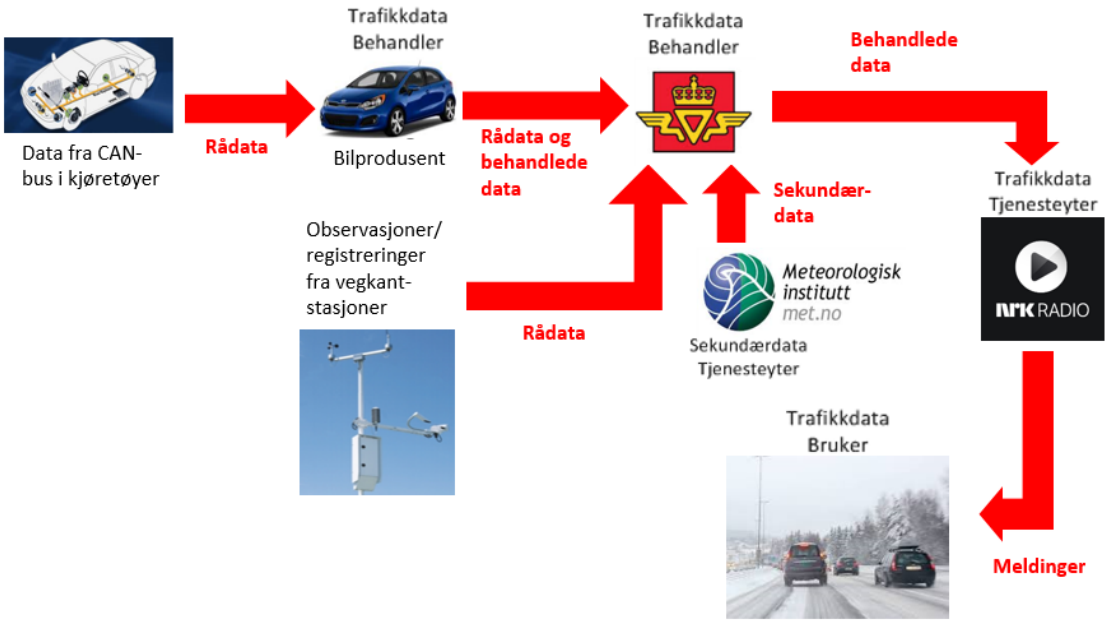
opprinnelig eier som gjør det mulig å verifisere sannhet og pålitelighet for den som har fått overført eierskapet.

Rådata vil kunne flytte seg gjennom verdikjeden, men eierskapet til rådata vil alltid forbli hos den samme aktøren, dvs. den aktøren som skapte data og som kan verifisere at data er sanne og pålitelige. For at dataene som flyttes i en verdikjede skal kunne benyttes av andre må det foreligge en *bruksrett* til dataene. Det er den som sitter med eierskapet som kan utstede denne bruksretten gjennom det avtaleverket som er grunnlaget for verdikjeden for trafikkdata. Bruksretten kan være gratis eller knyttet til en avgift. Bruksretten blir dermed en viktig faktor i forretningsmodeller knyttet til trafikkdata.

Eksempel

Figur 10 viser et eksempel på informasjonsstrømmer mellom ulike aktører i verdikjeden. En bilprodusent samler inn rådata fra sine kjøretøyer. Dette kan være rådata som kjøretøyets hastighet og de friksjonsforholdene som kan registreres ved hjelp av kjøretøyets sensorer og kombinasjon av sensorer. Kjøretøyprodusenten vil i dette tilfellet ha eierskapet til rådata fordi det er bare kjøretøyprodusenten som kan verifisere at dataene er sanne og pålitelige. Kjøretøyprodusenten sender deretter rådata og behandlede data til vegvesenet. Rådata kan være alle rådata eller et utvalg av rådata. Behandlede data kan være aggregerte data eller nye data som er fremkommet gjennom analyser av rådata. Eierskapet til rådata eller behandlede data tilfaller kjøretøyprodusenten, siden det er denne som har skapt dataene og er den eneste som kan verifisere at rådata og behandlede data er sanne og pålitelige.

Rådata og behandlede data sendes til vegvesenet gjennom nettverket til en organisasjon eller myndighet som leverer kommunikasjonstjenester. Ved hjelp av sikkerhetsmekanismer for overføringen kan mottaker kontrollere at dataene ikke er endret under vegs fra avsender og at de derfor er sanne og pålitelige. Alternativt kan en se på tjenesteyteren av kommunikasjonstjenester som en midlertidig eier av data siden det bare er tjenesteyteren som kan verifisere at dataene som sendes gjennom nettverket er sanne og pålitelige, dvs. de er ikke endret i løpet av transporten gjennom nettverket. For at mottaker av data skal kunne stole på opprinnelsen til data må det foreligge en avtale mellom avsender og mottaker (kjøretøyprodusent og vegvesenet) som sikrer kvaliteten på de dataene som vegvesenet får oversendt fra kjøretøyprodusenten. Kjøretøyprodusenten står fortsatt som eier av de rådataene og behandlede dataene som ble sendt videre til vegvesenet og SVV har bruksrett til rådata gjennom en bruksrettsavtale.



Figur 10: Eksempel på innsamling, behandling og levering av trafikkdata

Vegvesenet samler også inn rådata fra sine egne vegkantstasjoner, f.eks. data om trafikkstrømmer og vær- og føreforhold. Vegvesenet blir her eier av rådata siden det er vegvesenet som har skapt dataene og kan verifisere at disse rådataene er sanne og pålitelige. Vegvesenet mottar også sekundærdata, i dette eksemplet fra Meteorologisk institutt som også da er eier av disse sekundærdataene. Rådataene fra vegkantstasjonene og sekundærdataene fra Meteorologisk institutt benyttes til analyser og fremstilling av ny informasjon (Behandlede data) som sendes videre til rollen Trafikkdata tjenesteyter, som i dette eksemplet er NRK. Vegvesenet står som eier av de dataene som vegvesenet sender fra seg til NRK som har bruksrett til de behandlede dataene. Trafikkdata tjenesteyter(NRK) bruker de behandlede dataene til å generere meldinger som sendes ut til sluttbruker, i dette eksemplet til bilførere som befinner seg på den vegstrekningen hvor data er samlet inn. Vegvesenet står som eier av de behandlede dataene som benyttes av Trafikkdata tjenesteyter (NRK i dette eksemplet).

I dette eksemplet sitter altså *Statens vegvesen* med følgende trafikkdata eierskap og bruksrettigheter:

- Bruksrett til rådata og behandlede data som er samlet inn, behandlet og eiet av kjøretøyprodusenten, som igjen har gitt vegvesenet bruksretten
- Bruksrett til sekundærdata fra Meteorologisk institutt som eier disse dataene og som har gitt vegvesenet bruksretten
- Eierskap til rådata fra egne vegkantstasjoner
- Eierskap til behandlede data som er sendt til Trafikkdata tjenesteyter

Kjøretøyprodusenten sitter med følgende eierskap:

- Rådata hentet fra kjøretøyene. I dette tilfellet kan det være snakk om delt eierskap siden bilføreren i noen tilfeller kan verifisere at data er sanne, f.eks. at kjøretøyet har kjørt i en bestemt hastighet på en

bestemt vegstrekning eller at det har vært gjennomført en automatisk og kraftig oppbremsing pga. et hinder i kjørebanen. Dette vil kunne avtales gjennom kjøpsavtalen mellom bileier og bilforhandler.

Meteorologisk institutt sitter med følgende eierskap:

- Sekundærdata om klimatiske forhold

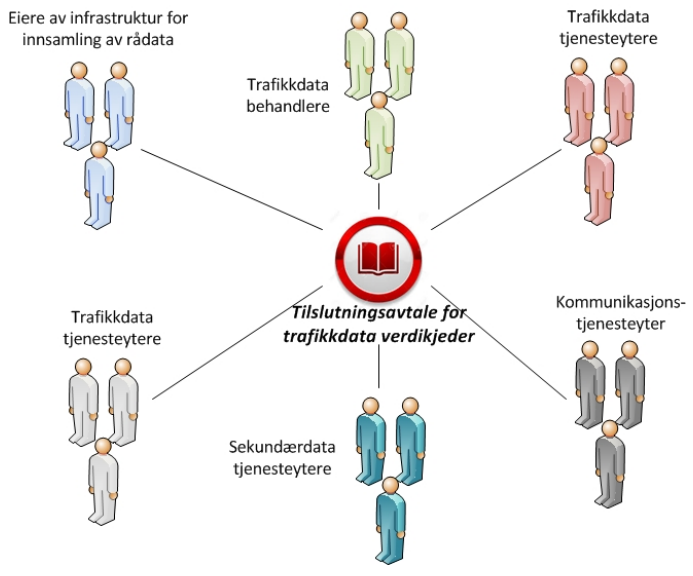
NRK sitter med følgende bruksretter:

- Bruksrett til behandlede data mottatt fra vegvesenet

Trafikkdata bruker vil i dette eksemplet ikke eie eller ha eksplisitt bruksrett til trafikkmeldingene. Meldingene fra NRK vil foreligge som informasjon sendt til alle bilførere i det aktuelle området og er en offentlig tjeneste som ikke krever noen avtale mellom bruker og tjenesteyter. En kan imidlertid tenke seg scenarioer hvor bilføreren/bileieren har inngått en avtale med en tjenesteyter om levering av trafikkinformasjon og betaler for denne type tjeneste. I dette tilfellet vil bilfører/bileier ha bruksrett til meldingene gjennom avtalen.

4.4 Avtaleverk for trafikkdata

Avtaleverk for å regulere eierskap og bruksrett til trafikkdata kan bygges opp som bilaterale avtaler mellom aktørene i verdikjeden eller som en multilateral tilslutningsavtale for alle aktørene. Bilaterale avtaler kan være en tilfredsstillende løsning med et lite antall aktører, men vil fort eskalere til et komplekst og uoversiktlig avtaleverk med mange aktører. En enklere løsning kan derfor være en multilateral tilslutningsavtale som de ulike aktørene slutter seg til, se Figur 11. En slik avtale beskriver rollene og ansvarsforholdene for de ulike typene aktører som slutter seg til verdikjeden for trafikkdata og hvilke rettigheter og plikter som er knyttet til de ulike rollene. Videre beskriver avtalen hvordan verdiene (trafikkdata) skal distribueres og hvordan de ulike leddene i verdikjeden skal kunne bruke, selge, gi bort, leie ut og destruere trafikkdata og eventuelle betalinger eller avgifter for dette.



Figur 11: Mulig løsning for et avtaleverk for verdikjeder for trafikkdata

Eiere av mobiltelefoner og kjøretøyer vil være eiere av infrastruktur for innsamling av trafikkdata. Disse vil ikke kunne inngå direkte i en tilslutningsavtale, men må indirekte tilknyttes gjennom avtalene med de som vil kunne defineres som trafikkdata behandlere, f.eks. bilprodusenter og mobiltjenesteleverandører.

4.5 Hva sier litteraturen om eierskap til data

Det er gjennomført et søk etter litteratur om eierskap til trafikkdata, men det er lite som er publisert om dette temaet. Det finnes imidlertid en del litteratur om eierskap til data på et generelt nivå. De mest relevante funnene er referert nedenfor og oppsummert i Tabell 1. Flere av funnene er knyttet til personlige data og data lagret i skyen.

Tabell 1. Litteratur om eierskap til data

Forfatter	År	Tittel
Al-Khouri, A.M	2012	*Data Ownership: Who owns my data?*
Chen, D. & H. Zhao	2012	*Data security and privacy protection issues in cloud computing*
e-Science City	-	Who owns the data?
Foss, K.	2015	Hvem eier dataene i tingenes internett?
Jarbekk, E.	2014	Big Data, Kommersialisering og eierskap til informasjon
Kaisler, S. m.fl.	2013	Big Data Issues and Challenges moving forward
Limoges, E. m.fl.	2000	Future of Urban Transportation data
Nielsen, M.	2013	Who owns Big Data?
Rendle, A.	2014	Who owns the data in the Internet of Things?
Wigan, M.R. & R. Clarke	2013	Big Data's Big Unintended Consequences

Chen & Zhao (2012) diskuterer datasikkerhet og personvern i nettskyer. I forbindelse med eierskap til de dataene som genereres, behandles og lagres sier artikkelen at i et tradisjonelt IT miljø er det vanligvis slik at brukere og organisasjoner eier og håndterer data. Mht. personlige data har dataeieren rett til å vite hva slags informasjon som er samlet inn og i noen tilfeller stoppe innsamling og bruk av personlig informasjon. Deling av data utvider bruken av data og gjør tillatelser til bruk av data mere komplekse. Dataeiere kan autorisere tilgang til data til en aktør og denne aktøren kan med tillatelse fra dataeieren dele disse dataene med andre aktører. Det er derfor viktig at dataeiere er nøye med å definere hvordan beskyttelsen av data skal videreføres når data deles med andre. Det må også vurderes nøye hvordan detaljeringsgraden skal være ved deling av data, f.eks. å aggregere data og filtrere bort personlig informasjon.

I Limoges et al. (2000) diskuteres det hvordan fremtidige urbane transportdata kan anvendes på en effektiv måte uten at det går på bekostning av enkeltindividers krav til beskyttelse av personlige data. Artikkelen har et kort kapittel om bekymringer knyttet til personvern og dataeierskap. Samfunnet er blitt mer og mer avhengig av omfattende utveksling av data og myndighetene i flere land har tatt skritt for å sikre disse datastrømmene. Det har etter hvert blitt en utfordring for transport- og kommunikasjonsorganisasjoner, selskaper og myndigheter å delta i og veilede i prosessen med informasjonshåndtering og eierskap til det beste for samfunnet. Spesielt nevnes all den geografiske informasjonen som samles inn. Denne informasjonen kan fort skape litt ubalanse i den viktige avveiningen mellom samfunnets ønske om mye data og folks villighet til at det samles inn denne type data. Det er derfor viktig at samfunnet er aktivt mht. å finne gode løsninger for eierskap og bruk av data.

Utilsiktede konsekvenser av Big Data berøres av Wigan & Clarke (2013). Ett av de punktene som omtales er dataeierskap, kontroll og rettigheter. Forfatterne av denne artikkelen hevder at eierskap av data ikke kan sammenlignes med andre eierskap, f.eks. eierskap av eiendommer. Under spesielle forhold kan data bli sett på som en intellektuell eiendel. Eierskap kan være et relevant konsept i spesielle kontekster, men som et generelt analytisk verktøy har nåværende bruk av begrepet eierskap av data liten verdi. Dette er imidlertid ikke gyldig for personlige data. Her vil den enkeltes rett til bruken av personlige data stå sterkt. Forfatterne bruker ikke begrepet eierskap i denne sammenhengen, men retten til bruken av data.

For mange internettselskaper er det å eie data en virkelig forretningsfordel og det er lite trolig de vil åpne opp deres datainfrastruktur for andre (Nielsen 2013). Eksempler på slike selskaper er Google og Facebook hvor eierskap av data er en av viktigste verdiene som selskapene sitter på. Det gir dem en unik fordel i forhold til andre konkurrenter fordi de dataene de sitter på er vanskelig å samle inn for andre i det omfanget som disse to selskapene sitter på.

For brukere som ønsker å bruke nettskyen er det en bekymring mht. hvem som skal eie brukerens data (e-Science City)[1]. Dette blir enda mer komplisert hvis flere aktører involvert. Hvis brukeren gir sine data til en skyleverandør som deretter setter bort hele eller deler av arbeidet til en annen lagrings- eller prosessleverandør, hvem er da ansvarlig hvis informasjon går tapt eller skadet? Eierrettigheter er vanligvis dekket av tre rettsområder - opphavsrett, konfidensialitet og kontrakt - som alle varierer avhengig av land. Så hvis data er opprettet i ett land, men deretter lagret i et annet land, så vil de rettsreglene som gjelder bli litt diffuse. I hovedsak er det to typer data i skyen: data som er opprettet på forhånd og lagt opp i skyen, og data som er opprettet i skyen. Man kan anta at data som er opprettet på forhånd bør tilhøre den som genererte data iht. loven om opphavsrett. Men data som er opprettet i skyen, enten av kunden eller leverandøren er en annen historie. Å bestemme hvem som eier innholdet her vil avhenge av både type informasjon og, til en viss grad, hvor ble det generert.

