Transportøkonomisk institutt

Personvern og forbrukerrettigheter i transport – Nordisk seminar

Inger-Anne Ravlum

TØI rapport 745/2004

TØI rapport
745/2004

Personvern og forbrukerrettigheter i transport

Nordisk seminar

Inger-Anne Ravlum

ISSN 0802-0175
ISBN 82-480-0457-0 Elektronisk utgave
Oslo, desember 2004

Tittel: Personvern og forbrukerrettigheter i transport - Nordisk seminar

Forfatter(e): *Inger-Anne Ravlum*

TØI rapport 745/2004
Oslo, 2004-12
38 sider

ISBN 82-480-0457-0 elektronisk versjon
ISSN 0802-0175

Finansieringskilde:
Nordisk Ministerråd

Prosjekt: 2833 IKT og personvern

Prosjektleder: Inger-Anne Ravlum

Kvalitetsansvarlig: Marika Kolbenstvedt

Emneord:
Informasjons- og kommunikasjonsteknologi; IKT; Intelligente transportsystemer; ITS; Personvern; Retningslinje; Nordisk Ministerråd

Sammendrag:
Nordisk ministerråd avholdt i november 2004 et seminar om personvern og forbrukerrettigheter i transport. Seminaret som samlet representanter for samferdselsmyndigheter, datatilsyn og forbrukermyndigheter fra alle de nordiske landene, konkluderte med at det er behov for en veiledning for hvordan sektormyndighetene kan sikre personvern når informasjons- og kommunikasjonsteknologi utvikles og tas i bruk i transportsektoren. Det er også behov for kunnskapsoverføring mellom transportformene, særlig fra sjø- og lufttransporten til de øvrige transportmyndighetene. For de transportgrenene som er pålagt å behandle personopplysninger, er utfordringen å begrense de opplysningene som behandles og sikre regler for sletting, retting og videre bruk. Det bør stilles krav til konsekvensutredninger - eks i form av Privacy Impact Assessments - når systemer som innebærer behandling av personopplysninger innføres. Den behandlingsansvarlige bør utføre konsekvensutredningen.

Rapporten finnes kun i elektronisk utgave

Title: Data Protection and Consumer Rights in Transport - Nordic Seminar

Author(s): *Inger-Anne Ravlum*

TØI report 745/2004
Oslo: 2004-12
38 pages

ISBN 82-480-0457-0 Electronic version
ISSN 0802-0175

Financed by:
Nordic Council of Ministers

Project: 2833 Transport Informatics and Data Protection

Project manager: Inger-Anne Ravlum

Quality manager: Marika Kolbenstvedt

Key words:
Intelligent Transport Systems; Information and Communication Tecnology; Protection of Privacy; Code of Conduct; Guidelines; Nordic Councils of Ministers

Summary:
The Nordic Council of Ministers held a conference in Oslo in November 2004 on protection of privacy and consumer rights in the transport sector. The conference, which was attended by representatives from transport authorities, the Data Inspectorates and Consumer Councils from all the five Nordic countries, concluded: There is a need for guidelines on how the transport authorities can ensure the implementation of the principles of privacy and consumer rights when intelligent transport systems and information and communication systems are applied in the transport sector; There is a need for systematic learning between the different modes of transport; Privacy Impact Assessments should be carried out when systems involving personal data are developed or implemented.

Language of report: Norwegian

Rapporten kan bestilles fra:
Transportøkonomisk institutt, biblioteket,
Postboks 6110 Etterstad, 0602 Oslo
Telefon 22 57 38 00 - Telefax 22 57 02 90

The report can be ordered from:
Institute of Transport Economics, the library,
PO Box 6110 Etterstad, N-0602 Oslo, Norway
Telephone +47 22 57 38 00 Telefax +47 22 57 02 90

Forord

Denne rapporten er en rapportering fra et seminar om personvern og forbrukerrettigheter i transport som ble arrangert i Oslo 15. november 2004 i regi av Nordisk ministerråd. Seminaret kom i stand etter initiativ fra Temagruppen for intelligente transportsystemer under den Nordiske embetsmannskomiteen for transport (NET). De nordiske samferdselsministerne sluttet seg til initiativet. Nordisk ministerråd ga deretter Transportøkonomisk institutt i oppdrag å utarbeide bakgrunnsmaterialet og å arrangere seminaret i samarbeid med Temagruppen for intelligente transportsystemer.

Seminaret samlet representanter fra alle de fem nordiske landene: Fra myndigheter med ansvar for alle transportgrenene, fra datatilsynsmyndigheter og forbrukermyndigheter. Seminaret skulle komme fram til forslag om nordiske retningslinjer for hvordan personvern og forbrukerrettigheter skal sikrest i utvikling, innføring og bruk av ITS i transport.

I denne rapporten gjengir vi innledningene i plenum, momenter fra diskusjonene i arbeidsgruppene og de viktigste konklusjonene fra seminaret, samt en oversikt over relevant litteratur og lenker. Rapporten inneholder også det bakgrunnsmaterialet som ble sendt deltakerne før seminaret. Førsteamanuensis Lee Bygrave ved Juridisk fakultet ved Universitetet i Oslo laget et eget notat til seminaret. Dette notatet og deltakerlista gjengis i vedlegg.

Inger-Anne Ravlum ved Transportøkonomisk institutt har vært prosjektleder og har skrevet denne rapporten. Det er mange som har bidratt til seminaret og den dokumentasjonen som er lagt fram her. Flere av seminardeltakerne har bidratt med interessante lenker og andre referanser. Camilla Andelius fra det svenske Vägverket laget et innspill om ITS og personlig integritet på vegtrafikkområdet i Sverige. Beate S. Dagslet fra det norske Datatilsynet bidro med et eget notat til seminaret der hun trakk opp enkelte personvernprinsipper som burde ivaretas i transportsektoren. Dagslet har også bistått i oppsummeringen av arbeidsgruppenes arbeid og diskusjonen i plenum. Lee Bygrave har bidratt med mange av referansene som er oppgitt i denne rapporten.

Gruppelederne Ulf Kjellerup fra Cowi i Danmark, Annegret Andersen fra Vegdirektoratet i Norge og Jan Kåre Haaheim fra Avinor i Norge har fått referatene fra gruppearbeidene og plenumsdiskusjonen til gjennomsyn. Trygve Roll-Hansen fra det norske Samferdselsdepartementet har også gitt sine bidrag til rapporteringen.

Oslo, desember 2004
Transportøkonomisk institutt

Sønneve Ølnes	*Marika Kolbenstvedt*
konstituert instituttsjef	avdelingsleder

Innhold

TØI-rapport 745/2004
Forfatter(e): Inger-Anne Ravlum
Oslo 2004, 38 sider

Sammendrag:

Personvern og forbrukerrettigheter i transport – Nordisk seminar

I samarbeid med Transportøkonomisk institutt arrangerte Nordisk ministerråd et seminar om personvern og forbrukerrettigheter i transport i Oslo 15. november 2004. Seminaret kom i stand etter initiativ fra Temagruppen for intelligente transportsystemer under den nordiske embetsmannskomiteen for transport (NET). Seminaret er et ledd i temagruppas engasjement for bruk av informasjonsteknologi i transportsektoren og innføring av såkalte intelligente transportsystemer. Temagruppen har i denne forbindelsen også drøftet implikasjoner for personvernet. Temagruppen tok derfor initiativ til et utredningsprosjekt om transporttelematikk og individ. Temagruppen arrangert også en konferanse i Oslo 24. - 25. september 2003 om intelligente transportsystemer, der ett av temaene var hensynet til personvern og forbrukerrettigheter. En av konklusjonene fra utredningen, som ble gjennomført av Cowi A/S, og fra seminaret i 2003 var at man på nordisk nivå burde arbeide videre med utvikling av handlingsregler eller retningslinjer for hvordan personvern og forbrukerrettigheter bedre kunne ivaretas når intelligente transportsystemer og andre informasjons- og kommunikasjonssystemer tas i bruk i transportsektoren. Dette ble temaet for det nordiske seminaret som ble arrangert i Oslo 15. november 2004.

Seminarets hovedkonklusjoner er:

- Personvernlovgivningen er generell og håndhevingen av den må i stor grad baseres på skjønn. Det er vanskelig for sektormyndigheter og andre aktører i transportsektoren å anvende prinsippene i personvernlovgivningen. Det er derfor behov for en veiledning for hvordan sektormyndighetene bedre kan bidra til at personvern og forbrukerrettigheter blir ivaretatt når informasjons- og kommunikasjonsteknologi og intelligente transportsystemer blir utviklet og satt i verk. Mer systematisk kunnskapsoverføring mellom transportformene og mellom de nordiske landene ble etterlyst. Luftfart og sjøtransport har tidlige erfaringer med behandling av personopplysninger og har måttet veie behovet for sikkerhet (”security”) opp mot personvern. De andre har noe å lære fra disse transportformene.
- Det er ulike synspunkter på om det er nødvendig å utvikle egne handlingsregler eller retningslinjer for personvern i transportsektoren. Noen mener lovgivningen slik den er i dag er tilstrekkelig, mens andre mener transportsektoren kan ha nytte av klarere retningslinjer for hvordan personvern systematisk skal veies inn som et sentralt hensyn når ny teknologi utvikles og tas i bruk.

Rapporten kan bestilles fra:
Transportøkonomisk institutt, Postboks 6110 Etterstad, 0602 Oslo
Telefon: 22 57 38 00 Telefax: 22 57 02 90

- Utfordringene i transportsektoren er forskjellig. For eksempel er transportørene innen luftfart og persontransport til sjøs pålagt å behandle personopplysninger. Her vil utfordringen i større grad være hvilke opplysninger som skal behandles, hvordan de skal behandles og regler for sletting, retting og videre bruk av opplysningene. Disse transportformene er også i større grad internasjonalisert og må forholde seg til et internasjonalt regelverk.
- Etterlysningen av retningslinjer for personvern i transport er først og fremst grunnet i behovet for at personvernimplikasjoner mer systematisk veies inn i beslutningsprosessen. Dette kan sikres ved at man stiller krav om konsekvensutredninger når informasjonsteknologi eller intelligente transportsystemer utvikles og tas i bruk. De nordiske land og EU har lang erfaring med Impact Assessments på miljøområdet. I Canada er det pålagt å gjøre tilsvarende vurderinger for personvern, såkalt Privacy Impact Assessment (PIA). Kravet om konsekvensutredninger kan stilles til både offentlige og private aktører.
- Etter loven er det i alle de nordiske landene den behandlingsansvarlige som er pålagt å ivareta personvernhensynene. Dette taler for at det er dem som utvikler og tar systemene i bruk som også må foreta eventuelle konsekvensutredninger. Det er likevel behov for en klarere sentral "policy" eller et politisk påtrykk for at dette skal skje.

