SINTEF A10918– Åpen

RAPPORT

Kan man reise anonymt i Norge?

Personopplysningsloven i transportsektoren

Liv Øvstedal

SINTEF Teknologi og samfunn
Transportforskning

Mars 2009

www.sintef.no

SINTEF

SINTEF RAPPORT

SINTEF Teknologi og samfunn
Transportforskning

Postadresse: 7465 Trondheim
Besøksadresse: S.P. Andersensv. 5
Telefon: 73 59 47 05
Telefaks: 73 59 46 56

Foretaksregisteret: NO 948 007 029 MVA

TITTEL

Kan man reise anonymt i Norge?
Personopplysningsloven i transportsektoren

FORFATTER(E)

Liv Øvstedal

OPPDRAGSGIVER(E)

Statens vegvesen Vegdirektoratet

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS REF.	
SINTEF A10918	Åpen	Finn Harald Amundsen	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	988-82-14-04728-8	503737	56 sider + 2 bilag
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
A10918_Personoppplysningsloven i transportsektoren.doc		Trond Foss	Solveig Meland
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
503737	2009-03-25	Ragnhild Wahl (forskningssjef)	

SAMMENDRAG

Høsten 2008 er det gjennomført intervju med aktører innenfor persontransport i Norge der temaet var behandling av personopplysninger. Rapporten inngår i Statens vegvesens etatsprosjekt om Personvern og trafikk. Resultatene er beskrivende og ikke nødvendigvis dekkende for de ulike transportgreinene. Informantene viser mange eksempler på behandling av personopplysninger med ulik lagringstid avhengig av formålet. Informasjonen på internett og i litteraturen peker også på at vi som trafikanter legger igjen mange og ulike spor. Generelt er dataene ikke sensitive og virksomhetene har i liten grad identifisert alvorlige konsekvenser for kundene. Virksomhetene synes å ha tydelig fokus på informasjonssikkerhet som fysisk sikkerhet, adgangskontroll, utveksling av informasjon m.m., men det er varierende grad av fokus på personvernet. Hensynet til personvernet avveies i forhold til effektivitet, datasikkerhet, kundevennlighet osv. En vesentlig motivasjon for å ivareta personvernet, er hensynet til virksomhetens og bransjens omdømme. Vi peker på at det kan være forskjeller mellom små og store aktører og mellom privat virksomhet og offentlig forvaltning. Det er viktig at den enkelte ansatte får tilstrekkelig kunnskap om personvernloven og interessene den skal ivareta, men det er også behov for å kunne se egne arbeidsoppgaver som en del av hele virksomheten. Avslutningsvis peker vi på at materialet gir noen begrunnelser for videre arbeid med en evt. sektorpolicy.

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Samferdsel	Transport
GRUPPE 2	Transportpolitikk	Transport policy
EGENVALGTE	Personvern	Privacy protection

Forord

I denne rapporten rapporterer vi første del av et prosjekt som inngår i Statens vegvesens etatsprosjekt Personvern og trafikk. Prosjektet består av flere delprosjekt der ulike sider ved personopplysninger i trafikk belyses. Prosjektgruppa hos SINTEF har bestått av prosjektleder Trond Foss, prosjektmedarbeidere Solveig Meland og Liv Øvstedal, og rådgivere Lillian Fjerdingen og Martin Gilje Jaatun.

Kontaktpersoner hos Statens vegvesen har vært Marianne Stølan Rostoft og Kjersti Bakken i Vegdirektoratet. Det er opprettet en referansegruppe for Statens vegvesens etatsprosjekt med følgende deltakere:

Sveinung Stangeland, Politidirektoratet

Rune Vidar Bråthen, Datatilsynet

Mona Høegh Amundsen, DSB

Christine Hafskjold, Teknologirådet

Tore Vaaje, Gjensidige

Bård Morten Johansen, Trygg Trafikk

Saksbehandlere i Datatilsynet har bidratt med innsikt og erfaringer i dialog om undersøkelsesopplegget. En stor takk til informantene som har bidratt med sin tid, erfaringer og kunnskap om temaet!

Trondheim, mars 2009

Ragnhild Wahl

Forskningssjef

INNHOLDSFORTEGNELSE

Sammendrag

Som en del av Statens vegvesens etatsprosjekt om Personvern og trafikk, er det gjennomført intervju med aktører for innenlands persontransport om behandling av personopplysninger. Gjennomføringen av intervjuene og resultatene dokumenteres i rapporten. Hensikten har vært å beskrive dagens praksis for behandling av personopplysninger i forhold til personopplysningsloven og forskriftene, om det er vesentlige forskjeller mellom veitransport og de andre transportformene, og hvordan eventuelle forskjeller bør og kan utjevnes. Med personopplysninger menes opplysninger og vurderinger som kan knyttes til en enkeltperson. Med behandling av personopplysninger menes enhver bruk av personopplysninger, som å samle inn, registrere, sammenstille, lagre, utlevere, eller en kombinasjon av slike bruksmåter. Behandling av personopplysninger reguleres av Lov om behandling av personopplysninger, men for de ulike anvendelsene kommer også andre lovverk inn.

Kapittel 1 beskriver bakgrunnen og målsettingen for denne intervjuundersøkelsen og de metodene som er valgt. Det er gjennomført en dokumentgjennomgang av personopplysningsloven, forskrifter og veiledere, som danner bakgrunn for en intervjuguide. Videre er det gjennomført en begrenset litteraturstudie og søk på internett, for å beskrive eksempler på behandling av personopplysninger i transportsektoren som fyller ut bildet som intervjuene gir. Studien er kvalitativ med et lite utvalg informanter. Informantene er valgt fra små og store aktører i ulike deler av landet, og dekker alle sektorene vei, bane, sjø og luft. Av denne grunn er det først og fremst transportørene sin stemme som målbæres i denne studien, men også forvaltningen er representert.

I kapittel 2 presenteres det viktigste lovgrunnlaget, hvilke interesser personvernet skal beskytte og noen viktige prinsipp i personopplysningsloven. Datatilsynet forvalter, behandler klager og gir informasjon om personopplysningsloven, mens Personvernnemnda behandler klager på vedtak fattet i Datatilsynet. Videre ser vi at elektronisk databehandling er en integrert del av de fleste områder av transportsektoren, men ikke alle former for elektronisk databehandling medfører behandling av personopplysninger. I kap. 2.4 presenteres ulike eksempler på behandling av personopplysninger, både eksempler som er felles for ulike typer transportmidler, og for de ulike sektorene vei, bane, sjø og luft, basert på informasjon tilgjengelig på internett og i litteraturen.

I kapittel 3 presenteres resultatene fra intervjuene. Resultatene er beskrivende og ikke nødvendigvis dekkende for de ulike transportgreinene. De fleste intervjuene ble gjennomført som planlagt, mens en aktør ble erstattet med en annen innenfor samme sektor, og ytterligere en aktør falt fra. Informantene viser mange eksempler på behandling av personopplysninger med ulik lagringstid avhengig av formålet. Generelt er dataene ikke sensitive og virksomhetene har i liten grad identifisert alvorlige konsekvenser for kundene. Virksomhetene synes å ha tydelig fokus på informasjonssikkerhet som fysisk sikkerhet, adgangskontroll, utveksling av informasjon m.m. En vesentlig motivasjon for å ivareta personvernet, er hensynet til virksomhetens og bransjens omdømme. Vi peker på at det kan være forskjeller mellom små og store aktører, og mellom privat virksomhet og offentlig forvaltning. Det er viktig at den enkelte ansatte får tilstrekkelig kunnskap om personvernloven og interessene den skal ivareta, men det er også behov for å kunne se egne arbeidsoppgaver som en del av hele virksomheten.

I kapittel 4 oppsummerer vi noen hovedpunkt fra intervjuene og viser at materialet gir grunnlag for et videre arbeid med en sektorpolicy eller bransjestandard.

Summary

As part of the National Road Authorities project on Privacy and traffic, interviews about the treatment of personal information are conducted with actors in the domestic passenger/person transport sector. Results from the interviews and how the interviews were conducted, are presented in the report. The aim has been to describe today's practice concerning treatment of personal information and how this corresponds with legislation. Are there differences in how personal information is treated between the road transport sector and other transport modes, and how can possible differences be reduced? Personal data is here information and assessments which can be related to a single person. Treatment of personal data is any use of personal information; to collect, register, save, compare, distribute, or any combination of such use. Treatment of personal information is regulated by the legislation on personal information protection, and for different applications other parts of legislation apply as well.

Chapter 1 describes the background for and the purpose of the interview survey and the chosen methods. To describe applications of personal information in the transport sector, a limited search of literature and internet information was conducted. The legislation, regulations and guidance on personal information protection were reviewed to form the base of the interview guide. The interview survey is qualitative, with few informants selected to represent both large and small actors from different parts of the country, and the different sectors; road; rail, sea, and air traffic. For this reason the survey mainly "voices" the transport operators, while the public administration is also represented.

In chapter 2 the legislation on personal information protection is shortly introduced, describing some main principles and vital interests to protect. The Data Inspectorate control, handle complaints and inform about the Personal Data Act, while the Privacy Appeals Board handle complaints on decisions of the Data Inspectorate. Electronic data processing is an integrated part of most activities within the transport sector, but not all forms of electronic data processing imply personal data. In chapter 2.4 examples of treatment of personal information in the transport sector are presented, based on literature and internet information. Applications common for all modes are presented first, followed by examples specific for each of the transport sectors.

The results from the interviews are presented in chapter 3. These are describing, but do not present the complete situation for all different modes. The informants presented many examples of how personal information is treated and how long the information is kept, depending on purpose. Generally the personal information in the transport sector is not sensitive, and serious consequences for customers were not identified. The enterprises seem to have a genuine focus on data security, including physical security, permission control, data distribution etc., with the reputation of the firm and the trade as the main motivation. We point out that there may be some differences between small and large organisations, and between private companies and public administration. For the staff involved, knowledge about the interests to protect and the Personal Data Act is important, but there is also a need for the employee to see how his or hers tasks and responsibilities are a part of the total activities of the company.

In Chapter 4 we sum up and comment some main points from the interviews, as well as some arguments for establishing a sector policy on personal information protection.

1 Innledning

Denne rapporten handler om hvordan de ulike bestemmelsene i Personopplysningsloven praktiseres i transportsektoren i dag, og hvordan hensynet til den enkeltes privatliv og integritet veies opp mot andre hensyn. I dette kapitlet presenterer vi bakgrunnen for rapporten, målsettingen med arbeidet og metodene som er lagt til grunn.

1.1 Rapporten inngår i etatsprosjektet Personvern og trafikk

Rapporten inngår som en av flere aktiviteter i Statens vegvesens etatsprosjekt om personvern. Personvern og trafikk er et 3-årig forsknings- og utviklingsprosjekt i Statens vegvesen der hensikten er å utvide kunnskapene om problemstillinger knyttet til personvern innenfor transportsektoren. Mange av transportsystemene er avhengige av IKT for å fungere sikkert og effektivt der informasjonssikkerhet må være tilfredsstillende mht. konfidensialitet, integritet og tilgjengelighet. I noen system vil informasjonen som behandles omfatte opplysninger som kan knyttes til et bestemt individ. Med behandling menes innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter. Personopplysninger innhentes på mange måter innenfor alle transportformer. Formålet kan være sikkerhet, trygghet (security), effektivitet, lønnsomhet, eller bedre tilbud og informasjon til trafikantene.

Informasjons- og kommunikasjonsteknologi (IKT) kan bidra positivt til flere transportpolitiske mål som bedre sikkerhet, mer miljøvennlig transport og effektive trafikkløsninger. Det utvikles teknologibaserte system for kontroll, overvåking og styring, av transportsystem og kjøretøy. Slike system kan gi oss informasjon automatisk. En økt innsamling av informasjon kan imidlertid brukes til sporing og overvåking av personer, noe som kan utgjøre en trussel for personvernet, og den teknologiske utviklingen går fort. Både i forhold til lover, forskrifter og organisering kan det være en utfordring for samfunnet å henge med og å være ”føre var”. Hovedmålet med behandlingen av informasjon som kan knyttes til et individ kan være å redusere risikoen i transportsystemet, men en konsekvens kan være at man kommer i konflikt med kravene i Personopplysningsloven og i forskriftene. Med risiko menes her ikke bare risikoen for en hendelse som medfører fare for trafikantenes liv og helse, men også risiko for hendelser som kan påføre trafikantene økonomiske tap eller krenkelse av personvernet. Statens vegvesen ønsker å bidra til at samferdselsmyndigheter oppnår mer kunnskap om grensesnittet mellom personvern og trafikk slik at eventuelle konflikter håndteres lettere. SINTEF, TØI og IRIS er engasjert til å belyse ulike problemstillinger innenfor etatsprosjektet.

I denne rapporten er temaet hvordan personopplysninger behandles innenfor ulike transportområder i dag og om det er forskjeller mellom transportformene.

Denne rapporten oppsummerer den første av flere problemstillinger som inngår i prosjektet ved SINTEF. I andre deler av prosjektet er temaet risikovurdering av intelligente transportsystem (ITS) i forhold til hvilke personopplysninger som behandles og hvordan de behandles. Et tredje tema er hvordan kunder og brukere oppfatter den personlige integriteten i transport.

1.2 Målsetting

Denne rapporten oppsummerer den første av flere problemstillinger som inngår i prosjektet og har som mål å beskrive:

- Hvordan praktiseres personopplysningsloven og forskriftene til den i transportsektoren i dag?
- Er det vesentlige forskjeller i hvordan opplysninger som kan knyttes til enkeltindivid behandles, i ulike driftsorganisasjoner eller mellom veitransport og andre transportformer?
- Hvordan bør og kan eventuelle forskjeller utjevnes slik at kunder og brukere ikke opplever forskjellsbehandling og ulike tolkninger av loven og forskriftene?

Veitransport omfatter mange ulike aktører som har aktiviteter knyttet til transport av personer og gods på vei. Vi har avgrenset problemstillingen til å gjelde innenlands persontransport.

Rapporten inngår i et prosjekt med bredere problemstilling. I *andre deler* av prosjektet, som rapporteres for seg, belyses temaene risikovurdering og brukernes aksept av tiltak:

- På hvilken måte kan nye intelligente transportsystem generere nye muligheter og organisasjoner for å behandle data som kan knyttes til et enkeltindivid?
- Hvilken risiko (konsekvens x sannsynlighet) er forbundet med behandlingen av slike opplysninger?
- Hva er akseptabelt risikonivå sett fra myndighetene, eiere og drivere av transportsystem, og fra kundene og forbrukernes side?
- Hva er forholdet mellom vurdert risiko og akseptabel risiko? Hvilke tiltak kan være aktuelle for å kompensere for eventuelle avvik mellom vurdert og akseptabelt risikonivå?

1.3 Metode

Dokumentgjennomgang og intervju med et utvalg aktører

Dokumentgjennomgang og intervju er de viktigste metodene som er benyttet for å belyse hvordan personopplysninger behandles i dagens transportløsninger. Problemstillingen er avgrenset til innenlands persontransport. Personopplysningsloven, forskrifter og veiledning er gjennomgått for å finne de artiklene, paragrafene og avsnittene som er av betydning for transportsektoren. Dette har dannet utgangspunkt for en veiledende liste med spørsmål for intervjuene. *Intervjuguiden* er presentert i vedlegg 1.

Som bakgrunn for intervjuene og for å få et bredere bilde av personvernutfordringene i transportsektoren er det gjennomført en begrenset litteraturgjennomgang og en gjennomgang av informasjon om aktører og bransjeforeninger i transportsektoren på internett. Dette bildet er ytterligere utdypet gjennom møter i et bompengeselskap og hos to aktører innen parkering.

Det er gjennomført intervju med et utvalg etater og utøvere for å belyse hvordan personopplysningsloven og forskriftene praktiseres innenfor de ulike transportgreinene. Det er valgt en kvalitativ innfallsvinkel med intervju med et lite utvalg aktører for å oppnå innsikt om problemområdet, se også kap. 3.1. Noen aspekt ved undersøkelsesopplegget ble diskutert i et arbeidsmøte med Datatilsynet før intervjuene ble gjennomført. Ved valg av informanter er det lagt

vekt på å få med aktører som representerer innenlands persontransport både på vei, bane, sjø og luft. Det er lagt vekt på at utvalget skal inkludere små og store aktører fra forskjellige deler av landet. Med dette som premiss består utvalget i stor grad av transportører, men også forvaltningen er representert. Myndighetenes, etatenes og organisasjonenes oppfatning av risiko for krenkelse av enkeltindividets personlige integritet er belyst. En oversikt over *informantene* er vist i vedlegg 2.

2 Personvern og transport

I dette kapitlet introduserer vi noen problemstillinger knyttet til personvern og persontransport. Vi presenterer ulike interesser knyttet til personvernet, det viktigste lovgrunnlaget i Norge og tilsynsmyndigheter. Deretter ser vi på ulike drivkrefter for økt bruk av teknologi og databehandling i transportsektoren, og noen av disse applikasjonene har personvernimplikasjoner. Vi presenterer eksempler på dagens bruk av personopplysninger innenfor de ulike transportgreinene (luft-, bane-, sjø- og veitransport), og noen hypoteser om hva som påvirker aksepten av tiltak som innebærer registrering av personopplysninger.

2.1 Hvilke interesser skal personvernet beskytte

I denne rapporten snakker vi om personvern i betydningen å beskytte personens integritet og å sikre persondata. En annen betydning av ordet kan være å sikre personens liv og helse. Personvern handler om å beskytte den enkeltes selvstendighet, uavhengighet og ukrenkelighet. Det er knyttet flere interesser til personvernet (Ravlum 2004).

De *individuelle* interessene er knyttet til retten til å ha et privatliv og til innsyn, fullstendighet og diskresjon. Hensynet til privatlivets fred tilsier at man ikke skal registreres eller overvåkes uten god grunn. Med innsyn menes at den enkelte skal ha kunnskap om hvilke data som registreres og hvorfor. Med fullstendighet tenker vi på at den enkelte har interesse av at dataene som registreres er korrekte, relevante og tilstrekkelige for formålet. Med diskresjon tenker vi på at den enkelte ønsker trygghet for at dataene oppbevares på en trygg måte, at tilgangen til opplysningene er begrenset, og at de som behandler dataene har taushetsplikt.

Forbrukerinteresser reguleres i kontrakt mellom kjøper og selger, basert på at man frivillig aksepterer de betingelsene som stilles.

Samfunnets interesser er knyttet til et robust, borgervennlig samfunn med vern mot maktmisbruk. Men fellesskapet ønsker også effektive og miljøvennlige transportløsninger og beskyttelse mot ulykker, kriminalitet og terror. Med borgervennlighet menes det at samfunnet skal være forståelig og oversiktlig, uten unødvendig kompliserte sammenhenger. Det skal for eksempel være mulig å ha innsyn i hvordan opplysninger man gir om seg selv blir brukt. Robusthet handler blant annet om hvor avhengig samfunnet gjør seg av elektronisk informasjonsbehandling. Store databaser og muligheten til å koble ulike registre kan også gi mulighet for kontroll og maktbruk. Vern mot maktmisbruk og vilkårlig kontroll peker derfor mot å begrense overvåkingsnivået. Disse behovene veies mot behovet for å overvåke trafikkflyt og miljøeffekter, og sikkerhet mot ulykker, kriminalitet og terrorhandlinger.

De ulike interessene harmonerer ikke nødvendigvis med hverandre, og de kan være i strid med andre interesser vi har som borgere og forbrukere. Juridisk fokuserer man på tre dimensjoner av personvern:

Integritetsfokusert personvern bygger på amerikansk tradisjon og ideer om privatliv (privacy) der man ser på personopplysninger som individets eiendom. Det integritetsfokuserte personvernet innebærer at alle skal ha rett til å kjenne til opplysninger som blir samlet inn om seg selv, og til en privatsfære som ingen har rett til å trenge innenfor uten tillatelse eller en god og legitim grunn.

Maktfokusert personvern bygger på en europeisk tradisjon knyttet til retten til å beskytte seg mot maktmisbruk, der man ser på personvernet som en grensegang mot overdreven markedsmakt, arbeidsgivermakt og privat og offentlig myndighetsutøvelse.

Beslutningsfokusert personvern legger vekt på at personopplysninger som brukes som grunnlag for beslutninger av det offentlige og av private (f eks banker og forsikringsselskap) må være korrekte og tilstrekkelige.

2.2 Lovgrunnlag og tilsynsmyndighet

De juridiske rammene for personvernet i Norge er:

- Personopplysningsloven (Lov 2000-04-14 nr 31: Lov om behandling av personopplysninger)
- Forskrift om behandling av personopplysninger (FOR 2000-12-15 nr 1265: personopplysningsforskriften)
- Personverndirektivet EU-direktiv 95/46/EF (Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger)
- Den europeiske menneskerettskonvensjonen (Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter, Roma 1950)

Personopplysningsloven er harmonisert med det europeiske direktivet.