Al-Khouri (2012) sier at det er mye forvirring rundt begrepet data. Data er bare et sett med karakterer som ikke har noen verdi dersom det ikke kan settes inn i en sammenheng. Data brukes til å gi informasjon. Sammenhengen og bruken av data gir en mening til data slik at den blir til informasjon. Eksempelvis er tallene -2 og 0,56 meningsløse i seg selv, men blir nyttig informasjon dersom man vet at -2 er temperatur på vegoverflate og 0,56 friksjonskoeffisient og at verdiene er målt på E6 ved Berkåk kl. 04:45 den 3. desember 2014. Data i seg selv har dermed ingen verdi og det kan være grunn til å anta at eierskapet til data er mindre relevant. Rådata har slik sett ingen verdi annet enn kostnaden for innsamlingen. Det er først når data settes i en sammenheng at data blir til informasjon som har en verdi og dette skjer første gang hos den trafikkdatabehandleren som har samlet inn data, gruppert dem og analysert dem. Så snart dataene får en verdi blir også spørsmålet om eierskapet mere relevant.

Rendle (2014) reiser spørsmålet om hvem som eier data i Internet of Things (IoT) og her mener forfatteren at dette er ingen. Det er ingen eiendomsrett til data i seg selv. Det er først når man samler inn dataene og aggregerer eller behandler data, og at det er knyttet en viss investering i denne innsamlingen og behandlingen, at det oppstår et eierskap. Det er derfor viktig å finne hvilke samlinger av data som kan eies og hvem som kan eie dem av to grunner. Den første grunnen er de enorme verdiene som kan ligge i utnyttelsen av dataene og det er derfor viktig å finne ut hvem som kan utnytte de og enda mere viktig, hvem som kan stoppe andre i å utnytte dem. Den andre grunnen er å skille de potensielle eierinteressene til de ulike aktørene i prosesseringskjeden. En rekke aktører vil bli involvert i dataenes livsløp. Det vil derfor være viktig å

[1] http://www.cloud-lounge.org/who-owns-the-data.html

identifisere hvem i denne kjeden som eier aggregeringen av dataene mht. hvem som har de økonomiske rettighetene til aggregeringen.

Aggregering av data kan beskyttes av databaserettigheter iht. Databasedirektivet (Directive 96/9/EC). Dette direktivet har definert tre ulike kriterier som skal oppfylles for at direktivet skal gjelde og for at skaperen av databasen skal være den som eier rettighetene til databasen (Rendle 2014). Skaperen er definert som den som:

- Tar initiativet til å skaffe til veie, verifisere og presentere innholdet i databasen
- Tar risikoen med investeringen med å skaffe til veie, verifisere og presentere innholdet

Det er også viktig å ha med eierskapet i kontrakter mellom de aktørene som er involvert i dataenes livsløp (ibid.). Hvis eierskap og databaserettigheter ikke er avtalt i kontraktene vil en oppleve store diskusjoner mellom de involverte aktørene pga. de store verdiene som kan ligge i den informasjonen som er lagret i databasen.

Eierskap til data representerer en kritisk og pågående utfordring, spesielt innenfor de sosiale media (Kaisler m.fl. 2013). Det ligger enorme mengder informasjon på serverne til Facebook, Twitter og andre tilsvarende medialeverandører. Denne informasjonen eies ikke av disse leverandørene selv om de vil kunne hevde det ut i fra lagringen av data. Eierne av brukerkontoene mener tilsvarende at informasjonen eies av dem og denne motsetningen kan bare avgjøres gjennom rettsapparatet. Forfatterne sier videre at med eierskap følger det en forpliktelse til å sikre nøyaktigheten på data. Dette gjelder kanskje ikke så mye privatpersoner, men i hvert fall organisasjoner, selskaper og myndigheter. Det skjer gjerne en blanding av data i Big Data-verdenen hvor pålitelige og verifiserbare data blandes med andre typer data som ikke trenger å være like pålitelige. Konklusjoner som trekkes på slike blandede data vil derfor kunne bli usikre og tatt på sviktende grunnlag. Noen problemstillinger som dukker opp i slike sammenhenger, og som også er relevant for trafikkdata, er følgende:

- Når går gyldigheten på data som er offentlig tilgjengelig ut?
- Skal ugyldige data fjernes fra den offentlige tilgjengeligheten?
- Hvor og hvordan skal man arkivere data som ikke lenger er gyldig og skal man overhode arkivere de?
- Hvem har ansvaret for kvaliteten og nøyaktigheten på data?

Eierskap til data består i å kunne bestemme hvordan dataene skal benyttes (Foss 2015a). Spørsmålet er hvem som skal bestemme over bruken. Utgangspunktet må være at den som skaper dataene må stå nærmest til å disponere om det som skapes. Andre som skal bruke dataene må da ha en avtale om bruksrett til dataene. I de eksemplene som er brukt av Foss (2015a) er det den som eier den infrastrukturen som samler inn data som er skaperen av data. Videre bruk av data skjer ved at den som eier infrastrukturen deler dataene med en leverandør (databehandler) som får bruke dataene iht. en avtale om bruksrett. For å få en slik bruksrett eller disposisjonsrett må den som ønsker slik disposisjonsrett tilby eieren en verdi som gjør det attraktivt for eieren å dele dataene, f.eks. en økonomisk godtgjørelse eller gjentjenester.

En forutsetning for å kunne bruke Big Data er at du har rett til å kunne bruke opplysningene. Denne retten kan du få gjennom avtaler med de som eier dataene (Jarbekk 2014). Andre lover som regulerer bruken av Big Data er Personopplysningsloven, Åndsverkloven og Markedsføringsloven. Mht. hvem som kan bestemme hvordan personopplysninger skal brukes er det *den det gjelder*. Via en avtale (eller annet rettsgrunnlag) kan kommersielle aktører bruke den tilgjengelige informasjonen. Mht. databasevern sier

forfatteren at data eller informasjon i seg selv ikke trenger være nok til beskyttelse iht. Åndsverkloven. Det er utvelgelsen og sammensetningen av data og informasjon som er avgjørende. Det refereres også til Åndsverklovens § 43 som sier at *Den som frembringer et formular, en katalog, en tabell, et program, en database eller lignende arbeid som sammenstiller et større antall opplysninger, eller som er resultatet av en vesentlig investering, har enerett til å råde over hele eller vesentlige deler av arbeidets innhold.*

4.6 Ansvar ved utlevering av data

4.6.1 Juridisk ansvar

Ett mulig produkt av økende innsamling og bruk av data er prediksjoner både mot det offentlig og mot allmennheten. Med utgangspunkt i data fra RSI-prosjektet kan det for eksempel utarbeides prediksjoner for vegstrekninger eller punkter på vegen med lav friksjon – altså prediksjoner som indikerer hvor det er glatt kjørebane. Dersom Statens vegvesen skal være leverandør av slike prediksjoner er det viktig at Statens vegvesen vurderer hvilke forbehold prediksjonen bør knyttes til og avklare eventuelt juridisk ansvar. I dag eksisterer flere prediksjonsbaserte tjenester basert på helt eller delvis offentlige data.

Ett eksempel er yr.no. Yr er den største værtjenesten i Norge og et samarbeid mellom NRK og Meteorologisk institutt. I tillegg til å formidle egne prediksjoner gjør yr.no data åpent tilgjengelig for andre. Bruk og nedlasting av data er knyttet til en rekke vilkår, og det understrekes at data på generell basis *ikke* er knyttet til en implisitt eller eksplisitt avtale om kvalitet på dataene (http://om.yr.no/info/datapolicy/). Slike avtaler regulerer blant annet omfang, kvalitet og ansvar mellom tjenestetilbyder og tjenestebruker. Det ser dermed ut til å være svake juridiske bindinger knyttet til utlevering av data og prediksjoner fra yr.

Et annet eksempel er bruk av GoogleMaps som kan inneholde prediksjoner, f.eks. om trafikk. I "Vilkår" (https://www.google.com/intl/no_no/help/terms_maps.html) som man finner med meget liten skrift nederst på kartsiden, står det bl.a. følgende om bruk av data:

Faktiske forhold: Bruk på eget ansvar. *Når du bruker kartdataene, trafikken, veibeskrivelsene og det andre innholdet i GoogleMaps eller Google Earth, kan de faktiske forholdene i noen tilfeller avvike fra kartresultatene og innholdet. Det er derfor viktig at du utviser skjønn og er klar over at du bruker Google Maps og Google Earth på eget ansvar. Du er ansvarlig for dine egne handlinger og eventuelle konsekvenser av disse.*

Dermed finnes allerede praksis og erfaringer med deling av prediksjoner basert på offentlige data. Det er imidlertid utenfor dette prosjektets kompetanse å vurdere hvilke juridiske forbehold og ansvar som vil være knyttet til deling av data fra Statens vegvesen, eksempelvis gjennom RSI-prosjektet. Slike vurderinger bør gjøres av jurister med tilstrekkelig kompetanse innen både juridiske og transportfaglige problemstillinger.

4.6.2 Utilsiktede konsekvenser

Et annet aspekt knyttet til prediksjoner er hvilke konsekvenser den informasjonen som ligger i prediksjonene vil gi. Gjennom å levere slik informasjon kan Statens vegvesen endre premissene for trafikanters, transportørers, entreprenørers og andres beslutningstaking og adferd. I forberedelse av utlevering av slik informasjon (og eventuelle data som kan produsere slik informasjon) er det viktig å gjennomgå mulige konsekvenser og særlig eventuelle uønskede hendelser det kan gi.

Det finnes en rekke metoder for å vurdere risiko og uønskede hendelser, og en god oversikt gis av Rausand og Utne (2009). De skiller blant annet mellom *identifisering av farekilder og uønskede hendelser* på den ene siden, og *konsekvensanalyse* på den andre. Selv om flere metoder kan benyttes for å identifisere uønskede hendelser er den enkleste metoden en såkalt "grovanalyse" (Hazard identification – HAZID). Analysen gjennomføres i syv trinn og resulterer i en matrise som beskriver aktivitet, trussel, uønsket hendelse, årsak til hendelse, konsekvens, risiko og risikoreduserende tiltak (ibid. s. 143). En forenklet versjon av grovanalyse er en matrise som beskriver sannsynlighet for at en uønsket hendelse oppstår og konsekvensen dersom den skulle oppstå. Matrisen kan være kvalitativ ved at den beskriver sannsynlighet og konsekvens tekstlig, og/eller kvantitativ gjennom å vurdere sannsynlighet og konsekvens på en skala fra 1-5 ((1= lite sannsynlig, 5 = svært sannsynlig, 1=lav konsekvens, 5= høy konsekvens).

I en risikoanalyse beskrives først hvilke hendelser som kan inntreffe, hvorfor hendelsene inntreffer og eventuelt hvem som utløste hendelsen. Deretter vurderes konsekvensene av hendelsene etter en på forhånd definert gradering av hendelsene. En slik gradering kan f.eks. være følgende:

- K = 5, hendelsen kan føre til tap av liv eller vedvarende helsetap (Meget alvorlig)
- K = 4, hendelsen kan føre til midlertidig tap av helse (Alvorlig)
- K = 3, hendelsen vil ikke medføre tap av helse eller liv, men kan medføre betydelig økonomisk tap som kan gjenopprettes (Moderat)
- K = 2, hendelsen vil ikke medføre tap av helse eller liv, men kan medføre økonomisk tap som kan gjenopprettes
- K = 1, hendelsen har ingen konsekvenser hverken mht. helse eller økonomi (Ubetydelig)

Videre vurderes sannsynligheten for at en hendelse skal inntreffe etter en på forhånd definert gradering av sannsynlighetene. En slik gradering kan f.eks. være følgende:

- S=4, meget høy sannsynlighet for at hendelsen inntreffer
- S=3, høy sannsynlighet for at hendelsen inntreffer
- S=2, moderat sannsynlighet for at hendelsen inntreffer
- S=1, lav sannsynlighet for at hendelsen inntreffer

Risikoen knyttet til en hendelse er produktet av konsekvens og sannsynlighet. Før risikoanalysen gjennomføres bør en definere akseptabelt risikonivå, eventuelt gradere risikoen i ulike nivåer.

Tabell 2 viser en slik gradering av risiko. Grønne områder indikerer hendelser med ubetydelig risiko (akseptabel), gule områder hendelser med betydelig risiko (vurderes) og røde områder hendelser med kritisk risiko (uakseptabel). Hendelser med risiko (produktet av konsekvens og sannsynlighet) mellom 1 og 4 er akseptable, hendelser med risiko mellom 5 og 9 må vurderes spesielt for å se om de enten har en konsekvens eller sannsynlighet som er for høy og alle hendelser med risiko over 9 er uakseptable. I den videre risikoanalysen vurderes tiltak slik at risikoen for alle hendelser kommer ned på et akseptabelt nivå. I noen tilfeller kan det være forhold som gjør at en legger spesiell vekt på konsekvenser slik det er gjort i eksemplet nedenfor og slik det er vist i Tabell 2 hvor hendelser som har en konsekvens som regnes som Alvorlig og Meget alvorlig også er farget rød selv om de har en verdi for risiko mindre enn 9.

I RSI-prosjektet skal Statens vegvesen distribuere meldinger om friksjonsforhold på punkter og strekninger i vegnettet. De uønskede hendelsene som kan inntreffe i den sammenheng kan grupperes i to hovedgrupper:

- Meldingen sier at friksjonsforholdene er utilfredsstillende, men meldingen er feil fordi det er feil i beslutningsgrunnlaget eller at meldingen sendes ut for sent, dvs. forholdene er ikke lenger utilfredsstillende (type-I-feil).
- Meldingen sier at friksjonsforholdene er tilfredsstillende, men meldingen er feil fordi det er feil i beslutningsgrunnlaget, f.eks. feil ved innsamlede data eller dataene er forsinket i overføring fra sensor til der beslutningen tas (type-II-feil).

Konsekvensene av den første gruppen uønskede hendelser kan gjerne være meget alvorlig eller alvorlig, dvs. K = 4 eller 5, mens konsekvensene av den andre gruppen kan være moderat, liten eller ubetydelig. Ut i fra vegvesenets visjon om trafikksikkerhet kan det medføre at et akseptabelt risikonivå ikke skal inkludere hendelser med Alvorlig eller Meget alvorlig konsekvens. Tabellen for RSI prosjektet kan derfor eksempelvis se slik ut:

Tabell 2. Eksempel på en gradering av risiko i RSI-prosjektet

Sannsynlighet	1	2	3	4	5	
Meget høy	**4**	**8**	**12**	**16**	**20**	**4**
Høy	**3**	**6**	**9**	**12**	**15**	**3**
Moderat	**2**	**4**	**6**	**8**	**10**	**2**
Lav	**1**	**2**	**3**	**4**	**5**	**1**
	Ubetydelig	**Liten**	**Moderat**	**Alvorlig**	**Meget alvorlig**	

Konsekvens

Selv om sannsynligheten for hendelsen er Lav eller Moderat er altså hendelsen uakseptabel pga. sin alvorlige konsekvens.

Uønskede hendelser i førevarslingssystemer hvor f.eks. RSI prosjektet vil kunne være en leverandør, kan være knyttet til følgende objekter:

- Kjøretøyets IKT system og sensorer (Kjøretøy ITS sub-system), f.eks. manglende data og feil i databehandlingen
- Kommunikasjonssystemet som overfører data mellom kjøretøy og kjøretøyprodusentens sentralsystem, f.eks. dekningsproblemer, nedetid og forsinkelser
- Kjøretøyprodusentens sentralsystem, f.eks. manglende data, feil i databehandlingen og forsinkelser
- Kommunikasjonssystemet som overfører data mellom kjøretøyprodusent og vegvesenet som Trafikkdata Tjenesteyter
- Vegkantutstyr (Vegkant ITS sub-system), f.eks. manglende data og feil i data pga. feil på sensorer
- Kommunikasjonssystemet som overfører data mellom vegkantutstyr og vegvesenet som Trafikkdata Behandler, f.eks. dekningsproblemer, nedetid og forsinkelser
- Vegvesenets sentralsystem (Trafikkdata Behandler), f.eks. manglende data, feil i databehandlingen og forsinkelser
- Sekundærdata fra Meteorologisk institutt, f.eks. feil i data eller feil i prognoser

- Kommunikasjonssystemet som overfører data mellom Meteorologisk institutt (Sekundærdata Tjenesteyter) og vegvesenet som Trafikkdata Behandler
- Kommunikasjonssystemet som overfører data fra vegvesenet som Trafikkdata Tjenesteyter til Trafikkdata Bruker, f.eks. dekningsproblemer, nedetid og forsinkelser
- Trafikkdata brukers medium som brukes for å ta imot meldinger fra vegvesenet som Trafikkdata Tjenesteyter. Brukers medium kan f.eks. være integrert i kjøretøyet og være en del av Kjøretøy ITS sub-system og det kan være en smarttelefon eller en PC, f.eks. hos en entreprenør.
- Trafikkdata Bruker, f.eks. feil tolking av melding, manglende oppfattelse av melding eller manglende aktivering av den relevante ITS applikasjonen.