Rapportens kapittel 1 gjengir plenumsinnledningene. Kapittel 2 oppsummerer resultatene fra gruppearbeidet og gjengir momenter fra diskusjonene i arbeidsgruppene og fra plenumsdiskusjonen. I kapittel 3 gir vi en oversikt over noen relevante publikasjoner, artikler og lenker. I kapittel 4 gjengis det bakgrunnsmaterialet som ble sendt seminardeltakerne før seminaret. Kapitlet inneholder en drøfting av personvernbegrepet, eksempler på systemer innen transportsektoren som innebærer behandling av personopplysninger og anbefalingene fra tidligere utredninger (Nordisk ministerråd 2002 og Ravlum 2004) og anbefalingene fra Temagruppens seminar i Oslo i 2003.

1 Presentasjoner i plenum

1.1 Juridiske rammer for personvern og konsument-rettigheter i transport[1]

Lee Bygrave, 1. amanuensis ved Juridisk fakultet, Universitetet i Oslo

Det norske begrepet personvern er noe diffust og brukes sjelden utenfor Norge. I Sverige snakker man om beskyttelse av personlig integritet og internasjonalt gjerne om ”dataprotection” eller ”privacy”. Personvern slik det brukes i Norge, er beskyttelse av integritet i forbindelse med behandling av personopplysninger.

Det finnes omfangsrike og detaljerte internasjonale bestemmelser om beskyttelse av personvernet. Dette er rettslig bindende juridiske regler. Det innebærer at de nordiske landene ikke kan velge nasjonale regler på området som avviker fra de internasjonale bestemmelsene.

Den europeiske menneskerettighetskonvensjonens (EMKs) artikkel 8, som blant annet slår fast at alle har rett til respekt for privatliv, familieliv, hjem og korrespondanse, er blitt et viktig personverninstrument i seg selv. *FNs konvensjon om sivile og politiske rettigheter* artikkel 17 har tilsvarende formuleringer. Den europeiske menneskerettsdomstolen (EMD) har slått fast at for å tilfredsstille EMKs artikkel 8, må stater iverksette et vern om personopplysninger. Formuleringene i artikkel 8 er rettet mot offentlig myndighet, men gjennom domsavsigelser er artikkelen også blitt gjort gjeldende for forholdet mellom private aktører.

I EU og EØS-området er det særlig *EU-direktivet 95/46/EF, traktaten om innføring av en europeisk grunnlov og EUs charter om grunnleggende rettigheter* som er de sentrale rettskildene. Direktiv 95/46/EF omhandler beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av sådanne opplysninger. Alle de nordiske landene har implementert direktivet i egen lovgivning. EF-domstolen har i en dom av 6. november 2003 (Lindqvist vs Åklagarkammeren i Jönköping) slått fast at direktivet også gjelder for personlige hjemmesider når disse er tilgjengelige for offentligheten. Traktaten har bestemmelser som hever beskyttelse av personopplysninger som en grunnleggende menneskerett i seg selv, uavhengig av EMKs artikkel 8. Charterets formuleringer er ikke rettslig bindende, men vil få betydning i den grad EF-domsstolen i Luxembourg velger å legge vekt på den.

Alle de nordiske land har utarbeidet lover i tråd med EU-direktiv 95/46/EF. Det er derfor en stor grad av harmoni om de grunnleggende prinsippene, men likevel betydelige forskjeller mellom de nordiske landene. I Norge er det fremdeles konsesjonsplikt for behandling av sensitive personopplysninger. I Sverige er det ingen konsesjonsordning i det hele tatt, kun krav om melding til

[1] Se vedlegg for konkrete henvisninger til bestemmelser etc.

Datainspektionen. Generelt er det gitt få retningslinjer fra domstolene for hvordan lovgivningen skal forstås. Det har i stor grad vært datatilsynsmyndighetene i de nordiske landene som har tolket loven, med liten etterkontroll fra domstolene.

I henhold til direktiv 95/46/EF har ikke EU- eller EØS-land anledning til å gi personopplysninger til tredjeland som ikke har tilstrekkelig beskyttelse av personvern i henhold til direktivet. Men det finnes unntak fra denne regelen, og Europakommisjonen kan inngå avtaler med tredjeland som tillater overføring av opplysninger under visse forutsetninger. En nylig inngått avtale mellom Bush-administrasjonen og EU-kommisjonen gjør det f eks mulig for amerikanske selskaper å motta opplysninger om europeiske flypassasjerer. Den såkalte artikkel 29-gruppen, som er en rådgivende arbeidsgruppe for personvern i EU, har samtidig kritisert denne avgjørelsen.

Direktiv 95/46/EF var opprinnelig begrunnet i de fire friheter (fri bevegelse av varer, tjenester, personer og kapital) og skulle sikre utveksling av informasjon mellom medlemslandene. I 2003 ble det slått fast at direktivet må tolkes i lys av den europeiske menneskerettskonvensjonen. Dermed har direktivet også fått en menneskerettsside.

For å tilfredsstille de ulike direktivene og konvensjonene, må de nasjonale myndighetene gjennomføre en lovgivning som bygger på noen grunnleggende personvernprinsipper:

- *Rettferdighet og rettmessighet*: Opplysningene skal behandles rettferdig og rettmessig:
    - Den behandlingsansvarlige skal ta i betraktning og ha respekt for de registrertes interesser og rimelige forventninger;
    - Inngrep som behandlingen medfører, skal ikke være uforholdsmessige;
    - Den registrerte skal ikke utilbørlig tvinges til å avgi opplysninger om seg selv eller til å godta at allerede innsamlede opplysninger brukes til visse formål;
    - Behandlingen skal dessuten være gjennomsiktig og forståelig for den registrerte.
- *Minimalitet*: Mengden av innsamlede personopplysninger skal begrenses til det som er nødvendig for å realisere formålet:
    - Så snart allerede innsamlede personopplysninger ikke lenger er nødvendige å beholde ut fra innsamlings-/bruksformålet, skal de slettes eller anonymiseres;
    - Det skal legges til rette for at enkeltindivider kan forbli anonyme ved transaksjoner med ulike organisasjoner.
- *Formålsbestemthet*: Personopplysninger skal behandles til uttrykkelig angitte, legitime formål og kun brukes i samsvar med disse formålene:
    - Formålet skal angis på en rimelig presis måte;
    - Formålet skal som et minimum være i samsvar med den behandlingsansvarliges ordinære, lovlige virksomhet;

  - Formålet bør muligens også være i samsvar med mer generelle etiske (og ikke bare rettslige) samfunnsnormer.

- *Opplysningskvalitet*: Personopplysninger skal være korrekte i forhold til det de er ment å representere, og skal være relevante, adekvate og fullstendige i forhold til deres bruksformål:
  - Behandlingsansvarlige skal etablere tiltak for å sjekke opplysningskvaliteten.
- *Medbestemmelse*: Den registrerte skal kunne delta i og ha en viss mulighet til å påvirke andres behandling av opplysninger om seg selv:
  - Behandlingsansvarlige skal sørge for at behandlingsoperasjonene sine er kjente, transparente og forståelige for de registrerte;
  - Behandlingsansvarlige skal så langt som mulig samle opplysninger direkte fra vedkommende person;
  - Personer skal i utgangspunkt selv kunne bestemme hvorvidt opplysninger om dem skal kunne samles inn av andre, og hva opplysningene skal kunne brukes til etter innsamling;
  - Personer skal kunne motsette seg visse typer behandlingsoperasjoner, og de skal kunne kreve at registrerte opplysninger om dem rettes eller slettes når disse er uriktige, ufullstendige eller ulovlige å registrere.
- *Informasjonssikkerhet*: Behandlingsansvarlige skal etablere tiltak for å sikre personopplysninger mot uautorisert eller utilsiktet tilgang, videregivelse, endring og/eller sletting
- *Sensitivitet*: Behandling av visse personopplysninger (i hovedsak om personers helse, seksualitet, rase eller etnisk bakgrunn, politiske, religiøse eller filosofiske oppfatninger, eller fagforeningsmedlemskap) skal – p.g.a. deres antatte sensitivitet – underkastes strengere regulering enn hva som gjelder for andre personopplysninger.
- *Andre og forholdsvis nye prinsipper*:
  - *Anonymitet*: teknologiske og organisatoriske forhold skal legges til rette for at en person kan forbli anonym ved inngåelse av transaksjoner med ulike organisasjoner. Hvis anonymitet ikke er mulig, skal transaksjonene kunne fullføres ved bruk av pseudonymer som gjør det vanskelig å identifisere personen, jf. f.eks. den tyske *Bundesdatenschutzgesetz* (1990) § 3a, jf. også artikkel 29 arbeidsgruppens rekommendasjon 3/97 (vedtatt 3. desember 1997).
  - *Helautomatiske beslutninger*: Helautomatiserte vurderinger av en persons personlige egenskaper skal ikke kunne utgjøre det eneste grunnlaget for beslutninger som griper inn i personens liv, jf. direktiv 95/46/EF artikkel 15.

1.2 Transporttelematikk, personvern og forbrukerrettigheter

Forsker ved Transportøkonomisk institutt, Inger-Anne Ravlum

Utgangspunktet er at alle har en sirkel av privatliv hvor ingen, uten tillatelse eller en legitim grunn, har rett til å trenge innenfor. Vi skal selv ha kontroll over *hvilke* opplysninger som finnes om oss og vi skal ha kontroll over *hvem* som skal ha tilgang til disse opplysningene. Det er ikke vanskelig å forestille seg den krypende fornemmelsen av usikkerhet og angst i samfunnssystem som ikke respekterer disse rettighetene.

Informasjon om andre forrykker maktforholdet mellom enkeltindivider og myndighetene, mellom arbeidstakere og arbeidsgivere eller mellom forbrukerne og markedsaktørene. Kontroll av PC-bruk, tidsregistrering av oppmøte på jobben, bruk av telefon eller e-post, gir en mengde informasjon om oss som får betydning for forholdet mellom arbeidstakere og arbeidsgivere. Opplysninger om reisevaner, innkjøp, billettbestillinger og kredittkortbruk gjør det mulig å skreddersy markedsframstøt direkte rettet mot oss. Maktbalansen mellom individene og myndighetene, arbeidsgiverne eller markedsaktørene forrykkes.

I flere kvalitative undersøkelser sier folk at for dem spiller det ingen rolle at andre samler inn opplysninger om dem, for de har jo ikke gjort noe galt. Men selv om vi ikke ”gjør noe galt”, er det da *ikke* greit om myndighetene eller andre har oversikt over det vi gjør. Og det er ikke bare *typen* opplysninger som er viktig – det er også *mengden*.

Likevel er samfunnet avhengig av personopplysninger for å treffe riktige beslutninger, enten det gjelder om du skal komme inn på videregående skole, ha rett til uføretrygd, få lån i banken eller få utbetalt erstatning fra forsikringsselskapet. Derfor må også opplysningene være korrekte og tilstrekkelige. Det må settes krav til hvordan opplysningene samles inn, hvordan de behandles videre og hvordan de oppbevares, justeres og slettes.

Disse kravene gjelder også for opplysninger som kan *tenkes* å bli brukt i framtida. Opplysninger om for eksempel røyke- og alkoholvaner kan på et senere tidspunkt bli brukt for å avgjøre hvem som har rett til gratis helsehjelp og hvem som skal betale en ekstra egenadel for ”sjølforskyldt” skade. Dermed er selve forekomsten av opplysninger viktig, selv om vi i dagens politiske kontekst ikke opplever opplysningene som integritetskrenkende. I disse ”security-tider”, er det kanskje grunn til å minne om at opplysninger vi innenfor vårt politiske system er trygge på at ikke blir misbrukt, kan tilfalle andre med andre hensikter.