Internasjonale forpliktelser

Norge er medlem av Europarådet og har underskrevet og ratifisert *European Convention on Human Rights*, Europarådets *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (ETS No. 108) og *Convention on Cybercrime*.

Norge er også medlem av Organisasjonen for økonomisk samarbeid og utvikling (OECD) og har adoptert retningslinjene *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980), *OECD Guidelines for Cryptography Policy* (1997) and *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002).

Tilsynsmyndighet

Datatilsynet (www.datatilsynet.no) er et uavhengig forvaltningsorgan som forvalter, behandler klager og gir informasjon om personopplysingsloven. Datatilsynet skal informere og gi råd i forhold til personvernet generelt og farer for personvernet spesielt, hjelpe bransjene med å utarbeide egne normer for atferd samt gi råd om sikring av personopplysninger. Videre skal Datatilsynet utøve tilsyn, kontrollere at lover og forskrifter blir fulgt, at feil eller mangler blir rettet opp og gi pålegg der loven gir hjemmel for det. Datatilsynet skal behandle konsesjoner og føre en offentlig oversikt over alle behandlinger som er meldt inn eller som har konsesjon. Datatilsynet skal rapportere om sine aktiviteter.

Personvernnemnda (www.personvernnemnda.no) er et klageorgan som skal behandle klager på vedtak som Datatilsynet fatter i medhold av personopplysningsloven og enkelte andre lover. Personvernnemnda fatter fortløpende vedtak etter mottatte klager.

I tillegg er det i henhold til Direktiv 95/46/EF en rådgivende og uavhengig arbeidsgruppe som overvåker at praktiseringen av regelverket er ensartet i medlemsstatene.

2.2.1 Personopplysningsloven

Personopplysninger, behandling og den registrerte

Formålet med personopplysningsloven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger. Med personopplysninger forstås i loven alle opplysninger og vurderinger som kan knyttes til en enkeltperson. Den registrerte er den som en personopplysning kan knyttes til.

Personopplysningsloven dekker alle data som kan knyttes direkte eller indirekte til individer og gjelder både offentlig og privat sektor. Personopplysningsloven gjelder for behandling av personopplysninger som helt eller delvis skjer med elektronisk hjelpemidler og annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister, dvs. både manuelle registre, dataregistre (§ 3) og opplysninger som offentliggjøres på internett.

Behandling av personopplysninger er enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter. Med personregister menes registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen (Personopplysningsloven §§ 1,2,3).

Sensitive personopplysninger defineres i loven som opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold og medlemskap i fagforeninger (Personopplysningsloven § 2).

Krav knyttet til behandling av personopplysninger

Personopplysningsloven (§ 1) beskytter retten til privatliv ved å sikre at persondata behandles i samsvar med grunnleggende respekt for retten til privatliv og retten til å beskytte personlig integritet, og ved å sikre kvaliteten på personlige data. Hovedprinsippet er at det er lov å samle inn og registrere personopplysninger hvis ett av følgende vilkår er oppfylt:

- Den enkelte har gitt samtykke
- Behandling av personopplysninger er hjemlet i særlov
- Det er nødvendig for å oppfylle en avtale med den registrerte
- Behandlingen er nødvendig for å utøve en oppgave av allmenn interesse eller for å utøve offentlig myndighet.

I henhold til Personopplysningsloven § 3 kan personopplysninger også behandles dersom dette er nødvendig for å vareta den registrertes vitale interesser, og for at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse eller ivareta en berettiget interesse der hensynet til den registrertes personvern ikke overstiger denne interessen.

Den ansvarlige, dvs. den som behandler personopplysningene, skal sørge for (§ 11)

- at personopplysningene bare nyttes til angitte formål som er saklig begrunnet
- at opplysningene ikke brukes til senere formål som ikke er i samsvar med det opprinnelige formålet, uten at den registrerte samtykker
- at opplysningene er tilstrekkelige og relevante for formålet, at de er korrekte og oppdaterte, og at opplysningene ikke lagres lengre enn det som er nødvendig.
- At det er gitt melding til Datatilsynet innen 30 dager før datainnsamlingen starter.

Personopplysningene skal bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet, og skal ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker. Senere behandling av personopplysningene for historiske, statistiske eller vitenskapelige formål anses ikke uforenlig med de opprinnelige formålene med innsamlingen av opplysningene dersom samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene den kan medføre for den enkelte.

Den enkelte har rett til innsyn i hvilke data som er registrert om dem (§ 18)og hvem som har samlet inn opplysningene (§§ 19, 20). Feil i data må rettes (§ 27). Alle har rett til å reservere seg fra direkte markedsføring (§ 26). Loven medfører en plikt til å informere den enkelte om beslutninger knyttet til dataene; om hvilke data det gjelder, hvem som har innhentet dem og hvor de er hentet fra. Unnlatelse kan straffes (§ 46). Loven gir restriksjoner med hensyn til datainformasjon til andre land (§§ 29, 30) i samsvar med Personverndirektivet (EU-direktiv 95/46/EF art. 25-26).

Personopplysningsloven krever at Datatilsynet skal informeres i forkant av datainnsamling (§§ 31, 32). I noen tilfeller kreves en lisens fra Datatilsynet, eksempelvis når sensitiv informasjon som rasetilknytning, religion og kriminelt rulleblad (§ 33) skal registreres, og for data til forsikringsbransjen, banker og telekommunikasjon.

Videoovervåking må varsles til Datatilsynet (§ 37). Videoovervåking på offentlig sted skal bekjentgjøres ved skilting (§ 40). Politiet kan bruke videoovervåking uten å varsle hvis det er viktig for etterforskningen av vesentlige kriminalsaker og de har domstolstillatelse (Straffeprosessloven 1981, § 202a).

2.3 Elektronisk databehandling i transportsektoren

Drivkrefter for nye teknologiske løsninger

Det er mange drivere for økt bruk av teknologi og nye teknologiske løsninger i transportsektoren. Samtidig påvirkes også transportsektoren av bruken av informasjonsteknologi ellers i samfunnet, som for eksempel e-handel og telependling (Ravlum 2004). Kundenes forventninger til transportsektoren kan også være en viktig drivkraft, se kap. 2.4.1 og 2.5.

Intelligente transportsystem (ITS) er system og tjenester hvor informasjons- og kommunikasjonsteknologi anvendes i transportmiddel eller nettverk som frakter personer eller

gods (Bang og Wahl 2007). Innføring av ITS kan bidra vesentlig til å nå samferdselspolitiske mål ved å gi myndigheter, operatører, transportører og enkeltindivid bedre grunnlag for beslutninger (Wahl m.fl. 2007). Trafikkstyring, overvåking og utstyr i kjøretøyene kan bidra til bærekraftig utvikling og bedre trafikksikkerhet. Bedre utnyttelse av eksisterende transportinfrastruktur bidrar til effektivitet og framkommelighet, mens forbedringer av utstyr og informasjon kan øke brukernytten og bidra til universell utforming. Bang og Wahl (2007) deler de viktigste anvendelsene av ITS i transportsektoren i seks områder:

Trafikantinformasjon:

Trafikantinformasjon gir trafikantene grunnlag for egne beslutninger. Etterspørselen etter trafikantinformasjon øker og det er etterspørsel etter multimodale system der man kan få informasjon om ulike transportformer i samme system, alt fra optimale kjøreruter og prisen på en kollektivreise til ledige parkeringsplasser. Informasjonen kan virke inn på beslutningen om å foreta en reise, tidspunktet for reisa, reisemålet, transportmidlet og reiseruta. Noen data er relativt statiske, mens andre data er dynamiske, noe som har betydning for formidlingsform. Kvaliteten på dataene i form av pålitelighet, tilgjengelighet og kostnad har betydning for valgene som gjøres. Vi skiller mellom informasjon som mottas før turen, underveis og etter gjennomført tur.

Betalingssystem:

I et elektronisk betalingssystem foregår betalingen ved bruk av en elektronisk billett eller brikke. Billetten kan for eksempel være et plastkort eller en papirbillett med elektronisk lagret informasjon. Vanligvis fungerer dette som en forenkling for brukeren ved at samme kort kan brukes på flere reiser eller på flere transportmidler. Relativt nytt er berøringsfrie kort.

Førerstøttesystem og navigasjon:

Førerstøttesystem for å bedre trafikksikkerheten har som mål å redusere muligheten for å gjøre feil, å redusere konsekvensene av feil eller å få trafikanten til å endre atferd. Andre har som formål å bedre komforten for fører og passasjerer.

Navigasjonssystem bidrar med informasjon om veien dit man skal. Noen system for veitransport har sanntidsinformasjon om framkommeligheten på veinettet og råd for alternative rutevalg for å unngå belastede strekninger, selv om slik informasjon i liten grad er tilgjengelig i Norge.

Overvåking og kontroll:

Enhetene som overvåkes kan være transportmidler eller individer i transportsystemet. ITS anvendes til overvåking av trafikkstrømmer, trafikkavvikling, potensielle konfliktsituasjoner, hendelser mm. Eksempler er automatiske hendelsesdetektorer i tunneler og identifikasjon av passasjerer ved hjelp av biometri på flyplasser.

Trafikk- og flåtestyring:

Eksempler på trafikk- og flåtestyring er prioritering av kollektivtransport og tiltak for å oppnå effektiv logistikk, færre køer og reduserte miljøutslipp ved fortløpende å tildele nye oppdrag til de enkelte sjåførene fra en sentral.

Drift av infrastruktur:

Ved å ha forskjellige typer sensorer som overvåker tilstanden på infrastrukturen, kan disse automatisk melde tilbake om feil, redusert funksjonalitet eller behov for preventive tiltak.

ITS omfatter i utgangspunktet alle transportformer. Datagrunnlaget vil i mange tilfeller være felles for flere tjenester og system. I de fleste tilfellene vil det offentlige levere data om transportinfrastrukturen, mens det kan være private aktører som leverer data om produkter og

tjenester. Det er derfor ønskelig at det etableres standarder og sikres interoperabilitet mellom systemene. Williams (2008) identifiserer følgende inndeling som benyttes i standarder: Transportinformasjon, trafikk- og flåtestyring, tjenester knyttet til kjøretøyet, godstransport, kollektivtransport, varsling av ulykker, betalingssystem, trafikksikkerhet, overvåking av vær og miljøfaktorer; katastrofehåndtering og koordinering, og nasjonal sikkerhet.

Når har teknologien personvernimplikasjoner?

Personvern er en aktuell problemstilling når data på elektronisk form kan spores tilbake til det enkelte individ. Samordning av stadig større system er en trend med implikasjoner for personvern, både kopling av informasjon fra ulike kilder som brukes av forsikringsselskap eller andre, og stadig større nett av for eksempel bomstasjoner eller flyplasser som utveksler informasjon.

Et viktig prinsipp i Datatilsynets veiledere er å utrede hvilke alternativer som har minst konsekvenser for personvernet og om alternative løsninger som ikke innebærer behandling av personopplysninger kan være tilstrekkelig for å oppnå hensikten. Vegdirektoratet pekerer på at noen tekniske system for å bedre trafikksikkerheten ikke krever personopplysninger, som alkolås, automatisk fartstilpasser (ISA) og fartssperre. Eksempler på automatisk lagring av personrelaterte opplysninger er automatisert fartskontroll over strekninger (streknings-ATK), atferdsregistrator som kan gi en tilbakemelding på kjøreatferd, og datalogger (svartboks) i kjøretøyene med informasjon som kan nyttes i analyse av en ulykke.

Teknologirådet (2007c) har identifisert fire grunnleggende teknologier, der de ulike anvendelsesområdene arver de truslene mot personvernet som er assosiert med de grunnleggende teknologiene: Kommunikasjonsteknologi, sensorer, datalagring og analyse og beslutningsstøtte. Utfordringer knyttet til kommunikasjonsteknologi er at uvedkommende kan registrere hva som blir kommunisert, hvem som utveksler informasjon hvor lenge og hvor en person befinner seg. Når det gjelder sensorer blir noen problemstillinger knyttet til videoovervåking, radiofrekvensidentifisering (RFID) og biometri belyst i kap. 2.4 og kap. 3. Utfordringer knyttet til sentrale databaser er at kobling av data avslører mer om personen, det ligger til rette for å utnytte dataene til andre formål enn det de opprinnelig var utsatt for (formålsglidning), og sentrale registre er utsatt i forhold til brudd på sikkerheten. Analyse- og beslutningsstøttesystem gjør det mulig å søke i svært store datamengder og koble data fra ulike registre.

2.4 Eksempler på personopplysninger i transportsektoren

Her presenterer vi noen tema og problemstillinger innenfor transport som det har vært oppmerksomhet rundt, og presentasjonen vil være preget av når dette skrives. Noen tema som er generelle for alle transportformene presenteres først, og deretter ser vi på situasjonen i de ulike transportgreinene. Mange av de samme eksemplene, men også andre, presenteres også i en rapport som tar opp flere forhold rundt personvern og it-risiko, lover og standardisering, organisering, roller og ansvarsfordeling innenfor elektronisk databehandling og personvern i transport (Meland m.fl. 2007). Mange peker på at forskjeller i infrastruktur, men også internasjonalt regelverk innen security, gir andre utfordringer for luftfart og internasjonal skipsfart enn for innenlandske transporter som ferge, buss, tog og bil. Hensikten er ikke en dyptpløyende analyse av situasjonen for de ulike transportgreinene, men å fylle ut det bildet som intervjuene med et fåtall informanter i bransjen skaper (se kapittel 3).

Bruken av personopplysninger i transportsektoren styres i ulik grad av personopplysningsloven avhengig av hvilken hjemmel eller lovgrunnlag som er relevant (Ravlum 2004). Førerkortregisteret er et eksempel på lovpålagt behandling. Fartskontroll er en myndighetsutøvelse og kan medføre rettskrav. Montering av svartboks i kjøretøy for å overvåke overholdelse av kjøre- og hviletidsbestemmelsene er eksempel på myndighetsutøvelse. For flåtestyring har blant annet arbeidsretten anvendelse. I samferdselssektoren er vilkårene for å behandle personopplysninger ofte oppfylt fordi det er gitt samtykke fra den enkelte. Bompengeabonnement og billettering med smartkort er basert på privatrettslige avtaler.

2.4.1 Mange eksempler er felles for flere kollektivmidler

Min side

Enkelte aktører ønsker at trafikantene skal ha oversikt over gjennomførte reiser via en personlig side på internett (”min side”) for kontroll og eventuell reklamasjon. Noen hevder at kundene forventer lagring og at dette er et krav etter bokføringsloven. Prinsipielt mener Datatilsynet at det ikke skal være forskjell i kravet til lagringstid for papirbillett og elektroniske billetter. De påpeker at dersom kunden ønsker detaljert logging av eget reisemønster, skal kunden selv aktivt be om dette. Sikkerheten ved tilgang på ”min side” diskuteres også; sikring av database mot uvedkommende, sikring av at innsyn gis til rette vedkommende og sikring av selve kommunikasjonen.

Elektronisk billettering

Elektronisk billettering benyttes på ferge, båt, fly, buss og bane. Billetten kan være et plastkort eller en papirbillett med elektronisk lagret informasjon. Relativt nytt er berøringsfrie kort. Vanligvis fungerer dette som en forenkling for brukeren ved at samme kort kan brukes på flere reiser eller på flere transportmidler. Overgangen fra papirbilletter til elektroniske kort gjør det mulig å detaljregistrere hver enkelt reise, hvem som reiser og til hvilket tidspunkt (Datatilsynet 2007b). Elektroniske spor registreres i stor skala og reiseatferd til enkeltpassasjerer kan kartlegges. Om atferden kan knyttes til en person avhenger imidlertid av om man reiser med et periodekort eller et anonymt kort (klippekort). Slike system finnes blant annet i Oppland, Hedmark, Rogaland, Sør-Trøndelag, Nordland og Troms, og er under oppbygging i andre fylker. Virksomhetene gir uttrykk for et ønske om å lagre alle kundedata og transaksjonsdata i en database. Datatilsynet viser til at behandlingen må være nødvendig og legitim. Ifølge Datatilsynet er det ikke hjemmel som tilsier lagring av reisemønster for annet enn faktureringsformål (Personvernnemnda 2007).

Datatilsynet framhever at det må være mulig å reise anonymt uten at reisemønsteret lagres i sentral database eller i kortet (billetten). Dette kan løses med forhåndsbetalte periodebilletter. Det anonyme alternativet skal være enkelt tilgjengelig.

Statistikken skal anonymiseres ved analyse av reisemønstre og når transportøren skal dele betalingen for reisen med andre transportører.

Kameraovervåking

Kameraovervåking er stadig mer vanlig, både for innfartskontroll, på terminaler, gater og åpne plasser, og i parkeringsanlegg, tunneler og transportmidler. Automatiske identifiseringssystem brukes for å gjenkjenne og identifisere nummerplater og ansikter. Et anslag er at NSB har om lag 400 kamera på Oslo Sentralstasjon og at det er om lag 5-600 kamera på Oslo Lufthavn Gardermoen (forskning.no 28.01.2008). Et fåtall overvåkingssystem har *aktiv* overvåking der noen sitter og følger med på det kameraet viser og zoomer inn når det skjer noe av interesse. Andre befinner seg på en skala fra delvis aktiv overvåking der personalet innimellom ser på monitorene, til *passiv* overvåking der opptakene spilles over etter en viss tid og bare analyseres når det har skjedd noe som gir lovlig grunnlag for det. Andre steder kan det kun være montert opp et kamera, uten film.

De fleste begrunner videoovervåking med at det er et effektivt redskap for å redusere kriminalitet, mens skeptikerne ikke ønsker et overvåkingssamfunn. En doktorgradsstudie av Mork Lomell presentert på forskning.no (04.05.2007, 19.12.2005) peker på at politiet benytter overvåking til å forebygge kriminalitet, mens privat overvåking og overvåking av transportterminaler i stor grad benyttes til å hindre uønskede personer i å oppholde seg på området. De fleste ble utvist på bakgrunn av utseende og ikke på grunn av oppførsel. Ifølge Mork Lomell er det liten grunn til å tro at videoovervåking på offentlig sted i seg selv reduserer kriminalitet. Det viser seg at aktiv overvåking medfører flere kontroller og ikke færre, med behov for kontrollører som kan rykke ut når de som følger med på kameraene ser noe mistenkelig. Blakstad m.fl. (2007 s. 28) diskuterer både analyse av erfaringsdata og erfaringsutveksling som aktuelle strategier for mer kunnskap om balansegangen mellom økt trygghet av tiltakene eller passasjerflukt som følge av engstelse ved overvåking.

Informasjon om personvernpolicy

Flere aktører (som Norwegian, NSB, Kolumbus, Bro & Tunnelselskapet) presenterer sine retningslinjer for personvern på internettsidene sine. Felles for disse er at de presenterer retningslinjene for selskapets internettsider, og de er ikke dekkende for alle virksomhetene i selskapet. Informasjonen på RUTER sine sider er kort, men ser ut til å gjelde generelt for behandling av personopplysninger. AutoPASS sine internettsider forklarer hvilke opplysninger som behandles. Mange av sidene oppgir en ansvarlig eller en kontaktperson for opplysninger om personvern (eksempelvis NSB og RUTER).

Trafikantene er en viktig drivkraft

NSB viser til at en overveiende del av kundene ønsker kameraovervåking (Datatilsynet 2005). Kolumbus viser til at kundene i fokusgrupper ytret ønske om full oversikt over alle trekk og innskudd på reisekontoen (Personvernnemda 2007).

2.4.2 Lufttransport

Reiseinformasjon, billetter og innsjekking

De fleste flyselskap tilbyr e-billetter, e-faktura, oversikt over egne reiser på internett (min side), og billettbestilling og innsjekking over internett og evt. mobiltelefon (wap). Man kan også få

sanntid trafikantinformasjon om forsinkelser, bytting av gate osv. for egne reiser på mobiltelefonen.

Nasjonalt og internasjonalt regelverk

Alle land med sivil luftfart har sluttet seg til den FN-baserte organisasjonen International Civil Aviation Organization (ICAO) og det internasjonale regelverket for sivil luftfart er likt for alle land. I tillegg fungerer European Aviation Safety Agency (EASA) som felles europeisk myndighet for sivil luftfart for alle EU- og EØS-landenes luftfartsmyndigheter.