Risikoanalyse av RSI konseptet er en kompleks oppgave. Vurdering av uønskede hendelser, potensielle konsekvenser og mulig sannsynlighet ved deling av data og prediksjoner fra Statens vegvesen bør derfor involvere eksperter fra mange områder. Eksempler på slike områder er kjøretøyteknologi, sensorteknologi, informasjons- og kommunikasjonsteknologi, meteorologi, vintervedlikehold og føreradferd og pedagogikk.

5 Aksept for logging og deling av trafikkdata

5.1 Innledning

Deling av data mellom de involverte aktørene er en grunnleggende faktor i kooperative ITS-løsninger. Det medfører behov for å studere en rekke problemstillinger knyttet til dataeierskap og deling av data. VDoIT har derfor særlig fokus på personers villighet til å og aksept for å dele data om blant annet egen reise- eller kjøreadferd.

Dette kapittelet svarer på problemstillinger rundt villighet i befolkningen til å dele data med andre og med Statens vegvesen. Det inneholder en beskrivelse og drøfting rundt holdninger til deling av data og strategier for rekruttering av brukere. Med "brukere" menes her førere av biler som logger data, som kan deles og brukes i myndighetenes styring av sikkerhet i trafikken. For Statens vegvesen vil det være viktig å få et stort dataomfang i RSI for å sikre kvalitet og representativitet i loggede data, og man er dermed avhengig av å oppnå et tilstrekkelig antall førere som er villig til å dele data.

For å beskrive holdninger til tiltak brukes gjerne begrepet "aksept". Dette er et omfattende forskningstema innenfor både ITS og andre typer transporttiltak som direkte berører trafikantene (f.eks. vegprising), fordi det er en viktig forutsetning for å få implementert slike tiltak på en best mulig måte og med tiltenkt effekt (Katteler 2005, Steg og Schuitema 2007). Den økende interessen for å forklare eller beskrive holdninger kan ses i lys av en økende anerkjennelse av at politikkutforming skjer i en tovegs dynamikk mellom myndigheter og trafikanter (Vlassenroot 2011).

Kapittelet dokumenterer erfaringer fra andre prosjekter og initiativer der deling av data har stått sentralt. Dette gjelder både deling av personlige reisedata, deling av data innen næringstransport og deling av atferdsdata. Til slutt oppsummeres implikasjoner av disse funnene for RSI og for VDoIT.

5.2 Aksept for å dele reise- og atferdsdata

5.2.1 Deling av reisedata med GPS

Selv om et stort antall undersøkelser har brukt GPS for å samle inn reisedata, har ganske få rapportert responsvariasjoner og vilje til å delta/dele data (Stopher 2008). Enkelte studier antyder en typisk svarprosent på omtrent en tredjedel (Roux m.fl. 2009, Stopher m.fl. 2008). Fordi rekruttering til GPS-baserte reisevaneundersøkelser ofte er knyttet til tradisjonelle reisevaneundersøkelser er svarprosenter vanskelig å måle. Seleksjon bidrar derfor til skjevheter i vilje til å spore egne reiser og dele reisedata.

Noen studier rapporterer brukeraksept av innsamling av GPS-baserte reisedata. De fleste studier er imidlertid fokusert på teknologisk gjennomførbarhet og vier lite ressurser til brukerne. Enkelte studier viser imidlertid at viljen til å spore reisene er høyere i husholdninger med høy inntekt, husholdninger med mer enn én bil og high-tech utstyr, yngre aldersgrupper, og hos menn (Hawkins og Stopher 2004, Roux m.fl. 2009).

5.2.1.1 Deling av egne reisedata ved bruk av mobilapplikasjon: SMiO

For å oppnå et bedre og mer målrettet kollektivtilbud trengs mer informasjon om reisemønster. Det gjennomføres derfor både nasjonale og lokale reisevaneundersøkelser, og Ruter AS gjennomfører jevnlig undersøkelser blant sine kunder. Det er imidlertid ønskelig med bedre data, både kvantitativt og kvalitativt.

Det finnes mengder av datakilder rundt i samfunnet som står ubenyttet, enten på grunn av manglende metoder og verktøy til å analysere data, eller fordi man ikke har funnet en hensiktsmessig måte å høste data på. Forskningsprosjektet Smidig Mobilitet i Oslo (SMiO) søker å gripe an denne problemstillingen ved å i) se på hvordan man smartere kan samle supplerende data til de tradisjonelle reisevaneundersøkelsene og ii) etablere metoder for å utnytte disse dataene slik at de blir til hjelp for hovedstadsområdets planleggere.

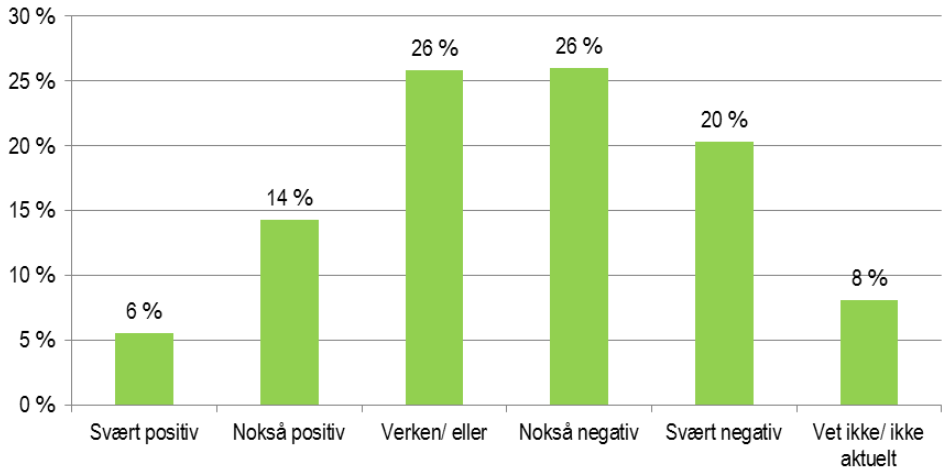
I prosjektet benyttes smarttelefonteknologi til å samle inn informasjon om reiseatferd og reiseruter for å kunne supplere eksisterende reisevaneundersøkelser.

Innen ferdigstillelsen av SMiO-prosjektet vil det være gjennomført kartlegginger om holdninger til deling av egne reisedata samt villighet til å dele egne data. I det følgende gjøres det kortfattet rede for utformingen av og resultatene fra disse kartleggingene. Den første kartleggingen omfatter den *generelle befolkningen* i Oslo og Akershus. Den andre kartleggingen er mer omfattende og retter seg mot kollektivbrukere som blir *forespurt om å dele egne data* i en demonstrator. Den siste kartleggingen er gjennomført blant kollektivbrukere som *har delt sine egne reisedata* i en demonstrator.

Kartlegging av holdninger blant befolkningen i Oslo og Akershus

Undersøkelsen ble gjennomført som del av Norstats webomnibus. Omnibusen sendes ut til brukere av Norstats webpanel, som består av over 80 000 respondenter over 18 år som på forhånd har sagt seg villige til å delta i slike undersøkelser. Omnibusen sendes ut med invitasjon på e-post til et landsrepresentativt utvalg fra panelet[2], og inneholder spørsmål om ulike tema fra ulike aktører. Fire spørsmål var bestilt til SMiO, disse ble kun stilt til respondenter hjemmehørende i Oslo eller Akershus. Det endelige utvalget besto av 743 personer. Litt over halvparten (53 %) bor i Oslo, den andre halvparten i Akershus.

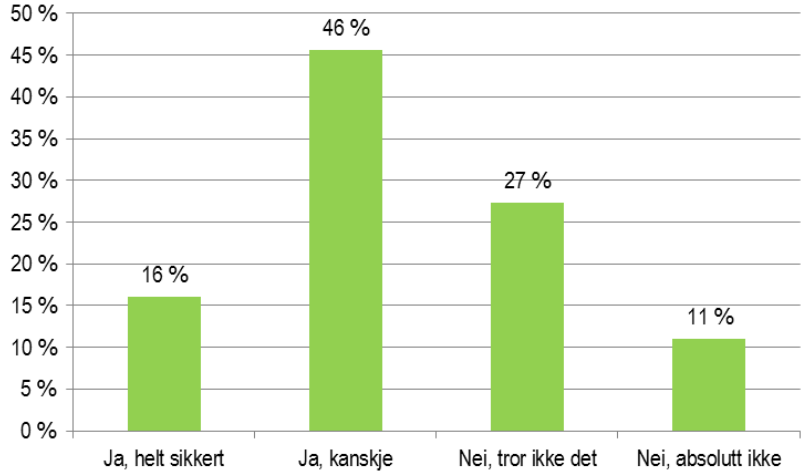
En rekke applikasjoner ber om å få vite hvor brukeren befinner seg. Dette gjelder både værtjenester, sosiale medier, treningsapplikasjoner mm. Respondentene ble spurt om sitt syn på å dele informasjon om hvor de befinner seg via slike applikasjoner. Som Figur 12 viser stiller nærmere halvparten av respondentene seg negative til dette. Omtrent en fjerdedel er verken for eller mot, mens 20 % er nokså eller svært positive. Spørsmålet er ikke aktuelt for 8 % av respondentene.



Figur 12: Syn på å oppgi posisjonering ved bruk av applikasjoner; Oslo og Akershus 2013. Prosent.

[2] Kvotert på kjønn og fylke

Respondentene ble også spurt om de kunne tenke seg å registrere sin egen reiseaktivitet via f.eks. en applikasjon dersom en slik funksjon blir tilgjengelig, slik det er tenkt i SMiO. Her svarer 16 % at de helt sikkert kan tenke seg å gjøre dette. Ca. 46 % kan kanskje gjøre det, mens 27 % er mer skeptiske og tror ikke de vil registrere reisene sine. I overkant av én av ti respondenter (11 %) kan absolutt ikke tenke seg å registrere sine reiser.



Figur 13: Holdning til å registrere egen reiseaktivitet med en mobilapplikasjon; Oslo og Akershus 2013. Prosent.

Dersom vi kun ser på de som bruker reiseapplikasjoner i dag, sier hele 73 % at de kanskje eller helt sikkert kunne tenke seg å registrere sine egne reiser. Dette tyder på at man kan forvente at flere vil akseptere egenregistrering etter hvert som de tar i bruk slike applikasjoner.

Tabell 3 viser hvordan aksept for registrering av egne reiser varierer med ulike personkarakteristika. De fire kategoriene på akseptvariabelen er her slått sammen til to for at tabellen skal bli lettere å lese – "Ja, helt sikkert" og "Ja, kanskje" er slått sammen til "Ja", mens "Nei, tror ikke det" og "Nei, helt sikkert ikke" er slått sammen til "Nei".

Av tabellen kan vi lese at andelen menn som er positive til egenregistrering er noe høyere enn blant kvinner, men denne forskjellen er ikke signifikant[3]. Det samme gjelder forholdet mellom Oslo og Akershus. Videre viser tabellen at aksepten for egenregistrering avtar med økende alder. Det ser også ut til at de med grunnskole er mindre positive enn de med høyere utdanning. Til slutt er det en høyere andel som er positive til egenregistrering blant de med høyest inntekt enn blant de med lavere inntekt. De med lavest inntekt er minst positive.

Selv om aksepten for SMiO-tanken varierer, er det så godt som ingen av undergruppene som har en andel positive på under halvparten. Unntaket er personer med grunnskole og de som aldri reiser kollektivt. Den sistnevnte gruppen er imidlertid ikke så interessant i denne sammenhengen, etter som problemstillingene i VDoIT ikke berører kollektivtrafikk.

[3] Pearson Chi-Square= 0,804, p=0,370

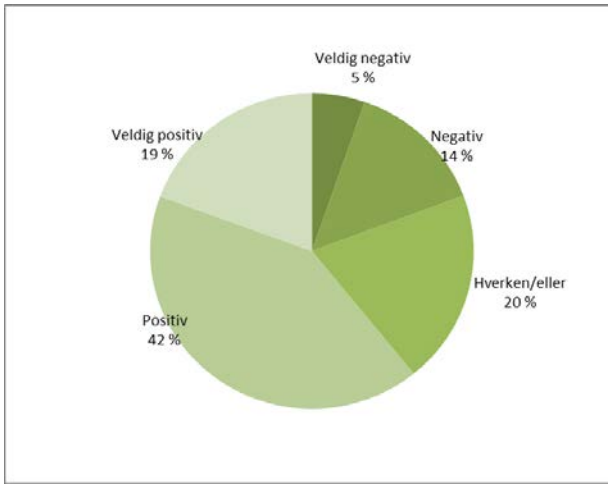
Tabell 3: Holdning til å registrere egne reiser med mobilapplikasjon – personkarakteristika; Oslo og Akershus 2013. Prosent.

	Registrere egne reiser via applikasjon?			
	Ja	Nei	Totalt	n
Andel	62 %	38 %	100 %	743
Kjønn				
Mann	63 %	37 %	100 %	357
Kvinne	60 %	40 %	100 %	386
Alder				
18-30 år	71 %	29 %	100 %	140
30-39 år	67 %	33 %	100 %	153
40-49 år	61 %	39 %	100 %	139
50 år +	55 %	45 %	100 %	311
Bosted				
Akershus	61 %	39 %	100 %	353
Oslo	63 %	37 %	100 %	390
Utdanning				
Grunnskole	47 %	53 %	100 %	34
Videregående skole	61 %	39 %	100 %	172
Uni./ høgskole mindre enn 4 år	67 %	33 %	100 %	224
Uni./ høgskole 4 år eller mer	61 %	39 %	100 %	307
Reisefrekvens kollektivt				
4-7 dager per uke	66 %	34 %	100 %	253
Ukentlig	66 %	34 %	100 %	145
Månedlig	66 %	34 %	100 %	163
Sjeldnere	51 %	49 %	100 %	154
Aldri	36 %	64 %	100 %	28
Inntekt i 1000 kr				
Inntil 200	57 %	43 %	100 %	28
201-400	69 %	31 %	100 %	85
401-600	62 %	38 %	100 %	114
601-800	63 %	37 %	100 %	100
801-1000	66 %	34 %	100 %	125
1000-1200	65 %	35 %	100 %	71
1200 +	78 %	22 %	100 %	64

Kartlegging av holdninger blant kollektivreisende i Oslo og Akershus
Aksept og villighet til å dele egne reisedata i en mobilapplikasjon ble undersøkt i en spørreundersøkelse blant 835 kollektivreisende i Oslo og Akershus.