For å ivareta personvernet, er det visse individuelle og samfunnsmessige eller kollektive, interesser som må ivaretas.

- *Diskresjon*: Vi skal som individer ha kontroll over opplysningene om oss selv, hvem som har tilgang til dem og hva de brukes til. Opplysninger om oss skal bare kunne brukes til det *formålet* de er samlet inn for, og det skal ikke samles *flere* opplysninger enn det som er relevant for formålet. Det skal legges begrensinger på hvem som har *tilgang* til opplysningene.
- *Fullstendighet*: Opplysningene om oss skal være riktige og fullstendige.

- *Innsyn:* Vi har rett til å vite hvilke opplysninger som finnes om oss. Dette er også en viktig forutsetning for at opplysningene skal være korrekte.
- *Privatlivets fred*: Hver og en av oss har en rett til å være i fred, uavhengig av om forstyrrelsen innebærer at det blir registrert opplysninger om oss eller ikke.
- *Et borgervennlig samfunn*: Som fellesskap har vi interesse av at samfunnet ikke er fullt ut automatisert. Det skaper avstand til saksbehandlingen og gjør det vanskeligere for individene å øve innflytelse.
- *Et robust samfunn*: Et samfunn som er avhengig av elektronisk informasjonsbehandling, er et sårbart samfunn.
- *Et begrenset overvåkingsnivå*: Samfunnet skal sikre et vern mot maktmisbruk og urimelig kontroll. Store databaser gir mulighet for kontroll og maktbruk, særlig hvis det er mulig å koble dem. Dette kan også frata oss som individer den reelle muligheten til å holde tilbake informasjon om oss selv.

Dermed er ivaretaking av personvernet noe mer enn et spørsmål om konsesjon eller ikke fra Datatilsynet. Det dreier seg i bunn og grunn om hvilket samfunn vi ønsker og hvilken makt og stilling vi ønsker at individene skal ha i framtidssamfunnet.

Transportsektoren

Men angår dette transportsektoren og transportpolitikken? Ja, fordi å kunne bevege seg rundt i samfunnet uten at andre kan følge bevegelsene våre, bør anses som en fundamental rettighet. Og fordi det allerede foregår en utstrakt behandling av personopplysninger i transportsektoren.

Bruk av IKT kan bidra til en mer effektiv, mer miljøvennlig og mer trafikksikker transport. Det er gode grunner for å ta i bruk ny teknologi for å fremme disse målene. Dermed vil vi i stor grad måtte veie disse hensynene opp mot personvernet – som også er et samfunnsgode det er gode grunner for å fremme og verne om. Det neste spørsmålet bør så være om man kan fremme disse gode samfunnsmålene og samtidig ivareta personvernet. Jeg mener det er fullt mulig å utnytte de fordelene ITS gir, uten å måtte gå for mye på akkord med de samfunnsverdiene som er innbakt i personvernet. Men dette gir seg ikke selv. Og det er gode grunner for det.

Man kan tenke seg det handlingsrommet man har for innføring av ITS som en trekant. Det ene hjørnet er de transportpolitiske målene: Effektivitet, miljø og sikkerhet – og etter hvert i økende grad også ”security”. Det andre hjørnet er befolkningens og dermed den politiske aksepten av bruken av ITS og av at personopplysninger skal behandles. Det tredje hjørnet er de juridiske rammene – i første rekke lov om behandling av personopplysninger som Datatilsynet forvalter.

De transportpolitiske målene trekker i retning av at man skal ta i bruk IKT – enten det gjelder alkolås, automatisk fartskontroll, sanntidsinformasjon på holdeplassene, betaling av bompenger ved hjelp av elektronisk registrering i vegkanten, GPS-dirigering av trafikken, elektronisk registrering av gods, svarte bokser, elektronisk billettering, irisidentifikasjon i luftfart (og ferje og tog?) – mulighetene er legio – og alle innebærer behandling av personopplysninger.

Setter så befolkningens aksept og de juridiske rammene begrensninger på bruk behandling av personopplysninger i transportsektoren?

I norsk lov, og jeg vil anta også i de øvrige nordiske landene, er de juridiske vilkårene for behandling av personopplysninger blant annet:

- Samtykke fra den registrerte,
- At det er nødvendig for å oppfylle en avtale,
- Nødvendig for å utføre en oppgave av allmenn interesse,
- Utøve offentlig myndighet,
- At behandlingen er hjemlet i annen lov, for eksempel vegtrafikkloven.

For de fleste formål i transportsektoren, vil ett eller flere av vilkårene være oppfylt:

- AutoPASS, smartkort i kollektivtrafikken etc er knytta til avtale.
- Flåtestyring, førerstøtte, transportmiddelkontroll (både for gods og kollektivtransport), terminalstyring og ettersporing av gods vil være et skjønnspørsmål der man må avveie ansattes rett til privatliv og arbeidsgivers styringsrett.
- Fartssperre og alkolås kan også knyttes til avtale, for eksempel når det gjelder yrkessjåfører, eller til en domsavsigelse, for eksempel som en betingelse i en promilledom.
- Svart boks /ferdsskriver er nå et standardtilbud i mange nye kjøretøy. Man kan tenke seg at dette etter hvert kan gi forsikringsmessige fordeler.
- Informasjon gjennom SMS, GPS etc er en avtale eller et abonnement.
- Trafikktelling og overvåkingen av trafikken for eksempel i tunneler eller på andre strekninger *kan* gjøres uten registrering av personopplysninger. Men for planleggingsformål er det ønskelig å kunne skille mellom for eksempel lokal og regional trafikk på vegen. Det krever at kjøretøyet identifiseres ”sånn omtrent”. Det kan gjøres gjennom registrering av autoPASS-brikken, men der noen av sifrene utelukkes fra registreringen. I dette siste tilfellet vil jeg anta at Datatilsynet vil ha et ord med i laget.

Hovedbildet er altså at det ikke er noen særlige juridiske begrensinger mot å ta i bruk IKT i transportsektoren – heller ikke løsninger som innebærer at personopplysninger behandles.

Og en av de viktigste grunnene til dette er at mye av behandlingen skjer med samtykke fra den enkelte av oss. Vi inngår avtale om å passere bomringen, avtale om bruk av elektroniske billetter, abonnement på informasjon om trafikkforholdene, vi gir fra oss personlig informasjon om oss selv for å nye godt av billigere forsikring.

Det neste spørsmålet er da om befolkningen eller vi som kunder forsvarer vårt personvern?

Vi har gjort to undersøkelser av hvordan folk veier de ulike aspektene opp mot hverandre. Den ene er en veikantundersøkelse med 314 respondenter, den andre er en såkalt fokusgruppeundersøkelse. Ingen av disse undersøkelsene har et

representativt utvalg, så vi kan ikke trekke statistiske slutninger om hva den norske befolkningen mener. Resultatene fra undersøkelsene gir likevel mulighet for å gjøre noen antakelser.

Undersøkelsene viser:

- Folk er ikke opptatt av personvern generelt, de stoler på at "systemet" ivaretar deres interesser.
- Mange sier at de har ingenting å skjule – de bryr seg derfor lite om at opplysninger blir behandlet.
- Det er noe skepsis til at opplysninger kan utnyttes av markedsaktører, men heller ikke de som sier dette, tar konsekvensen av det ved å begrense for eksempel bruk av kort.
- Det viktigste for valg av informasjonskilder i trafikken er at de er enkle å bruke. Personvern spiller ikke noen avgjørende rolle.
- Det er likevel kun 17 pst av respondentene i vegkantundersøkelsen som stoler på at informasjonen ikke kommer uvedkommende i hende. Selv blant de som *ikke* stoler på at opplysningene ikke kommer uvedkommende i hende, sier 75 pst at det ikke påvirker deres valg av informasjonskilde.

Det kan se ut som det er en motsigelse mellom første og siste punkt. Dette kan henge sammen med at de ikke anser konsekvensene av misbruk av opplysningene som særlig store.

Likevel er det ikke alt som aksepteres. Det som ser ut til å vekke motstand er bruk av automatisk fartskontroll og faren for at myndighetene kan bruke IKT som et virkemiddel for økt skattlegging – særlig vegprising. Og denne motstanden begrunnes med argumenter fra personvernet, som "Storebror ser deg".

Motstanden mot behandling av personopplysninger går altså ikke på behandlingen i seg selv, men på at myndighetene kan innskrenke vår individuelle frihet.

Når vi har *individuelle* fordeler av bruk av IKT, for eksempel gjennom at trafikkflyten blir mer effektiv og betalingen på bussen eller i bomstasjonen blir mer effektiv, er det ikke særlig motstand mot behandling av personopplysninger.

Andre undersøkelser underbygger at folk flest ikke har særlige motforestillinger mot kameraovervåking av stasjonsområder eller andre offentlige steder. Ofte er begrunnelsen å forhindre vold eller annen kriminalitet. Men samtidig vet vi at dette virkemidlet har svært liten effekt. I den grad det har effekt, er det for å bidra til oppklaring av forbrytelser *etter* at de er begått. Automatisk fartskontroll har imidlertid en dokumentert effekt på trafikksikkerheten. Men her er altså motstanden større.

De tiltakene som gir oss individuelle fordeler og som ikke involverer myndighetene og som ikke samles inn for å fatte beslutninger som angår oss, har liten motstand. I all hovedsak er dette systemer som skal øke effektiviteten: Bompasseringen skal gå litt kjappere, trafikkflyten skal bli litt bedre, vi får noe bedre kunnskap om hvor godset beveger seg.

Dette er i for seg greie og akseptable målsettinger. Problemet er at disse systemene genererer en mengde informasjon, og verken vi som individer eller lovverket setter særlig begrensinger på innhenting av personopplysningene.

Samtidig er det sterke drivkrefter for økt bruk av slike systemer. I disse tilfellene har transportmyndighetene, individene (eller kundene), systemutviklerne og transportørene felles interesse. Og jo mer utbredt systemene blir, jo vanskeligere blir det å si nei takk!

Det er altså tvilsomt om enkeltpersoner er tilstrekkelig i stand til å ivareta sitt eget personvern. Dermed blir ansvaret for systemutviklere og ikke minst sektormyndighetene enda større. Sektormyndighetene har antakelig en større innvirkning på personvernets framtidige stilling enn alle de nordiske datatilsynene til sammen. For det er i de daglige valgene av krav til ulike systemer at det tas avgjørelses som vil få store konsekvenser for mengden av personopplysninger som behandles i transportsektoren.

Målet om å få informasjonssystemer som er ganbare på tvers av transportformer og på tvers av landegrenser, gjør at mengden informasjon som er tilgjengelig vil bli enda større – og anvendelsesområdene blir tilsvarende utvidet. Dette er nok noe av bakgrunnen for at Nordisk ministerråd ønsker dette seminaret, og ønsker å få vurdert muligheten av å utarbeide felles handlingsregler eller retningslinjer for hvordan personvernet kan ivaretas på en bedre måte i transportsektoren som helhet.