I Norge har Luftfartstilsynet ansvaret for å utgi forskrifter basert på Luftfartsloven, som regulerer alle deler av sivil luftfart. Disse heter "Bestemmelser for Sivil Luftfart (BSL)", og er tilgjengelig på Luftfartstilsynets nettsider (www.luftfartstilsynet.no).

En sentral forskrift i forhold til sikkerhet er *Forskrift om bruk av system for sikkerhetsvurdering og sikkerhetsoppfølgingsplaner innen flysikringstjenesten* (BSL A 1-10). Avinor har et regelverk bestående av håndbøker, prosedyrer og instrukser for alle sikkerhetskritiske arbeidsoperasjoner. Det sentrale regelverket er felles for alle i konsernet. Det er tilgjengelig for alle ansatte og innleide konsulenter på Avinor sine intranettsider. I tillegg har hver enkelt flyplass, kontrollsentral eller annen organisatorisk enhet lokale regelverk basert på det sentrale regelverkets fellesmaler.

Trygghet eller sikkerhet - kontroll av passasjerer, bagasje og frakt

Sentralt i forhold til personvern er *Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten* (BSL A 2-1). Forskriften er fastsatt av Samferdselsdepartementet og hjemlet i Luftfartsloven og gir forskrifter om adgangskontroll, sikkerhetskontroll av bagasje, kroppsvisitasjon og id-kontroll av trafikanter som sender bagasje. Den gjelder for lufthavner med ervervsmessig luftfart, de deler av militære lufthavner som benyttes til ervervsmessig luftfart, luftfartsselskap som driver ervervsmessig luftfart, virksomheter som leverer varer eller tjenester til en lufthavn og andre som arbeider på eller i tilknytning til en lufthavn.

På alle Avinors lufthavner gjennomføres det *sikkerhetskontroll* av passasjerer, bagasje og frakt. Kontrollen gjennomføres for å hindre at noen bringer med seg gjenstander som kan benyttes til å begå ulovlige handlinger mot luftfarten. Sikkerhetskontrollen kan gjennomføres med bruk av teknisk utstyr som f. eks. røntgenmaskiner og metalldetektorportaler. I tillegg kan det gjennomføres manuell kontroll. Prosjektet *Kriminalitetskontroll, risiko og teknologi* peker på at sikkerhetskontrollene på flyplassene ikke er så sikre som vi liker å tro (forskning.no 28.01.08). De viser til en kontroll som Luftfartstilsynet gjennomførte, som viste at kreativt plasserte kniver og patroner ikke ble avslørt av teknologien, mens andre måtte legge igjen sjampo og tannkrem. Moderne overvåkning handler i stor grad om å skape offentlige rom som ikke oppfattes som risikofylte.

Fra 1. mars 2007 må alle flyreisende som tar med seg mer enn bare håndbagasje vise *ID-kort* ved innsjekking og ved ombordstiging. Det åpnes for at *biometri*, for eksempel i form av fingeravtrykk, kan benyttes for å oppfylle kravet i bestemmelsen. Hensikten er å gjøre luftfarten tryggere ved å sikre at den som sjekker inn bagasje også reiser med det samme flyet. ID-kortet må vise navn, bilde og fødselsdato (eksempelvis pass, førerkort, bankkort og skolebevis). Personer under 18 år som reiser ifølge med voksne trenger ikke å vise eget ID-kort. Barn eldre enn 12 år som reiser alene, må i utgangspunktet vise ID-kort. Når barn reiser alene uten ID-kort eller

mulighet til å identifiseres av medpassasjerer, kan flyselskapet sørge for andre alternativ som sikrer kontroll, blant annet ved at de følges av flyselskapets personell fra innsjekking til ombordstiging.

Passasjerer som kun reiser med håndbagasje trenger ikke fremvise ID-kort verken ved innsjekking eller ombordstiging. For å unngå forskjellige system for ulike grupper kan flyselskapene legge inn som reisevilkår at alle passasjerene må vise ID-kort.

SAS Norge har tatt i bruk biometri på innenlands flygninger

På internettsidene til SAS kan vi lese om biometri (www.sas.no): Myndighetene i Norge har pålagt flyselskapene å kontrollere alle som sjekker inn bagasje. For å gjøre dette raskt og enkelt har SAS Norge tatt i bruk biometri, eller fingeravtrykkslesere, som erstatter prosessen med å vise legitimasjon ved innsjekking og ombordstigning. Formålet med bruk av fingeravtrykk er å kontrollere at det er samsvar mellom personen som sjekker inn bagasje og personen som går om bord, ikke å sjekke personens identitet. De som ønsker det kan velge å vise identifikasjon som før.

Bilde av fingeren tatt ved utgangen sammenlignes mot tilsvarende bilde tatt når passasjeren leverte bagasjen. Når bildene er like er SAS sikre på at samme person har vært begge steder. Persondata i forbindelse med fingeravtrykk oppbevares i et sentralt register i København under reisa og slettes når reisa er avsluttet. Bildet av fingeravtrykket koples ikke opp mot noe register og det lagres ikke. Utlevering av informasjon om fingeravtrykkene er lite hensiktsmessig fordi den tekniske løsningen er bygget opp slik at informasjonen slettes umiddelbart etter avslutning av reisa. En eventuell utlevering av slike persondata kan bare skje dersom det er lovhjemmel for utlevering og det også er teknisk mulig. SAS Norge oppgir hvem som er behandlingsansvarlig på sine internettsider.

Utviklingen innen internasjonal flytransport

Prosjektet om *Kriminalitetskontroll, risiko og teknologi* peker på at en stor del av grensekontrollen utføres av private flyselskap som har et økonomisk ansvar for å kontrollere reisedokumentene våre (forskning.no 28.01.08). IKT brukes som et styringsverktøy for å utveksle informasjon mellom ulike aktører på et område som tidligere var statens oppgave. IKT fører til mer proaktiv grensekontroll og rammer i hovedsak grupper som allerede er marginalisert.

I USA benyttes et system der man tar bilde av alle 10 fingrene for nøyaktig verifisering av utenlandske personers identitet (VG 27.03.2008). Ved å bruke biometriske system vil de hindre ulovlig innreise til USA og kan beskytte passasjerene mot identitetssvindel hvis reisedokumentene blir stjålet. Hensikten er at det ikke skal være mulig å forfalske identiteten. Ifølge Teknologirådet (2007a) er det flere muligheter for forfalskning med alvorlige konsekvenser for den som blir utsatt for det.

2.4.3 Banetransport og sjøtransport

Reiseinformasjon og billetter

Selskapene tilbyr billettbestilling, oversikt over egne reiser på internett (min side), e-billetter og e-faktura. Hvis man registrerer kredittkortet man bruker i kortleseren hos Flytoget, får man

kvitteringen på e-post (www.flytoget.no). Velger man å bruke det samme kortet som for flyreiser med SAS, får man imidlertid tilsvarende kvittering fra SAS. Dette er et eksempel på at samordnet betaling medfører at flere deler av reisen registreres i samme register.

Kameraovervåking

NSB gjennomfører kameraovervåking på noen av sine tog. Datatilsynet framhever at det ikke er påvist fordeler ved å totalovervåke togene, men at det kan være akseptabelt å overvåke inngangspartiene og lokomotivføreren for å ivareta sikkerheten til personell og reisende (Datatilsynet 2006). Personvernnemnda hevder at personvernulempene er beskjedne, fordi opptakene bare vil bli avspilt og brukt ved mistanke om straffbare forhold. Imidlertid krever overvåking i passasjerområdene konsesjon, fordi bildene kan inneholde sensitive personopplysninger.

Passasjerlister på båt- og fergeruter

Elektronisk billettering, kameraovervåking m.v. er også aktuelt for båt- og fergereiser. På strekninger over et visst antall nautiske mil kreves passasjerlister. Det er ulike måter å samle inn passasjerinformasjonen på; papirlister der passasjerene skriver eget navn, lydopptak der passasjerene sier hva de heter, datalister på grunnlag av bestilling osv. I dette prosjektet er det ikke undersøkt i hvilken grad det kreves legitimasjon i forbindelse med passasjerlister.

2.4.4 Veitransport

Veitransport omhandler både private reiser med bil, kollektivtransport og næringstransport. Det er først og fremst lagt vekt på å belyse eksempler som angår persontransport.

Bilen er en databank – som kan sladre

Datateknologien i dagens nye biler registrerer sjåførens kjørestil, komfortinnstillinger for ulike sjåfører, bruk av sikkerhetsbelte, bilens hastighet, motorturtall, om bremsene er brukt, om ABS-bremsene og antiskrenssystemet (Elektronic stability programme ESP) fungerte, GPS-informasjon (posisjon, tidspunkt og fart), og om det er ulovlige bilnøkler i omløp (Samferdsel 2008). Bilene både sender og mottar informasjon. Det er knyttet markedsinteresser til informasjon både til føreren og om føreren. De færreste vet at nye bilnøkler kan ha en databrikke hvor mye informasjon om bilen og eieren er lagret. En bilnøkkel vil kunne brukes til å stjele bileierens identitet. Interessante spørsmål som er reist, er hva bileieren vet om sin egen bil og hvem som har informasjonsplikt overfor bileieren: Hvilke system er integrert, hvilke er aktivert og hvem har tilgang til data? De som håndterer bilene; importører, bilselgere og -verksteder, har ansvaret for at reglene følges.

Registrering av bompasseringer

Det praktiseres ulike retningslinjer for sletting av passeringsopplysninger for ulike betalingsformer; periodeavtaler, forskuddsbetalte avtaler og etterskuddsbetaling av enkeltpasseringer (Datatilsynet 2007a). Skattedirektoratet kan etter ligningsloven kreve innsyn i opplysninger om konkrete kjøretøy benyttet i næringsvirksomhet for å belyse påstander i ligningen. Datatilsynet legger vekt på at bompengeselskapene kan oppbevare passeringsopplysninger for kunder som eksplisitt ønsker dette. Det er imidlertid viktig at oppbevaringen avtales særskilt og at kundene samtykker aktivt. Kundene må også være innforstått med at skattemyndighetene og andre kontrollmyndigheter kan kreve tilgang til opplysningene som er lagret.

- *Periodeavtaler* er forhåndsbetaling for et fritt antall passeringer for en viss tidsperiode. Passeringsopplysninger for periodeavtaler slettes tre måneder etter at passeringen er gjennomført. Antallet passeringer har ikke betydning for betalingen, og regelverket skattedirektoratet forvalter krever ikke oppbevaring av passeringsopplysningene. Salgsdokumentasjonen for selve tjenesteleveringen (avtalen) skal oppbevares i 10 år i samsvar med krav til bokføring.

- *Forskuddsbetalte* avtaler (klippekort) omfatter avtaler der kunden på forhånd betaler en bestemt sum for et bestemt antall passeringer. Passeringsopplysningene slettes senest juni året etter at passeringen har skjedd. Salgsdokumentasjonen for selve tjenesteleveringen oppbevares i 10 år, i samsvar med krav til bokføring. Tjenesteleveringen omfatter detaljer om kjøpinngåelsen (transaksjon/faktura), men ikke passeringsopplysninger. Regelverket Skattedirektoratet forvalter krever ikke oppbevaring av passeringsopplysninger for forskuddsbetalte avtaler.

- *Etterskuddsfakturering* eller betaling med kredittkort omfatter kunder som passerer bommen uten forhåndsinngått avtale. Det gjelder også passeringer uten brikke der det ilegges tilleggsavgift, men ikke ved myntinnkast. Det tas bilde av bilens nummerskilt som lagres inntil tjenesten er betalt. Betaling skjer etter at tjenesten (dvs. bompasseringen) er levert. Skattedirektoratet mener at tjenesteleveringen omfatter passeringsopplysningene, som skal oppbevares i 10 år i samsvar med krav til bokføring. Datatilsynets utgangspukt er at opplysningene kun skal oppbevares inntil fakturaen er betalt.

Helautomatisering av noen bomringer gjør at det ikke lenger finnes et reelt anonymt alternativ, blant annet rundt større byer som Oslo og Bergen. I den forbindelse blir det pålagt å innføre og aktivt informere om et avtalealternativ som gjør at alle data som kan knyttes til person slettes i løpet av 72 timer (Datatilsynet 2007c). Samtidig bør den enkelte bilist kunne inneha flere brikker, f.eks. for å skille mellom private reiser og reiser i jobb. Med helautomatiserte bomringer mener Datatilsynet også at det bør utvises større forsiktighet ved bruk av AutoPASS-brikker til andre formål (avgiftsinnkreving i miljøsoner, parkering osv) og at det er spesielt viktig at informasjonsplikten overfor trafikanten overholdes.

På sikt legges det opp til samordnede betalingssystem for bompenger i Europa.

Automatisk nummerskiltgjenkjenning

I Norge er automatisk nummerskiltgjenkjenning med videoovervåking og sjekk mot en database, blant annet aktuelt i parkeringsanlegg. Automatisk nummerskiltgjenkjenning eller registrering av bombrikke kan også bli aktuelt for adgangskontroll/betaling i miljøsoner.

Satellittovervåking

Lokaliseringsteknologi (GSM, GPRS og satelittsystem) kan spore kjøretøy og personer, eksempelvis via mobiltelefon, gps-system i bil eller eCall. Fra 2009 skal alle nye biler være utstyrt med en sensormodul eCall, satellittposisjonering og kommunikasjon via mobiltelefonnettet, som automatisk ringer opp et nødnummer dersom kjøretøyet er innblandet i en ulykke. Bekymringer for personvernet er knyttet til muligheten for kontinuerlig dataoverføring og ikke bare ved ulykke, til overføring av tilleggsdata og til evt. uautorisert tilgang til databaser der eCall-data er lagret.

Elektronisk billettering

Forbrukerrådet (2008) har ikke registrert mange klager på elektronisk billettering. De anbefaler at det skal være tilbud om sporingsfire alternativ, at det ikke skal være dyrere å betale kontant og at det opprettes felles klageordning.

Statens vegvesens håndbok 206: *Elektronisk billettering* både beskriver og gir retningslinjer for mange forhold knyttet til elektronisk billettering. Den skal bidra til å gjøre elektronisk billettering enkelt og å samordne system på lokalt, regionalt og nasjonalt nivå. Når det gjelder lagringstid, peker den på at dette må avveies i forhold til aktuelt lovverk. Håndboka er veiledende (blått omslag). Vegdirektoratet forutsetter at anbefalingene følges i prosjekt som mottar statlig støtte og anbefaler at løyvemyndighetene setter krav i kontrakter.

I en tale i 2007 sier statssekretær Erik Lahnsten: ”*Etter hvert har vi sett at det også har blitt et økende behov for effektiv samordning og forvaltning på området elektronisk billettering. I dag er dette delvis håndhevet av staten og delvis av lokale myndigheter, mens de private virksomhetene ofte faller utenfor. Dette har vist seg dyrt og uoversiktig og gir dårlige løsninger for kundene.*

Samferdselsdepartementet har derfor satt i gang et arbeid med å få i stand en felles forvaltning for elektronisk billettering. Forvaltningens oppgaver vil kunne deles inn i hovedgruppene administrativ, merkantil- og teknisk forvaltning. Typiske oppgaver vil være forvaltning av et felles avtaleverk, etablering av kommersielle regler, håndtering av regler for kostnadsfordeling, overordnet ansvar for utveksling av transaksjoner, sikkerhetsadministrasjon og testing. Vi håper å få organet operativt i løpet av 2008.

I flere fylker er de nye elektroniske billetteringssystemene nå over i en stabil driftsfase. Behovet for å innføre felles reiseprodukter på tvers av fylkesgrensene blir derfor stadig sterkere. Det jobbes blant annet med en felles pilottest for ungdomskort på Vestlandet, flere samarbeidsprosjekter innenfor Østfoldfylkene og etter hvert også i Trøndelag og Nord-Norge.”

Kameraovervåking

For at kameraovervåking skal være lovlig må den begrunnes i et saklig behov og en berettiget interesse. I veilederen fra Datatilsynet (2004) nevnes sikring mot innbrudd, tyveri, hærverk, sikring av bevis til straffesaker og å ivareta liv og helse, som behov som kan være saklig, forutsatt at det foreligger et konkret problem eller en overhengende risiko for et slikt problem. Bruk av andre tiltak for forebygging skal være vurdert. Kameraovervåking skal meldes til Datatilsynet, det skal skiltes, opptakene skal sikres og tilgangen bør begrenses til den som er sikkerhetsansvarlig. Opptakene skal bare oppbevares så lenge det er saklig grunn og slettes etter senest sju dager.

I Datatilsynets veileder (2004) står følgende om transport: ”*I transportmidler som buss, tog, drosjer og ferger vil folk i varierende grad føle seg i en nærmest privat situasjon, og kravet til diskresjon vil være relativt høyt. Dette gjør at kameraovervåkingen normalt bare vil være tillatt dersom den skal ivareta passasjerenes eller sjåførens sikkerhet. Kameraene bør derfor kun fange opp problemområdene og ikke hele området. Overvåkingen bør også, dersom det er gjennomførbart, legges til de tidspunktene da behovet er til stede, og ikke foregå kontinuerlig.*”

Ifølge Datatilsynet gjennomføres kameraovervåking i drosjer slik at den begrenser seg til tidspunktet der passasjeren setter seg inn i bilen og reisens start (Datatilsynet 2005). Det anses ikke nødvendig å dokumentere hele reisen.

Utsending av personopplysninger

I Rogaland reagerte innbyggere på at de uoppfordret hadde fått tilsendt en e-billett påtrykt eget navn og fødselsdato. Det er først hvis mottakeren selv velger å opprette en reisekonto hos Kolumbus (underskrevet avtale) at det registreres opplysninger om kortinnehaveren. Det vil fremdeles være mulig å reise anonymt.

Statoil Norge AS sendte ifølge Adresseavisa (17.10.08) ut 30 000 brev i en reklamekampanje påtrykt adressatens personnummer, synlig i vinduskonvolutten.

Ikke alltid lett å reise anonymt

Lavprisekspressen er eksempel på et ekspressbusstilbud basert på forhåndsbestilte og –betalte billetter på internett og med telefon. Bussen stopper bare på de holdeplassene det er bestilt reise til eller fra. Dette gjør det vanskeligere for den som vil betale kontant og reise anonymt. Du er bare garantert påstigning på startholdeplassen og pauseholdeplassen, på andre holdeplasser må man i tilfelle håpe på at andre trafikanter skal på eller av (www.lavprisekspressen.no).

Det er gjennomført forsøk på automatisk detektering av trafikantenes mobiltelefoner på holdeplass, for å kunne tilby aktuell reiseinformasjon til hver enkelt (Tveit m.fl. 2008).

2.5 Aksept for behandling av personopplysninger i transportsektoren

Rapporten *Makt, beslutninger og integritet* (Ravlum 2004) oppsummerer en rekke forhold knyttet til befolkningens aksept av tiltak i transportsystemet som innebærer registrering av personopplysninger. Det er forskjeller i aksept i forhold til alder, kjønn og utdanning. Det er også forskjeller avhengig av om man bor i byer og tettsteder eller i spredt bebyggelse, enten det

kommer av forskjeller i grunnleggende holdninger eller i hvordan man opplever problemene som tiltakene søker å løse. Følgende hypoteser kan oppsummeres:

- Aksepten av tiltak er høyere om fordelene ved bruken av IKT tilfaller individene enn om fordelene er av mer samfunnsmessig art. Vi er mer tilbøyelige til å akseptere innskrenkinger av frihet eller inngripen i vårt personvern når vi har *individuelle* fordeler av det. Å avstå fra individuell frihet i bytte for *kollektiv* trygghet og effektivitet ses på som mer betenkelig. At fordelene ved IKT - tiltaket kan individualiseres, kan derfor være viktig for befolkningens aksept.
- Aksepten er høyere dersom personopplysningene gis på frivillig grunnlag (kjøpsavtaler etc.) enn om registreringene påføres uten direkte samtykke (f.eks. automatisk trafikkontroll)
- Folk har høyere aksept for tiltak som kun angår det integritetsfokuserte personvernet (stor tiltro til systemet), enn for tiltak som berører makt- og beslutningsfokusert personvern.
- Resultatene tyder på at det ikke er hvilke opplysninger som behandles, men formålet for behandlingen som har betydning for folks aksept. Man kan anta at det er større aksept for inngripen i personvernet hvis det er nødvendig for å oppnå målsettinger som verdsettes høyt.
- Personvernhensynet kan lettere ivaretas der det ikke er sammenfallende interesser mellom de ulike aktørene og drivkreftene dermed ikke blir like sterke.