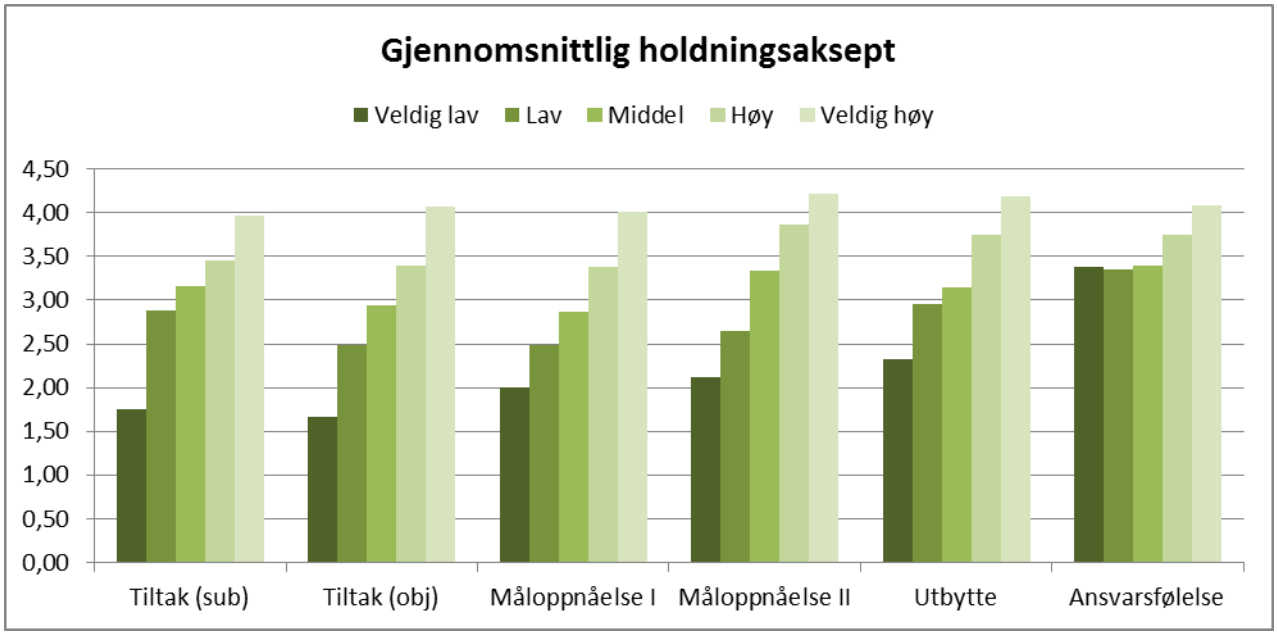
Studien kartla både *holdningsaksept* og *aktiv aksept* til deling av egne reisedata. Holdningsaksept ble målt ved spørsmålet '*Hvordan stiller du deg til innføring av et system som beskrevet over?*' der *1=veldig negativ, 2=negativ, 3=hverken positiv eller negativ, 4=positiv og 5=veldig positiv.* Aktiv aksept ble målt ved spørsmålet '*Er du interessert i å delta i dette prøveprosjektet?*'.

Figur 14 viser h*oldningsaksept* til systemet for å dele data om egne kollektivreiser. Figuren viser at over halvparten av de kollektivreisende (61 %) er positive til et slikt system, mens 1 av 5 er negative. Den gjennomsnittlige holdningsaksept er noe høyere blant menn (3,67) enn blant kvinner (3,47), men noe overraskende finnes ingen forskjeller mellom utdanningsgrupper, yrkesaktivitet, reisemønster og -frekvens. Holdningsaksept er videre høyere i den yngste aldersgruppen (under 20 år) og lavere i den eldste aldersgruppen (over 60 år).



Figur 14: Holdningsaksept til system for å dele egne reisedata (n=800)

Den viktigste forklaringen på holdningsaksept er den enkeltes forståelse av tiltaket. Figur 15 viser gjennomsnittlig holdningsaksept (min=1, max=5) blant personer med ulik grad av tiltaksforståelse (subjektiv og objektiv), ulik grad av forventninger til måloppnåelse, ulik grad av opplevd utbytte og ansvarsfølelse. Figuren viser tydelig at større forståelse av tiltaket, større tiltro til tiltakets effektivitet og forventet utbytte for egen person gir økende holdningsaksept. I grupper som er særlig enige i at kollektivreisende skal bidra til å løse utfordringer i kollektivsystemet er også holdningsaksepten tydelig høyere enn hos andre.



Figur 15. Gjennomsnittlig holdningsaksept blant respondenter med ulik grad av tiltaksforståelse (n=793), forventning til måloppnåelse (n=791, n=495), opplevd utbytte (n=791) og ansvarsfølelse (n=795).

Til sammen 63 % av respondentene var villige til å rapportere egne reisedata i det systemet som ble beskrevet. Dette er i samsvar med funn i kartleggingen av befolkningens aksept til å dele data. Kartleggingen viser videre at *aktiv aksept* er høyere hos menn enn kvinner, at aksepten synker med økende alder og at aksepten er lavere i grupper som reiser kollektivt ukentlig eller sjeldnere.

5.2.1.2 Deling av data innen næringstransport: NonStop

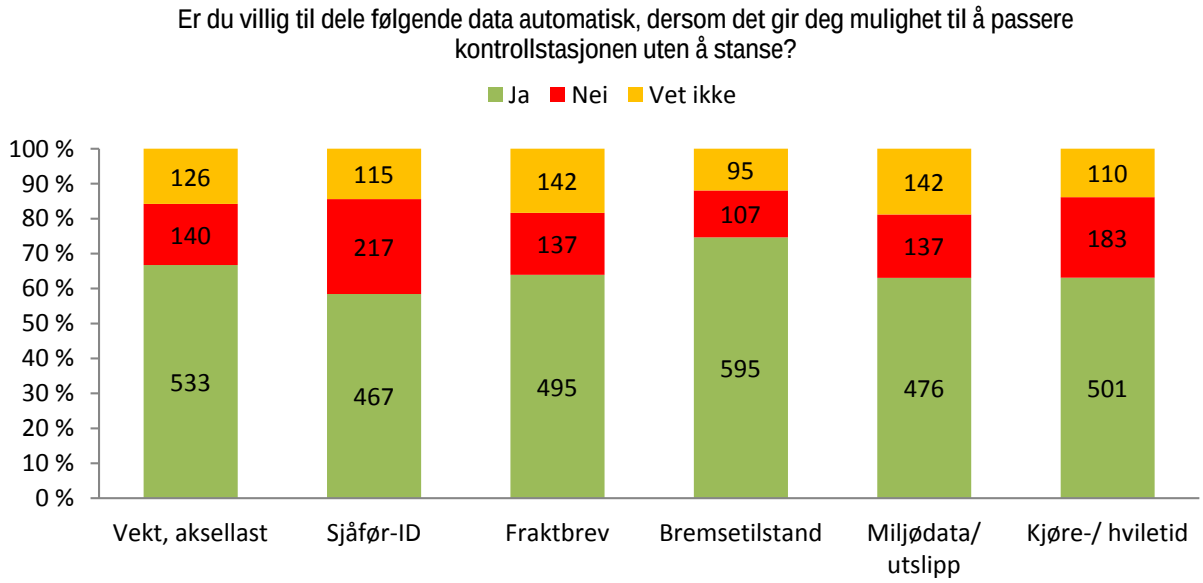
NonStop er et forsknings- og utviklingsprosjekt som inngår i Forskningsrådets SMARTRANS-program. Formålet med NonStop-prosjektet er å utvikle, implementere og evaluere et automatisk system for målrettet utvelgelse av kjøretøy for tungbilkontroll. Prosjekteier er Statens vegvesen (Vegdirektoratet), mens SINTEF er forskningspartner og har ansvar for prosjektledelse. Norges Lastebileier-Forbund (NLF) og CIBER inngår også som partnere i prosjektet.

I prosjektet ble det gjennomført en undersøkelse blant transportbedrifter i Norge, rundt temaet kontrollvirksomhet og effektivisering og kvalitetsheving av denne. En del av undersøkelsen fokuserte også på muligheter for å etablere et system hvor data om kjøretøyet eller forhold ved transportoppdraget sendes automatisk (f.eks. via AutoPASS-brikken) mens kjøretøyet er på vegen. Tanken bak et slikt system er at dersom dataene viser at alle forhold er i henhold til regelverket, kan kjøretøyet passere kontrollstasjonen uten å stoppe. Men dette forutsetter aksept for at slike data deles automatisk.

Undersøkelsen det her refereres til er gjennomført som en web-undersøkelse blant 1 018 respondenter i bedrifter som er medlemmer av bransjeorganisasjoner som Norsk Lastebileier-Forbund (NLF), Maskinentreprenørenes forbund (MEF), NHO Transport, NHO transport og logistikk og Transportarbeiderforbundet.

Sjåførene som deltok i undersøkelsen, ble spurt om de var villige til å dele ulike typer informasjon automatisk i et system som ble beskrevet – mot at dette gir dem mulighet til å passere kontrollstasjonen uten å stanse. Resultatet er vist i figuren nedenfor. Den grønne delen av søylene representerer sjåførene som er

villige til å dele data automatisk, den røde delen representerer de som ikke ønsker å dele data på denne måten, mens gult område viser de som er usikker. Høyden på søylene viser prosentandel som har gitt de ulike svarene.



Figur 16. Yrkessjåførers villighet til å dele data automatisk. n=(774-799).

Generelt er sjåførene velvillig innstilt til automatisk deling av data, dersom dette gjør kontrollsituasjonen mer effektiv. I størrelsesorden 58 -74 % av sjåførene ønsker å dele de datatypene som er skissert i spørsmålet; vekt/aksellast, sjåfør-ID, fraktbrev, bremsetilstand, miljødata/utslipp og kjøre-/hviletid. Tilsvarende er andelen som svarer negativt på spørsmålet i størrelsesorden 13 -27 %. Størst skepsis er knyttet til automatisk deling av sjåfør-ID, muligens fordi dette oppleves som mer personlig enn deling av data om kjøretøyet. Det kan også skyldes at relevansen av å dele sjåfør-ID oppleves som mindre enn deling av de andre typene data.

De som har svart at de ikke ønsker å dele informasjon om kjøretøyet eller transportoppdraget automatisk, begrunner dette i hovedsak med personvernhensyn eller at de tror et slikt system vil være for enkelt å jukse med for de som ønsker å unndra seg kontroll.

5.2.2 Deling av data om kjøretøyet og kjøreatferd

5.2.2.1 Hendelses- og atferdsregistratorer

Det fins ulike typer tekniske innretninger som ved hjelp av kjøretøyets on-board diagnostics (OBD II) overvåker og registrerer parametere ved kjøretøyet og førerens kjøreatferd. Typiske data som registreres er fart, posisjonering, bremse- og akselerasjonsmønster og drivstofforbruk(Horrey m.fl. 2012), men det finnes også flere mulige typer informasjon som kan logges (f.eks. forhåndsdefinerte indikatorer som logger potensielt farlige situasjoner og hendelser). Loggingen kan enten foregå kontinuerlig eller kun ved hendelser etter på forhånd angitte grenseverdier (f.eks. relatert til fart, nedbremsing, akselerasjon mm.). I mange tilfeller inneholder også disse systemene en form for feedback-løsning til førerne, som kan gi læring for å oppnå mer trafikksikker atferd.

De fleste studier av bruk av atferdsregistrator er foretatt blant ansatte i bedrifter og organisasjoner med egne bedriftsbiler (Horrey m.fl. 2012), og har fokusert på systemets innvirkning på kjøreatferd og/eller

trafikksikkerhet. Det fins foreløpig lite kunnskap om *aksept* for å ha atferdsregistrator i bilen, på tross av at dette er en svært viktig forutsetning for å ta i bruk systemet. Mye tyder på at aksepten avhenger av det man opplever som hensikten med systemet. For ansatte i virksomheter kan denne typen teknologi oppleves som unødvendig overvåkning. Bekymring for at ulike interessenter (som f.eks. forsikringsselskaper, bilfabrikanter og ulike deler av myndighetsapparatet) skal få tilgang til og bruke data på uønskede måter er også til stede og gjør slike systemer kontroversielle (Bustamante og Fernando 2006a, Bustamante og Fernando 2006b)

For mange kan det imidlertid være aktuelt å "ofre" personvernhensyn hvis de får noe tilbake. Ulike typer incentivordninger kan derfor stimulere til å kjøre med slike systemer på tross av at man stiller seg negativ til idéen.

5.2.2.2 Belønningssystemer

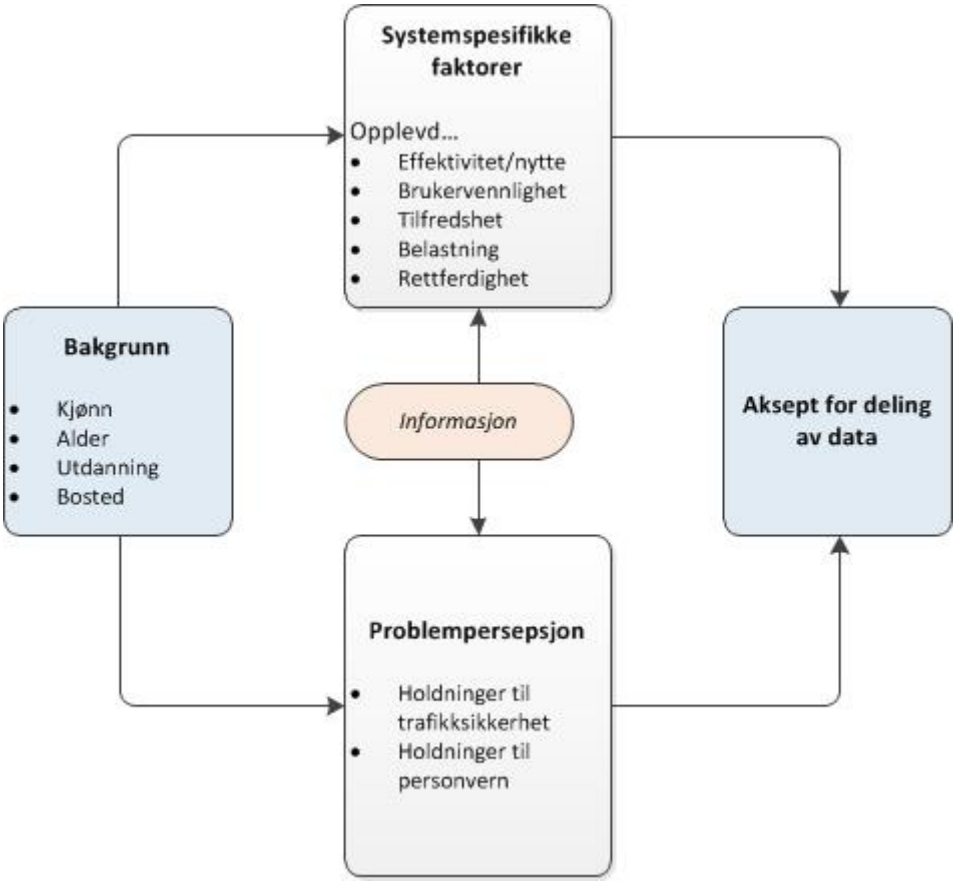
De seneste årene har det kommet flere studier hvor såkalte Pay-as-you-drive (PAYD)- og Pay-as-you-speed (PAYS)-løsninger, det vil si hvor forsikringspremien er knyttet til den enkelte forsikringstakers bruksmønster og/eller fartsatferd (Bolderdijk m.fl. 2011, Dijksterhuis m.fl. 2015, Lahrmann m.fl. 2012, Merrikhpour m.fl. 2014, Stigson m.fl. 2013). Disse konkluderer med at slike ordninger vil ha positiv effekt på kjøremengde og/eller ulike variabler for kjøreatferd (fart, akselerering, bremsing, svingebevegelser) og derved ha positive effekter på sikkerhet, miljø og klima (Lahrmann m.fl. 2012)

Potensialet ved bruk av PAYS-ordninger kan være stort i utsatte risikogrupper som f.eks. ungdom. Effekter vil avhenge av hvordan insentivordningen er strukturert og presentert (Dijksterhuis m.fl. 2015). Spesielt viktig er det at responsen (belønningen eller straffen) er relativt sikker og at den kommer raskt etter den atferden som er i fokus for ordningen (Abrahamse m.fl. 2005, Lehman og Geller 2008, Skinner 1974). Størrelsen på belønningen har vist seg å være mindre viktig enn tidspunkt for belønning og hvor sikker den er (Bjørnskau og Elvik 1992, Skinner 1974, Zaal 1994). Studier tyder videre på at et poengsystem eller lignende kan benyttes i stedet for tilbakemelding om monetære besparelser, fordi individer ikke er særlig sensitive for utvekslingen mellom slike poeng og den endelige belønningen (Bagchi og Li 2011, Hsee m.fl. 2003).

5.3 Faktorer som påvirker aksept

Innenfor temaet vegprising har man lenge forsket på hva som påvirker aksept av atferdsvridende tiltak (se f.eks. Schade og Schlag 2003, Stern m.fl. 1993). Slik forskning er mindre utbredt innenfor ITS-området, hvor akseptundersøkelser i stor grad har vært begrenset til rene brukerevalueringer av utvalgte egenskaper ved f.eks. et førerstøttesystem (opplevd nytte, irritasjon m.m.) (Vlassenroot m.fl. 2008). De senere årene har det imidlertid blitt gjennomført mer helhetlige studier av holdninger til ulike typer ITS (bl.a. Vlassenroot m.fl. 2010), mange med utgangspunkt i kjente psykologiske rammeverk som Ajzens *Theory of Planned Behavior* (TPB) (Ajzen 1991, Ajzen 2002) og *Value-belief-norm (VBN) theory* (Steg m.fl. 2005, Stern 2000).