Spørsmål til gruppearbeidet

Oppgaven i gruppene går ut på å vurdere om det er ønskelig og mulig å utarbeide felles retningslinjer og hva de eventuelt skal inneholde. Om det ikke blir fellesnordiske regler eller regler som spenner over alle transportformene, vil likevel arbeidet og innspillet fra dere kunne være nyttig for de nasjonale regjeringenes arbeid med personvern. Det er kanskje særlig tre spørsmål det er viktig å få belyst:

1. **Hvem bør eventuelt ha ansvaret for å utarbeide slike retningslinjer** (transportmyndighetene / etatene eller overordnet departement)?

   Det er ikke nok å erkjenne at personvernet er utfordret. Det må antakelig aktiv handling til fra sektormyndighetenes side for at personvernet systematisk skal veies inn sammen med andre hensyn man skal ivareta i transportsektoren. Men hvem skal ta ansvaret for at det faktisk skjer?

2. **Hva skal eventuelle retningslinjer ivareta?**

- Det må ikke alltid være det mest effektive virkemidlet – enten det gjelder effektivisering, trafikksikkerhet eller security som bør velges. Man kan oppnå akseptabel effektivitet med tiltak som samtidig begrenser behovet for å behandle personopplysninger skal velges.
- Man bør alltid stille seg spørsmålet om det er strengt nødvendig i det gitte tilfellet at personopplysninger skal behandles. Kanskje er det tilstrekkelig med anonymiserte opplysninger.
- I de fleste tilfellene – antakelig med unntak av en del securitytiltak – bør det finnes anonyme alternativer som vi kan velge hvis vi vil. Det kan ikke være et vilkår for å kunne bevege seg i samfunnet at vi skal gi fra oss opplysninger om oss selv.

3. Hva bør retningslinjene inneholde?

- Regler for utredning / vurdering av alternative løsninger?
  Bør beslutningsfatterne pålegges å vurdere om det finnes alternativer som gjør det mulig å ferdes uten å legge igjen spor? Og bør det være regler om at slike alternativer skal være reelle, det vil si at de skal være like tilgjengelige og like billige som det andre alternativet?
- Regler for saksbehandling, for eksempel regler for remis / ytrande / høring og for hvilke hensyn som systematisk skal veies inn?
- Regler for ivaretaking av personvernhensyn når offentlig myndighet gir tilskudd til utvikling og iverksetting av ulike systemer? Det offentlige er samarbeidspartner både gjennom forskning og utvikling, ved at tiltak er initiert og igangsatt av myndighetene eller at myndighetene inngår i et samarbeid med andre aktører om systemer som innebærer behandling av personopplysninger.
- Hvis det så er gitt at behandling av personopplysninger skal finne sted: Bør sektormyndighetene ha en sjekkliste på hvordan systemene bør utformes? Man kan for eksempel stille krav til at færrest mulig opplysninger skal registreres, at lagringen skal være kortest mulig, at opplysningene skal samles i lokale databaser, eller i elektroniske kort framfor i sentrale baser.

2 Gruppearbeid og plenums-diskusjon

2.1 Oppsummering fra gruppene

Det synes å være enighet blant seminardeltakerne om at dagens lovgivning er vanskelig tilgjengelig for aktørene i transportsektoren, og at personvernet på mange måter er utfordret i sektoren. Det er likevel ikke full enighet om at dette tilsier at det skal lages egne handlingsregler for hvordan personvernet og forbrukerrettighetene bedre kan ivaretas i transportsektoren. Noen mener den nasjonale lovgivningen bør være tilstrekkelig, mens andre mener det trengs handlingsregler eller krav om konsekvensutredninger for at personvernhensynene i tilstrekkelig grad skal bli veiet inn i beslutningsprosessene.

De som heller i retning av at det er behov for noen bransjevise atferdsnormer eller handlingsregler, synes å samle seg om en løsning som innebærer krav om konsekvensutredninger ved innføring av IKT-systemer. Ei gruppe viste eksplisitt til erfaringen fra miljøkonsekvensanalyser, Regulatory Impact Assessment (RIA) eller Privacy Impact Assessment (PIA). PIA er nå obligatorisk i Canada. Kapittel 3 inneholder ulike referanser om PIA.

Seminardeltakerne synes også å samle seg om at det i første rekke er de som tar beslutninger eller som har ansvaret for behandling av personopplysninger, som må utføre konsekvensanalysen. Likevel legger flere vekt på at det vil kreve politisk oppmerksomhet og engasjement fra nasjonale myndigheter – for eksempel ministeriene – for at arbeidet skal få tilstrekkelig tyngde.

En løsning som innebærer krav om konsekvensutredninger, gjør det også unødvendig på det nåværende tidspunktet å ta stilling til hvorvidt regelverket skal være tverrsektorielt og fellesnordisk. PIA er først og fremst en prosessmetode og stiller krav til hvilke vurdering som skal gjøres og hvilken dokumentasjon på konsekvenser for personvernet som skal ligge til grunn for en beslutning. RIA er velkjent som metode innen EU og burde derfor egne seg også for arbeid overfor EU.

Beate S. Daglset fra det norske Datatilsynet oppsummerte i plenum framleggene fra gruppearbeidet på følgende måte:

> Det ser ut til at gruppene mener at ansvaret for å utarbeide eventuelle retningslinjer i første rekke er et politisk ansvar, men at de aktuelle myndighetene og etatene må trekkes med som viktige premissleverandører. Det ser også ut til at det er enighet om at et felles nordisk grunnlag i dette arbeidet er viktig, ikke minst for å skape debatt innad i EU.
>
> Alle gruppene har lagt vekt på personvern og i mindre grad på forbrukerinteressene. Likevel vil det vel være slik at de prinsippene som gjelder for personvernet, også gjelder for forbrukervernet.

Prinsippene for både personvernet og for forbrukervernet må gjøres lettere tilgjengelige for dem som skal ivareta dem. Prinsippene er i stor grad nedfelt i lovverket. Men fordi loven er generell og forutsetter utøvelse av skjønn, er prinsippene vanskelig tilgjengelig. Fra Datatilsynets side er det derfor viktig at prinsippene blir mer tilgjengelige. Det kan også se ut til å være behov for veiledning når myndighetene skal avveie hensyn til effektivitet, økonomi, forbrukerrettigheter og personvern.

Formålet med eventuelle retningslinjer bør være at aktørene kan gjøre rede for hvorfor de enkelte løsningene er valgt. Dette kan for eksempel skje gjennom en konsekvensutredning. I tillegg kan dette legges til grunn ved vurdering av anbud, eller krav til slike vurderinger kan være en del av anbudsutlysningene.

2.2 Momenter fra de enkelte arbeidsgruppene

Hvem skal ha ansvaret for å lage eventuelle handlingsregler:

Gruppe I: For å få til et nødvendig politisk trykk bak handlingsreglene, bør ansvaret for utarbeidelsen av dem ligge på et politisk nivå. På grunn av ulik tilnærming i personvernlovgivningen mellom de nordiske land, bør arbeidet med retningslinjene skje på nasjonalt nivå. Likevel er det nødvendig med utveksling av erfaringer. Man kan på sikt lage fellesnordiske handlingsregler. Det nordiske samarbeidet bør danne felles grunnlag for en debatt i EU.

Gruppe II: Gruppa mener at samferdselsmyndighetene bør ta initiativ til og lage retningslinjer for personvern og forbrukerrettigheter i transport og ta dette opp i Nordisk Råd. Det bør settes ned brede sammensatte grupper av myndigheter og aktører som skal komme fram til ”Codes of Conduct”.

Gruppe III: De som skal håndheve reglene bør ha et eierskap til dem. Det tilsier at de som skal anvende reglene eller skal bestille systemene også er dem som bør utarbeide retningslinjene. For å påvirke design og implementeringsteknikk, bør de som skal anvende IKT-systemene inn så tidlig som mulig i fastleggingen av arkitektur og vurdere de tekniske mulighetene for overvåking og registrering. Antakelig bør ansvaret deles mellom flere aktører. Reglene må ikke nødvendigvis være sektorovergripende eller fellesnordiske. Man bør heller arbeide overfor EU.

Skipsfarten må følge internasjonale regler (IMO og ILO). Ansvar legges i stigende grad på rederiene og det er etter Sjøfarteverkets synspunkt dem – eventuelt Rederiforbundet – som må utarbeide handlingsregler (bransjevise normer). Myndighetenes oppgave er kontroll og ettersyn og å legge grunnlaget for at rederienes ansvar kan følges opp.

Forutsetninger for at handlingsregler skal kunne fungere:

Gruppe I: Codes of conduct vil bidra til å få et bedre personvern. Men det er noen forutsetninger som må oppfylles: 1: Retningslinjene og informasjonen om dem må komme fram til dem som utarbeider IKT-systemene. 2: Det må være et politisk trykk bak retningslinjene. I Norge og Sverige er det svært lite diskusjon om personvern i transport, mens det i Danmark har vært en mer bred diskusjon.

Hva skal handlingsreglene ivareta?

Gruppe II: Handlingsreglene skal ivareta personvern og forbrukerrettigheter. Man bør også se nærmere på muligheten for å ivareta forbrukerrettigheter ved innføring av nye IKT-systemer og ivareta muligheten til å være anonym. Unntaket er i de tilfellene myndighetene har bestemt at registrering skal finne sted, for eksempel ut fra sikkerhetshensyn. Man bør også samle informasjon om de nordiske lovene og retningslinjene.

Gruppe III: Reglene er ofte meget generelle og de er ikke detaljerte nok til at de gir mening i den enkelte sak. Kanskje skal man starte med å identifisere hvilke feil man allerede har gjort, lære fra dette og formulere lærdommen positivt i form av Codes of Conduct (dvs ha man *bør* gjøre, og ikke nødvendigvis hva man ikke skal gjøre). Reglenes generelle natur gjør at det blir vanskelig å lage handlingsregler, det kan kanskje være mer relevant å lage en eksempelsamling (good / bad practice).

Forbrukerhensyn bør også ivaretas. Dette gjelder for eksempel ved misbruk av monopolstilling. For å ivareta sikkerheten, kan tilskuere til landskamp i forball i Danmark bli avkrevd personnummer under henvisning til at det er frivillig å være tilskuer (samtykke). I arbeidsgiver – arbeidstakerforhold avgir man sjelden et egentlig frivillig samtykke. I Norge vurderer Datatilsynet å kreve konsesjonsplikt for helautomatiske betalingsposter på vegnettet.

Hva bør handlingsreglene inneholde?

Gruppe I: I gruppa var det diskusjon om hvorvidt det var behov for med utfyllende prinsipper i forhold til det som er dekket av lovverket. Gruppa konkluderte likevel med: 1: Prinsippene for personvernlovgivningen må gjøres lettere tilgjengelig for dem som skal anvende dem. Prinsippene må tydeliggjøres og komme tidlig inn i prosessen slik at konsekvensene kan utredes og man kan unngå trusler mot personvernet. 2: Det må være et politisk fokus på dette. 3: Når systemer skal iverksettes, må det utredes alternative tiltak. 3: Det bør gis veiledning om avveiningene som aktørene må gjøre i forhold til personvernet. 4: Det bør foreligge konsekvensanalyser for alle systemer før de innføres.