Ravlum (2004) tar ikke opp spørsmål knyttet til yrkessjåfører. Er det større aksept for tiltak knyttet til yrkesutøvelse? Skjer det en tilvenning som gjør at yrkessjåfører som er vant til å bli overvåket i arbeidstida, i mindre grad reagerer på registrering som følge av fritidsskjøring? Eller reagerer de i større grad fordi de føler seg totalovervåket? Heller ikke denne rapporten handler om de som har trafikken som yrke, men om trafikantene. Men de forholdene som er nevnt her har betydning for gjennomføring av tiltak og kan være verdt å undersøke nærmere i andre sammenhenger.

3 Intervju om personopplysninger i transportsektoren

I dette kapitlet ser vi nærmere på hvordan Personopplysningsloven og forskriftene praktiseres for persontransport i Norge. Informasjon om dette er samlet inn gjennom intervju med et utvalg aktører, der hensikten har vært å få fram viktige forhold knyttet til personvern for den aktuelle etaten/bedriften og evt. barrierer i forhold til å følge Personopplysningsloven. I intervjuene og analysene har vi også søkt å belyse følgende problemstillinger:

Er det ulike utfordringer knyttet til personvern for de ulike transportgreinene? Hvilke rutiner har aktørene for å møte utfordringene? Er utfordringene for personvernet forskjellig i små bedrifter i forhold til store organisasjoner eller system som fungerer på tvers av etater og bedrifter? Kan ulik motivasjon (sikkerhet, security, effektivitet) for å innføre behandling av personopplysninger ha betydning for utførelsen? I hvilken grad kan trafikantene oppleve forskjellsbehandling og ulike tolkninger av loven og forskriftene?

Det første delkapitlet beskriver gjennomføring av intervjuene, mens resultat fra intervjuene presenteres i de øvrige delkapitlene. Resultatene er beskrivende, men ikke nødvendigvis dekkende for de ulike transportgreinene.

3.1 Gjennomføring av intervju

Intervju med 9 aktører i transportsektoren

Det er gjennomført 9 intervju med ansatte i 8 selskap som representerer private og offentlige aktører av ulik størrelse: Administrasjonsselskap og utøvere for kollektivtransport på vei, bane, luft og sjø, drosjetransport og bompengeselskap. Intervjuene er gjennomført i perioden august – desember 2008. I tillegg er det i samme periode gjennomført møter med representanter for parkeringsordninger og administrasjons- og driftsselskap for bompenger, som gir bakgrunn for noen av de samme problemstillingene.

Ved valg av informanter er det lagt vekt på at de representerer innenlands persontransport både på vei, bane, sjø og luft, med store og små aktører fra forskjellige deler av landet. Med dette som premiss består utvalget i stor grad av transportører, men også forvaltningen er representert. Noen aspekt ved undersøkelsesopplegget ble diskutert i et arbeidsmøte med Datatilsynet før intervjuene ble gjennomført. Muligheten for å inkludere myndighetene i utvalget ble drøftet. Siden alle transportformer skulle inngå, har vi valgt å prøve å få fram situasjonen slik den ser ut fra de som er utøvende, mens det ville kreve en større innsats å innhente synspunkter fra et utvalg personer i ulike myndighetsposisjoner.

Det ble gitt opp å oppnå kontakt med ett firma, mens ett firma takket nei til å delta. Siden noen informanter ønsket å være anonyme, har vi valgt å presentere hvilken transportform de representerer og hvilken rolle de har i virksomheten. En oversikt over *informantene* er vist i vedlegg 2.

Kombinasjon av e-postkorrespondanse og telefonintervju

Ett av flere moment som ble drøftet i møte med Datatilsynet, var hvem i en etat eller virksomhet vi burde snakke med. I en bedrift kan det være ulike personer og avdelinger som har ansvar for

den daglige behandlingen av data, og andre som gjennomfører vurderinger av nye løsninger for bedriften. Når vi kontaktet virksomhetene, ba vi om å få snakke med den som er ansvarlig for it-løsningene og som i praksis tar avgjørelsene på vegne av bedriften/etaten. Deretter presenterte vi kort formålet med undersøkelsen og at hensikten med den første henvendelsen var å avklare hvem i bedriften vi burde snakke med. Å få kontakt med rette vedkommende kunne imidlertid ta tid, gjerne som en kombinasjon av gjentatte oppringinger og e-post. Når det ble oppnådd kontakt, men også hvis det ikke var mulig å oppnå kontakt per telefon, ble en kort informasjon om prosjektet og intervjuguiden oversendt på e-post. På den måten fikk virksomheten mulighet til å velge hvem som skulle svare på henvendelsen, og informanten kunne evt. innhente opplysninger om noen av temaene.

Når avtale var oppnådd, ble vedkommende ringt opp på avtalt telefonnummer til avtalt tid. Spørsmålene i intervjuguiden (vedlegg 1) dannet utgangspunkt for samtalen, med mulighet for å kunne gå i dybden og stille flere spørsmål der det var interessante problemstillinger. Hensikten har vært å få fram de viktigste forholdene knyttet til personvern for den aktuelle etaten/bedriften og evt. barrierer i forhold til å følge Personopplysningsloven. For noen var det behov for å stille de samme spørsmålene flere ganger, men for ulike problemstillinger – f. eks. både knyttet til videoovervåking og til elektronisk billettering. Dette betyr at resultatene blir beskrivende, men ikke nødvendigvis dekkende for de ulike transportgreinene.

En virksomhet mente at vi burde snakke med to av de ansatte med ansvar på ulike avdelinger. En av informantene valgte å svare skriftlig og ett intervju ble gjennomført hos informanten, mens de øvrige ble gjennomført som telefonintervju. Hvert intervju tok om lag en time. Under intervjuene ble det gjort notater med papir og blyant, og det ble ikke brukt lydopptak. I tillegg har to av informantene supplert med egne notater. Renskrevne notater er deretter sendt til hver informant som ble bedt om å bekrefte at referatet er greit, eller forslå endringer og tilføyelser.

Erfaringer med telefonkontakt

For to firma var det vanskelig å trenge igjennom og nå fram til ”rette vedkommende”. Avdelingene var plassert flere steder i landet slik at det kunne være vanskelig for sentralbordet å vite hvor henvendelsen burde rettes. Telefonen ble gjerne satt over til ulike kontor der den ringte lenge uten å bli tatt. I begge tilfellene har ulike kollektivselskap fusjonert til større enheter, og det er mulig at dette har betydning for hvor oversiktlige organisasjonene framstår. Det viste seg imidlertid å fungere noe bedre å sende e-post. Det er derfor grunn til å tro at henvendelser fra publikum som sendes skriftlig, kommer fram til rette enhet også i disse virksomhetene. Mens det kan være en bekymring at publikum med spørsmål om personvern per telefon vil kunne ”slite litt” med å få svar.

Presentasjonen av resultater

Mens kvantitative undersøkelser kjennetegnes av reliabilitet, validitet og generalisering, krever kvalitative undersøkelser troverdighet, sporbarhet og overførbarhet.

Med *troverdighet* menes at både intervjuobjektene og andre skal kunne kjenne seg igjen i framstillingen. Etter hver samtale ble det skrevet et referat som informantene har fått til gjennomsyn, med unntak av det første intervjuet der dette ikke ble avtalt. En person har kommet med merknader til referatet som er tatt til følge. Oppsummeringen baserer seg i hovedsak på

intervjuerens formuleringer i referat fra samtalene, og ikke på direkte sitat fra informantene. Dette er informanter som har sagt seg villig til å bidra med informasjon. De kan selvfølgelig til en viss grad velge hva de ønsker å fortelle og hva de vil si mindre om. Det som presenteres kan derfor være "et noe glanset bilde". Det er allikevel intervjuerens inntrykk at informantene svarte både på det de opplevde som uproblematisk og på spørsmål de var mindre bekvemme med.

Synspunkter og arbeidsformer for f.eks. politikere og overordnende myndigheter kommer i liten grad fram i denne rapporten, men blir belyst innenfor noen tema i andre deler av Statens vegvesens etatsprosjekt om personvern og trafikk. Trafikantenes synspunkter kommer heller ikke fram her, annet enn indirekte, men disse blir belyst i andre deler av etatsprosjektet.

Med *sporbarhet* menes at det skal redegjøres for gjennomføringen av undersøkelsen. Hvordan undersøkelsen er gjennomført er presentert her og i kapittel *1.3 Metode.* Det er lagt vekt på å presentere svarene samlet, slik at den enkelte informanten ikke skal identifiseres, samtidig som bredden i svarene kommer tydelig fram. Både det at informantene er anonymisert og at det ikke går tydelig fram hvem som svarer hva, kan gjøre det vanskeligere for leseren å danne seg sitt eget bilde av situasjonen.

Med *overførbarhet* menes at konklusjonene skal kunne overføres til andre situasjoner. Intervjuene peker på flere tema som bør overveies i forbindelse med personvernspørsmål. Valg av tema og informanter ble også drøftet med Datatilsynet i forkant av undersøkelsen, for å sikre at problemstillingene som ble tatt opp var relevante. Med et lite utvalg informanter er det ikke grunnlag for å trekke konklusjoner, men heller peke på mulige sammenhenger og tema som bør være gjenstand for videre refleksjoner.

3.2 Behandling av personopplysninger

3.2.1 Prosesser og rutiner som inkluderer bruk av personopplysninger

I intervjuene ble det gitt følgende eksempler på behandling av personopplysninger ved innenlands persontransport:

Kunderegister

Ved elektronisk billettering (buss, ferje, båt, bane, fly) registreres navn, adresse og nødvendige kredittopplysninger i et kunderegister, som en del av avtalen mellom kunden og selskapet. Et selskap benytter i tillegg fødselsnummer for å identifisere riktig kunde. For belasting av bompenger registreres i tillegg bilens registreringsnummer.

Ved bestilling av drosje kan telefonnummer og adresse for kunder som har ringt inn registreres. Adressen det ble ringt fra forrige gang kommer opp på skjermen sammen med evt. forklaring om veien.

Billetter og betaling

Generelt vil det være slik at man legger igjen elektroniske spor hvis man betaler med kredittkort eller over internett. Hvis man betaler for drosjetransport med kredittkort, skal sjåføren alltid be om underskrift.

For flyreiser registreres navn, hvem man reiser sammen med, e-postadresse, telefonnummer og kredittkortopplysninger, der noen av opplysningene er lovpålagt. Spesielle behov i forhold til mat og assistanse kan inngå. Bookinginformasjonen blir liggende som regnskapsbilag i 10 år.

På båtruter med lugar kan det registreres navn, fødselsår, kjønn, spesielle behov og kredittkortopplysninger. Personopplysningene inngår som del av en avtale mellom kunden og selskapet. Disse opplysningene kan være lagret inntil en måned. For regnskapet lagres bookingreferansenummer i forhold til faktura, andre opplysninger lagres ikke.

For de som ønsker det sendes bekreftelse og evt. e-faktura på e-post (inngår i avtale). Det kan skje at det er problemer med å få fram e-posten, men det er ikke opplevd tilfeller der e-posten har kommet til uvedkommende.

Elektronisk billettering

Det er ulike løsninger i ulike selskap. I ett selskap sendes reiseinformasjonen for hver reise direkte til betaling. Den enkelte reisa blir også registrert hos kollektivselskapet, men disse kobles ikke mot personopplysningene i kunderegisteret.

Andre selskap lagrer nødvendige data for å kunne sende regning (navn, adresse m.m.) og alle reiseopplysninger: Dato, klokkeslett, rute, hvilken holdeplass man går på og hvilken sone man går av. I databasen lagres alle data i en periode til regningen er betalt. De som har reisekonto og forhåndsbetaling kan se oversikt over sine reiser på internett. Reiseopplysninger som dato, klokkeslett, rute, hvilken holdeplass man går på og hvilken sone man skal til, lagres også på selve kortet, men slettes igjen etter 20 minutter. En annen løsning er at de ti siste bevegelsene ligger lagret i kortet, for å kunne håndtere beregning av billettpris ved overgang osv. Disse skrives over fortløpende.

Ved bompenger oppbevares passeringsregistreringer til 30 dager etter at passeringene er betalt. Det varierer derfor med type avtale hvor lenge den enkelte registrering er i systemet. Etter pålegg fra Datatilsynet er bompengeselskapet pålagt å opplyse den enkelte kunde om et betalingsalternativ der passeringene slettes innen 24 timer i sentralsystemet og innen 72 timer lokalt i utstyret langs veikant. Ved dette alternativet står kunden svakere ved en evt. klage, ved at man ikke kan gå tilbake og se på historiske passeringer. I tillegg har systemet vært slik at de siste 100 passeringene ligger registrert i brikken i den enkelte bilen. Datatilsynet har gitt Statens vegvesen pålegg om å slå av denne funksjonen.

"Din side"

Kunden velger selv om de vil opprette egen profil eller booke reiser uten. På "min side" har de oversikt over tidligere reiser. Disse slettes per i dag ikke. Datatilsynet har pålagt dem å informere kundene om hvordan de kan avslutte "min side".

Kundene kan velge å få tilsendt tilbud på e-post (inngår i avtale). Kundene må da aktivt krysse av for dette alternativet. Det er enkelt å avslutte tjenesten ved å fjerne avkryssingen.

Plassbestilling (sjø, bane)

På noen lengre kollektivruter er det mulig å bestille plass. Det er ulike opplegg fra telefoninnringning, internettbestilling og bestilling av plass ved kjøp av billett. Ved innringing registreres navn, adresse og avgangstidspunkt. Når turen er kjørt slettes disse listene. For noen selskap skrives det ut lister som viser belegget for hver avgang. Dette er rene transaksjonsopplysninger som ikke legges i database. Papirlistene makuleres etter at turen er ferdig.

Passasjerlister, assistanse og adgangskontroll (luft, sjø)

Passasjerlister basert på bookinginformasjon sendes til avgangsflyplassen dagen før avgang, som flere telex-meldinger over et system som tilbys av en tredjepart på vegne av Avinor. Listene oppbevares i 3 dager (78 timer) etter avgang. Hvis det skjer noe alvorlig med flyavgangen (ulykke etc.) overtar politiet eierskapet til passasjerlista.

Assistanse besørges av firma som flyselskapene kjøper tjenester fra. For personer som trenger assistanse sendes det en kort melding til eksternt firma som besørger assistanse på mottaksflyplassen.

SAS beskriver sin løsning med bruk av fingeravtrykk for adgangskontroll på sine internettsider (se evt. kap. 2.4.2). Norwegian tester ut en annen teknologi på Rygge flyplass, der fingeravtrykket lagres i form av tallkoder. Norwegian sier at evt. innføring er et kostnadsspørsmål, men at det også kan gi besparelse av tid og mannskap.

For ferje- og båtturer på strekninger lengre enn en gitt grense (i antall nautiske mil) er det påbud om å registrere navn på passasjer. Dette kan gjøres med skriftlige lister eller opptak der passasjerene sier hva de heter, som lagres på tape. Tapen lagres maksimalt en måned.

På noen passasjerruter får passasjerene et personlig kort som benyttes som adgangskontroll for av- og påstigning ved midlertidige stopp underveis. Kortene gjøres ugyldig etter bruk.

Regnskap

Gjennom bookingprosessen lagres en rekke data, som lagres som regnskapsbilag i regnskapssystemet. Dette oppbevares i henhold til regnskapsloven. På sikt kan det tenkes at det gjøres et utvalg av hvilke data som skal lagres, for å spare lagringskapasitet.

Kameraovervåking

Noen transportmidler har kameraovervåking. Disse er godt skiltet fordi noe av hensikten er at folk skal vite om det og oppføre seg ordentlig. Disse er meldt til Datatilsynet. Opptaket lagres lokalt i transportmidlet og slettes etter noen dager. Det kreves dokumentasjon for lovlig grunnlag for å kunne ta ut videoopptakene.

Ved bompassering blir det automatisk tatt bilde av alle kjøretøy som passerer uten avtale/brikke. De fleste av disse bildene sjekkes automatisk mot betalingsinformasjon. Hvor stor andel av bildene som må behandles manuelt avhenger av kvaliteten på utstyret ved veikant. I tillegg har noen bomanlegg videoovervåking med tanke på hærverk o.l.

GPS

Drosjesentralen har mulighet til å følge de bilene som er på jobb på kartet med GPS. Dette gir først og fremst mulighet til å registrere informasjon om sjåførene, siden det skal litt mer til å vite hvilke passasjerer som sitter på med hvilken bil. Kartet kobles ofte ikke opp. Ved nødanrop kommer kartet automatisk opp og viser bare den bilen som har varslet.

Offentlig betalte transporter

Brukere av transporttilbud for funksjonshemmede registreres med navn, adresse personnummer, brukernummer, bilde, og evt. om man er rullestolbruker. Bildene lagres med personnummer som identifikasjon. Pga økonomibilagene til kommunen lagres hver tur med tidspunkt og fra- og til-sone for hver person.

For elever som skal ha skoleskyss registreres navn, adresse, skole og klassetrinn, og evt. behov for spesialtransport pga funksjonsnedsettelse (bokstavkode). Noen steder registreres også personnummer. Hver tur registreres for hver elev med tidspunkt og hvem som betaler for de ulike turene avhengig av formålet, for eksempel om eleven skal til behandling, til avlastning, delta på aktiviteter eller hjem osv. Kommunen skal ha detaljerte oversikter for regnskap som sysselsetter relativt mange hos transportørenes økonomiavdelinger.

3.2.2 Rettslig grunnlag for å behandle personopplysninger

Hovedprinsippet er at det er lov å samle inn og registrere personopplysninger hvis den enkelte har gitt samtykke, hvis det er nødvendig for å oppfylle en avtale, utføre en oppgave av allmenn interesse eller utøve offentlig myndighet, eller hvis behandlingen av personopplysninger er hjemlet i lov (se kap. 2.2.1).

Avtale mellom kunde og selskap

Mange av opplysningene som registreres i transportsektoren inngår som del av en avtale mellom kunden og selskapet, der det stilles krav til at samtykket skal være frivillig, utrykkelig og informert. Dette gjelder eksempelvis kunderegistre, plassbestilling, passasjerlister, e-faktura, passeringsregistreringer og oversikt over registrerte reiser ved abonnementsordninger (bompenger, elektronisk billettering, fordelsordninger osv.).

Informert samtykke

I noen tilfeller kan det være tvil om den registrerte har gitt et informert samtykke. Dette gjelder for eksempel praksisen med å registrere telefonnummer og adresse når man ringer etter drosje (som kommer opp på skjermen neste gang man ringer fra samme telefonnummer). Samtidig kan man si at dette i de aller fleste tilfeller er informasjon som ligger lett tilgjengelig allerede. Et annet tilfelle er registrering av skoleelever for å formidle skoleskyss (hjemlet i lov, dermed er det ikke nødvendigvis et krav at den registrerte samtykker). Her leverer skolene lister over elever, hjemmeadresse, skole og klassetrinn osv. ut fra opplysninger som foreldrene oppga når eleven ble skrevet inn på skolen.

Ivareta myndighetsutøvelse, rettslige forpliktelser og berettigede interesser

Passasjerlister for flyturer og lengre båt- og ferjeturer er lovpålagte oppgaver. For å kreve inn bompenger også fra de som ikke har avtale, blir det tatt bilde av bilens registreringsnummer og faktura blir sendt til bilens eier. Innkreving av bompenger kan hjemles i veiloven eller veitrafikkloven, avhengig av om hensikten er finansiering av utbygging eller regulering av trafikken. Kameraovervåking kan evt. begrunnes i allmenn interesse, å ivareta den registrertes vitale interesser eller at den behandlingsansvarlige eller tredjeparter som opplysningene utleveres til kan ivareta en berettiget interesse der hensynet til den registrertes personvern ikke overstiger denne interessen.

Behovet for å registrere opplysninger for å få refundert reiseutgifter i forbindelse med nødvendige helsetjenester (trygdekjøring) er hjemlet i Lov om pasientrettigheter. Behandling av personopplysninger for å administrere kjøring av skoleelever er hjemlet i Opplæringsloven. Transportordningen for funksjonshemmede er en frivillig fylkeskommunal oppgave, og det er ingen lovhjemlet rett til slik transport. Dette er et tilbud der man må søke om å bli bruker av ordningen.

3.2.3 Omfanget av behandling av personopplysninger i persontransport

Kan man reise anonymt?

Man kan reise anonymt ved å betale kontant som passasjer på buss, drosje og bane, og på lokale båt- og fergeruter. På flyruter og lengre båt- og fergeruter er det ikke mulig å reise anonymt pga pålegg om passasjerlister. For noen bomanlegg finnes ikke reelle anonyme alternativ fordi man også ved kontant betaling må oppgi bilens registreringsnummer.

På direkte spørsmål kommenterte en av informantene at det ikke er noe stort poeng i å kunne reise anonymt i Norge. Dette ble begrunnet med at vi i liten grad er anonyme i Norge, men legger fra oss en rekke spor overalt uansett, blant annet med mobiltelefon og betalingskort.