Med bakgrunn i de akseptstudier som er gjennomført innen transportsektoren generelt og for ITS-tiltak spesielt, har vi skissert en teoretisk forklaringsmodell for hva som vil påvirke holdninger til å dele data, der formålet med deling av data er økt trafikksikkerhet. En slik modell er presentert i Figur 17.



Figur 17 Forklaringsmodell for aksept av deling av data

Hovedessensen i Figur 17 er at bakenforliggende variabler som kjønn, alder og utdanning mv. påvirker holdninger til personvern (*vil mitt behov for personvern bli ivaretatt på en måte som er tilfredsstillende for meg?)* og holdninger til trafikksikkerhet (*er glatte veger et problem for trafikksikkerheten og er dette noe jeg er opptatt av?).* Forståelsen av de utfordringer teknologien er ment å løse omtales i litteraturen som problempersepsjon. Problempersepsjon påvirker den enkeltes aksept eller avvisning av et tiltak. Dersom en situasjon kan vurderes som et samfunnsproblem, gir dette ofte støtte til tiltak som skal løse dette problemet.

Bakgrunnsvariablene forventes også å påvirke hvorvidt man har erfaring med ulike typer teknologiske systemer som logger posisjonerings- og/eller atferdsdata. Holdninger til trafikksikkerhet er også viktig. Både oppfatninger av hvor viktig trafikksikkerhet er, av glatte veger som årsak til alvorlige ulykker og av myndighetenes ansvar for og evne til å gripe inn for å løse slike problemer, antas å være viktig for hvilke konsekvenser man tror at deling av data vil ha. Konsekvensene kan både være positive i form av økt trafikksikkerhet, og negative i form av at man må gjøre noe rent praktisk for å logge/dele og av at man kan oppleve en viss grad av overvåkning.

Videre kan en rekke systemspesifikke indikatorer antas å være av betydning for om man er positiv eller negativ til bruk. Nærmere bestemt omfatter disse variabler som den enkeltes oppfatning av systemets effektivitet, brukervennlighet, nytte, tilfredshet, belastning (i form av merarbeid, stress, distraksjon, irritasjon, frustrasjon, usikkerhet) og rettferdighet. Disse faktorene påvirkes både av bakgrunnsvariabler, tidligere erfaringer og problempersepsjon, og av den informasjon og kunnskap den enkelte har om det aktuelle systemet/tiltaket. Korrekt og tilstrekkelig informasjon om et tiltak kan mange ganger være en

forutsetning for at et foreslått tiltak oppnår aksept (Link og Polak 2001), og studier har vist at tiltak er blitt nedstemt på grunn av misforståelser knyttet til utformingen av tiltaket (Gaunt m.fl. 2007).

5.4 Implikasjoner for RSI og VDoIT

Innholdet i dette kapitlet kan brukes til å lage en strategi for rekruttering av førere som er villige til å logge data i RSI. Sentrale spørsmål ved utforming av en slik strategi vil handle om i) å definere ønsket antall deltakere og hvor mange som må kontaktes/spørres for å oppnå ønsket antall, ii) å definere hvem man ønsker som deltakere, og iii) å definere forutsetninger og insentiver for å oppnå deltakelse fra mange nok i den definerte målgruppen.

5.4.1 Rekruttering

Det er foreløpig ikke kjent hvor mange deltakere (bileiere) man ønsker i RSI-prosjektet. Erfaringer fra SMiO og andre studier viser at man som et utgangspunkt må regne med at under halvparten av de som spørres vil benytte seg av et tilbud om å logge og dele data uten noen form for kompensasjon utover bedre allmenn trafikkinformasjon og, i neste instans, trafikksikkerhet. Rent generelt kan man si at dette er en ganske vag "belønning" som man ikke kan vite om vil komme til nytte for en selv. Det trengs derfor et over middels stort engasjement for trafikksikkerhet for å være villig til å delta. På den andre siden er heller ikke kostnadene for å delta særlig store, gitt at man stoler på at nødvendige personvernhensyn blir ivaretatt. Anonymitet og personvern er et sentralt punkt i rekrutteringen, og det vil være avgjørende at man klarer å inngi tillit til at data blir forsvarlig behandlet.

Deltakelsen vil selvsagt være mulig å påvirke med mer konkrete insentiver. Det vanligste er å motta en form for rabatt, dette kan være på bilforsikring eller på kjøp av bil. I RSI vil antakelig det siste være mest aktuelt av disse to, siden en kjøretøyprodusent er partner i prosjektet. Studier viser at belønningen er mest virkningsfull når den er kortsiktig, altså mottas her og nå, i stedet for at det er noe som kan oppnås på lang sikt.

5.4.2 Målgruppe

Målgruppen for rekrutteringen kan være private eller yrkessjåfører. NonStop-undersøkelsen som er omtalt i pkt. 6.2.1 viser at det fins et stort engasjement for trafikksikkerhet blant norske yrkessjåfører. Her kan imidlertid arbeidsavtaler virke kompliserende og hindre deltakelse, ettersom han/hun som kjører bilen mens den logger data, ikke nødvendigvis eier bilen.

Som vist tidligere i rapporten, viser erfaringer fra SMiO og andre studier at aksept for å dele data avtar med økende alder. Den øker imidlertid med høyere utdanning og inntekt. Det ses videre en tendens til at menn har høyere aksept for å dele data enn kvinner. Det kan derfor være hensiktsmessig å spisse fokus mot unge og middelaldrende menn med høy inntekt når man skal rekruttere bileiere. Spørsmålet er om disse også er de som vil være motivert til å delta ut fra trafikksikkerhetshensyn. Siden mange kjøretøyprodusenter ønsker å bygge en merkevare rundt sikkerhet kan man imidlertid anta at dette i stor grad vil være tilfelle.

6 Forretningsmodeller for kooperativ ITS

6.1 Innledning

I henhold til sektoransvarsprinsippet skal Statens vegvesen fremme løsninger som bidrar til at transportpolitiske målsettinger nås. Fordi kooperative ITS–løsninger antas å ha stort potensiale for å løse utfordringer i transportsystemet er det viktig å synliggjøre for aktører i posisjon til å beslutte og/eller påvirke virkemiddelbruk verdier (gevinster) kooperative ITS løsninger kan gi og hvordan disse kan innhentes. For å synliggjøre verdier (gevinster) og forutsetninger for å realisere disse er det hensiktsmessige å definere à priori forretningsmodeller. En forretningsmodell beskriver begrunnelsen for hvordan en organisasjon skaper, leverer, og fanger verdi.

For Statens vegvesen har det vært et mål med VDoIT å få økt kunnskap om hvordan man kan bruke tankegang rundt forretningsmodeller for å stimulere til økt implementering av ITS. Mer spesifikt ønsker de å bruke forretningsmodeller til å i) beskrive hvilke inntektsstrømmer knyttet til utrulling av ITS som ikke kan komme fra andre, ii) beskrive hvilke påkrevde aktiviteter/ressurser som andre aktører enn SVV ikke er villige til å ta ansvar for, og iii) synliggjøre verdi (gevinster) både internt i SVV og for eksterne aktører.

I det nedenstående beskrives det teoretiske rammeverket rundt forretningsmodeller, med spesiell vekt på forretningsmodeller for åpne data. Videre beskrives resultater fra en workshop der en forenklet forretningsmodell for RSI ble diskutert.

6.2 Om forretningsmodeller

6.2.1 Hva er en forretningsmodell?

Selv om mange forsøk er gjort på å definere begrepet forretningsmodell, er ingen enkelt definisjon fullt ut akseptert i næringslivet eller i akademiske kretser (Shafer m.fl. 2005). Forretningsmodeller brukes i en rekke disipliner, som strategi, teknologi, informasjon, e-business og innovasjon, og ulike disipliner har ofte ulike perspektiver på hva en forretningsmodell er eller bør være. Det er likevel generell enighet om at forretningsmodeller bidrar til å forklare hvordan en organisasjon skaper og leverer verdi til sine kunder (Kamoun 2008, Teece 2010). En generell definisjon av forretningsmodeller forslås av Osterwalder og Pigneur (2010), som sier at "*en forretningsmodell beskriver begrunnelsen for hvordan en organisasjon skaper, leverer, og fanger verdi*".

Forretningsmodeller kan gi svar på følgende sentrale spørsmål (Magretta 2002):

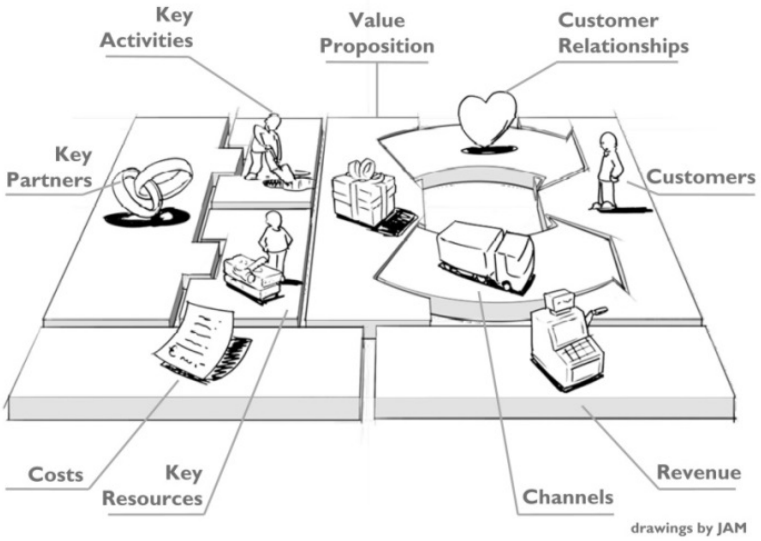
- Hvem er kunden?
- Hvordan kan man tjene penger i denne bransjen?
- Hvilken underliggende økonomisk logikk forklarer hvordan man kan levere verdi til kunde for en passende kostnad?
- Hva er de viktigste kostnadsdriverne i å levere verdi til kunden?

Et viktig aspekt i utvikling av forretningsmodeller er å undersøke aktiviteter som utføres av en gitt organisasjon i et verdikjedeperspektiv. Amit og Zott (2012:12) definerer organisasjonens forretningsmodell som et system av sammenhengende og gjensidig avhengige aktiviteter som bestemmer hvordan organisasjonen kommuniserer med sine kunder, partnere og leverandører. De understreker at forretningsmodellen består av konkrete aktiviteter - et såkalt aktivitetssystem - som har som mål å

tilfredsstille forventet behov i markedet. De understreker videre viktigheten av å spesifisere hvilke aktører som skal utføre hvilke aktiviteter og hvordan disse aktivitetene er knyttet sammen. Amit og Zotts orientering mot samhandlingsprosesser er spesielt relevant for forretningsmodeller der offentlige og private aktører må samarbeide for å etablere en etterspurt tjeneste.

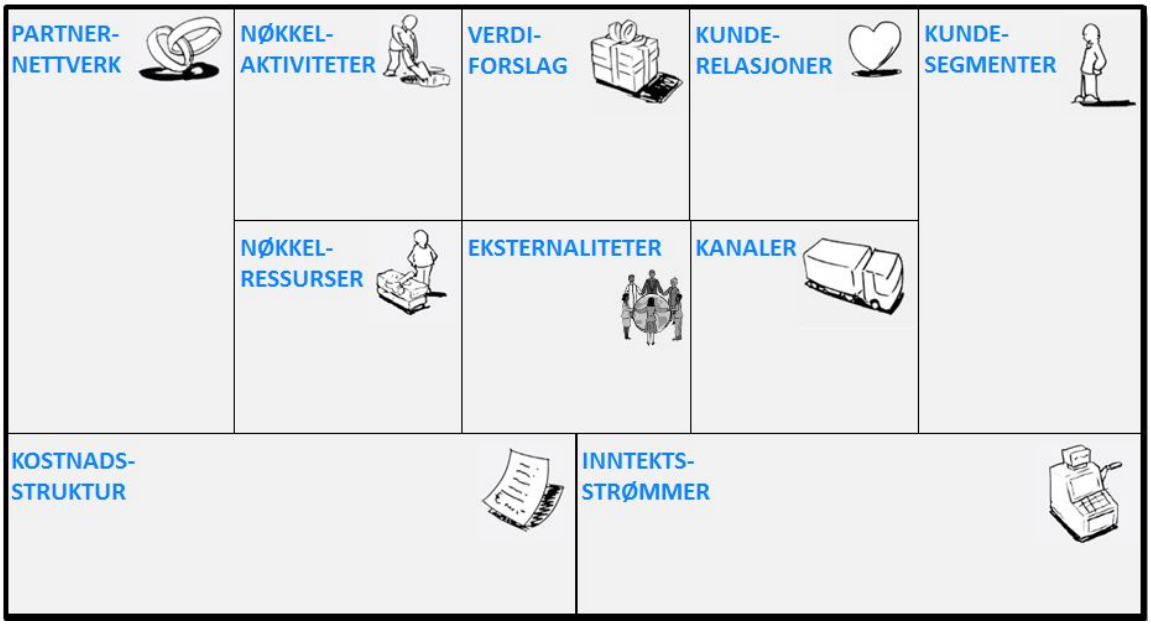
6.2.2 Hva består en forretningsmodell av?

De fleste som beskriver forretningsmodeller er enige om at en forretningsmodell består av ulike elementer som må fungere sammen. En levedyktig forretningsmodell avhenger av ulike segmenters gode samspill. Johnson og kolleger (2008) beskriver fire sentrale segmenter: kundens verdiforslag, ressurser, prosesser og profittformel. Osterwalder og Pigneur (2010) har definert ni byggesteiner innenfor en "Business Model Canvas", som illustrert i Figur 18. Deres modell er anerkjent for å tilrettelegge utvikling av forretningsmodeller og byggesteinene som utgjør rammeverket er beskrevet nedenfor.



Figur 18: Elementer i en forretningsmodell

Osterwalder og Pigneur kaller sitt rammeverk for "Business Model Canvas". Det henspiller på et blankt lerret som kan fylles med ideer innenfor en gitt struktur (se Figur 19). Modellen har blitt et av de mest anerkjente verden over for utvikling av forretningsmodeller. Rammeverket brukes av en rekke store selskaper, slik som GE, 3M, SAP, Ericsson, Oracle og NASA. I Norge har rammeverket også blitt populært, og anvendes av organisasjoner som Innovasjon Norge, SIVA og næringshager over hele landet. I Europeiske prosjekter finner vi også at rammeverket benyttes hyppig. I de videre avsnittene er de ni elementene i forretningsmodellen forklart nærmere.



Figur 19: Business Model Canvas (Osterwalder & Pigneur, 2010)

Verdiforslag beskriver hva man tilbyr av verdi til kunden gjennom produkter og tjenester. Et verdiforslag skaper verdi for et eller flere kundesegmenter gjennom en bestemt sammensetting av vare- og tjenestetilbud som oppfyller kundesegmentets behov. Viktige spørsmål å stille er:

- "Hvilken verdi skal man levere til sine kunder?"
- "Hvilket problem er det produktet eller tjenesten løser for kunden?"

Kunderelasjoner sier noe om hvilken type tilknytning man skal etablere til ulike kunder. Eksempler på dette er personlig assistanse, selvbetjening, kundeforum og møteplasser for å skape innhold og verdi sammen med kunden (ofte kalt "co-creation").

Kundesegmentene definerer de forskjellige grupper folk eller organisasjoner et selskap søker å nå og betjene. For å bedre tilfredsstille kunder kan man gruppere dem inn i segmenter med felles behov, oppførsel eller andre egenskaper. Viktige spørsmål å stille er:

- "For hvem skaper vi verdi?"
- "Hvem er våre viktigste kunder?"

Kanaler angir hvilke ulike måter man kan oppnå kundekontakt gjennom, slik som i butikk, på web og mobil. Her beskriver man hvordan bedriften får kontakt med og kommuniserer med sine kundekontakter ved levering av verdiforslaget. Det er fornuftig å tenke gjennom om man skal bruke samme kanal eller ulike måter å nå kundene på i ulike faser av kjøpsprosessen (awareness, interest, desire, action/purchase, delivery, after sales).