Gruppe II: Det bør være regler som sikrer mot innsamling av opplysninger ut fra ”nice to know”. Det bør gis retningslinjer for overføring av personopplysninger selskaper imellom, pålegg om å vurdere alternative systemer og hvordan man skal sikre informasjonssystemer mot misbruk og innsyn fra uvedkommende.

Gruppe III: Det er en meget stor spredning i hvordan de enkelte transportsektorene er organisert. Noen er meget desentralisert i næringsstrukturen, mens andre er sterke monopoler.

Sjøfarten er meget desentralisert og reguleres internasjonalt. Ut fra sikkerhetshensyn (9/11) gir ILO-konvensjon 185 pålegg om utstedelse av ID-kort for alle sjøfolk. (Se kapittel 3 for link til denne ILO-konvensjonen.) Man kan legge inn biometriske data. I Norge har man valgt å gjøre dette som strekkoder og ikke som en datachips. Denne løsningen gir færre muligheter til behandling av personopplysninger enn en dataships ville gjort og er dermed et eksempel på at den tekniske løsningen man har valgt, er mer i tråd med personverninteressene enn et annet alternativ. Generelt utvikles det flere systemer for overvåking av skipsfarten: ISPS-kode for skip og havner, PORT-NET som er et dokumentløst

sporingssystem for gods og oversikt over alle anmeldelser fra fartøyer og meglere til myndighetene og et automatisk identifikasjonssystem for fartøy. Transparents / åpenhet om opplysninger som registreres er også et hensyn som må veies opp mot at opplysningene kan være konkurransesensitive.

Hvordan kan handlingsreglene utformes?

Gruppe III: Man kan stille krav til konsekvensutredninger i form av Regulatory Impact Assessment (RIA), som er godt kjent fra vurdering av miljøkonsekvenser. Blant andre Canada bruker denne teknikken for vurdering av konsekvenser for personvernet: Privacy Impact Assessment (PIA). RIA/PIA er en prosessmetode som er best kjent i den angelsaksiske verden, men den anvendes også i stor grad i EU. Denne prosessmetoden sikrer at man stiller de nødvendige spørsmålene så tidlig som mulig. Man kan stille krav til en slik vurdering når en myndighet treffer beslutning om å anvende eller implementer IKT-system. Metoden kan også anvendes på mer strategiske beslutninger av offentlig myndighet om iverksettelse av større systemdesign. RIA/PIA har den fordelen at prosessen kan brukes både i konkrete beslutningssituasjoner og samtidig sikrer at man formelt drar inn alle interessenter i beslutningsprosessen gjennom krav til høringer. Ved å systematisk evaluere flere RIA/PIA-prosesser kan man generere en mer generell code of conduct. RIA/PIA er en veldokumentert prosess og innholdet kan lett skreddersys til de hensyn som skal integreres i transportsektorens IKT-systemer. Se kapittel 3 for en liste over referanser til bruk av RIA/PIA.

Konklusjon fra gruppene:

Gruppe II: Med bakgrunn i dette seminaret, bør Nordisk ministerråd engasjere en utreder og sette ned ei prosjektgruppe med deltaker fra hvert land som har som mandat å komme fram til en minimalistisk Code of Conduct. Innen utgangen av 1. kvartal 2005 bør man ha forslag til videre prosess. Arbeidet bør settes i gang raskt og dette forslaget bør legges fram for Embetsmannskomiteen (NET).

Gruppe III: Man bør vurdere krav om RIA/PIA når IKT-systemer skal tas i bruk. Reglene må ikke nødvendigvis være sektorovergripende eller fellesnordiske. Man bør heller arbeide overfor EU.

2.3 Momenter fra plenumsdebatten

Utarbeiding av retningslinjer:

- Eventuelle retningslinjer må komme raskt. Systemer med implikasjoner for personvernet er allerede i ferd med å bli gjennomført. Noen generelle over-ordnete prinsipper bør i alle fall på plass. Dette kan være til hjelp for dem som skal ta beslutninger. Man må unngå at det settes i verk systemer og tiltak som må rettes opp i ettertid. Et eksempel på dette er innføring av helautomatiske bomstasjoner uten et reelt anonymt alternativ.

- Det er nødvendig med politisk engasjement og støtte for å få retningslinjer igjennom.

Ulike avveininger

- Man bør trekke med forbrukermyndighetene i for eksempel gjennomgang av standardvilkår for systemutforming. Kommersielle interesser kan ofte være sammenfallende med interessene til den enkelte forbruker. Disse hensynene er ikke nødvendigvis i konflikt med personvernhensyn, men det er viktig med et samarbeid.

- Det er for generelt og enkelt å hevde at det alltid skal finnes mulighet til å bevege seg uten å legge igjen spor. Noen sektorer er pålagt å behandle personopplysninger. Dette gjelder blant annet for passasjerlister på fly og skip. Det må derfor være unntak for luftfart og sjøtransport og i andre sammenhenger der sikkerheten krever det. Oppmerksomheten må da rettes mot hvordan opplysningene skal behandles, hvor lenge opplysningene skal oppbevares og hvordan opplysningene skal beskyttes. Avtalen mellom EU-kommisjonen og USA åpner for overføring av opplysninger fra europeiske passasjerlister til USA. Andre antiterrortiltak setter også begrensninger for en generell rett til å bevege seg sporfritt.

- Det er viktig med åpenhet rundt behandling av personopplysninger.

Behov for kunnskap og kompetanseoverføring

- Det er et behov for å klargjøre de generelle og skjønnsmessige begrepene i personvernlovgivningen. Dette gjelder blant annet frister for sletting og krav til utforming av systemene.

- Etater som skal innføre IKT mangler kompetanse om personvern. Da er det også vanskelig å gi råd. Det må gis opplæring på etatsnivå. Dette kan i sin tur lede til at det etableres ”codes og conduct”. Representanter for datatilsynene foreslo at store etater bør vurdere å etablere et personvernombud. Da kan man lettere få kompetanse i etaten.

- Innen luft- og sjøfart har man allerede foretatt noen avveininger av sikkerhetshensynene opp mot personvern. Kan disse erfaringene overføres til andre transportformer som veg og bane?

- Det er viktig å få satt ned ei bredt sammensatt arbeidsgruppe som kan få fram og belyse alle relevante hensyn.

- Man bør legge til rette for utveksling av nasjonale erfaringer.

3 ITS och personlig integritet för vägtrafikområdet i Sverige

Følgende innspill til seminaret er utarbeidet av det svenske Vägverket:

Inledning

När det gäller diskussionen kring ITS för vägtrafikområdet kontra personlig integritet så har den inte förts så intensivt i Sverige. Det har dock framkommit i flera undersökningar som gjorts att allmänheten i de flesta fall inte oroar sig särskilt mycket för att de personuppgifter som kan finnas registrerade skulle missbrukas. De flesta verkar vara av den uppfattningen att de fördelar som ITS för med sig väger tyngre än de nackdelar som finns med systemen. Att systemen ofta är mycket komplexa och svåra att överblicka bidrar naturligtvis till att allmänheten inte helt kan omfatta vilka konsekvenser som ITS kan ha för deras personliga integritet.

Det kan dock konstateras att i ett samhälle med en ökande användning av tekniska system där personuppgifter registreras, behandlas och eventuell också lagras ökar behoven av tydliga förhållningsregler hur utformningen och användningen av dessa system ska se ut för att värna den personliga integriteten.

Svensk lagstiftning

Det finns många lagar som på olika sätt berör vägtrafik och integritet, men de två viktigaste lagarna i Sverige inom detta område är Personuppgiftslagen (PUL) samt Lagen om allmän kameraövervakning. I Sverige, som har en stark tradition av offentlighetsprincipen, är det en svår avvägning mellan att låta information vara tillgänglig för allmänheten och skyddet för den personliga integriteten. En annan svårighet är att utvecklingen går så otroligt fort att lagstiftningen har svårt att hålla jämna steg med den nya tekniken.

Personuppgiftslagen (PUL)

Personuppgiftslagen reglerar behandling av personuppgifter som helt eller delvis är automatiserad. Men lagen gäller även behandling av uppgifter som ingår eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. PUL är relevant i många tillämpningar av transportinformatik och integritet, men den har stora kryphål och kritikerna höjer varnande röster att teknikutvecklingen håller på att springa ifrån lagen.

Lagen om allmän kameraövervakning

I Lagen om allmän kameraövervakning regleras obemannad videoinspelning. Syftet med lagen är att styra kameraövervakningen så att största möjliga nytta uppnås och samtidigt tillgodose den enskildes intresse för skydd av den personliga

integriteten. För att få använda kameraövervakning krävs det tillstånd från Länsstyrelsen. Vägverket är dock undantaget denna tillståndsplikt vad gäller trafikövervakning med kameror samt vid betalstationer för trängselskatt. Polisen kan utan tillstånd och utan krav på skyltning bedriva hastighetsövervakning med kameror utmed vägnätet.

Svenska exempel

Vägavgifter och personlig integritet

Området vägavgifter berörs i allra högsta grad av problematiken med skyddet av den personliga integriteten. I många system loggas det tidpunkt och position för fordonet när det kör in på ett avgiftsbelagt vägavsnitt samt när det lämnar sträckan. Detta medför i många fall att det är möjligt att ta reda på var fordonet har befunnit sig vid specifika tidpunkter, och detta är naturligtvis information av känslig karaktär. Vägtrafikskatteutredningen beskriver en svensk modell där utgångspunkten är att ansvaret för att rätt betalning sker ligger på den betalningsskyldige. Därför behövs det inte ske någon loggning av fordonet och inga känsliga uppgifter registreras. För att säkerställa att betalningen efterlevs krävs dock stickprovskontroller där fordon slumpvis registreras och krävs på verifikation att de hade betalat för att köra just där. Om dessa stickprovskontroller görs via övervakningskameror så kommer ju frågan om den personliga integriteten upp igen. Det huvudsakliga målet är dock att skapa ett system som i minsta möjliga utsträckning registrerar uppgifter om den enskilde personen.

ISA – Intelligent Stöd för Anpassning av hastighet

I Sverige har det genomförts ett stort projekt med ISA. ISA är ett stödsystem som ska hjälpa föraren att alltid veta vilken hastighet som gäller på det vägavsnitt som fordonet befinner sig på. Fordonet är utrustat med en enhet där information om vägnät och hastighetsbegränsningar finns samt en GPS-modul som håller reda på fordonets aktuella position. I det inledande forskningsförsöket skulle delar av fordonsflottans position och hastighet loggas vilket föranledde en diskussion kring hur projektet skulle hantera frågan om personlig integritet. Integritetsproblematiken löstes genom avtal med förarna som reglerar hur informationen kommer att användas och hanteras. Positioneringen kunde inte stängas av, men föraren hade alltid valet att inte längre vara med i projektet. Enligt avtalet ägdes all information av deltagaren i projektet vilket innebar att informationen inte kunde lämnas vidare till t.ex. polis utan deltagarens godkännande. ISA har nu gått in i en ny fas där systemet ska implementeras och då har integritetsproblematiken lösts genom att det inte kommer att loggas några uppgifter om fordonet utan systemet kommer att vara slutet. Tanken är dock att ISA ska kunna användas för kvalitetssäkring av transporter och då blir det aktuellt med loggning av fordon. Uppgifterna kommer då att ägas av det aktuella företaget vilket innebär att även ansvaret för att dessa uppgifter behandlas på ett korrekt sätt ligger hos dem. Ansvariga för ISA inom Vägverket diskuterar om det ska arbetas fram rekommendationer för hur företagen ska hantera detta.