Hva slags data registreres

Generelt er opplysningene som lagres, ikke sensitive. Først og fremst registreres navn og adresse og evt. fakturaopplysninger. Helseopplysninger registreres ikke. For offentlig betalte transporter kan det imidlertid registreres en bokstavkode som angir om personen trenger spesialbil (rullestoltransport) eller ikke. I noen tilfeller lagres også en kort melding om forhold sjåføren bør vite om.

Ut fra prinsippet som å lagre minst mulig, valgte ett selskap fødselsnummer i kombinasjon med navn og adresse for å sikre at man fakturerer riktig kunde. Selskapet erfarer at disse opplysningene ikke gir unike treff og mener at personnummer ville vært en bedre løsning. De ønsker å kunne hente inn personnummer fra Skatteetaten for å ”vaske” kunderegisteret 2-3 ganger årlig, for å sikre at fakturaen blir riktig og går til rette vedkommende.

I tillegg registreres tidspunkt og reisestrekning for den enkelte tur. Med adgangskort kan også av- og påstigninger underveis registreres. Ett selskap oppgir å registrere kjønn (dette inngår som en del av avtalen mellom kunden og selskapet). På cruiseskip og båttransport med lugar kan restaurantregninger og barkjøp etc. være registrert sammen med avgangstidspunkt og

reisestrekning. Det er også kameraovervåking i noen transportmidler og på noen transportterminaler, samt ved passering av bomanlegg.

Man ser også behov for personnummer for utførelse av skoleskyss, både for å planlegge framtidig behov, for å gi den enkelte det vedkommende har krav på, og for riktig fakturering til kommunene. For å beregne hvilke rettigheter den enkelte har og hvor lang reiselengde kommunen skal belastes for, er man avhengig av å ha korrekt bostedsadresse.

Ut fra intervjuene ser det ut til at registreringen er mest omfattende for offentlig betalte transporter. Blant annet for å kunne fordele kostnadene på ulike etater, så dokumenteres både reisestrekning og tidspunkt for hver reise for hver person, samt i noen tilfeller også formålet med reisa.

3.2.4 Er det forskjell mellom veitransport og persontransport på bane, sjø og luft?

Gjennom de intervjuene som er gjennomført, er det ikke kommet fram vesentlige forskjeller i hvilke personopplysninger som behandles, i veitransporten i forhold til andre transportformer. Med veitransport menes her alle former for transport på vei, samt relaterte aktiviteter (parkering, bensinstasjoner etc.). Det er innslag av både privat ferdsel og organisert kollektivtrafikk både i veitrafikken og båt- og flytrafikken. En gjennomgang fra intervjuene og eksemplene i kapittel 2, viser at det er eksempler på følgende behandling av personopplysninger både innenfor veitransport og for andre transportformer (bane, sjø og luft): Kunderegistre, passasjerlister, adgangskontroll, plassreservasjon og billettbestilling på internett, elektronisk billettering, registrering av hver enkelt tur, og kameraovervåking i transportmiddel og på terminal.

En forskjell innen adgangskontroll er at flyselskapene prøver ut eller har innført biometri, sammenligning av bilder av fingeravtrykk, for å registrere personer.

3.3 Ansvar og opplæring i organisasjonen

3.3.1 Ansvar, opplæring og rutiner

Behandlingsansvarlig og databehandler

Behandlingsansvarlig defineres i Personopplysningsloven (§ 1) som den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Databehandler er den som behandler personopplysninger på vegne av den behandlingsansvarlige.

I intervjuene spurte vi hver enkelt hvem som var behandlingsansvarlig og hvor mange som var databehandlere i egen organisasjon. De ser ut til å ha en god forståelse av begrepet. Flertallet viser til at en av toppsjefene (administrerende direktør, divisjonsdirektør etc.) er juridisk og overordnet behandlingsansvarlig, enten alene eller sammen med andre i organisasjonen som har medansvar innenfor sitt område. Noen peker på at hver systemeier har ansvar for at rutiner og regler følges på sitt område. En svarte at administrasjonen, inkludert teknisk sjef, er behandlingsansvarlig.

Flere kunne gi klar beskjed om hvor mange databehandlere det er i organisasjonen og vise til at disse har rolledefinert tilgang, det vil si at hver enkelt bare har tilgang til de registrene de trenger for å gjøre den jobben de skal utføre. I noen tilfeller er det vanskelig å oppgi antall databehandlere, fordi salgsnettet kan være omfattende. Det kan være et stort antall og en stor

andel av de ansatte som i begrenset omfang har befatning med personopplysninger. I dette utvalget gjaldt dette ikke aktører innenfor veitransport.

Internopplæring og de ansattes bevissthet

Når det gjelder internopplæring og de ansattes bevissthet, spriker svarene veldig. De fleste svarer at de har noe om personopplysninger og datasikkerhet i internopplæringen, noen har også informasjon om Personopplysningsloven, men at Personopplysningsloven ikke gjennomgås direkte. De mener likevel at de gir en tydelig opplæring med hensyn til hvordan informasjon behandles, hva som er taushetsbelagt informasjon og hva man ikke forteller til publikum. Flere organisasjoner har klare rutiner i forhold til telefonhenvendelser. Hos en av virksomhetene er regelen at informasjon om bestemte turer aldri besvares per telefon. Noen organisasjoner viste henvendelsene til politiet, andre henviste til at den som ønsker informasjon må møte opp personlig og legitimere seg. En virksomhet krevde både navn på den reisende samt to ulike opplysninger knyttet til reisa for å oppgi informasjon. I noen bedrifter er IT-reglement utarbeidet og kjent for de ansatte. Hos en av virksomhetene er varsomhet med å oppgi informasjon nedfelt i virksomhetens etiske regler (grunnregler som blir terpet i organisasjonen). En virksomhet forteller at Datatilsynet i tillegg har pålagt dem å utarbeide en databehandleravtale. Noen forteller at det er pekt ut personer i organisasjonen som har et spesielt ansvar.

Andre kjenner ikke til opplæring på området. En ansatt sier at han har måttet sette seg inn i Personopplysningsloven og annet lovverk på området på eget initiativ, etter at problemer innenfor vedkommendes arbeidsområde allerede var avdekket. Han peker på at andre har bestemt hvilke registreringer som skulle gjennomføres, og at det burde være en selvfølge at de ansatte får en innføring i de lover og krav som de må kjenne til for å gjennomføre sine oppgaver, men kjenner ikke til at dette har vært en del av internopplæringa. Han kjenner heller ikke til at det er personer innenfor organisasjonen som har et spesielt ansvar og som han kan spørre til råds.

Mange mener at bevisstheten hos de ansatte er høy. Flere peker på at ansatte skriver under taushetserklæring, og at også firma som jobber for dem (underleverandører) må skrive under taushetserklæring.

Veitransport ser ikke ut til å skille seg ut fra andre transportformene på dette området.

Eksempel på en organisasjon med tydelig fokus på vern av personopplysninger

Nedenfor trekker vi fram ett eksempel på en organisasjon som har et tydelig fokus på vern av personopplysninger. Ut fra et fåtall intervju med begrenset varighet har vi ikke grunnlag for å si at denne organisasjonen gjennomfører rutinene bedre enn andre. Men i dette intervjuet framkommer flere momenter, blant annet ryddighet mht. dokumenter, som ikke belyses av de andre:

Kunnskap om behandling av personopplysninger er en vesentlig del av personalopplæringen (opplæringsplan) – både for ansatte i teknisk drift og for kundebehandling over skranke, telefon og e-post. Alle skriver under taushetsplikt på ansettelseskontrakten, både fast ansatte, vikarer og innleid hjelp. Også ansatte hos underleverandører av tjenester har taushetsplikt i forbindelse med de oppgavene de utfører for organisasjonen, og innbefattes av opplæringsplanen.

Det er god oppdatering av rutinene på intranett, samt påminning på e-post og egne håndbøker. Det legges stor vekt på ryddighet. Papirer skal holdes innelåst og forlates ikke på pulten. De har også sjekket rutinene hos selskapet som utfører makulering.

Den personen som ble intervjuet har en oppfatning om at bevisstheten er høy hos egne medarbeidere. Blant annet pga. gjennomtrekk i stillingene, er kundebehandlere organisert i grupper med erfarne gruppeledere som de kan spørre til råds. Det blir aldri gitt opplysninger om den enkelte reise over telefon, bare på grunnlag av skriftlige henvendelser der man kan se at opplysningene kommer fra rette vedkommende. Alle henvendelser fra politiet blir vurdert i hvert enkelt tilfelle av behandlingsansvarlige (adm. dir.), blant annet på grunnlag av avtalen med hver enkelt.

Rutiner for å opplyse den enkelte om hvilke opplysninger som registreres

I Personopplysningslovens § 2 legges det vekt på at et samtykke skal være en frivillig, uttrykkelig og informert erklæring fra den registrerte, om at han eller hun godtar behandling av opplysninger om seg selv. §§ 18-24 regulerer retten til innsyn og informasjonsplikten. § 20 legger for eksempel vekt på at den registrerte ikke har krav på varsel dersom innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov, varsling er umulig eller uforholdsmessig vanskelig, eller det er på det rene at den registrerte allerede kjenner til informasjonen varslet skal inneholde. Det er med andre ord ikke krav om å informere den registrerte i alle tilfeller. Mange av opplysningene registreres på grunnlag av en avtale med kunden. Her presenterer vi alle informantenes svar under ett, uten å skille på hvilke data som registreres eller formålet med disse:

I forbindelse med avtaler, informeres det ved at den enkelte må gi samtykke til at opplysningene registreres, og det er alltid mulig å melde seg av. En av informantene informerer aktivt om hvilken avtaleform som medfører minst lagring av data. En av virksomhetene sier at Datatilsynet har pålagt dem å informere bedre (mer presist) om hvordan de registerte dataene benyttes og hvordan kunden kan slette en opprettet ”min side”. En av aktørene oppgir at alle opplysninger som hentes inn i arbeidet med markeds- og trendanalyser skjer på grunnlag av at kunden aktivt aksepterer at informasjonen samles inn og brukes til dette formålet. Utsending av tilbud på e-post skjer bare ved aktiv påmelding.

Noen svarer at de opplyser om de registreringene de foretar på forespørsel. De har ikke opplevd at det etterspørres mer informasjon om behandling av personopplysninger på nettsidene deres. En av informantene sier at de prinsipielt erkjenner nødvendigheten av at folk skal vite hva som registreres om dem. Men de tror at folk blir unødvendig skeptiske hvis de skulle ringe dem opp bare for å fortelle at de er oppført i et register med navn og adresse. Andre oppgir at de ikke har rutiner for å opplyse kundene om hvilke data som registreres eller hva som er formålet.

Når det gjelder skoleskyss vises det til at foreldrene oppgir opplysninger i forbindelse med innskriving i skolen. Da gir de samtykke til at opplysningene registreres i et elevregister og brukes til de formål som er nødvendige i forbindelse med skolegangen. De oppgir at myndighetene (iht. Forvaltningsloven) ikke er pliktige å søke konsesjon for å opprette elevregister. Skoleskyss er hjemlet i opplæringsloven (§§ 7, 13).

I forbindelse med kameraovervåking oppgir alle at disse er forskriftsmessig skiltet.

Det ser ikke ut til å gå skillelinjer mellom transportgreinene når det gjelder å informere om hvilken informasjon som registreres, men heller i forhold til formålet med registreringen.

3.3.2 Krav til behandling av personopplysninger

Personopplysningsloven (§ 11) gir en rekke krav til behandling av personopplysninger, se kap. 2.2.1. Med sikring av *konfidensialitet* menes beskyttelse mot at uvedkommende får innsyn i opplysningene (se for eksempel Datatilsynet 2002). Med *integritet* menes at opplysningene ikke blir endret som følge av utilsiktet eller uautorisert aktivitet. Med *tilgjengelighet* menes at tilstrekkelige og relevante opplysninger er til stede når det er behov for dem.

Dataene skal være relevante, korrekte og oppdaterte

Transportaktørene er avhengige av at datasystemene fungerer og gjennomfører nødvendige tiltak for å sikre dataene med hensyn til integritet, tilgjengelighet og sikkerhet mot innsyn, ut fra virksomhetens behov. Disse tiltakene ivaretar også behovet for vern av personopplysninger. De har tenkt igjennom situasjoner som snoking, svindel, misligheter, virus, bevisst sabotasje og driftsavbrudd. Eksempler på tiltak er bruk av brukernavn og passord, Bank-ID, høy sikkerhet ved ekstern pålogging utenfra, brannmur på pc og nettverk, lukkede system med separate servere og nett for ulike registre, nettverk med høy grad av sikkerhet, fysisk sikre datarom der bare klarert personell har adgang, og kryptering ved overføring av informasjon. Alle data lagres på server og ikke lokalt på harddisken på pc'ene. I noen tilfeller må også noe informasjon lagres lokalt. Det er klare rutiner for lagring på flere sikre steder med automatisk og manuell backup, og for overskriving av data. Å sette bort driften til profesjonell tredjepart og å bruke anerkjente leverandører nevnes også som del av kvalitetssikringen. En av virksomhetene påpeker at de lærer og endrer rutiner på grunnlag av hendelser.

En virksomhet forteller at Tollvesenet av og til har bedt om å få utlevert passasjerlister på grunnlag av mistanke. Senere har Tollvesenet bedt om å få en portal slik at de kan overvåke passasjerlistene fortløpende, noe som ikke blir imøtekommet. En virksomhet forteller at de har hatt besøk av et it-firma som tilbød seg å samle alle e-faktura for kunden slik at kundene kunne motta samleregninger for ulike typer tjenester. Dette ble avslått fra virksomhetens side. Hvis kunden ønsker dette, må kunden selv sørge for at e-fakturaen sendes til det eksterne firmaet ved å oppgi en annen e-postadresse. En virksomhet forteller at de har endret retningslinjene for å oppgi reiseinformasjon etter en hendelse der ett familiemedlem har oppnådd å endre bestillingsdata for andre familiemedlemmer.

Et eksempel på rutiner for å sjekke om dataene er korrekte er visuell kontroll før innlegging, og deretter logisk sjekk av dataene som er lagt inn i registeret.

Det er begrensinger på hvilke ansatte som har tilgang til hvilke data, og et fåtall har tilgang til å endre eller fjerne data. Noen få kan ha tilgang til relativt mye. I noen tilfeller kan bare en saksbehandler om gangen ha tilgang til og gjøre endringer i registeret. De har faste retningslinjer for gjentatte operasjoner uten rom for skjønn fra kunde eller saksbehandler. Hvis de ansatte har logget seg på med eget passord og brukernavn kan det spores hvem som har foretatt endringer. Andre tiltak er taushetserklæring og klare regler for hvilke opplysninger som kan gis til publikum. Noen virksomheter peker på at de har hatt gjennomgang av rutinene, med tildeling av nye rettigheter og adgangskontroll. Som eksempel på utfordringer peker de på at det kan bli tungvindt å bruke pc'ene hvis de skal sikres helt. Med dagens minnepinner kan for eksempel mye data lastes ned på kort tid.

Mange av intervjuobjektene framhever likevel at man ikke helt kan gardere seg mot menneskelige feil.

Så lite som mulig; personopplysningene skal være saklig begrunnet

Det gjennomføres vurderinger av behovet for personopplysninger, med den hensikt å registrere så lite som mulig. Dette er en kontinuerlig oppfølging samt utløses av sak, behovet for nye data eller nye system. Med unntak av en informant opplyser alle at de ikke registrerer flere data enn de trenger, det medfører bare merarbeid. En av informantene påpeker at det i løpet av en reise automatisk lagres en rekke data; der ikke alle er like nødvendige. Bare en av informantene har opplevd at systemene de blir tilbudt har lagt opp til å registrere flere data enn de strengt tatt har bruk for.

For e-billettering ble det i ett system valgt å benytte fødselsnummer istedenfor personnummer ut fra prinsippet om å registrere så lite som mulig. Deres vurdering i ettertid er at de burde valgt personnummer for å sikre korrekte og tilstrekkelige data; nemlig at faktura basert på reiseopplysninger kommer til rett person. Deres erfaring er at fødselsnummer sammen med navn og adresse ikke er tilstrekkelig for å få unike treff. Tilsvarende blir det påpekt at personnummer er nødvendig for å sikre forsvarlig saksbehandling for skoleskyss. For å beregne hvilke rettigheter den enkelte har og hvor lang reiselengde kommunen skal belastes for, er man avhengig av å ha korrekt bostedsadresse.

En av virksomhetene lagrer en rekke data om hver reise for eget analyse- og planleggingsformål. Datatilsynet har ikke hatt innvendinger i forhold til hvilke data som lagres, men pålegger virksomheten å informere kunden bedre om bruken av dataene. Dette er ikke sensitive data, men en del av disse opplysningene er slike som kunden ikke selv er bevisst på at blir registrert.

Lagres så kort tid som mulig

Hvor lenge dataene lagres kan ha betydning for om opplysningene bare brukes til opprinnelig (avtalt) formål eller er tilgjengelige også for andre hensikter. Hvor lenge dataene lagres henger sammen med formålet. I flere av intervjuene kunne ikke informantene redegjøre nøyaktig for lagringstida for alle typer data. Dette er naturlig da de heller ikke er bedt om å forberede seg på en slik oversikt. Noen av anslagene er derfor omtrentlige.

Kunderegistre er kontinuerlige og inneholder opplysninger som navn, adresse, evt. gyldighetsområde for periodekort og faktureringsopplysninger. Med unntak av e-billetter registreres ikke reiseinformasjon. Registre for skoleskyss oppdateres hver sommer. Etter avsluttet videregående skole blir registreringen lukket. En avsluttet registrering blir beholdt en viss tid, med tanke på at elever kan flytte tilbake til skoledistriktet eller gjenoppta skolegang. Det viste seg å være noe usikkerhet i forhold til hvor lenge en avsluttet registrering faktisk befinner seg i systemet.

Videoopptak lagres et visst antall dager før det automatisk slettes/spilles over. Passasjerlister o.l. lagres også relativt kort tid (til turen er kjørt – inntil en måned). Ifølge informantene kan også annen personlig informasjon knyttet til reiser i noen tilfeller bli lagret inntil en måned, selv om disse ikke knyttes til regnskapet.

Det velges ulike løsninger for å lagre informasjon i selve smartkortet for å håndtere overgangsbillettering; hver enkelt hendelse lagres i et kort tidsintervall, eller det lagres et visst antall bevegelser i kortet som skrives over fortløpende. Når det gjelder lagring av hendelser på

AutoPASS-brikken ga informantene inntrykk av usikkerhet med hensyn til om Statens vegvesen har slått av denne funksjonen.

Flere aktører har vært i lengre dialog med Datatilsynet om lagringstid for data knyttet til e-billettering. Som en av informantene påpeker så finner de ikke samsvar mellom Datatilsynets oppfatning om at dataene bør slettes fortest mulig – som av noen aktører blir oppgitt å være etter senest 30 dager, mens andre oppgir 3-5 måneder - og regnskapsloven. Slik de oppfatter bedrifts- og regnskapslovgivningen skal regnskapsdata lagres elektronisk i 3 år og oppbevares i 10 år. En løsning kan være å lagre data mot et kortnummer, men uten informasjon som knytter dette mot en person.

To selskap benytter en løsning der reiseinformasjonen sendes direkte til betaling. Enkeltreisa registreres hos kollektivselskapet, men kan ikke knyttes til personinformasjon. Noen selskap lagrer reiseinformasjon for e-billettering så lenge som nødvendig for å gjennomføre fakturering (inkludert mulighet for å klage). Andre har den oppfatning at bedrifts- og regnskapslovgivning går foran personopplysningsloven og at data i all fall bør oppbevares for hele foregående år; til selvangivelsen for enkeltpersoner og firma er behandlet. Andre lagrer all reiseinformasjon som regnskapsbilag i 10 år. Mange tilbyr kundene oversikt over sine reiser på ”din side” på internett, noe som i praksis kan bety at dataene lagres over lang tid.

Et argument for lengre lagringstid er kunden kan ønske at kortet gjenskapes ut fra historiske data fordi kortet har blitt tapt eller ødelagt, dvs. at historiske data knyttes til det nye kortet. Dette vil være vanskelig med streng håndhevelse av begrensinger i lagringstiden. De peker også på at kundene framover i tid vil forvente personifisert kundeservice med internettsider som gir oversikt over kundens foretatte reiser, belastning av konto, preferanser i forhold til seteplassering osv. Reiseplanleggere for ulike transportmidler forventes også, der informasjonen om kunden evt. må være tilgjengelig for flere aktører. (Disse forholdene er redegjort for i Statens vegvesens håndbok 206: Elektronisk billettering.)