Nøkkelpartnere er det totale nettverket av leverandører og partnere som får forretningsmodellen til å fungere. Her finnes noen viktig typer samarbeidsforhold man kan etablere med nøkkelpartnere:

- Strategiske allianser mellom ikke-konkurrenter
- "Co-opetition" (strategisk samarbeid mellom konkurrenter)

- Joint ventures for å utvikle nye foretak
- Forhold mellom kjøper og selger for å sikre tilgang på varer og tjenester

Nøkkelaktiviteter er de viktigste aktivitetene som kreves for å få forretningsmodellen til å fungere. Aktiviteter kan sammenlignes med forretningsprosesser, og kan være ulike prosesser innen utvikling, produksjon, salg, leveranse, service og support. Viktige spørsmål å stille er "hvilke nøkkelaktiviteter krever"

- "… verdiforslaget?"
- "… distribusjonskanalene?"
- "… forholdet til kundene våre?"
- "… inntektsstrømmene?"

Nøkkelressurser er de viktigste ressursene som kreves for å få forretningsmodellen til å fungere. Disse kan være fysiske, finansielle, intellektuelle eller menneskelige, og kan eies eller leies av bedriften, eller kjøpes fra nøkkelpartnere.

Inntektsstrømmer angir hvordan man skal tjene penger på verdiforslaget. Vil man ha ulike inntjeningsmodeller for forskjellige kundesegmenter?

Kostnadsstruktur beskriver utgiftene til bedriften. Hvilke nøkkelressurser koster oss mest? Hvilke aktiviteter koster oss mest?

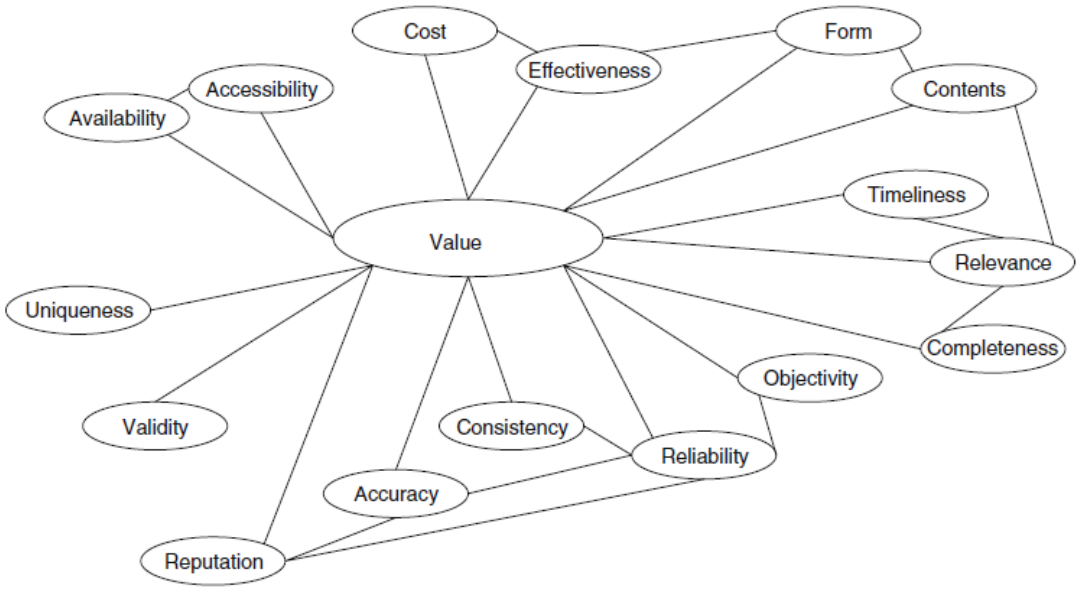
I tillegg til de tradisjonelle byggesteinene beskrevet av Osterwalder og Pigneur, foreslår prosjektet TURBLOG (2011) at en tiende byggestein inkluderes: **eksternaliteter**. Inkluderingen av denne blokken er relevant i tilfeller der forretningsmodellen skal produsere verdier som ikke nødvendigvis er knyttet til en konkret inntektsstrøm og en betalingsvillig aktør. Eksternaliteter omfatter sosiale og miljømessige verdier som forretningsmodellen skaper, samt andre ikke-finansielle verdier.

6.3 Forretningsmodeller for gjenbruk av åpne, offentlige data

Generering, håndtering og bruk av data kjent som PSI (Public Sector Information) er et omfattende temaområde som de siste årene har sett økende interesse fra både praksisfelt og forskning. I det videre omtales PSI som åpne, offentlige data. Tidligere publikasjoner vier først og fremst PSI oppmerksomhet som en pådriver for transparent, deltakende og samarbeidsbasert offentlig styring.

6.3.1 Egenskaper ved verdifull informasjon

Mange publikasjoner fokuserer i stor grad på å kvantifisere verdien av offentlige data og å identifisere hvordan organisasjoner kan gjøre forretning av denne type data. Verdien av data er uløselig knyttet til den informasjonen den kan skape, og en rekke miljøer har diskutert hvilke attributter ved informasjonen som bidrar til å skape verdi (Herrala 2007, Leviäkangas 2011). Disse verdiene er gjengitt i Figur 20.



Figur 20. Verdifulle egenskaper ved informasjon (Leviäkangas 2011:49)

Informasjonens *kostnad* er utelukkende knyttet til pengekostnader, men henger tett sammen med effektivitet. *Effektivitet* beskriver graden av (adferds)endring informasjonen bidrar til, og kan således indikere høy eller lav kostnadseffektivitet. *Tidsriktig* informasjon møter etterspørselen etter informasjon på et gitt sted og innenfor et gitt tidsrom. Dette henger sammen med *relevans*: om informasjonen ikke er tilgjengelig på riktig tid eller riktig sted er den heller ikke relevant. Relevans handler også om *fullstendig* informasjon: dersom informasjonen er ufullstendig er den ikke relevant. Informasjonens *form* er også viktig for at den skal kunne forstås og hensyntas.

I mange tilfeller vil *objektiv* informasjon være avgjørende, særlig når tredjepart er involvert. Dette er nært knyttet til *pålitelighet*, *nøyaktighet* og *konsistensgrad*.

Validitet viser til at informasjon er hva den utgir seg for å være, mens *unik* informasjon har et særlig konkurransefortrinn fremfor informasjon som tilbys fra flere, ulike kilder. Informasjon med *godt omdømme* antas videre å være mer ettertraktet og verdifull enn informasjon av lik kvalitet som av ulike årsaker har dårligere omrømme.

Sist er *tilgang* til og *tilgjengeligheten* til informasjon avgjørende, og har særlig stor verdi for potensielle brukere.

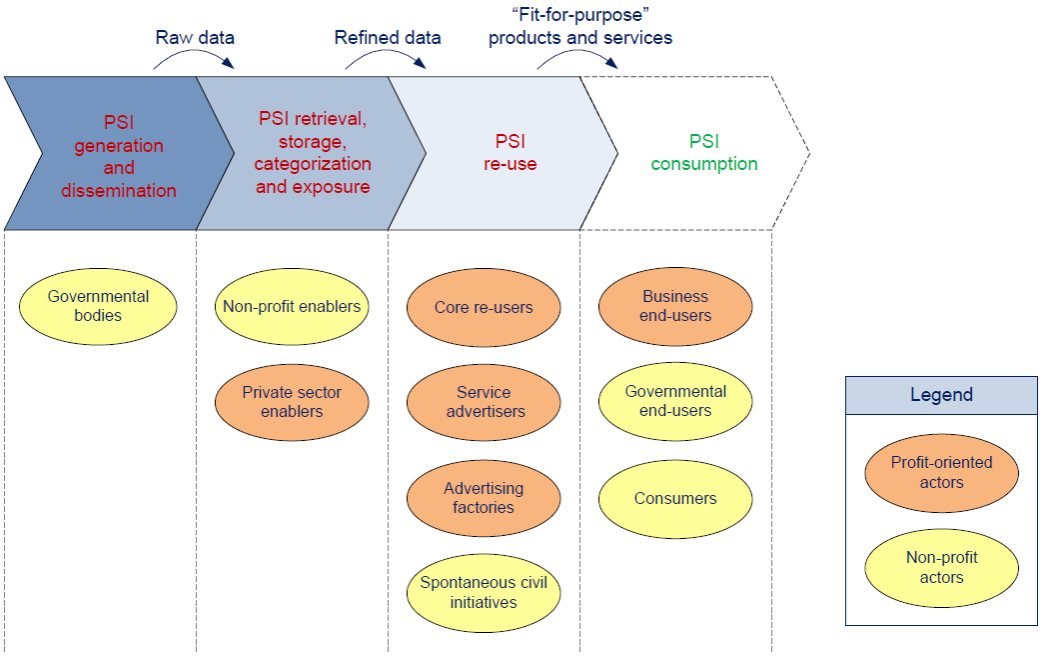
Leviäkangas (2011:50) vektlegger at samfunnets verdsetting av Information hovedsakelig kommer av sosioøkonomiske nytte-kostnadsanalyser som inkluderer eksternaliteter. Han beskriver netto nytte for samfunnet som summen av fordelene informasjon gir til brukere, tjenesteytere og eksternaliteter på den ene siden, og kostnader knyttet til investeringer, driftskostnader og subsidier hos offentlige og private aktører på den andre siden.

6.3.2 Roller og modelltyper

Både private og offentlige aktører kan være tilbydere og brukere av offentlige data. Ferro og Osalla (2012, 2013) skiller mellom to hovedgrupper brukere av offentlige data:

i) brukere som formidler data, og
ii) brukere som bygger annen informasjon og andre tjenester rundt offentlige data.

En finere inndeling er gjengitt i Figur 21. Figuren viser for det første de ulike fasene offentlige data gjennomgår på vei fra rådata, via foredling til formålsbestemte produkter og tjenester: i) *generering og formidling*, ii) *nedlasting, gruppering og tilgjengeliggjøring*, iii) *foredling og gjenbruk*, og iv) *sluttbruk*. For det andre viser figuren hvilke roller som er involvert i de ulike fasene, og skiller mellom roller som er og ikke er profittorienterte.



Figur 21: Roller involvert i utvikling og gjenbruk av åpne, offentlige data (Ferro og Osella 2013)

Basert på casestudier av konkrete eksempler på produkter og tjenester som tilbys på det kommersielle markedet presenterer Ferro og Osella (2013) åtte idealtyper av forretningsmodeller for å hente verdier fra gjenbruk av offentlige data. De tre første er basert på etablerte arketyper av modeller, og vil derfor kun beskrives med eksempler knyttet til offentlige data. De øvrige modellene er foreslått spesifikt med tanke på åpne, offentlige data.

Premiummodellen. I denne modellen tilbys et produkt eller en tjeneste karakterisert ved høy kvalitet og verdi. Dette kan f.eks. være data av særlig høy kvalitet eller data som oppdateres kontinuerlig. Produktet/tjenesten gir inntekter gjennom to alternative inntektsstrømmer: i) betaling per bruk der brukeren betaler for enkelttilgang til data, eller ii) gjentakende tilgangsgebyr som gir tilgang til data så lenge gebyr for tilgangsperioden er betalt.

Freemiummodellen. I denne modellen tilbys et unikt og verdifullt produkt/tjeneste gratis. Dette skaper en stor kundebase, og tilbys sammen med betalingspliktige tilleggstjenester brukeren får lyst til å anvende etterhvert som han/hun blir mer fortrolig med hovedtjenesten (Bakås m.fl. 2014). Knyttet til offentlig data kan hovedproduktet som tilbys f.eks. være antall passeringer i en gitt bomstasjon, mens betalingspliktige tilleggstjenester kan omfatte kjøretøykategori, passeringstidspunkt etc.

Barberhøvelmodellen. I denne modellen selges et produkt eller en tjeneste til en overkommelig oppstartspris, mens tilleggsutstyr som er nødvendig for å bruke produktet sikrer høyere margin gjennom levetiden til produktet. Navnet på modellen stammer fra Gillettes salg av barberhøvler og blader. Prisen på høvelen er relativt lav, slik at de skal velge deres system for barbering. Deretter selges hvert enkelt blad, som bør byttes ut jevnlig, til en relativt sett langt høyere pris (ibid.). Modellen har klare likhetstrekk med freemiummodellen, men skiller seg ut ved at barberhøvelmodellen forutsetter at bruker også betaler for hovedproduktet. Ferro og Osella (2013) knytter denne til infrastruktur, og fremholder at med tanke på offentlige data vil modellen gi alle gratis tilgang til skyplattformer med APIer (barberhøvelen).

I tillegg til disse tre modellene beskriver Ferro og Osella fem andre arketyper med egenskaper som er særegne for offentlige data. Disse kan imidlertid ikke sies å være arketyper av forretningsmodeller, da de benytter seg av de samme prinsippene som ligger til grunn i overnevnte arketyper for å innhente verdi. Fordi det er logikken bak inntektsstrømmene som skiller ulike arketyper av forretningsmodeller fra hverandre, vil to ulike modeller med like prinsipper for verdiinnhenting tilhøre samme arketype. De gjenstående typene vil imidlertid beskrives nedenfor fordi de byggeblokkene som beskrives er relevante for å utvikle forretningsmodeller basert på offentlige data.

Open Source. Denne modellen er særlig beskrevet av Ferro og Osella (2013) med tanke på offentlige data. Denne modellen legger vekt på at alle produkter, tjenester og enkle rådata skal tilbys gratis og i et åpent format. Kostnader forbundet med å tilby data dekkes gjennom andre inntekter (ofte også basert på offentlige data) og tilleggstjenester. Modellen har store likhetstrekk til åpen programvare gjennom at data tilbydes i åpent format som tillater frie tilføyelser, bruk og redistribusjon uten tekniske barrierer. Ved at modellen tilbyr gratis data med betalingspliktige tilleggstjenester tilsvarer logikken bak inntektsstrømmene prinsippene i freemiummodellen. Som beskrevet av forfatterne gir modellen imidlertid et relevant innspill knyttet til verdiforslag (åpne formater).

Etterspørselsbaserte og tilbudsbaserte dataplattformer. Ved å opprette plattformer som katalogiserer, harmoniserer (format) og formidler data og APIer har nytteeffekter både for de som ønsker å laste opp og laste ned offentlige data. Ved bruk av en slik plattform vil data "kommodiseres", og går fra å være datasett til datastrømmer. På den ene siden vil en slik plattform kunne gi brukere av offentlige data ett enkelt datapunkt å forholde seg til, samtidig som de får tilgang til en rekke dataressurser gjennoms standardiserte APIer (etterspørselsbasert plattform). Brukere kan her betale etter freemiummodellen. Samtidig gir plattformen dataeiere mulighet til å videreformidle sine data til mange brukere gjennom ett enkelt punkt (tilbudsbasert plattform), og dataeiere kan betale et periodisk gebyr for å formidle sine data som settes i henhold til forventede gevinster for dataeier. Selv om dette ikke kan regne som en arketypisk forretningsmodell gir den nyttige innspill til nøkkelaktiviteter og kommunikasjonskanaler.

Gratis lokkeprodukt. Her beskriver Ferrero og Osella en modell der sluttbrukere lokkes til et gratis produkt/tjeneste de opplever som nyttig. Hensikten med produktet/tjenesten er å gjøre sluttbruker kjent med merkevaren og øke sluttbrukers oppmerksomhet rundt og villighet til å kjøpe andre produkter/tjenester. Dette er også i praksis en freemiummodell.

White-label. I denne modellen settes ansvaret for formidling av produkter/tjenester til tredjepart, men markedsføres som tilbyders egen merkevare.

6.4 Forretningsmodell for RSI

I det følgende beskrives resultater fra en workshop der en forenklet forretningsmodell for RSI ble diskutert. Deltakere på workshopen var seks sentrale personer fra ITS-seksjonen i Vegdirektoratet, én person fra Statens Vegvesen Region Midt, samt tre personer fra SINTEF Teknologi og samfunn.