Summering

Det kan konstateras att det är långt kvar att gå innan att det kan garanteras att den personliga integriteten inte kränks i samband med ITS. Sammanfattningsvis kan sägas att läget i Sverige präglas av en ljum debatt rörande den personliga integriteten. En av anledningarna till detta är att det finns en tilltro till att systemen och de insamlade uppgifterna inte kommer att missbrukas. En annan anledning är att det är mycket svårt att överblicka de konsekvenser som de komplexa tekniska systemen kan få för den egna situationen. Den mycket snabba tekniska utvecklingen innebär att det näst intill är omöjligt för lagstiftarna att hålla jämna steg.

4 Referanser, aktuell litteratur

Internasjonale instrumenter og personvernlovgivning generelt

Blume P. 2003
Databeskyttelsesret. København: Jurist- og Økonomforbundets Forlag, 2. utgave.

Blume P. 2002
Protection of Informational Privacy København: Jurist- og Økonomforbundets Forlag.

Bygrave L.A. 2002:*Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague/London/New York: Kluwer Law International, 2002).

Europaparlamentet 2004
European resolution on the First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153 INI

Norden

Blume P. (red.) 2001:
Nordic Data Protection. København: Jurist- og Økonomforbundets Forlag.

Blume P. og U. Kjellerup 2002:
Utredningsprojekt vedrørende Transporttelematikk og Individ. Juridisk kortlægning, København: Nordisk Ministerråd

Nordic thematic group on ITS 2003:
Integration of ITS – Intelligent Transport Systems, Compendium. Oslo: Samferdselsdepartementet.

Nordisk Ministerråd 2002:
Utredningsprosjekt vedrørende transporttelematikk og individ. Sluttrapport. København.

Danmark

Blume P. 2000:
Personoplysningsloven. København: Akademisk Forlag.

Blume P. 2003:
Behandling af persondata. En kritisk kommentar. København: Jurist- og Økonomforbundets Forlag.

Nielsen K.K. og H. Waaben 2001
Lov om behandling af personoplysninger – med kommentarer. København: Jurist- og Økonomforbundets Forlag.

Norge

Schartum D.W. og L.A. Bygrave 2004:
Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger. Bergen: Fagbokforlaget.

Wiik Johansen M. , K.-B. Kaspersen og Å.M. Bergseng Skullerud 2001:
*Personopplysningsloven. Kommentarutgave.*Oslo: Universitetsforlaget.

Coll L.M. og C.A. Lenth 2000:
Personopplysningsloven : En håndbok. Oslo: Kommuneforlaget

NOU 1997:19
Et bedre personvern? Oslo: Statens forvaltningstjeneste.

Ravlum I-A 2004:
Makt, beslutning og integritet. IKT og personvern i transport. TØI rapport 703/2004. Oslo: Transportøkonomisk institutt.

Selmer K 1994
Hvorfor Datatilsyn. Oslo: Institutt for rettsinformatikk.
www.jus.uio.no/iri/forskning/lib/rapporter/datatilsyn/hvorfor_datatilsyn.html

Sverige

Öman S. og H.O. Lindblom 2000:
Personuppgiftslagen: En kommentar. Stockholm: Norstedts Juridik

Lindkvist, A, S. Forwars, P. Kronborg, S. Obrenovic 2002:
Vem vet var Du är och vad Du gör. Transportinformastikk och personlig integritet. Rapport 2002:5. Stockholm: TFK – Institutet för transportforskning.

SOU 1997:39
Integritet, Offentlighet, Informasjonsteknik. Statens offentliga utredninger, Justitiedepartementet, Betänkande av Datalagskommittén

Spesielt om Regulatory Impact Assessment / Private Impact Assessement

Bygrave, L.A. 2002:
Data Protection Law: Approaching Its Rationale, Logic and Limits, The Hague / London / New York: Kluwer Law International, s 370-375.

Flaherty D.H. 2000:
"Privacy impact assessments: An essential tool for data protection", i *Privacy Law & Policy Reporter*, 2000, bind 7, sider 85-90.

Greenleaf G. 2002:
"Canada makes privacy impact assessments compulsory", i *Privacy Law & Policy Reporter*, 2002, bind 8, sider 190-191.

Stewart B. 2002:
"Privacy impact assessment roundup", i *Privacy Law & Policy Reporter,* 2002, bind 9, sider 90-91.

Stewart B. 1999:
"Privacy impact assessment: towards a better informed process for evaluating impact assessments", i *Privacy Law & Policy Reporter*, 1999, bind 5, s 147-149.

De fleste av artiklene finnes på: http://www.austlii.edu.au/au/journals/PLPR/

Aktuelle lenker

Danmark

Datatilsynet: http://www.datatilsynet.dk/

Personopplysningsloven, forslag:
http://www.retsinfo.dk/_GETDOC_/ACCN/199912L00147-ÅLF1

Finland

Den finske Dataombudsmannen: http://www.tietosuoja.fi/

Norge

Det norske Datatilsynet: http://www.datatilsynet.no

Lov om behandling av personopplysninger: http://www.lovdata.no/all/nl-20000414-031.html

Sverige

Datainspektionen: http://www.datainspektionen.se/

Datainspektionens uttalelse om trangselsavgifter og personvern:
http://www.datainspektionen.se/pdf/remissvar/trangselavgifter.pdf

Regjeringskanseliets rettsdatabaser (søk eks på personuppgiftslag" og "sekretesslag"):
http://62.95.69.15/sfs/sfst_form.html

Andre lenker:

ILO 2003: ILO-konvensjon 185 om Seafarers' Identity Documents Convention (Revised), 2003 http://www.ilo.org/ilolex/english/convdisp1.htm

5 Bakgrunnsmateriale til seminaret

5.1 Hva er personvern?

5.1.1 Innledning

I juridisk teori nærmer man seg personvernbegrepet med tre litt ulike innfallsvinkler: Det integritetsfokuserte personvernet, det maktfokuserte personvernet og det beslutningsfokuserte personvernet. I tillegg kan personvernet forstås i form av ulike interesser som tillegges borgerne av et samfunn. Den såkalte ”teori om beskyttelsesinteresser” identifiserer de interessene som det er relevant å avveie. I de tilfellene der myndighetene skal utøve et visst skjønn i fortolkningen av loven, spiller denne teorien en rolle (Nordisk ministerråd 2002). De tre fokus for personvernet og de ulike interessene blir presentert under.

5.1.2 Ulike fokus for personvernet

Det integritetsfokuserte personvernet

Personvernet kan betraktes ut fra et fokus på den personlige integritet. Borgerne ønsker og skal ha kontroll over opplysninger om seg selv, særlig opplysninger som oppleves som personlige. Begrepet dekker mer enn ønsket om at opplysninger ikke skal bringes videre uten samtykke. Det dekker også et ønske om å få ”være i fred” – å ha en sirkel av privatsfære som ingen har rett til å trenge innenfor uten tillatelse eller en god og legitim grunn. Regler om beskyttelse mot krenking av privatlivets fred og bestemmelser om taushetsplikt begrunnes ut fra slike hensyn.

Det maktfokuserte personvernet

Særlig innen den europeiske tradisjonen er det i tillegg lagt vekt på at individene har rett til å beskytte seg mot maktmisbruk. Personlige opplysninger kan forrykke maktbalansen mellom enkeltpersoner og det offentlige eller private markedsaktører. Markedsaktører kan bruke opplysninger om forbruksmønster og vaner til å manipulere oss som kunder. Tilsvarende kan tilgang på personlige opplysninger gjennom tidsregistreringer, registrering av e-post og internettbruk eller lignende, forrykke maktforholdet mellom arbeidsgiver og arbeidstaker. Også maktforholdet mellom borger og stat kan påvirkes av forvaltningsorganets/myndighetenes tilgang på personlige opplysninger om enkeltborgere – eller summen av opplysninger som det offentlige har om den enkelte. Orwells ”1984” og begreper som ”Storebror ser deg”, viser hen til et samfunn der myndighetsutøvere har full informasjon om sine undersåtters personlige forhold. ”I dette perspektivet kan personvernet ses som en grensegang mot det som av enkelte grupper i

befolkningen oppleves som ”overdreven” markedsmakt, offentlig (og privat) myndighetsutøvelse og arbeidsgivermakt”(NOU 1997:19 kapittel 3).

Det beslutningsfokuserte personvernet

Personopplysninger brukes som grunnlag for beslutninger. Dette gjelder for beslutninger som tas av forvaltningen (f eks arbeidsledighetstrygd) og som tas av private (f eks tildeling av lån fra banken og forsikringsoppgjør). Behandlingen av slike personopplysninger skal sikre riktige og rettferdige avgjørelser. Opplysningene må derfor være korrekte og tilstrekkelige, og det må settes krav til hvordan opplysningene behandles. I dette perspektivet er man ikke bare opptatt av opplysninger som blir brukt eller som i nær framtid vil bli brukt til å fatte beslutninger. Man setter også fokus på opplysninger som kan *tenkes* å bli brukt til å fatte beslutninger.

5.1.3 Personverninteresser – individuelle og kollektive

Individuelle interesser

De individuelle interessene går på muligheten den enkelte har for å kontrollere hvilke opplysninger som samles inn om seg, hvem som får tilgang til dem og hva de brukes til (*diskresjon*). Dette leder for eksempel til at innsamling av personlige opplysninger bør begrenses til det som er relevant for formålet og at det legges begrensninger på hvem som har adgang til registrene. I tillegg har den enkelte interesse av at opplysningene er riktige og fullstendige (*fullstendighet*). Den enkelte skal også ha en rett til å vite hvilke opplysninger som registreres om seg (*innsyn*). Innsyn er også en viktig forutsetning for å kunne sikre at opplysningene er riktige. Endelig har den enkelte rett til å være i fred, uavhengig av om ”forstyrrelsen” innebærer at opplysninger blir registrert eller ikke (*privatlivets fred*).

Kollektive interesser

Den første kollektive interessen er et *borgervennlig samfunn.* Borgerne skal kunne forstå saksbehandlingen, og en gjennomautomatisert saksbehandling skaper en avstand mellom den enkelte og samfunnet. Et samfunn som i høy grad er avhengig av elektronisk informasjonsbehandling er i tillegg et sårbart og mindre *robust samfunn*. Den siste kollektive interessen er å ha et *begrenset overvåkingsnivå*. Samfunnet skal ha et vern mot maktmisbruk og urimelig kontroll. Store databaser gir mulighet for kontroll og maktbruk, særlig hvis det er mulig å koble ulike registre. Dette kan frata individene muligheten for å holde tilbake opplysninger om seg selv.