En av virksomhetene lagrer en rekke data knyttet til reisa som regnskapsbilag i 10 år. Per i dag lagrer de alle data, fordi de ønsker å nytte dataene i analyse av kundeatferd for planlegging av egen virksomhet. På sikt kan det tenkes at de velger ut hvilke data de trenger å lagre for å spare lagringskapasitet.

Et annet hensyn er et samfunnsmessig behov for god reisevanestatistikk. Statistisk sentralbyrå ønsker detaljert informasjon og tjenlig aggregeringsnivå diskuteres. Er det mulig å anonymisere dataene og samtidig ta vare på informasjon knyttet til f.eks. kjønn, alder og bosted?

En av interessentene oppsummerer at det er forskjellige regelverk og interesser som kommer til anvendelse: Effektiv servicerettet kundebehandling, personens interesser for privatlivets fred, tilstrekkelige data for korrekt fakturering, regnskapslovens regelverk for lagring av regnskapsdata, bedriftens interesser for god statistikk for å planlegge tilbudet, samfunnets interesser for godt statistikkgrunnlag og kundevennlig kollektivtransport.

Informantene etterlyser klarere retningslinjer og prinsipielle avklaringer mellom regelverk. De opplever at de får forskjellige svar på ulike tidspunkt og avhengig av hvilken saksbehandler som svarer, slik at ulike virksomheter forholder seg til ulike anbefalinger. De oppfatter det også som et problem at personopplysningsloven og regnskapslovgivningen er under ulike departement, noe som gjør det vanskelig å avklare hvilket lovverk som har prioritet over det andre og hvilke retningslinjer som bør følges. Informantene opplever at det går med svært mye tid til å prøve å

avklare slike uklarheter (uten å få gode svar). Det kan være en ide å utarbeide veiledning til Personopplysningsloven for transportsektoren.

- *og bare brukes til opprinnelig formål*

Systemeier har ansvar for at dataene bare blir brukt i samsvar med opprinnelig formål og kundens samtykke. Aktørene viser til at alle ansatte har taushetsplikt, og at de har rutiner for henvendelser som skal rettes til behandlingsansvarlige. Ved henvendelser fra myndigheter og boktettersyn krever de samtykke fra den det gjelder eller rettskraftig dom for å gi opplysninger. For flere av registrene er det rolledefinert tilgang, slik at de ansatte bare har tilgang til de dataene de har behov for, for å utføre jobben. For noen typer data er det klare rutiner i forhold til lagringstid.

En virksomhet oppgir at de utarbeider anonymisert statistikk i samsvar med Personopplysningsloven. En annen virksomhet utarbeider markeds- og trendanalyser ut fra informasjon der de har innhentet samtykke spesielt for dette. En av virksomhetene samler automatisk inn en rekke data knyttet til reisa som lagres som del av regnskapsbilaget fordi de ønsker å nytte dataene i analyse av kundeatferd for planlegging av egen virksomhet. Enda en virksomhet sier at de har diskutert muligheten for å ta ut statistikk som grunnlag for markedsføring, men de har ikke sett det hensiktsmessig. Ett selskap opplyser at kommunen har etterspurt statistikk for transportordningen for funksjonshemmede som viser trafikken mellom ulike soner (fra/til-soner) fordelt på tidsrom, som grunnlag for å planlegge organisert felleskjøring. Dette er en henvendelse som selskapet per i dag ikke har oppfylt.

Kommentarer til ombruk av data:

Data som er samlet inn for å utføre fakturering benyttes av en virksomhet for å analysere kundeatferd for å planlegge egen virksomhet. En annen virksomhet har vurdert å gjøre det som grunnlag for markedsføring. I begge tilfeller kan dette sannsynligvis gjennomføres uten å knytte reisedata til person (anonymiserte data), men det kan kreve andre lagringsformer med separate registre. Det er også et spørsmål om disse dataene trenger å lagres like lenge som regnskapsbilag.

I ett tilfelle er det forvaltningen som etterspør statistikk for sin planlegging av tjenesten. Dette gjelder transport for funksjonshemmede. For disse personene blir det som nevnt sendt inn relativt spesifiserte opplysninger som grunnlag for fakturering. Når man vet at dette er en liten og på mange måter synlig (stigmatisert) gruppe som får utdelt et lite antall turer fordelt på vanlig drosje og spesialbil, så er det lett å tenke seg at den enkelte kan bli identifiserbar selv om man bruker sone-til-sone fordeling og ikke gateadresser. Hvis det skal gjennomføres er det i alle fall viktig å tenke igjennom aggregeringsnivå for at den enkelte skal være anonym. Samtidig, hvis det skal oppfylle hensikten, vil kommunen sannsynligvis ha behov for å skille mellom behov for spesialbil og vanlig bil. Rent umiddelbart oppleves det som bekymringsfullt at det er myndighetene som her ber om ombruk av data utover opprinnelig formål, uten at premissene synes å være tilstrekkelig klarlagt.

Kobling av data fra ulike registre

Flere av aktørene oppgir eksplisitt at de ulike registrene de har ikke blir koblet og at det er lagt inn sperrer som vil gjøre dette vanskelig.

To informanter sier at det hadde vært ønskelig å kunne hente data fra folkeregistret for å sjekke personnummer, navn og adresse direkte, både ut fra effektivisering av arbeidet og for å få korrekte og tilstrekkelige data for rettferdig kunde- og saksbehandling.

Risikovurdering

For de fleste selskapene blir risikovurderinger av datasikkerhet og personvern gjennomføres med jevne mellomrom, med fullstendig gjennomgang med flere års mellomrom og mindre omfattende evaluering av endringer underveis. De vurderer sannsynlighet og konsekvens av mulige hendelser for å vurdere risikokostnad og prioritere tiltak. Noen framhever viktigheten av jevnlige vurderinger som del av et fastlagt program. En aktør viser til at det gjennomføres risikovurdering som en løpende aktivitet hele året, samt årlig revisjon. IT-avdelingen har kontinuerlig fokus på dette. En av informantene forteller at de ikke har regelmessige gjennomganger som del av et fastlagt program, men at de vurderer sikkerheten løpende blant annet på grunnlag av hendelser. Denne bedriften søker å lære både av hendelser i forhold til eget system, og hos andre selskap: Kunne dette ha skjedd hos oss?

Eksempler på hendelser som ble nevnt som uheldige for *bedriften*: For bedriftens del er konsekvensene for omdømme viktigst, i forhold til publikum og oppdragsgivere. En aktør peker på at en uheldig episode ikke bare vil skade omdømmet, men vil kunne gi vesentlige endringer i aktørens aktiviteter, uavhengig av om den uheldige episoden skjer hos dem eller andre aktører. Kundene vil ikke skille mellom de ulike aktørene, noe som vil medføre at alle må endre arbeidsform. Ifølge en virksomhet er det verste som kan skje hvis uvedkommende får tilgang til hele lista med kundenes kredittkortnumre. For noen er det verste som kan skje at opplysningene blir borte fordi det vil være svært arbeidskrevende å registrere disse på nytt. For andre gir manglende statistikkgrunnlag problemer med å dokumentere inntekter som er grunnlaget for overføring av midler mellom det offentlige, private virksomheter og privatpersoner.

Eksempler på hendelser som ble nevnt som uheldige for *kunden*: Flere peker på at de ikke har data som er spesielt sensitive for kundene og at de ikke har sannsynliggjort store konsekvenser for den enkelte kunde. Et eksempel er at privatkunden eller bedriftskunden ikke kan dokumentere reiseutgifter overfor ligningsmyndighetene. Et annet eksempel er at uvedkommende får tilgang til opplysningene. Kunder kan oppleve den personlige integriteten som krenket hvis de ikke ønsker at andre skal vite hvor de har vært.

3.3.3 Policy ved innkjøp og utvikling av nye produkter

En ting er å gjennomføre en risikovurdering av den databehandlingen som finner sted. Dette inkluderer en oversikt over personopplysningene, formål og hjemmel, samt plikt til informasjon, innsyn, melde- og konsesjonsplikt. Hensikten er å identifisere hendelser som kan medføre risiko, samt sannsynligheten og konsekvensene av disse.

Mer grunnleggende er bevisstheten ved kjøp av nye produkter og tjenester, og ved utvikling av disse. Ved å stille noen grunnleggende spørsmål allerede før produkter utvikles/kjøpe, kan man redusere behovet for korrigerende tiltak i etterkant:

- Kan alternative metoder som ikke innebærer behandling av personopplysninger benyttes?
- Er valgt metode den som i minst grad innebærer risiko ved behandling av personopplysninger?
- Er det samsvar mellom interessene som forsvarer behandlingen og risikoen ved behandling av personopplysninger?

Korte intervju med en informant i hver organisasjon gir ikke et utfyllende bilde av graden av bevissthet ved nyervervelser. Vi stilte likevel noen spørsmål for å få en ide om i hvilken grad vern av personopplysninger ble tillagt vekt (se vedlegg 1, spørsmålene 10-12).

En av virksomhetene sannsynliggjør at dette er et grunnleggende tema ved valg av og utvikling av IKT-tjenester og ved kjøp av eksterne tjenester. Dette dokumenteres fortløpende. De har ikke tradisjon for å velge rimeligere men mindre sikre løsninger. En av aktørene peker på at HMS-ansvarlig og markedsansvarlig har ulike roller og ansvar når IKT-løsninger og informasjonstjenester skal kjøpes, slik at effektivitetshensyn avveies mot sikkerhet og vern av personopplysninger. Eksterne IT-konsulenter og ansatte i firma som jobber for dem må skrive under på erklæring om konfidensialitet. Andre peker på at de ikke har overgripende regelverk, men starter med å vurdere hvilke lover og regelverk som kommer til anvendelse ved anskaffelse av nye løsninger. Hensynet til personopplysninger avklares i forhold til formålet med IKT-løsningen. Flere peker på at de kjøper produkter fra anerkjente firma med mange kunder som følger ISO-standarder etc., og at flere kunder i samarbeid er med på utviklingen av nye løsninger. Noen følger Statens standardavtale ved kjøp av programvare, og krever at produktet skal følge norsk regelverk.

Ved innkjøp og utvikling av produkter for elektronisk billettering har flere av aktørene hatt dialog med Datatilsynet for å avklare hvilke forhold det er viktig å ta hensyn til. De etterlyser prinsipielle avklaringer og klarere retningslinjer på et område som vil få stadig økende aktivitet. Uttalelsene kan tolkes slik at forsøk på avklaringer tar for mye tid i utviklingsarbeidet, samtidig som de opplever at lite blir klart.

En av informantene sier at de i liten grad har utredet personvernhensyn ved egenutvikling av system. Det sier seg selv hvilke opplysninger de trenger til ulike formål, og å innhente opplysninger utover dette vil gi unødvendig merarbeid. Andre peker på at de har arvet både it-utstyr, programvare og arbeidsoppgaver fra andre institusjoner i forbindelse med endret organisering av funksjoner. De kjenner ikke til hvilke vurderinger som er gjort. Enkelte av informantene har bare ansvar for selve registrene og kjenner ikke til hvilke vurderinger som ligger til grunn for forhandlinger og kontrakt ved kjøp av transporttjenester (på grunnlag av de registrene de administrerer). Personvern synes generelt ikke å være et tema ved kjøp av transporttjenester, men det henvises til at det kreves at leverandøren følger opp det regelverket som gjelder.

Kommentarer til forskjellig bevissthet ved kjøp og utvikling av nye løsninger:

Bevisstheten i forhold til nye løsninger synes ikke å være forskjellig mellom transportgreinene, men heller i forhold til virksomhetene størrelse og organisering. Det er kortere vei fra tanke til handling i en mindre organisasjon. Samtidig kan enkeltpersoner føle seg som gissel i større organisasjoner der funksjonene er atskilte og man bare gjør "jobben sin" uten fullt ut å kjenne avgjørelsene bak valg av system.

En av aktørene framhever at de har hatt samme konsulent for it-løsninger over lang tid, noe som gjør at konsulenten kjenner behovene deres godt. På den annen side kan virksomheten da gjøre seg sårbar ved at de er prisgitt denne konsulentens oppmerksomhet på personvern og kjennskap til lovverk på området.

Dialog med kundene

Aktørene har dialog med kundene gjennom sine markedsavdelinger og markedsframstøt. Det hevdes at kundene har klare forventninger om videreutvikling av personifiserte tjenester, som internettsider som gir oversikt over gjennomførte reiser og reisebestilling med ulike aktører, der personlig informasjon om preferanser og "faste" reiser er lagt inn. Informert samtykke er grunnlag for registrering av opplysningene. De har også dokumentert at kundene ønsker videoovervåking. Det er derfor ikke bare teknologiske muligheter, men også kundenes forventninger om enkle, bekvemme og trygge løsninger som er drivkrefter bak økt registrering. Dette aktualiserer behovet for drøftinger og prinsipielle avklaringer.

3.4 Hvilke oppfatninger har informantene?

På slutten av intervjuet ble det stilt en rekke spørsmål der informantene ble bedt om å svare ut fra egen oppfatning. De kunne altså si sin mening uavhengig av den jobben de har, samtidig preger jobben hvilken erfaring man har og hvilke tema som engasjerer. På noen av spørsmålene gir svarene preg av at de tenker ut fra sin jobbvirksomhet.

3.4.1 Oppfatninger om trafikantenes bevissthet

Hvor bevisste vil du si at folk flest er på spørsmål knyttet til personopplysninger?

Folk er ikke veldig bevisste, men ikke helt ubevisste heller. Noen mener at bevisstheten generelt er ganske delt; noen bryr seg, andre ikke. Andre peker på at ungdom er lite bevisste og legger fra seg mange spor. De er først og fremst opptatt av å få tilgang til tjenestene. De fleste tror ikke det er så farlig. Noen mener at folk reagerer stadig mindre – som del av en utvikling der vi i stadig større grad må oppgi personrelaterte opplysninger nærmest overalt, der den enkelte er bundet av systemet for å få gjort det man skal. Det kan være en del av en samfunnsutvikling der det private har blitt offentlig i mange sammenhenger.

Aktørene erfarer i liten grad at kundene har bekymringer eller etterspør mer informasjon om behandling av personopplysninger på nettsidene deres. Folk er også villige til å akseptere inngrep i privatlivet for å oppnå et bedre tilbud. Kundene ønsker for eksempel kameraovervåking, gitt at opptakene brukes som forutsatt.

Folk flest er bevisste og skjermer bruken av personnummeret, og de vil vite hvorfor det skal oppgis. Samtidig oppgir de personnummeret for å oppnå tjenester de ønsker og ser ikke hvordan de som enkeltpersoner kan skjerme seg. En av informantene viser til at vi tidligere ble lært opp til å passe på personnummeret vårt. Dette henger igjen i folks bevissthet, men Datatilsynet legger ikke lengre like stor vekt på at personnummeret er privat informasjon. Han viste til en undersøkelse der NRK ba folk om å opplyse personnummeret sitt, der alle de spurte svarte at det hadde de ikke noe med. De samme personene oppgir villig personnummeret ved kjøp av en mobiltelefon på Elkjøp.

Hvordan tror du skandaleoppslag om personopplysninger på avveie påvirker folks holdninger til å inngå avtaler eller til å gi fra seg opplysninger?

Noen peker på at slike uheldige episoder skjer i Norge stadig vekk. Saker, en eller flere, vil kunne skade de aktuelle aktørenes (myndighet, selskap, bransje) omdømme som helhet. En av informantene mener at dette er lite sannsynlig med de sikkerhetsrutiner som finnes i dag, også andre er tvilende til om det kan skje i transportsektoren. Andre peker på at det har skjedd og kommer til å skje, men at folk i liten grad reagerer på den type informasjon som da kommer fram. Det er få eksempler på at dette har ført til skade for enkeltpersoner, og media gjør ofte betydningen av hendelsene større enn det er grunnlag for. Generelt reagerer folk mer på sensitive opplysninger som helseopplysninger og finansopplysninger. Men hvis noen kan følge en bestemt person over en viss tid, så kan det være følsom informasjon.

En av informantene tror ikke folk er særlig opptatt av dette eller at enkeltstående saker vil påvirke folks holdninger til å inngå avtaler eller gi fra seg opplysninger, mens en annen sier av erfaring at det går over. Noen mener at folk blir mer skeptiske en stund, men at det glir over. Det er vanskelig for enkeltpersoner å gardere seg så lenge man ønsker å motta tjenester og aksepterer forutsetningene. Andre mener at folk blir mer bevisste på sikt. Det er viktig at publikum kan stole på den parten som etterspør opplysninger. Hvis man oppdager at det er lett for andre å få utlevert informasjon om uvedkommende, så vil man bli mer bevisst i forhold til å bruke systemet.

Slik du ser det, er det forskjell på om det avkreves personopplysninger av vanlige trafikanter eller for yrkessjåfører?

Flere svarer at de ikke ser noen prinsipiell forskjell på private reiser og reiser i yrkessammenheng, i begge tilfeller handler det om individer. Majoriteten har ikke noe å skjule. Overvåking er samtidig positivt og negativt, det kan bidra til trygghet og beskytte mot uriktige beskyldninger.

Andre legger vekt på at ansatte må forholde seg til ett strengere regelverk som i mange tilfeller overstyrer personopplysningsloven, som kjøre- og hviletidsbestemmelser for sjåfører. Store kjøretøy medfører for eksempel større ansvar i forhold til miljø, kjøretider, trafikksikkerhet osv, og noen legger vekt på at profesjonelle utøvere skal kunne spores. På tog er det registrering av energiforbruk (samfunnsnyttig formål) som kan knyttes til den enkelte ansatte. På tog og fly er det ”svarte bokser” der dataene analyseres etter ulykker. Det diskuteres å innføre videoopptak av togføreren som kan analyseres etter en ulykke, men da må det innføres klare regler for hva opptakene skal kunne brukes til.

Kommentar:

I noen tilfeller der informanten mente at det ikke er prinsipielle forskjeller på å registrere private reiser og reiser foretatt som del av yrket, så var dette informanter i virksomheter der sjåfører overvåkes i betydelig større grad enn kundene.

3.4.2 Sammenhengen mellom formålet og aksept for registrering av opplysninger

Har hensikten med tiltaket betydning for om registrering av personopplysninger bør aksepteres?

Hensikten med behandlingen bør vurderes opp mot tiltakene. Det er viktig at kunden opplever å få noe igjen og å tilby et reelt anonymt alternativ. En av informantene mener at tiltak for sikkerheten er viktigere enn andre formål. Folk aksepterer mye hvis de ser nytten for seg. Det må samtidig overveies om hensikten kan oppnås på andre måter. Som et eksempel kan man være enig i at man bør ha oversikt over passasjerene i et fly, men at det kan gjøres på andre måter enn ved fingeravtrykk. En av informantene mener at hensikten og gjennomføringen må tåle offentlig debatt, og begrunnelsen må være reell. Et eksempel er om bøtlegging av fartsoverskridelse ved streknings-ATK virkelig bidrar til bedre trafikksikkerhet, eller om anonym analyse av dataene vil gi grunnlag for tiltak som gir minst like god forbedring av sikkerheten. Data bør anonymiseres hvis det er tilstrekkelig for å oppnå hensikten.

En av informantene rettferdiggjør bruk av personnummer med effektivisering, fordi det krever færre ansatte.

Synes du det er greit å registrere personopplysninger uavhengig av formål, hvis det inngår i en avtale mellom leverandør og kunde?

Nei. Det må opplyses godt og det må finnes alternativer. Registreringene må være relevante i forhold til avtalen, og det må gagne den personen det gjelder eller andres sikkerhet, en reell vinn - vinn situasjon. Det er også behov for at myndighetene (bl.a. Datatilsynet) kan overvåke rimeligheten i avtaler og legge føringer for om virksomheten i det hele tatt kan spørre om/kreve registrering i den grad det kreves i dag. Når det spørres om opplysninger som går litt for mye innpå en som person, må man kunne hoppe av og ikke inngå avtale. Det er ikke nok at kjøper kan reservere seg. Vi trenger også beskyttelse mot oss selv, som enkeltperson er man ofte nødt til å godta mye for å få gjort vanlige tjenester.

3.4.3 Myndighetenes og aktørenes ansvar

Etter din mening, hvem vil du si har ansvaret for å vurdere det totale omfanget av personopplysninger innenfor transportområdet?

Vi spurte om hvem som har ansvaret for å vurdere det totale omfanget av personopplysninger i transportsektoren. Vi utdypet dette med å peke på at hver enkelt trafikant legger igjen spor flere steder på samme reise og på ulike transportmidler.