6.4.1 Bakgrunn

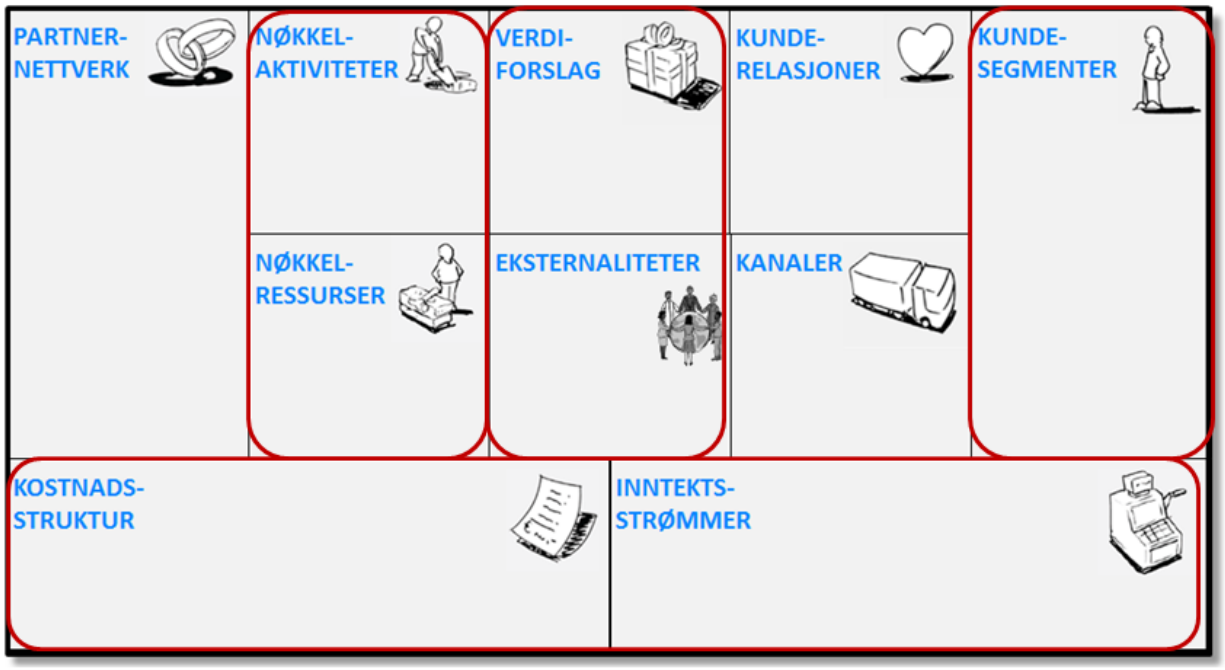
Bakgrunnen for workshopen er at Statens vegvesen ønsker bedre kunnskap om hvordan de kan stimulere til ITS, i tilfellet RSI hvordan de kan stimulere til økt instrumentering av kjøretøy slik at biler kan benyttes som sensorer. Dette vil gi data som kan nyttiggjøres til overvåkning av vegnettet, og videre til informasjon til bilførere. Siden Statens vegvesen er avhengig av samarbeid med bilprodusenter for å oppnå slik instrumentering, ønsker de å kunne bruke rammeverk for forretningsmodeller som analyseverktøy inn i slikt samarbeid.

6.4.2 Gjennomføring

Siden tankegangen rundt forretningsmodeller var ukjent for flere av deltakerne i workshopen, startet den med en presentasjon av Osterwalder og Pigneurs rammeverk for forretningsmodeller. Hvert enkelt av segmentene i rammeverket (jf. kap. 6.2.2) ble gjennomgått. Av tidsmessige hensyn ble imidlertid kun seks av segmentene i rammeverket diskutert videre i workshopen:

- Nøkkelaktiviteter
- Verdiforslag
- Kundesegmenter
- Nøkkelressurser
- Kostnadsstruktur
- Inntektsstrømmer

I tillegg ble eksternaliteter vurdert som så viktig at dette ble diskutert som et eget segment. For at alle skulle ha en referanse til aktørbildet ble livsløp for trafikkdata presentert (jf. kap. 2). Utgangspunktet for diskusjon av forretningsmodell for RSI ble derfor som vist i Figur 22.



Figur 22 Utgangspunkt for diskusjon om forretningsmodell for RSI

6.4.3 Resultater

Diskusjonen rundt forretningsmodell for RSI startet med å definere hvem som er potensielle **kunder**. En rekke potensielle kundegrupper ble foreslått:

Kundesegmenter

Bilkjøper (BK)
Bileier (BE)
Bilfører (BF)
Bilprodusent (BP)
Bilselger (BS)
Eksterne tjenesteytere (ETY)
Entreprenør (ENT)
Flåteeier (FE)
Forsikringsselskaper (FO)
Forskningsmiljø (FoU)
Infrastrukturleverandør (INFL)
Kommunikasjonstjenesteyter (KTY)
Media (MED)
Offentlige etater (OFF)
Pressgrupper (PRESS)
Trafikkdatabehandler (TDB)
Trafikkdata tjenestetilbyder (TDT)
Transporttjenesteyter (TTY)
Vegoperatør (VO)

Etter å ha definert potensielle kundegrupper gikk diskusjonen videre til **verdiforslag**, altså hva slags verdi RSI kan sies å skape for ett eller flere kundesegmenter. Følgende verdiforslag ble identifisert gjennom diskusjonen.

Verdiforslag

Aktiv sikkerhet (BF, TTY)
Bedre beslutningsgrunnlag (VO)
Bedre vedlikehold av infrastruktur (TTY, BF)
Beholde/styrke markedsposisjon (BP)
Data om friksjon (BP, TDB, TDT, FoU, MED, PRESS)
Data om hendelser (BP, TDB, TDT, FoU, MED, PRESS)
Forutsigbar/effektiv tidsbruk (BF, TTY, TDT)
Gjennomføre overvåkning (VO)
Informasjon[4] om friksjon (TDT, ENT, OFF, MED, FoU, PRESS, BF)
Informasjon om hendelser (TDT, OFF, MED, FoU, PRESS, BF)
Kommunikasjonstjenester (KTY)
Kontroll av kjøretøy (VO, BE, BF)
Kontroll av utført vedlikeholdsarbeid (VO)
Lavere forsikringsutbetalinger (FO)
Lavere forsikringspremie (BE, FE)
Markedsføring/merkevarebygging (BP, BS)
Mer effektiv/presis trafikkstyring (VO, BF, TTY)
Reduserte driftsutgifter (VO)
Reduserte utgifter til infrastruktur (VO)
Redusert utviklingsrisiko (BP, VO, OFF)
Utbygging av infrastruktur (INFL)
Økt trygghetsfølelse (BK)

Eksternaliteter er verdiforslag (goder) som ikke nødvendigvis er eksplisitt etterspurte eller som er tilknyttet en betalingsvillig kunde, slik som f.eks. miljøgevinster. I RSI kan slike eksternaliteter være følgende:

Eksternaliteter

Mindre miljøforurensing pga. mer presis vinterdrift (OFF)
Redusert antall ulykker (OFF)
Økt innovasjon (OFF)

[4] Skiller seg fra data ved at informasjon er data som er behandlet og tilpasset et formål

Etter verdiforslag gikk diskusjonen videre til **nøkkelaktiviteter** i RSI, altså aktiviteter som er nødvendig for å produsere verdiforslagene og få forretningsmodellen til å fungere. Nøkkelaktiviteter i RSI ble funnet å være:

Nøkkelaktiviteter

Avklare ansvar for/kunnskap om datakvalitet (VO, BP)
Avklare dataeierskap (VO, BP, OFF, TDB, TTT)
Avklare jus og lovgivning (BP, VO, OFF)
Avklare og sikre personvern (BP, VO, OFF)
Bearbeiding av data (TDB)
Beslutningsprosesser (VO)
Bygge kompetanse rundt bruk av data og datatyper (VO, FoU)
Exit-strategi (VO)
Formidling/salg av data (TDT)
Informasjon tas i bruk (ENT, TTY, BF, VO, MED, OFF, PRESS, BP)
Innsamling av data (BP, ETY)
Instrumentering av kjøretøy (BP)
Kvalitetskontroll av data (BP, VO)
Lagring av data (BP, VO)
Overføring av data (KTY, INFL)
Politiske forankring (VO)
Rekruttering av kjøretøy (BP, VO)
Security management (ETY)
Stimulere til bruk av RSI (OFF)
Stimulere privat innovasjon (VO)

Nøkkelressurser er de viktigste ressursene som kreves for å kunne gjennomføre nøkkelaktivitetene. Disse kan være fysiske, finansielle, intellektuelle og menneskelige. I workshopen ble følgende nøkkelressurser identifisert:

Nøkkelressurser

Bilførere
Bilprodusenter
Databaser med tilgangsstyring
ITS infrastruktur/lokale nettverk
Kommunikasjon: teleselskaper
Kompetanse (IKT, friksjonsfag, pedagogikk, jus)
Kompetente brukere av data
Meteorologiske tjenester
OBD2-moduler/nye kjøretøymodeller
Personell (TDB, IKT for drift, vegforvaltere, ENT, TDT, jurister)
Vegsystemer med kommunikasjonsmuligheter

Kostnadsstruktur beskriver utgiftene ved å tilby verdiforslagene. Følgende kostnadsfaktorer ble identifisert i workshopen (i parentes angis hvem som antas å være primær bærer av kostnadene):

Kostnadsstruktur

Drift av infrastruktur for innsamling, bearbeiding og formidling av data (VO, KTY, BP, ETY)
Incentiver for bruk av RSI (OFF)
Incentiver for privat innovasjon (OFF)
Investere i infrastruktur for innsamling, bearbeiding og formidling av data (VO, KTY, BP, ETY)
Investere i utstyr til kjøretøy (BP, VO, BE)
Kjøp av båndbredde/datatrafikk (BP, VO, BE)
Utviklingskostnader for RSI (inkl. montering) (BP, VO)

Til slutt ble det diskutert hvilke **inntektsstrømmer** man kan se for seg basert på verdiforslagene for RSI, og hvem som vil få disse inntektene:

Inntektsstrømmer

Investeringer i RSI (OFF)
Reduserte driftsutgifter (VO, ENT)
Reduserte drift- og investeringskostnader (gjennom offentlig incentiver) (BP, TTY)
Reduserte forsikringsutbetalinger (FOR)
Reduserte tidskostnader (TTY, BF)
Reduserte ulykkeskostnader (VO, OFF, FOR)
Reduserte utgifter til infrastruktur (VO)
Salg av båndbredde (KTY)
Salg av data (BP, VO)
Salg av informasjon (BP, VO, TDB, ETY)
Salg av kjt (BP, BS)
Salg av tjenester (TDT, VO, ETY)

6.4.4 Diskusjon

Utgangspunktet for forretningsmodellen for RSI er at Statens vegvesen er avhengig av bilprodusenter og deres kunder for å oppnå økt instrumentering av kjøretøy slik at biler kan benyttes som sensorer. Dette vil gi data som kan legge til rette for eksternaliteter som redusert antall ulykker, mindre miljøforurensing og økt innovasjon som følge av tilgang på data som kan videreforedles til produkter som etterspørres. For at slike data skal være nyttige på denne måten trengs et minimum antall instrumenterte kjøretøy, slik at kvaliteten på dataene blir god nok til at Statens vegvesen kan være rimelig sikker på at det vil medføre positiv nytte.

Et sentralt spørsmål for Statens vegvesen er derfor hvem som skal dekke det eksternalitetene koster. Bilprodusenter har i utgangspunktet ingen inntektsstrøm på å gi fra seg slike data og at samfunnet får nytte av de nevnte eksternalitetene. Det ble imidlertid identifisert flere kostnader som i utgangspunktet vil falle på bilprodusent, knyttet til instrumentering av kjøretøy. Kun to verdiforslag ble identifisert som "rene" verdiforslag for bilprodusent. Disse var begge knyttet til merkevarebygging og markedsføring, i form av å skape/videreføre et salgbart inntrykk av bilprodusenten og bilmerket som et sikkerhetsbevisst valg.

Økt instrumentering ser altså ut til å være betinget av at bilprodusenter ser et markedspotensial i å levere sikkerhetsrelatert informasjon til eiere/førere av deres kjøretøy, og til samfunnet for øvrig. Det er tvilsomt om slik merkevarebygging vil fungere for de bilprodusenter som ikke er "først ute", men som gjør det samme som andre bilprodusenter har gjort fra før. Det er heller ikke sikkert at bilprodusenter som prøver å appellere til andre kundegrupper enn de mest sikkerhetsbevisste vurderer dette som en aktuell markedsstrategi.

Dersom bilprodusenter ikke opplever at det fins en slik nytte, som oppveier for kostnader, kan det bli nødvendig at offentlige myndigheter betaler for å oppnå de forventede eksternalitetene. I den grad et tilstrekkelig antall bileiere ikke er villig til å signere en nødvendig avtale om logging og videreformidling av data fra sitt kjøretøy, kan det også bli nødvendig at det offentlige kompenserer i form av incentiver som f.eks. redusert årsavgift.

En annen mulighet for bruk av kjøretøy som sensorer ligger i at bilprodusenter tvinges til å instrumentere biler med teknologi som muliggjør slik datainnsamling. Dette må i tilfelle bestemmes av EU, og er relativt usannsynlig i og med at flere sterke EU-land har store bilprodusenter som er viktige for økonomi og arbeidsplasser.

I EUs ITS Action Plan og ITS-direktiv[5] stadfestes at sikkerhetsrelaterte data og prosedyrer skal tilbys gratis til brukere. I verste fall kan dette tolkes som en risiko for bilprodusenter som tilrettelegger for datainnsamling i sine kjøretøy, ved at de kan bli tvunget til å utlevere slike data. Det er imidlertid usikkert hvem som skal definere hva som er sikkerhetsrelatert og etter hvilke kriterier dette skal defineres. Statens vegvesen har derfor i teorien en mulighet til å definere dette, og til å ta ansvar for å utlevere data i bearbeidet form, altså som informasjon. Dette vil kreve utstrakt testing og kvalitetskontroll av data, slik at man ikke risikerer å utlevere informasjon som har motsatt effekt av det man ønsker – nemlig redusert trafikksikkerhet. Dette kan f.eks. oppstå ved at bilførere har en forventning om å bli varslet ved trafikkfarlige forhold, men slik varsling mangler pga. at man ikke har data for den aktuelle strekningen.

[5] http://ec.europa.eu/transport/themes/its/road/action_plan/
EU-direktiv 2010/40/EU: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010L0040

7 Konklusjon

VDoIT har hatt som mål å bidra til økt kunnskap om såkalte *ikke-teknologiske aspekter* rundt kooperativ ITS og håndteringen av data som genereres fra kooperativ ITS. Dette er viktig for å oppnå vellykket implementering av kooperative ITS-løsninger, i tråd med målene i Nasjonal transportplan. Prosjektet er gjennomført ved å bruke FoU-prosjektet RSI som case.

For å bidra til vellykket implementering av RSI har prosjektet fokusert på å formidle kunnskap om i) trafikkdatas livsløp og hvilke roller og tjenester som er sentrale i dette, ii) brukeres aksept for logging og deling av data, og iii) forretningsmodeller med forslag til hvordan ulike aktørgrupper kan se nytte av at kjøretøy brukes som sensorer på vegnettet. Prosjektet har hatt en dialogbasert form, slik at kunnskap har blitt formidlet både gjennom møter, en workshop og gjennom denne rapporten.

Denne rapporten har oppsummert aktuell kunnskap fra de ovennevnte kunnskapstema, og ved hjelp av denne foreslått hvordan Statens vegvesen kan bidra til økt utbredelse av kooperativ ITS eksemplifisert ved RSI. Sentralt i dette står spørsmålet om hvordan noe som er nyttig for "alle andre" (eksternaliteter) også kan ses som nyttig nok for en enkelt aktør (omtalt som kundesegment i forretningsmodellen) til at denne velger å gjennomføre de nøkkelaktiviteter som er nødvendig for at forretningsmodellen skal fungere. De mest sentrale kundesegmenter i dette er bilprodusent, bilkjøper/bilfører og offentlige myndigheter/vegoperatør (her representert ved Statens vegvesen).

Statens vegvesen kan påvirke bilprodusent og bilkjøper enten rent normativt ved å peke på fordeler som ligger i bruk av bilen som sensor for oss alle, eller ved gjennom dialog stimulere til at bilprodusent ser nytten av å kunne bruke dette i merkevarebygging og dermed økt salg. Vegvesenet kan også påvirke økonomisk ved å kompensere for de kostnader bilprodusent ser ved nødvendig instrumentering av sine biler, og/eller for den ulempe bilkjøper/bilfører ser med logging og deling data fra sin kjøring ved å skape incentiver.