Interesser i motstrid med hverandre?

Disse ideelle interessene er ikke helt i harmoni med hverandre. For eksempel vil ønsket om fullstendige opplysninger trekke i retning av at flere opplysninger tas med enn det interessen om diskresjon tilsier. Vi kan være interessert i at de automatiske bomstasjonene registrerer hvem som passerer og når, slik at vi er sikre på at rett person blir avkrevd betalingen. Ønsket om diskresjon og minst mulig overvåking trekker i motsatt retning.

5.1.4 Forbrukerinteresser

Noen personverninteresser kan også stå i motstrid med andre interesser vi har som borgere og forbrukere. Forholdet mellom bilisten og bompengeselskapet er en kontrakt mellom kjøper og selger. Som kjøper har vi interesse av en kvittering på at vi har betalt for den tjenesten vi har benyttet. På den andre siden ønsker vi mest mulig effektiv passering av bomstasjonen og har derfor godtatt at vi ikke får kvittering. Dette illustrerer at også våre forbrukerinteresser kan stå i motstrid til hverandre og vi kan bli nødt til å avveie for eksempel effektivitet mot trygghet i kjøpsforholdet.

5.2 Eksempler på systemer som innebærer behandling av personopplysninger

Personopplysninger registreres i ulike sammenhenger i transportsystemet. Under er noen eksempler gjengitt. Eksemplene er hentet fra en utredning fra det norske Datatilsynet (under arbeid).

Veg:

- Registrering ved passering av bomstasjoner,
- Automatisk fartskontroll,
- Registrering av kjøre- og hviletider,
- Vegprising,
- Førerkortregister,
- Motorvognregister,
- Register for prikkbelasting (gjentatte forseelser fører til inndragning av førerkort),
- Ferdsskrivere,
- Elektronisk kjøretøykontroll,
- Kontinuerlig stedfesting av kjøretøy.

Kollektivtrafikk:

- Registrering ved elektronisk betaling på bane, taxi, buss, båt og fly,
- Kameraovervåking,
- Passasjerlister for båt og fly,
- Passasjeropplysninger i reisebyråer,
- Registrering av biometriske kjennetegn (fingeravtrykk, iris-scanning, stemme- og ansiktsgjenkjenning).

Individuell ferdsel på sjø

- Registrering i småbåtregisteret og registeret for båtførere.

5.3 Anbefalinger fra tidligere utredninger

5.3.1 Anbefalinger fra Cowi A/S

I rapporten ”Transporttelematikk og individ” (2002) utarbeidet av COWI A/S for Nordisk ministerråd, vises det til at de tekniske mulighetene for transporttelematikk utvikles så raskt at lovgivningen har problemer med å følge etter. I rapporten heter det at en uheldig og tett kombinasjon av systemer for transport-

telematikk, kombinert med andres systemer allerede i dag kan anvendes til forholdsvis detaljert kartlegging av enkeltpersoners gjøren og laden. Dette aspektet blir ikke alltid fanget opp av lovgivningen. Det foreslås derfor at det undersøkes i hvilket omfang og på hvilket grunnlag registreringer av borgerne foretas.

Cowi foreslår at det utvikles en "Codes of Conduct" som inneholder retningslinjer for design og innretning av de tekniske løsningene. Slike "Codes of Conduct" kan utformes som:

- Krav om konsekvensvurderinger av borgernes integritet og forbrukersikkerhet ved transporttelematiske systemer.
- Utviklingen av handlingsregler bør foregå i fellesnordisk regi for å sikre interoperabilitet og en styrket nordisk posisjon overfor EU-reguleringen på området.
- Bedre informasjon til de operative aktørene slik at man kan ta høyde for eventuelle konflikter med personvernet i en tidlig fase av utviklingen av teknisk design.
- Før IKT-systemer etableres, bør de evalueres av kompetente personer med innsikt i personvern og forståelse for transporttelematikk. Evalueringen bør gå gjennom bruken av personopplysninger, vurdere mulighetene for misbruk og overveie alternativer. Eventuelle dispensasjoner fra lovverket bør kun gis etter en slik kritisk vurdering.
- Det bør settes ned en fellesnordisk evalueringsgruppe som løpende skal evaluere nye tekniske løsninger. Gruppen skal bestå av juridisk og teknisk kompetanse og bør fungere som rådgivende organ for forbrukermyndigheter og datatilsyn i de nordiske landene.

Rapporten er behandlet av temagruppa for ITS under Nordisk embetsmannskomité for transport (NET), av NET og i Nordisk ministerråd. Orientering om denne behandlingen vil bli gitt i løpet av seminaret av Trygve Roll-Hansen, medlem av NETs temagruppe for ITS.

5.3.2 Anbefalinger fra Transportøkonomisk institutt

Transportøkonomisk institutt har på oppdrag fra det norske Samferdselsdepartementet gjort en utredning av forholdet mellom personvern og brukt av transporttelematikk (TØI 2004). I og med at grunnlaget for å behandle personopplysninger i transportsektoren gjerne er samtykke fra den registrerte, understrekes rapporten det at sektormyndighetene må ha et særskilt ansvar for at personvernet ikke blir undergravet i transportsektoren. Det foreslås derfor at samferdselsmyndighetene utvikler egne handlingsregler som transportetatene må følge opp i arbeidet med utvidet bruk av informasjonsteknologi i sektoren. Slike handlingsregler bør bygges opp slik at følgende hensyn blir ivaretatt:

- Bruk av informasjonsteknologi for å fremme samferdselspolitisk mål om sikkerhet og effektivitet må veies opp mot personvernhensyn. Det bør ikke være slik at det tiltaket som gir høyest effektivitet (i trafikkavvikling, betaling eller for å fremme trafikksikkerhet) skal velges. Andre tiltak med mindre konsekvenser for personvernet kan være tilstrekkelige i forhold til formålet.

- Man bør velge de tekniske løsningene som bidrar til oppfylling av de transportpolitiske målene, men som samtidig har minst mulig negative konsekvenser for personvernet. Primært bør tiltak uten konsekvenser for personvernet velges.
- Myndighetene bør sette krav til at en vurdering av alternativer blir gjennomført, spesielt i tilfeller der myndighetene er avtalepart, gir tilskudd til utvikling av systemene eller har ansvaret for ordningene.
- Overordnet myndighet bør kreve at det blir gitt en eksplisitt begrunnelse hvis det blir valgt løsninger som er mer inngripende overfor personvernet enn alternative løsninger.
- Anonyme alternativer må alltid være tilgjengelige for brukerne. Behandling av personopplysninger kan ikke være et vilkår for å kunne bevege seg på offentlig infrastruktur eller ta del i det alminnelige samfunnet.

5.4 Innspill fra det norske Datatilsynet

Det norske Datatilsynet, ved Beate Dagslet, har på spørsmål fra det norske Samferdselsdepartementet laget et eget innspill til retningsliner for personvern og forbrukerrettigheter spesielt med sikte på dette seminaret. Innspillet gjengis i sin helhet under:

”Selv om en aktør (for eksempel en transportør, eller en initierende myndighet) har et grunnlag til å behandle personopplysninger etter personopplysningsloven, så kan det likevel være at behandlingen av personopplysninger ikke er i samsvar med grunnleggende personvernhensyn. Grunnleggende personvernhensyn er at den enkelte skal ha kontroll med opplysninger om seg selv. Kort sagt hvem samler inn hvilke opplysninger og hvorfor? For en nærmere presentasjon gir punkt 5.1 foran en god oversikt.

Et behandlingsgrunnlag (jf den norske lovens § 8) kan foreligge hvis den reisende samtykker til at personopplysningene registreres og brukes. Et samtykke kan for eksempel innhentes via en avtale. Et annet grunnlag kan være at det er fastsatt i lov at registrering skal skje. Dersom en virksomhet innenfor transportområdet har en berettiget interesse i å registrere og bruke opplysningene, kan dette også være grunnlag for å registrere og bruke opplysninger, hvis dette ikke krenker hensynet til de reisendes personvern.

Retningslinjer for bruk av IKT på transportområde bør ha et fokus på de grunnleggende personvernhensyn.

1. Rett til å reise uten å legge igjen spor - anonymt

En grunnleggende rettighet nedfelt i konvensjoner og direktiver som ligger til grunn for personvernlovgivningen, er at det skal være mulig å velge å *ikke* legge igjen opplysninger om seg selv. Det skal være mulig for eksempel å benytte kollektive transportmidler eller passere en bomstasjon, uten at det registreres *hvem* som passerte *hvor* og til *hvilket tidspunkt*. I enkelte sammenhenger finnes det ikke noe valg - man må godta at det registreres personopplysninger om seg selv. For eksempel gjelder dette passasjerlister på fly og båter. Dette er registreringer som er *lovhjemlet*. Dersom det ikke finnes en lovhjemmel for å registrere opplysninger må det sørges for et sporfritt alternativ.

- *Er det mulig å lage en oversikt over lovhjemlede registreringer i retningslinjene?*

Allerede på *planleggingsstadiet* av tiltak som gjør bruk av IKT, vil det være viktig å legge til rette for at de som ønsker det skal kunne gjøre seg nytte av et tilbud eller ferdes som før, uten å legge igjen spor. Dette kan for eksempel skje ved å etablere flere betalingsalternativer. Rent teknisk skal det ikke være umulig å få til løsninger som ivaretar dette. Betalingsmiddelet, for eksempel en type smartkort, kan være knyttet til en konto som det trekkes penger fra. Hvorvidt denne kontoen igjen skal kunne knyttes til et bestemt individ eller ikke skal være valgfritt.

Det er meget viktig at det sporfrie alternativet er *reelt*. Det er ikke nok at det eksisterer. Alternativet må være kommunisert (*informasjon)* slik at individene vet de har et valg og at alternativet er like *tilgjengelig* som andre alternativer. *Prisen* på det sporfrie alternativet kan heller ikke stå i vesentlig misforhold til de øvrige alternativene.

Det kan spørres om det er noen grunn til at det skal være dyrere. Det vil naturlig nok koste å være anonym i form av at disse reisende ikke kan forvente like kundevennlige tjenester.

- *Retningslinjene bør sikre at det etableres rutiner rundt informasjon / tilgjengelighet / pris for sporfrie alternativet.*

I forlengelsen av dette bør det diskuteres om, og eventuelt i hvilken grad, virksomheten skal *legge frem hvilke vurderinger* som er tatt for å legge til rette for et sporfritt alternativ.

2. Dersom det registreres personopplysninger

Har lovgiver bestemt at registrering skal skje, eller at individet velger at opplysningene skal registreres, bør dette skje på en slik måte at tiltaket/ gjennomføringen er minst mulig belastende for personvernet. F.eks gjennom å ta hensyn til følgende punkter:

a. Færrest mulig opplysninger

Bare de nødvendige opplysninger skal registreres. Dette følger av personvernlovgivningen (den norske personopplysningsloven § 11 bokstav b).