Myndighetene: Noen av informantene mener at Datatilsynet har ansvaret for å vurdere det totale omfanget av personopplysninger som registreres innenfor transportområdet i Norge og for å utarbeide retningslinjer. En av informantene peker på at mange involverte aktører ønsker å ha noe å si, men at Datatilsynet har mye de skulle ha sagt og gjør en jobb for borgerne. Samtidig blir det antatt at Datatilsynet har liten kapasitet i forhold til å skulle overvåke alle samfunnsområder. En av informantene mener at Datatilsynet har en veiledningsplikt som de ikke følger opp, men istedenfor henviser den enkelte bedrift og saksbehandler til å gjøre egne vurderinger på grunnlag av henvisninger til div. internettsider osv. En av informantene peker på at virksomhetene må forholde seg til regelverk under forskjellige departement (for eksempel personopplysningsloven, regnskapsloven osv.), noe som gjør det vanskelig å få avklart hvilke regler som faktisk gjelder og få konkrete svar og veiledning. Informanten mener det hadde vært bedre om departementene avklarer dette seg imellom slik at virksomhetene har ett kontaktpunkt.

Hver enkelt av oss har selvfølgelig også et ansvar og velger de som skal bestemme etc. men det er vanskelig for den enkelte å påvirke hver enkelt avtale. Derfor er det riktig at myndighetene kan gripe inn og vurdere f.eks. rimeligheten av en avtale.

Den enkelte virksomheten: Den enkelte bedrift har et ansvar i forhold til hvilke opplysninger de trenger å be om, og at disse opplysningene ikke kommer ut. Det må gjerne være regler (fra myndighetene), men det er hva som skjer i praksis som teller. Datatilsynets ansvar er å etterse at lovene følges og at behandlingen ikke bryter loven.

Kommentar:

Det er noen som setter stort fokus på den enkelte bedriftens ansvar. Samtidig synes ikke dette å samsvare helt med at hele bransjer kan bli skadelidende hvis en bedrift trår feil?

Har myndighetene et ansvar for å opplyse og bevisstgjøre folk på omfanget av og evt. konsekvenser av personopplysninger?

Myndighetene har et særlig ansvar for å informere og bevisstgjøre folk, og å informere om rettigheter. Det kan være vanskelig å bevisstgjøre folk, men det er viktig å peke på hva som kan bli konsekvensene. Utviklingen går fort. Det er ikke lenge siden vi bare ble registrert i manuelle system. Når disse registrene ble overført på data ble vi informert om at alle registre holdes separate. Nå samkjøres for eksempel trygdesystemet og skattelister, til tross for tidligere forsikringer. Mange føler seg mistenkeliggjort og overvåket.

En informant peker på at oppslag i media kan bidra til bevisstgjøring, samtidig som han peker på at medieoppslagene gjerne kan være mer balanserte. Det er lett å få store oppslag ved å klage på at noe er byråkratisk og omstendelig, men det kan også vinkles positivt at årsaken er tiltak som bidrar til å begrense innsyn fra andre.

Har organisasjoner som din et ansvar for å opplyse og bevisstgjøre folk på omfanget av og evt. konsekvenser av personopplysninger?

Innenfor enkelte virksomhetsområder har virksomheten et helt klart ansvar. Egen organisasjon har ansvar for å forklare hvorfor man registrerer opplysninger og hva som er hensikten.

Andre mener at egen organisasjon skal forsvare det nivået de legger seg på og følge krav og forskrifter. Bedriftene opplyser om hva som registreres i forbindelse med samtykke. Det er ikke deres oppgave å opplyse og lære opp publikum, men informasjonen skal være lett tilgjengelig for dem som etterspør den. For mye bevisstgjøring vil kanskje gjøre folk mer skeptiske enn de er i utgangspunktet.

Hvilke farer ser du for misbruk av opplysninger og hvilke forutsetninger må være tilstede?

Misbruk krever tilgang, anledning og motiv. Man kan aldri sikre seg 100 % mot tap, at uvedkommende får tilgang eller ”utro tjener”. At noen får innsyn og tilgang til personrelaterte forhold som ikke vedkommer andre, kan skje ved uhell, at noen gjør feil, og ved at ansatte velger å misbruke eller kopiere data. Faren kan være større ved evt. papirutskrift eller hvis noen lagrer data på egen harddisk, fordi dataene da kan komme på avveie, også etter at den er kassert. Bedrifter kan velge å utnytte data til andre formål enn det som var forutsatt.

Forutsetningene er både svikt eller manglende sikkerhetsprosedyrer for IKT og interesse av misbruk. Holdninger og informasjon er viktig for å unngå interne lekkasjer. Selv om noen bedrifter har gode rutiner for ulike henvendelser fra private og det offentlige, så vet man ikke hva andre organisasjoner og bedrifter har. Nysgjerrighet og stolthet over å vite noe andre ikke vet, kan være tilstrekkelig motivasjon. Det forekommer misbruk av andres identitet, som det er vanskelig for den som blir utsatt for det å komme ut av. Noen selskap selger opplysninger som andre selskap benytter til markedsføring.

De fleste informantene er enige om at den type informasjon som de registrerer er svært lite interessant for andre, dermed skulle motivasjonen for misbruk være liten.

4 Diskusjon og oppsummering

Avslutningsvis forsøker vi å oppsummere hva intervjuene forteller om status med hensyn til sikring av personopplysninger innenfor innenlands persontransport med ulike transportmidler. Generelt er dataene som samles inn ikke spesielt interessante for andre, men det kan være hensiktsmessig å være føre var på grunnlag av omfanget av registreringene. Det synes å være forskjellig praksis med hensyn til lagring av data, spesielt i forhold til regnskapsloven, til tross for samarbeidsmøter og veiledningsmateriale. Vi antyder noen forskjeller mellom små og store virksomheter og mellom private virksomheter og offentlig forvaltning. Vi trekker også fram noen forhold i materialet som kan begrunne et videre arbeid med å utarbeide en sektorpolicy for personvern.

4.1 Hovedpunkt fra intervjuene

Personopplysningene i transportsektoren er ikke sensitive

Vi legger fra oss en mengde elektroniske spor som trafikanter i Norge ved betaling med kredittkort for billetter, bensin og parkering, via mobiltelefon og bompengebrikken, ved bestilling på internett, plassreservasjoner og passasjerlister, og med kameraovervåking på terminaler og transportmidler. Mange mottar også faktura/kvittering for utført reise på e-post, andre kan se oversikt over egne foretatte reiser på internett. Noen av disse opplysningene kan knyttes mot en bestemt person, og disse kaller vi personopplysninger.

Mange billetter kan bestilles over internett, lengre kollektivreiser har plassreservasjon og på flyreiser og lengre sjøreiser er det krav om passasjerlister. Ved bruk av drosje og lokal kollektivtransport er det mulig å reise anonymt så lenge man betaler kontant. For elektronisk billettering finnes flere løsninger. I noen system lagres få personifiserte data. I andre system lagres hele reisehistorikken til den enkelte, avhengig av hvilken betalingsform kunden har valgt. Som bilist kan man i stor grad være anonym hvis man betaler kontant, men i noen bompengeanlegg er det ikke helt anonyme alternativ.

Det er i liten grad sensitive personopplysningene som behandles i transportsektoren. Oppfatningen blant aktørene er dessuten at informasjonen i det enkelte registeret i liten grad er interessant for andre enn den det gjelder, evt. med unntak av personer som ønsker å ”kikke” noen de kjenner ”i kortene”. Mange av personopplysningene registreres som del av en avtale, der trafikanten blir gjort oppmerksom på hvilken informasjon som registreres når avtalen inngås. Kameraovervåking skiltes tydelig, siden noe av poenget er at publikum skal vite om det.

Opplæring og rutiner i egen virksomhet

De fleste virksomhetene har ikke personopplysningsloven som et spesifikt tema i internopplæringen. De har likevel en tydelig opplæring med hensyn til hvordan informasjon behandles og hva som er taushetsbelagt informasjon. De har klare rutiner i forhold til henvendelser fra publikum og fra offentlige instanser. De opplever at kollegene har høy bevissthet rundt personvern.

Andre opplever at dette ikke var tema i internopplæringen, og at de på egenhånd har måttet sette seg inn i problemområdet etter hvert som arbeidsoppgavene har krevd det. Det kan synes som at

ansatte i organisasjoner der ansvarsområdene er klart atskilt, kan føle at de sitter med ansvaret og utfordringen alene, dersom det ikke er spesielt utpekte i organisasjonen som har et spesifikt ansvar for hensynet til personvern (eksempelvis HMS-ansvarlig eller IT-ansvarlig).

Virksomhetene har et tydelig fokus på datasikkerhet og gjennomfører mange tiltak for å sikre konfidensialitet, integritet og tilgjengelighet. Dette gjelder fysisk sikring, passordbeskyttelse og rolledefinert tilgang, kryptering av informasjon som sendes mellom enheter osv.

Flere viste til tydelige rutiner for jevnlig risikovurdering av datasikkerhet og personvern, for andre synes dette å bli utløst av endringer i systemet. For den enkelte kunde er det ikke sannsynliggjort store konsekvenser ved brudd på datasikkerheten. For virksomhetene er konsekvenser i forhold til omdømme viktigst, både overfor oppdragsgivere og kunder. Kunder skiller ikke mellom ulike aktører, slik at uheldige episoder kan påvirke omdømmet til og medføre endringer for hele bransjer.

Intervjuobjektene framhever at man ikke helt kan gardere seg mot menneskelige feil.

De har i varierende grad rutiner som fokuserer på personvern ved kjøp og utvikling av nye løsninger. For noen er dette grunnleggende, for andre kan utfordringene komme mer overraskende underveis i prosessen. Felles er imidlertid at de søker å klargjøre lover og regler tidlig og innlede dialog med Datatilsynet der de ser behov for det. Ellers viser de til at de bruker standard avtaler, velger anerkjente firma med mange kunder, eller at de samarbeider med flere aktører for å utvikle løsningen. En aktør hadde et langvarig forhold til samme konsulent. Dette kan være et riktig valg. Men det kan også stilles spørsmål ved om det på sikt gir rom for at nye og kritiske spørsmål blir stilt.

Personvern synes generelt ikke å være et tema ved kjøp av transporttjenester, men det henvises til at det kreves at leverandøren følger opp det regelverket som gjelder.

Prinsippet om minimalisme – så lite og så kort tid som mulig

Med ett unntak oppgir alle at de ikke lagrer flere opplysninger enn det som er strengt nødvendig, og at det er uaktuelt fordi det vil medføre ekstraarbeid. Flere av aktørene oppgir eksplisitt at de ulike registrene de har ikke blir koblet og at det er lagt inn sperrer som vil gjøre dette vanskelig.

Et hovedargument for kort lagringstid er at dette effektivt sikrer at opplysningene bare blir brukt til opprinnelig formål. Hvor lenge data lagres avhenger av formålet, men også av ulik praksis i de ulike selskapene. Typisk er at passasjerlister slettes etter relativt kort tid, mens mange reiseopplysninger lagres til et visst antall dager etter at regningen er betalt eller på ubestemt tid. Generelt lagres det mye data om oss ganske lenge. Det er først og fremst to argumenter som benyttes for å forsvare lang lagringstid:

1) Kundene forventer tjenester der de har full oversikt over tidligere reiser og påløpte utgifter. De forventer også enkle reisebestillingstjenester med personlig profil, gjerne for flere transportmidler og selskap. Også når det gjelder utgiftsoversikten ser de en fordel i å ha alle transportrelaterte utgifter i samme oversikt.
2) Aktørene forstår regnskapsloven og relatert regelverk slik at lagring over lengre tid er pålagt.

I tillegg ble driftsmessige argument nevnt, og bedrifts- og samfunnsmessige argument for å etablere god statistikk for å planlegge kollektivtilbudet. For statistikkformål vil det i de fleste tilfeller være tilstrekkelig med anonymiserte data.

Den mest detaljerte statistikken, ut fra det materialet vi har fått innblikk i, gjelder personer med nedsatt funksjonsevne, enten det gjelder skoletransport eller transportordning for funksjonshemmede. For transporten fra skolen registreres også formålet på reisemålet, for å fordele regninga på ulike offentlige etater. Ett selskap opplyser at kommunen etterspør sone-til-sone statistikk for transportordningen for funksjonshemmede som grunnlag for å planlegge organisert felleskjøring. Selv om dette ikke er utført, oppleves det rent umiddelbart som bekymringsfullt at det er myndighetene som ber om ombruk av data utover opprinnelig formål, uten at premissene synes å være tilstrekkelig klarlagt. Hvis det skulle gjennomføres, ville det i all fall være viktig å tenke igjennom aggregeringsnivå for at den enkelte skal være anonym. I intervjuene er det bare i saksbehandling for det offentlige at det framkommer at personnumre benyttes. I ett tilfelle argumenteres det for effektivitetshensyn i tillegg til forsvarlig saksbehandling.

At det offentlige her framstår forskjellig fra private virksomheter, kan ha årsak i et lite utvalg intervju der offentlige etater ikke selv har kommet fram med informasjon. Det kan ha årsak i saksområde og lovgrunnlag, eller forskjeller knyttet til beslutningsfokusert og maktfokusert personvern i forhold til det integritetsfokuserte personvernet.

Litt her og litt der

To informanter diskuterer muligheten av å koble registre. Hvis personnummer, navn og adresse i eget register kan sjekkes direkte mot folkeregisteret, vil det medføre mer korrekte data og effektiv og riktig saksbehandling.

Det ser ut til at bevisstheten rundt å skille egne registre er høy. De fleste aktørene har en oppfatning av at deres data ikke er sensitive og at deres system er trygt nok. De er derfor ikke bekymret for å lagre data lenge. Hvor det til slutt blir av gamle data når dagens organisasjon har vært gjennom en rekke omorganiseringer/fusjoner, kan være en bekymring. En annen bekymring kan være at vi legger igjen flere og mer innholdsrike spor i ulike sammenhenger, med ”ubegrenset” lagringskapasitet, der andre aktører i samfunnet kan ha tilgang til stadig bedre søkemuligheter, regnekraft og metoder til å kunne sammenstille og analysere data.

Interessekonflikt mellom kort datalagringstid og kunder som vil beholde alle muligheter

Den intuitive responsen til folk flest er at de vil har full oversikt over egne reiser og egne utgifter. Dette gjelder for eksempel ”din side” hos kollektivselskapene og bompengeselskapene. De vil ha oversikt over utgiftene og kunne klage hvis de oppdager feil. Det krever en grundigere gjennomgang av problemstillingen før motforestillinger dukker opp. De fleste har ikke selv opplevd at opplysninger om dem har kommet på avveie. Mange er verken klar over hvilken sikkerhetsteknologi som benyttes, muligheten for å bryte den eller muligheten for å koble informasjon mellom ulike dataregistre. Et annet moment er at vi ofte har det travelt med å få ordnet det vi skal – vi har derfor ikke tid til å lese alt som står før kontrakten underskrives og stoler mer på magefølelsen.

Både teknologi og folk flest er drivkrefter for mer personopplysninger

Markedskreftene vil i seg selv være en drivkraft for å implementere stadig nye muligheter som skal gi oss bedre tilbud, og publikum ønsker utviklingen velkommen. Vi vil ha det som er enklest for oss og som gir de beste løsningene. En av informantene var inne på at vi er del av et samfunn der mer og mer av det private blir offentlig, med reality-tv og facebook som eksempler. En annen pekte på at utviklingen har gått veldig fort. Det er uoversiktlig å prøve å sette seg inn i situasjonen i dag, og enda vanskeligere å se for seg situasjonen noe fram i tid.

Virksomhetene har selv egeninteresse i de løsningene de foreslår. Bortsett fra de store organisasjonene, syntes det ikke å være så stor bevissthet på å gjennomføre risikovurdering for personopplysninger som en integrert del av planleggingen av nye løsninger. Fokus er i større grad på hva løsningene kan gjøre og hvordan markedet mottar dem.

Det vil derfor være behov for en institusjon som Datatilsynet som kan holde oppmerksomheten om temaet oppe og bidra til en bevisstgjøring både av privatpersoner og i arbeidssammenheng. I forhold til publikum etterlyste informantene ”noen” som kan gå inn og se på om avtaler er rimelige, og vurdere om man faktisk skal lagre så detaljrike opplysninger selv om personen gladelig gir tillatelse til det. I forhold til de profesjonelle aktørene ser det også ut til å være behov for en ”motpart” som kan korrigere virksomheter når de går for fort fram og ikke har sett på konsekvensene utover sine egne arbeidsoppgaver. Om dette skal organiseres som i dag eller om man skulle hatt større grad av bransjeråd, sjekklister etc. før man tar opp saken med Datatilsynet, kan diskuteres.

Behov for avklaringer, råd og veiledning

Ved innkjøp og utvikling av produkter for elektronisk billettering har flere av aktørene hatt dialog med Datatilsynet for å avklare hvilke forhold det er viktig å ta hensyn til. De etterlyser prinsipielle avklaringer og klarere retningslinjer på et område som vil få stadig økende aktivitet. Uttalelsene kan tolkes slik at forsøk på avklaringer tar for mye tid i utviklingsarbeidet, samtidig som de opplever at lite blir klart.

Til dels er dette et klassisk problem der de som jobber ute i felten vil ha presis veiledning og klare svar, mens de som har jobbet mye med et tema opplever at det ikke er så enkelt og at det er mange avveininger som må gjøres. Denne situasjonen har dels bakgrunn i at det dukker opp nye tema der ulike problemområder avdekkes underveis, det vil si at man ikke har alle svarene når dialogen og diskusjonen starter. Datatilsynet fører tilsyn med mange ulike bransjer og kan heller ikke forventes å ha detaljkunnskap om alle løsninger. Samtidig har prosessen vært så langvarig at verden og premissene til dels endrer seg underveis.

I tillegg er Datatilsynets utgangspunkt at ethvert tiltak må vurderes konkret, under forutsetning av at formålet skal søkes oppnådd på den minst inngripende måte (proporsjonalitetsprinsippet). I hvilken grad det er gjennomført risikovurdering og sannsynliggjort at risikoen er forsvarlig har betydning for om tiltaket kan gjennomføres. Det er derfor ikke bare tiltaket og formålet som må vurderes konkret, men også de sikkerhetstiltakene som er iverksatt.

Det er likevel overraskende at de ulike virksomhetene har valgt prinsipielt forskjellige løsninger uten at de kommenterer forskjellen til de andre. Fungerer erfaringsoverføringen mellom aktører innenfor samme bransje godt nok, eller er det slik at mange finner opp kruttet samtidig? Hvilken

rolle har bransjeorganisasjonene, fylkeskommunene og andre offentlige myndigheter i å sette temaet på dagsorden og diskutere retningslinjer?

Det finnes veiledningsmateriale både hos Datatilsynet og hos Statens vegvesen, og elektronisk billettering er tema for samarbeidsmøter og seminar. Ifølge Vegdirektoratet forutsettes det at anbefalingene i håndbok 206: *Elektronisk billettering* følges i prosjekt som mottar statlig støtte, og de anbefaler at løyvemyndighetene tar dette med som krav i kontrakter. Når det gjelder lagringstid, peker imidlertid håndboka på at dette må avveies i forhold til aktuelt lovverk. Men at det skal være så vanskelig å avklare forholdet til regnskapslov etc. kan synes merkelig, for dette må da være et felles tema for mange bransjer?

Meland m.fl. (2007 s. 51) peker på flere tiltak for å støtte bransjen; klare retningslinjer og krav på personvernområdet, etablering av tekniske standarder for betalingsmedier i integrerte system tilknyttet transport, og etablering av støttefunksjon som samler erfaringer og assisterer i tekniske spørsmål. Det er viktig at publikum kan stole på den parten som etterspør opplysninger. Feil håndtering hos en aktør kan ramme større deler av bransjen og framtidige muligheter. Det forventes store endringer framover som kan gjøre det riktig med et ”føre var” prinsipp, siden det vil være vanskelig å fjerne informasjon som allerede er i ”omløp”, mens det sjelden er vanskelig å tilføre ny informasjon. Det kan synes riktig å etablere bransjeveiledning nå som omfatter hele transportsektoren uavhengig av transportmiddel og evt. offentlige tilskudd. Man vil sannsynligvis ikke få fram statiske retningslinjer, men vil måtte gjenta prinsipielle diskusjoner med jevne mellomrom og justere veiledningen etter hvert.

4.2 Oppsummering og refleksjoner for videre arbeid

Kan man reise anonymt i Norge i dag?

Det ser ut til at det kan være vanskelig å reise anonymt i Norge i dag. Man må i så fall være relativt bevisst og velge både transportmiddel, reiserute og betalingsform ut fra ønsket om å reise anonymt. De opplysningene som etterspørres om oss og som lagres, er ikke sensitive. Bekymringen ligger heller i omfanget av data som lagres om oss og at en del data synes å bli lagret ”til evig tid”.