Statens vegvesen kan benytte kunnskapen som er fremkommet og delt i VDoIT også i andre tilfeller enn RSI, hvor de ønsker å bidra til økt utbredelse av ITS. Denne rapporten gir for det første verktøy til å systematisere hvilke roller og aktører som inngår i trafikkdata sitt livsløp fra logging/registrering til anvendt trafikkinformasjon. Dette er nødvendig for at Statens vegvesen skal kunne bidra til eller påse at trafikkinformasjon blir produsert, har nødvendig kvalitet og når frem til rette vedkommende. Det brukes også til å studere hvilket ansvar Statens vegvesen kan pådra seg ved å distribuere trafikkdata i form av rådata, som behandlede data og som ITS-tjenester, f.eks. i form av trafikkinformasjonsmeldinger.

For det andre gir rapporten en oppsummering av kunnskap om trafikanters aksept for å logge og dele data fra sine turer, hvilke grupper som har minst og størst aksept og hvilke forhold som påvirker aksepten i positiv og negativ retning. Slik kunnskap er viktig for å kunne stimulere til deling av data, f.eks. gjennom informasjon og incentivordninger.

Den siste delen av rapporten viser hvordan forretningsmodeller kan brukes for å systematisere hvem som er potensielle kunder og som dermed vil ha en interesse i økt utbredelse av ITS, hvem som kan tjene penger på det, hva slags verdiforslag eller goder det er betalingsvilje for og hva som vil utgjøre viktige kostnadselementer (og for hvem). Dette kan brukes til å identifisere hvilke utfordringer som må løses for at økt utbredelse av ITS skal skje, og bidra til at man lettere forstår hvilke strategier som vil være nyttig i dette arbeidet.

Videre forskning

I forlengelsen av dette prosjektet er det flere problemstillinger som bør følges videre. Dette gjelder særlig eierskap til trafikkdata og Statens vegvesens rolle i håndtering av slike data. Selv om det i liten (eller ingen) grad ser ut til å finnes noen definisjon på eierskap til trafikkdata utover det som er forsøkt definert i denne

rapporten, finnes det i flere byer utstrakt praksis med håndtering av trafikk- og transportdata. Ved å undersøke denne praksisen kan også Statens vegvesen utvikle retningslinjer for håndtering og forvaltning av data, samt bygge bevissthet rundt dataeierskap i ulike deler av datas livsløp. Det vil være særlig relevant å hente erfaringer fra europeiske byer med etablerte prosedyrer for datahåndtering.

Gjennom prosjektet VDoIT er RSI-prosjektet ofte løftet frem som eksempel på kooperativ teknologi. I forlengelsen av arbeidsseminaret der en forretningsmodell for RSI ble utformet kan det også være hensiktsmessig å utforme forretningsmodeller skreddersydd for de viktigste aktørene i RSI-prosjektet. Foruten Statens vegvesen vil dette være kjøretøyprodusent og kommunikasjonstjenestetilbyder, og det vil derfor være relevant med supplerende arbeidsseminarer for utarbeiding av rollespesifikke forretningsmodeller.

Sist vil det være aktuelt å fortsette arbeidet med å etablere et større forskningsprosjekt om utrulling og implementering av kooperativ teknologi.

8 Referanser

Abrahamse, W., L. Steg, C. Vlek og T. Rothengatter (2005): *A review of intervention studies aimed at household intervention conservation.* Journal of Environmental Psychology, 25 (3), s. 273-291.

Ajzen, I. (1991): *The theory of planned behavior.* . Organisational behaviour and human decision processes, 50 s. 179-211.

Ajzen, I. (2002): *Attitudes, personality and behaviour.* Open University Press, Buckingham

Al-Khouri, A. M. (2012): *Data Ownership: Who Owns 'My Data'?* International Journal of Mangement & Information Technology, 2 (1), s.

Amit, R. og C. Zott (2012): *Creating Value through Business Model Innovation.* MIT Sloan Management Review, 53 (3), s. 41-49.

Aquilina, K. (2010): *Public security versus privacy in technology law: A balancing act?* Computer Law & Security Review, 26 (2), s. 130-143.

Bagchi, R. og X. Li (2011): *Illusionary progress in loyalty programs: Magnitudes, reward distances, and step-size ambiguity.* Journal of Consumer Research, 37 (5), s. 888-901.

Bakås, O., K. Y. Bjerkan, A. B. Sund og M. E. Nordtømme (2014): *L6.1 Forretningsmodeller. Suksesskriterier og merverdi ved konsolideringssenter i Oslo.* GBO prosjektnotat L6.1 SINTEF Teknologi og samfunn http://www.sintef.no/contentassets/067ef756b7644281ad2514bef7955c53/gbo/gbo-l-6.1-forretningsmodeller.pdf.

Bjørnskau, T. og R. Elvik (1992): *Can road traffic law enforcement permanently reduce the number of accidents?* Accident Analysis & Prevention, 24 (5), s. 507-520.

Bolderdijk, J. W., J. Knockaert, E. M. Steg og E. T. Verhoef (2011): *Effects of Pay-As-You-Drive vehicle insurance on young drivers' speed choice: Results of a Dutch field experiment.* Accident Analysis & Prevention, 43 (3), s. 1181-1186.

Bustamante, N. og A. Fernando (2006a): *Policy Implications of ubiquitous technologies in the car: privacy, data ownership and regulation.* Massachussettes Institute of Technology, Thesis

Bustamante, N. og A. Fernando (2006b): *Policy implications of ubiquitous technologies in the car: privacy, data ownership, and regulation.* Massachusetts Institute of Technology

Chen, D. og H. Zhao (2012): "Data Security and Privacy Protection Issues in Cloud Computing", paper presentert på Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering - Volume 01,

Dijksterhuis, C., B. Lewis-Evans, B. Jelijs, D. de Waard, K. Brookhuis og O. Tucha (2015): *The impact of immediate or delayed feedback on driving behaviour in a simulated Pay-As-You-Drive system.* Accident Analysis & Prevention, 75 s. 93-104.

e-Science City Who owns the data? Hentet fra http://www.cloud-lounge.org/who-owns-the-data.html 2015.12.03

Eriksson, L. og T. Bjørnskau (2012): *Acceptability of traffic safety measures with personal privacy implications.* Transportation Research Part F: Traffic Psychology and Behaviour, 15 (3), s. 333-347.

EU (2010): Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

Ferro, E. og M. Osella (2012): "Business Models for PSI re-use: a multidimensional framework", paper presentert på Using open data: opilcy modeling, citizen empowerment, data journalism, Brussels http://www.w3.org/2012/06/pmod/pmod2012_submission_16.pdf

Ferro, E. og M. Osella (2013): "Eight Business Model Archetypes for PSI re-use", paper presentert på Open Data on the Web workshop, London http://www.w3.org/2013/04/odw/odw13_submission_27.pdf

Foss, K. (2015a): Hvem eier dataene i tingenes internett? Hentet fra http://www.digi.no/debatt/2015/03/06/hvem-eier-dataene-i-tingenes-internett 2015.12.03

Foss, T. (2015b): *Fra ARKTRANS til kravspesifikasjoner for ITS applikasjoner.* SINTEF A26423

Gaunt, M., T. Rye og S. Allen (2007): *Public Acceptability of Road User Charging: The Case of Edinburgh and the 2005 Referendum.* Transport Reviews: A Transnational Transdiciplinary Journal, 27 (1), s. 85-102.

Hawkins, R. og P. R. Stopher (2004): *Collecting Data with GPS: Those who reject, and those who receive.* Working Paper ITS-WP-04-21 The Institute of Transport Studies

Herrala, M. (2007): *Value of transport information.* VTT Research Notes 2394 VTT

Hoppe, T., S. Kiltz og J. Dittmann (2011): *Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures.* Reliability Engineering & System Safety, 96 (1), s. 11-25.

Horrey, W. J., M. F. Lesch, M. J. Dainoff, M. M. Robertson og I. I. Noy (2012): *On-Board Safety Monitoring Systems for Driving: Review, Knowledge Gaps, and Framework.* Journal of Safety Research, 43 s. 49-58.

Hsee, C. K., F. Yu, J. Zhang og Y. Zhang (2003): *Medium maximization.* Journal of Consumer Research, 30 (1), s. 1-14.

Jacobs, B. (2010): "Architecture Is Politics: Security and Privacy Issues in Transport and Beyond", i Gutwirth, S., Y. Poullet og P. De Hert (red.): *Data Protection in a Profiled World*, Springer Netherlands, s. 289-299

Jarbekk, E. (2014): Big Data, kommersialisering og eierskap til informasjon. Hentet fra http://www.nbef.no/fileadmin/Kursprogrammer/2015/1550150_FM-konferansen-2015/Eva-Jarbekk_Big-data-rettslig-rammeverk_NBEF-FM-konferansen-2015.pdf 2015.12.03

Johnson, M. W., C. M. Christensen og H. Kagermann (2008): *Reinventing Your Business Model.* Harvard Business Review, December 2008 s. 57-68.

Kaisler, S., F. Armour, J. A. Espinosa og W. Money (2013): Big Data: Issues and Challenges Moving Forward. System Sciences (HICSS), 2013 46th Hawaii International Conference on, 7-10 Jan. 2013

Kamoun, F. (2008): *Rethinking the Business Model with RFID.* Communications of the Association for Information Systems, 22 (1), s. 635-658.

Katteler, H. (2005): *Driver acceptance of mandatory intelligent speed adaptation.* European Journal of Transport and Infrastructure Research, 5 (4), s. 317-336.

Lahrmann, H., N. Agerholm, N. Tradisauskas, K. K. Berthelsen og L. Harms (2012): *Pay as You Speed, ISA with incentives for not speeding: Results and interpretation of speed data.* Accident Analysis & Prevention, 48 s. 17-28.

Lehman, P. K. og E. S. Geller (2008): "Applications of social psychology to increase the impact of behaviour-focused intervention", i Steg, L., A. P. Buunk og T. Rothengatter (red.): *Applied Social*

Psychology: Understanding and Managing Social Problems, Cambridge:Cambridge University Press, s. 57-86

Leviäkangas, P. (2011): *Building Value in ITS Services by Analysing Information Service SUpply Chains and Value Attributes.* International Journal of ITS Research, 9 s. 47-54.

Limoges, E., C. L. Purvis, S. Turner, M. Wigan og J. Wolf (2000): "Future of Urban Transportation Data", paper presentert på Transportation Research Borard, Washtington D.C.

Link, H. og J. Polak (2001): How acceptable are transport pricing measures? Empirical studies in nine European countries. Conference Proceedings European Transport Conference 2001, Cambridge

Magretta, J. (2002): *Why Business Models Matter?* . Harvard Business Review, s. 86–92.

Merrikhpour, M., B. Donmez og V. Battista (2014): *A field operational trial evaluating a feedback–reward system on speeding and tailgating behaviors.* Transportation Research Part F: Traffic Psychology and Behaviour, 27, Part A s. 56-68.

Nicholson, A., S. Webber, S. Dyer, T. Patel og H. Janicke (2012): *SCADA security in the light of Cyber-Warfare.* Computers & Security, 31 (4), s. 418-436.

Nielsen, M. (2013): Who owns Big Data? Hentet fra https://www.bbvaopenmind.com/en/article/who-owns-big-data/?fullscreen=true 2015.12.03

Osterwalder, A. og Y. Pigneur (2010): *Business Model Generation: A Handbook for Visionaries,Game Changers, and Challengers.* John Wiley and Sons Ltd.,

Potoglou, D., N. Robinson, C. W. Kim, P. Burge og R. Warnes (2010): *Quantifying individuals' trade-offs between privacy, liberty and security: The case of rail travel in UK.* Transportation Research Part A: Policy and Practice, 44 (3), s. 169-181.

Rausand, M. og I. B. Utne (2009): *Risikoanalyse - teori og metoder.* Tapir Akademiske Forlag, Trondheim

Raya, M. og J.-P. Hubaux (2005): "The security of vehicular ad hoc networks", paper presentert på Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, Alexandria, VA, USA

Rendle, A. (2014): Who owns the Internet of Things? Hentet fra www.united-kingdom.taylorwessing.com/download/article_data_lot.html 2015.12.03

Roux, S., P. Marchal og J. Armoogum (2009): "Acceptability of the use of new technologies by interviewees in surveys", paper presentert på New Techniques and Technologies for Statistics, Brussels

Ryu, D. H., H. Kim og K. Um (2009): *Reducing security vulnerabilities for critical infrastructure.* Journal of Loss Prevention in the Process Industries, 22 (6), s. 1020-1024.

Schade, J. og B. Schlag (2003): *Acceptability of transport pricing strategies.* Elsevier, Amsterdam

Shafer, S. M., H. J. Smith og J. C. Linder (2005): *The power of business models.* Business Horizons, 48 s. 199-207.

Skinner, B. F. (1974): *About behaviorism.* Knopf, New York

Steg, L., L. Dreijerink og W. Abrahamse (2005): *Factors influencing the acceptability of energy policies: A test of VBN theory.* Journal of Environmental Psychology, 25 s. 415-425.

Steg, L. og G. Schuitema (2007): "Behavioural Responses to Transport Policy Pricing: A Theoretical Analysis.", i Gärling, T. og L. Steg (red.): *Threats from Car Traffic to the Quality of Urban Life*, s. 347-366

Stern, P. C. (2000): *Toward a Coherent Theory of Environmentally Significant Behavior.* Journal of Social Issues, 56 (3), s. 407-424.

Stern, P. C., T. Dietz og L. Kalof (1993): *Value orientations, gender, and environmental concern.* Environment and Beahvior, 25 s. 322-348.

Stigson, H., J. Hagberg, A. Kullgren og M. Krafft (2013): *A one year pay-as-you-speed trial with economic incentives for not speeding.* Traffic Injury Prevention, 15 (6), s. 612-618.

Stopher, P., E. Clifford og M. Montes (2008): *Variability of Travel over Multiple Days: Analysis of Three Panel Waves.* Transportation Research Record: Journal of the Transportation Research Board, 2054 (-1), s. 56-63.

Stopher, P. R. (2008): "Collecting and Processing Data from Mobile Tehcnologies", paper presentert på The 8th International Conference on Survey Methods in Tarnsport, Annecy, France

Teece, D. J. (2010): *Business Models, Business Strategy and Innovation.* Long Range Planning, 43 (2-3), s. 172-194.

TURBLOG (2011): Deliverable 2: Business Concepts and Models for Urban Logistics. Seventh Framework Programme. Hentet fra http://www.transport-research.info/Upload/Documents/201307/20130703_153326_39686_D2_BusinessConceptsModelsForUrbanLogistics.pdf

Vlassenroot, S. (2011): *The Acceptability of In-Vehicle Intelligent Speed Assistance (ISA) Systems: from Trial Support to Public Support.* Delft University of Technology

Vlassenroot, S., K. Brookhuis, V. Marchau og F. Witlox (2008): Measuring acceptance and acceptability of ITS. Theoretical background in the development of a unified concept. TRAIL Research School, Delft

Vlassenroot, S., K. Brookhuis, V. Marchau og F. Witlox (2010): *Towards definfing a unified concept for the acceptability of Intelligent Transport Systems (ITS): A conceptual analysis based on the case of Intelligent Speed Adaptation (ISA).* Transportation Research Part F, 13 (3), s. 164-178.

Whyte, W. (2012): "Security, Privacy identifications", i Eksandarin, A. (red.): *Handbook of Intelligent Vehicle*, London:Springer, s. 1271-1311

Wigan, M. R. og R. Clarke (2013): *Big Data's Big Unintended Consequences.* IEE Computer Society, 46 (6), s. 46-53.

Zaal, D. (1994): *Traffic law enforcement. A review of the litterature.* Monash University Accident Research Centre, Melbourne

Zelinka, T., Z. Lokaj og M. Svitek (2011): Data security in ITS telecommunications solutions. The 5th International Conference on Communication and Information Technology, Greece

Øvstedal, L. (2009): *Kan man reise anonymt i Norge?* SINTEF Rapport A10918 SINTEF

Øvstedal, L., L.-E. Lervåg og T. Foss (2010): *Personvern i intelligente transportsystemer.* SINTEF Rapport A10670 SINTEF

Teknologi for et bedre samfunn

www.sintef.no