Er det forskjeller mellom de ulike transportgreinene?

Ut fra den informasjonen vi har her, er det vanskelig å se at veitransport skiller seg spesielt ut i forhold til annen innenlands persontransport. Mange av temaene innenfor kollektivtransport er uavhengig av transportmiddel.

En forskjell er at aktørene er færre innenfor bane- og luftfart. Dermed er den mer overskuelig for kunden og det offentlige, og består av relativt store profesjonelle aktører. Luftfart og sjøtransport har også strenge regelverk for internasjonal trafikk, som kan påvirke både organisering og måten virksomhetene tenker på, også når det gjelder innenlands trafikk. Innenfor sjøtransport, men kanskje spesielt veitransporten, er det åpning for mange og små aktører på en rekke områder. Dette kan gjøre situasjonen mer sårbar.

Den største forskjellen i bevissthet og mellom valgte løsninger fant vi *innenfor* veitransport.

Bør forskjeller utjevnes?

Innenfor kollektivtrafikken ser det i dag ut til å være relativt store forskjeller i forhold til hvilke data som lagres og hvor lenge de lagres. De som lagrer mye data lenge, har innhentet tillatelse eller har en avtale med kunden, men det er likevel ikke sikkert at dette er den beste løsningen. Det er allerede pekt på at kundene er en av drivkreftene for økt bruk av persondata, uten at konsekvensene helt er overveid. Som nevnt under avsnittet om *Behov for avklaringer, råd og veiledning*, kan det derfor være nødvendig å etablere noen bransjeråd for å sørge for at noen minimumskriterier overholdes.

Den andre store forskjellen ser ut til å være mellom de som er privatkunder og de som blir tilkjent en offentlig tjeneste. Tildeling av skoleskyss, trygdereise i forbindelse med helsetjenester, transportordning for funksjonshemmede osv., er en myndighetsutøvelse der myndighetene ser det som en del av sin oppgave å kontrollere at ingen får mer enn de har rett til eller utnytter systemet. For mange er nok dette relativt problemfritt. Men de som er avhengig av flere av samfunnets tjenester kan oppleve at den totale registreringen blir svært omfattende der de må gi fra seg detaljerte opplysninger på svært mange områder – helse, bolig- og familiesituasjon, arbeidsliv/trygd, og også transport. Det vil derfor være behov for stadige avveining mellom databehov for samfunnets kontroll og den enkeltes rett til å skjerme sitt privatliv, der man ikke kan se på transportsektoren isolert.

Hypoteser og refleksjoner for videre arbeid

En kvalitativ intervjustudie med et fåtall informanter gir ikke grunnlag for bastante konklusjoner. Vi kan *likevel* trekke fram noen hovedpunkter om behandling av personvernopplysninger i transportsektoren:

- Virksomhetene innenfor transport befinner seg på *alle nivå* fra de som jobber aktivt for å være ledende/best, til de som mener at andre fordeler veier tyngre enn å følge regelverket til punkt og prikke. Virksomhetenes behandling av personopplysninger i forhold til personvern kan eksempelvis beskrives som ulike nivå: 1) risikoreduksjon, 2) forholder seg til minimumsstandarder, og 3) være ledende/best.
- Det er sammenheng mellom virksomhetens oppgaver, formålet med databehandlingen og risiko i forhold til omdømme, og virksomhetens nivå på behandling av personopplysninger i forhold til personvern. Det viktigste motivet for å forholde seg til personvernet er virksomhetens *omdømme* (som grunnlag for virksomhetens eksistens).
- *Større* virksomheter, både offentlige og private, er mer profesjonelle på IT-sida. På den annen side kan det være vanskelig for den enkelte ansatte å overskue konsekvenser av hvordan de gjennomfører sine arbeidsoppgaver. Er det større behov for opplæring, instrukser, system og formalisert interngjennomgang i større bedrifter?
- Personbehandling ved noen typer myndighetsutøvelse skiller seg ut: Den kan fremstå som urettferdig nettopp fordi myndighetsutøvelsen skal være så rettferdig; enkeltpersoner blir ilagt mye større dokumentasjonsplikt enn andre for å få tilgang til et tilsvarende tilbud (kompensasjonsprinsippet).

Materialet gir grunnlag for følgende begrunnelser for å arbeide med en felles policy eller bransjestandard innenfor transportsektoren:

- Uheldige omstendigheter hos en aktør vil ha *konsekvenser for en gruppe* tilsvarende aktører.
- Det er stor *forskjell* i hvordan aktørene tenker når det gjelder gjennomføring av elektronisk billettering, med forskjellige avveininger mellom personvernet og andre interesser (kundetilfredshet, andre lover osv.). Dette til tross for at det er avholdt felles møter mellom myndigheter og flere aktører, samt egne konferanser/seminar. Er det et poeng i at myndighetene regulerer for å få like tilbud rundt om i landet, eller er alt greitt så lenge det er avtalt med kunden?
- Fra Datatilsynets side vektlegges viktigheten av at trafikanten får informasjon om databehandlingen. Den enkelte aktør kan imidlertid bare gjøre rede for den behandlingen som foregår hos dem, mens teknologien kan medføre behandling også hos andre (f.eks. AutoPASS, elektronisk billettering). Det er vanskelig for aktørene å informere om det *totale omfanget*, og det er vanskelig for enkeltpersonene å overskue det totale omfanget.
- De fleste privatpersoner er ikke redd for å gi fra seg opplysninger fordi de mener at de ikke har noe å skjule. Noen mener at dette kan svekke personvernet på sikt. Er det bransjens oppgave å utnytte tiltroen til systemet eller å ”redde folk fra seg sjøl”?

Hva kan myndighetene gjøre for å øke kompetansen og oppmerksomheten i bransjen, for å sikre et minimumsnivå eller for å bedre dette nivået? Skar (2007) peker på at både opplæring, tilsyn og regelverk gir bedre informasjonssikkerhet. Han peker videre på at det er enkelt for ”alle” å innføre tekniske sikkerhetstiltak, men når det gjelder sikkerhetskultur er dette noe som må skapes gjennom bevisstgjøring hos de enkelte. Punktene nedenfor er eksempler på ulike virkemidler som kan bidra til å øke oppmerksomheten og kompetansen om å sikre personopplysninger innenfor transportsektoren:

- Styrke Datatilsynet med egne fagfolk på transport, evt. regionale ombud
- Styrke personvern som tema under teknologirådet
- Etablere et informasjonsprogram der bransjeorganisasjonene involveres
- Lage en bransjeveileder (og avklare hvem som har ansvaret for oppdatering av denne)
- Myndighetene definerer sin egen policy på området, med mål om å være et forbilde for bransjen

Referanser

Adresseavisa (2008): *Spredte 30.000 personnummer*. Notis. Trondheim.

Bang, Børge og Wahl, Ragnhild (2007): *ITS – IKT i transportsektoren. Klargjøring og avgrensing.* SINTEF rapport STF50 A07010. Trondheim: SINTEF Teknologi og samfunn. http://www.sintef.no/upload/Teknologi_og_samfunn/Veg%20og%20samferdsel/Rapporter/A07010_ITS%20-%20IKT%20i%20transportsektoren.pdf (2008-01-28)

Blakstad, Helene Cecilie; Nordland, Odd og Fjerdingen, Lillian (2007): *Security og beredskap for skinnegående transport.* Trondheim: SINTEF Teknologi og samfunn.

Datatilsynet (2002): *Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven*. Oslo: Datatilsynet.

Datatilsynet (2004): *Når har du lov til å overvåke med kamera?* Oslo: Datatilsynet.

Datatilsynet (2005): *Oversendelse av klage – fjernsynsovervåking NSB persontog AS.* Brev til Personvernnemda datert 05.09.2005. Oslo.

Datatilsynet (2006): *Kameraovervåking i buss og tog* (09.08.2006) Gunnel Helmers. www.datatilsynet.no (2008-11-11)

Datatilsynet (2007a): *Bompasseringer til ligningskontoret* (31.10.2007) Trude Talberg-Furulund. www.datatilsynet.no (2008-11-11)

Datatilsynet (2007b): *Elektronisk billettering* (04.07.2007) Sverre Engelschiøn. www.datatilsynet.no (2008-11-11)

Datatilsynet (2007c): *Tidsbegrenset konsesjon til å behandle personopplysninger – Automatiske bomstasjoner i Oslo og Bærum.* Brev fra Datatilsynet til Statens vegvesen datert 2007-12-11. http://www.datatilsynet.no/upload/Dokumenter/konsesjoner/Konsesjon%20bompenger%20Oslo.pdf (2008-11-11)

Europaparlamentet (1995): *Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.* http://www.personvern.uio.no/pvpn/regler/eudirektiv.html (2008-01-24)

Fornyings- og administrasjonsdepartementet (2000): *FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (personopplysningsforskriften).* http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html (2008-01-24)

Forbrukerrådet (2008): *Sluttbrukerens behov til elektronisk billettering.* Innlegg på seminaret Elektronisk billettering i kollektivtrafikken (ITS Norge) ved Martin Halsos.

Forskning.no (2005): *Ser overvåkerne fra innsiden* 19.12.05 Anders J. Graven http://www.forskning.no/Artikler/2005/desember/1134632844.59

Forskning.no (2007): *Videoovervåking i praksis* (En presentasjon av doktorgradsstudien til Heidi Mork Lomell) 04.05.2007 Else Koppang Frøjd http://www.forskning.no/artikler/2007/mai/1178106431.7 (2008-11-13)

Forskning.no (2008): *Det privatiserte overvåkingssamfunnet* 28.01.2008 Bjarne Røsjø. www.forskning.no (2008-01-30)

Helse- og omsorgsdepartementet (1999): *LOV 1999-07-02 nr 63: Lov om pasientrettigheter* (pasientrettighetsloven). http://www.lovdata.no/all/hl-19990702-063.html#2-6

http://www.avinor.no/avinor/sikkerhet/40_Regelverk (2008-03-28)

http://www.luftfartstilsynet.no/security (2008-03-28)

http://www.sas.no/no/Alt-om-reisen/Biometri (2008-03-28)

Justis- og politidepartementet (2000): *Lov 2000-04-14 nr 31: Lov om behandling av personopplysninger*. JD 2000 hefte 8. http://www.lovdata.no/all/nl-20000414-031.html (2008-01-24)

Justis- og politidepartementet (1981)*: LOV-1981-05-22-25Lov om rettergangsmåten i straffesaker (Straffeprosessloven)*. http://www.lovdata.no/all/nl-19810522-025.html (2008-12-09)

Lahnsten, Erik (2007): *Fra enkeltlinjer til sammenhengende kollektivtrafikk.* Innlegg på Nor-way bussekspress – generalforsamling i Oslo 28.11.2007. Samferdselsdepartementet.

Meland, Solveig; Samstad, Hanne; Wahl, Ragnhild og Killi, Marit (2007): *Utfordringer innenfor personvern, ansvar og roller ved ITS-anvendelser i transportsektoren.* Trondheim: SINTEF / TØI.

Personvernnemnda (2007): *Kolumbuskortet*. Personvernnemndas avgjørelse av 20. desember 2007. Oslo

Privacy International (2007): *The Privacy and Human Rights Report for 2007.The 2007 International Privacy Ranking*. www.privacyinternational.org (2008-01-10)

Ravlum, Inger.Anne (2004): *Makt, beslutninger og integritet. IKT og personvern i transport.* TØI rapport 703/2004. Oslo: Transportøkonomisk institutt. http://www.toi.no/getfile.php/Publikasjoner/T%D8I%20rapporter/2004/703-2004/703-2004.pdf (2008-1-15)

Samferdsel (2008): *Bilen er en databank – som kan sladre* (Are Wormnes). Samferdsel nr. 4 2008. Oslo: Transportøkonomisk institutt. http://samferdsel.toi.no/article19853-1036.html (2008-06-11)

Skar, Tom-Andre (2007): *Opplæring, tilsyn, regelverk – gir det bedre informasjonssikkerhet?* Masteroppgave. Gjøvik: Avdeling for informatikk og medieteknikk, Høgskolen i Gjøvik.

Statens vegvesen (2004/05): *Håndbok 206: Elektronisk billettering. Del 1*. Oslo: Vegdirektoratet.

Teknologirådet (2007a): *Notat om personvern i samferdselssektoren*. Notat til Transport- og kommunikasjonskomiteen (udatert). http://www.teknologiradet.no/FullStory.aspx?m=28&amid=3258 (2008-11-13)

Teknologirådet (2007b): *Slik blir du overvåket*. www.teknologiradet.no (2008-01-21)

Teknologirådet (2007c): *Sikkerhet og personvern. Oversikt over sikkerhetsteknologier*. Oslo: Teknologirådet.

Tveit, Ørjan; Lie, Arne; Bang, Børge og Flø, Marianne (2008): *AKTA Demonstrator 2 Automatisk deteksjon av passasjerer ved holdeplass.* SINTEF rapport A7110. Trondheim: SINTEF Teknologi og samfunn. http://www.sintef.no/upload/Teknologi_og_samfunn/Veg%20og%20samferdsel/Rapporter/2008/A7110%20Rapport%20AKTA%20Demonstrator%202.pdf (2008-12-09)

Utenriksdepartementet (1953): *Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter* LOV-1950-11-04 Den europeiske menneskerettighetskonvensjon http://www.lovdata.no/all/nl-19501104-000.html (2008-01-24)

VG (2008): *Krever ti fingeravtrykk*. 27.03.2008 Kim Daniel Lindegaard. www.vg.no/pub/vgart.hbs?artid=504870 (2008-08-11)

Wahl, Ragnhild; Skjetne, Eirik, Bang, Børge og Tveit, Ørjan (2007): *Fremtidig ITS-anvendelse i transportsektoren.* SINTEF rapport STF50 A07005. Trondheim: SINTEF Teknologi og samfunn. http://www.sintef.no/upload/Teknologi_og_samfunn/Veg%20og%20samferdsel/Rapporter/A07005_%20Fremtidig%20ITS-anvendelse%20i%20transportsektoren.pdf (2008-01-28)

Williams, Bob (2008): *Intelligent Transport Systems Standards.* Boston: Artech House.

www.autopass.no; www.lavprisekspressen.no, www.sas.no, www.norwegian.no, www.ruter.no, www.transport.no

VEDLEGG 1:

INTERVJUGUIDE: UNDERSØKELSE OM PERSONOPPLYSNINGER I TRANSPORTSEKTOREN

SINTEF Teknologi og samfunn gjennomfører en undersøkelse for Statens vegvesen. Hensikten er å lære mer om bruken av personopplysninger i transportsektoren. Vi vil derfor intervjue aktører innenfor ulike transportformer som luftfart, vei-, bane- og sjøtransport.

Vi avtaler et tidspunkt for telefonintervju. Nedenfor ser du de viktigste spørsmålene, slik at du kan se hva intervjuet vil dreie seg om. Ønsker du å svare skriftlig på noen av spørsmålene, kan du sende inn svarene i forkant av intervjuet.

Personopplysningslova gjelder alle opplysninger og vurderinger som kan knyttes til en enkeltperson. Lovas virkeområde er behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler og annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister. Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

Behandling av personopplysninger omfatter enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter. Dette kan f.eks. være håndskrevne lister, dataregistre, video- eller fotoovervåking osv. med informasjon som kan knyttes til en person.

BEHANDLING AV PERSONOPPLYSNINGER

1. Hvilke eksempler har du på at dere i din organisasjon behandler personopplysninger?

   For hvert eksempel:

   a) Hva er formålet for behandlingen?

   b) Hvilket vilkår (lovlig begrunnelse) har dere for å behandle personopplysninger?

2. Er noen av dataene som samles inn sensitive? (rase, etnisitet, religion, politisk oppfatning, fagforeningsmedlemskap, kriminalitet, helse, seksuelle forhold)

ANSVAR OG RUTINER I ORGANISASJONEN

3. Hvem er behandlingsansvarlig i bedriften? (Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes. Personopplysningsloven § 2:4)

4. Hvem er databehandler? (Den som behandler personopplysninger på vegne av den behandlingsansvarlige. Personopplysningsloven § 2:5)

   Hvor mange personer (anslag) jobber med databehandling etc. knyttet til personopplysninger?

5. Har dere gjennomført en risikovurdering av databehandlingen som gjennomføres?

Har dere rutiner for å vurdere om fordelene står i forhold til ulempene, med hensyn til behandling av personopplysninger? Blir vurderingene gjentatt etter at behandlingen er satt i verk?

6. Hvilke rutiner har dere for å opplyse den enkelte om hvilke opplysninger som registreres om vedkommende og formålet med registreringen?
7. Hvilke sikkerhetstiltak er satt i verk for å sikre tilfredsstillende informasjonssikkerhet? (personopplysningene som lagres er relevante, korrekte og tilstrekkelige, sikkerhet mot tap og manipulasjon, uvedkommende får ikke tilgang til personopplysninger)

   Hvordan og hvor ofte kontrolleres det at tiltakene følges og er tilstrekkelige?
8. Hvilke tiltak eller rutiner har dere som sikrer at personopplysningene bare benyttes til angitte formål? Hvilke rutiner har dere for å slette personopplysninger som det ikke lenger er behov for å lagre?
9. Inngår kunnskap om personopplysningsloven som del av internopplæring? Hvor stor bevissthet vil du si at det er hos medarbeiderne i din organisasjon i forhold til ansvaret knyttet til personvernopplysninger?

INNKJØP AV PRODUKTER OG TJENESTER

10. Hvilke krav stilles til utredning av personvernhensyn når det velges IKT løsninger i din bedrift? (Begrunne løsninger som innebærer behandling av personopplysninger, begrunne hvorfor ikke den løsningen som har minst konsekvenser for personvernet er valgt, utrede om alternativer uten behandling av personopplysninger kan være tilstrekkelig for å oppnå hensikten)
11. Hvilke rutiner har dere for å vurdere konsekvensene mht personopplysninger ved kjøp av f.eks. informasjons- eller transporttjenester?
12. I hvilken grad vil du si at personvern tillegges vekt når din organisasjon deltar i utviklingen av nye tekniske løsninger eller tjenester?

DIN OPPFATNING

13. Etter din mening, hvem vil du si har ansvaret for å vurdere det totale omfanget av personopplysninger innenfor transportområdet?
14. Hvor bevisste vi du si at folk flest er om spørsmål knyttet til personopplysninger?
15. Slik du ser det, er det forskjell på om det avkreves personopplysninger av den vanlige trafikant eller for yrkessjåfører?
16. Slik du ser det, har myndighetene og organisasjoner som din et ansvar for å opplyse og bevisstgjøre folk på omfanget av og evt. konsekvenser av behandling av personopplysninger?
17. Har hensikten med tiltaket betydning for om registrering av personopplysninger bør aksepteres? (om hensikten er sikkerhet mot ulykker, sikkerhet mot terror, effektivitet, personlige fordeler for trafikanten osv)
18. Synes du det er greitt at det registreres personopplysninger, uavhengig av formål, hvis det inngår som del av en kjøpsavtale mellom leverandør av en tjeneste og enkeltpersonen? (Eksempel: Synes du det er greitt hvis nye biler har utstyr som registrerer kjøremønster osv. der registreringene knyttes til forsikringsavtalen?)

19. Med din kjennskap til registre med personopplysninger, hvilke farer kan du se for evt. misbruk? Hvilke forutsetninger må være tilstede for at et misbruk skal kunne skje?
20. Blant annet i Storbritannia har det vært skandaleoppslag om personopplysninger som har kommet på avveie. Hvor sannsynlig tror du det er at dette kan skje med personopplysninger fra transportsektoren i Norge? Hvordan tror du dette vil påvirke folks holdninger til å inngå avtaler eller å gi fra seg opplysninger?

VEDLEGG 2: INFORMANTER

Det er gjennomført intervju med et utvalg informanter. Disse representerer følgende funksjoner og aktører:

- Administrasjon av skoleskyss for fylkeskommunen
- Administrasjonsselskap for kollektivtransport, leder av informasjonsteknologiavdelingen
- Administrasjonsselskap for bompengefinansiering
- Baneselskap, leder av informasjonsteknologiavdelingen
- Drosjeselskap, teknisk leder
- Flyselskap, informasjonsteknologiavdelingen
- Kollektivselskap buss, båt, ferge, leder av informasjonsteknologiavdelingen
- Kollektivselskap buss, administrasjonssjef

Trondheim
Address: NO-7465 Trondheim, Norway
Phone: +47 73 59 30 00
Fax: +47 73 59 33 50

Oslo
Address: P.O. Box 124, Blindern, NO-0314 Oslo, Norway
Phone: +47 22 06 73 00
Fax: +47 22 06 73 50