Opplysningene skal kun benyttes til det som er formålet med behandlingen, som regel administrasjon av kundeforholdet eller som en sikkerhet ved eventuelle ulykker. Er det ønskelig å bruke opplysningene f.eks til markedsføring overfor kunden av annet enn egne produkter må kunden eksplisitt samtykke til dette.

- *Mulig med innspill på hvilke opplysningstyper som er absolutt nødvendige ("need to know") og hvilke det er ønskelig å ha og hvorfor ("nice to know")?*
- *Innspill på hva opplysningene skal brukes til, og om hva av dette som krever eget samtykke?*

b. Lagres i kortest mulig tidsrom

Opplysninger skal ikke oppbevares lengre en det som er nødvendig for de forskjellige formålene (personopplysningsloven § 28). Det blir viktig å finne ut hvor lenge opplysningen må oppbevares for kundeadministrasjon. Hvis det

opereres med forhåndsinnbetaling som kunden så debiteres fra, er hensynene forskjellig fra der det skjer en etterbetaling. Hensynet til kravene i annen lovgivning, som regnskapsloven, må også ivaretas.

- *Hvilke hensyn for oppbevaring finnes og hva kan slettefristen være?*

c. Lokal /sentral database

Lagring av opplysninger knyttet til kunden er å foretrekke at blir lagret i kortet og ikke i en sentral database. Dette gjelder særlig der det er et behov for å verifisere at rett person har rett kort i besittelse.

Men en slik løsning vil søke å sikre at det ikke kan dannes profiler hos andre som sier noe om individets bevegelser. Vedkommende sitter med sine egne opplysninger.

- *Når er det behov for å autentisere innehaveren av kortet? Og i andre sammenhenger må det etableres en sentral database?"*

5.5 Tidligere seminar i regi av Nordisk ministerråd

5.5.1 Innledning

NETs temagruppe for ITS arrangerte et nordisk seminar om "Integration of ITS – Intelligent Transport Systems" i Oslo 24. og 25. september 2003. Ei av arbeidsgruppene under seminaret behandlet personvern. Arbeidsgruppas anbefaling var at det etableres en "Codes of Conduct" for transporttelematikk med henblikk på beskyttelse av individenes integritet og forbrukerrettigheter.

Under gjengis delene av kompendiet fra seminaret som angår denne arbeidsgruppa: Referat fra hvilke problemstillinger som ble drøftet og momenter fra diskusjonen, samt sammendrag av de forberedte innleggene. Det meste av rapporteringen fra denne delen av seminaret er på engelsk. Der det finnes rapportering på skandinaviske språk, gjengis dette. Kompendiet kan skaffes ved henvendelse til det norske Samferdselsdepartement (trygve.roll-hansen@sd.dep.no).

5.5.2 Problemstillinger og diskusjon

Problemstillinger

- Hvorledes det undgås, at systemer unødigt og/eller utilsigtet krænker individers integritet og forbrugerrettigheder.
- Hvorledes den almene accept af de eksisterende telematik-systemer i de nordiske lande kan opretholdes.
- Hvorledes det sikres, at borgerne oplever systemernes fordele.
- Hvorledes det sikres, at regeringerne tager et ansvar for at beskytte borgeres integritet og forbrugerrettigheder.
- Hvorledes fokus kan rettes mod den offentlige interesse i stedet for de tekniske muligheder.

Referat fra diskusjon i plenum

The central aspect of the discussion was how to avoid that manufacturers and buyers of ITS inadvertently violate the individual integrity. In general the public accept the use of a wide range of ITS but this acceptance depends on trust to the legislation and authority's administration. Just one example of misuse of personal data can make a general scepticism against ITS.

The government has a responsibility for protection of the individual integrity and consumers rights when ITS is used. In general the public acceptance and legislation are similar in the Nordic countries and therefore it would be profitable to coordinate governmental activities to establish an extended protection for the citizens.

Finally it is essential that we keep the public interest in mind when we design and use ITS. We shall not be seduced by the possibilities of ITS.

Based on the discussions in the workshop the participants agreed to recommend establishment of a Code of Conduct with the purpose to protect the citizens against violations of their integrity and rights in connection to use of electronic payment of traffic services.

5.5.3 Forberedte innlegg i arbeidsgruppa

The Technical/political space for action in relation to protection of citizens' rights

Mads Holm-Petersen, Vejdirektoratet, Danmark

There are two essential aspects of protection of citizen's rights:

1. ITS will often involve some sort of surveillance of individuals and storage of data from the surveillance. In worst case this can lead to violation of the citizens´ right to be let alone.
2. The use of electronic payment IT systems is getting more and more widespread. The use of electronic payments leads to some legal issues of consumer protection.

The issue of this workshop is to throw light on the technical and political space for action in relation to protect the citizens´ rights.

The central impacts on individual rights from the IT systems are related to:

- Electronic registration and payment for traffic services
- Registration for traffic regulation, information and planning
- Registration/surveillance for prevention of criminal acts and investigation
- Identification of passengers and staff for prevention of terrorist acts and rescuing in case of catastrophes

Electronic registration and payment for traffic services

The use of electronic registration and payment for traffic services for example urban toll, road pricing, public transport and highway toll are expected to grow in the coming years. Often the systems are designed for registration in high speed without physical contact. This means that the systems must work without any

active actions from the payer and the payer will not instantly receive a receipt for the payment.

Registration for traffic regulation, information and planning

There are a commonly spread wish among traffic planners to use registration of identifiable personal data with the purpose of traffic regulation, information and planning. This registration has the primary goal to improve traffic flow, traffic safety and environment. But the registration can cause violations on the individual integrity.

Registration/surveillance for prevention of criminal acts and investigation

Registration of persons to prevent traffic violations or as part of a criminal investigation is common in the Nordic countries and all registrations from the IT systems shall be made available for the police if they get a court order. This use of registration can be taken as a violation of the integrity by some individuals and are likely to cause some scepticism against registration.

Identification of passengers and staff to prevent terrorist acts and rescuing in case of catastrophes

Finally Identification of passengers and staff to prevent terrorist acts and rescuing in case of catastrophes are nowadays a demand in many countries. This use of registration can be taken as a violation of the integrity by some individuals and are likely to cause some scepticism against registration.

Acceptance of TIS registration

Previous studies on the topic show a wide public acceptance on registration for traffic regulation, information and planning. The acceptance depend on the personal benefits from the ITS. While there are a wide spread acceptance of systems that involve personal benefits, there are less acceptance of systems where the benefits are more unclear for the individual.

Systems that increase the quality of information, improve the traffic flow and increase the speed of electronic payment in the traffic has a wide spread public acceptance. The public is more reserved on registration that has the purpose to improve traffic safety and other collective benefits. Finally there are a general scepticism for regulation with the purpose of enforcement of speed regulation and registration for commercial reasons.

Legal aspects

The legislation in the Nordic countries imply some basic rules on where, when and how registration of individuals are acceptable. The registration has to be:

- Necessary;
- As gentle as possible; and
- Secure against misuse.

In the discussion on whether the registration is necessary and sufficient the central question is which has the most weight; personal integrity or traffic security, flexible flow of traffic etc.

To some extent the legislation dictate the priority but a wide range of ITS are lying in the borderland of priorities. It is the impression that the manufacturers

and buyers of ITS do not have a clear picture of the priorities dictated in the legislation. This means that some systems do not comply with the legislation on account of inattention.

Befolkningens oppfattelse av krenkelsene

Inger-Anne Ravlum, TØI, Norge

De samferdselspolitiske fordelene ved de mange tekniske mulighetene som finnes, må veies opp mot andre hensyn som beslutningstakerne må ivareta. Et slikt hensyn er eksisterende lovgivning som kan sette begrensinger eller gi muligheter for anvendelsen av de tekniske løsningene. I relasjon til telematikk gjelder dette ikke minst personvernlovgivningen. Et annet hensyn er hvordan befolkningens stiller seg til innføring av transporttelematikk. Befolkningens aksept vil både henge sammen med deres vurdering av positive konsekvenser av transport-telematikken *og* deres vektlegging av personvern og forbrukersikkerhet.

Man kan nærme seg personvernbegrepet med tre litt ulike innfallsvinkler: Det integritetsfokuserte personvernet, det maktfokuserte personvernet og det beslutningsfokuserte personvernet. I tillegg kan personvernet forstås i form av ulike interesser som tillegges borgerne av et samfunn. Personvernlovgivningen søker å ivareta alle disse aspektene, men setter klarest grenser for registrering av personopplysninger.

Undersøkelser av hvordan folk stiller seg til ulike former for registrering av personopplysninger og overvåking for eksempel av stasjonsområder, viser at de er lite bekymret for selve registreringen av personopplysninger (integritetsfokusert personvern). Derimot opplever folk en klar uro og motvilje mot registrering som kan forrykke maktforholdet mellom individer og myndighetene eller mellom individer og ulike markedsaktører (maktfokusert personvern). Denne siden ved personvernet er imidlertid mer et politisk enn et juridisk spørsmål. Ved å tilnærme seg problemstillingen ved hjelp av det maktfokuserte personvernet, kan man lettere forstå at motstand mot automatisk trafikkontroll kan opptre samtidig med en full aksept av ulike elektroniske betalingsordninger, smartkort og video-overvåking av stasjonsområder.

I tillegg ser det ut til at den enkelte har lettere for å akseptere tekniske løsninger som har negative konsekvenser for personvernet, hvis løsningene samtidig inne-bærer en individuell fordel. Løsninger som tar sikte på å fremme et kollektivt gode, som for eksempel trafikksikkerhet, har større vanskeligheter med å bli akseptert.

Vi har dermed en situasjon der lovgivningen på den ene siden og folks aksept på den andre setter ulike grenser for hvilke tekniske løsninger som kan tas i bruk, avhengig av om løsningene berører det integritetsfokuserte eller det maktfokuserte personvernet. Om intensjonen med personvern og alle aspektene ved begrepet skal tas i vare, må sektormyndighetene utvikle handlingsregler for hvordan personvernet skal ivaretas. Slike regler bør blant annet sikre at man til en hver tid velger de løsningene som i minst mulig grad innebærer en forringelse av de ulike sidene ved personvernet.

Intelligent transport systems and protection of personal privacy

Annegret Andersen, Vegdirektoratet, Norge

- What kind of personal data do you handle with when you use intelligent transport systems?
- The requirements of the law when handling with personal data.
- Necessity
- Judgment between different considerations
- Information security

- The importance of the considerations. Which has the most weight?
- Personal integrity or traffic security?
- Personal integrity or flexible flow of traffic?

- Does the law solve all approaches?
- Do we really need toll-roads?

- Intelligent transport systems without using personal data – a Utopian idea?
- Impossibility
- Challenge

The political space for action in relation to protection of privacy

Thomas Jørgensen, Transportministeriet Danmark

The dilemmas regarding on the one hand the technological potential related to ITS and on the other hand the necessary protection of the rights and integrity of the individuals are in many respects basically political. In each case a balance must be found between the goal pursued – be it increased safety, a better flow of traffic, or more efficient law enforcement – and the practical and emotional protection of the persons involved.

These dilemmas have been described and discussed in a recent report prepared by COWI for the Theme Group for ITS under the Nordic Council. In order to find the right balance in the individual case, the report shows, several factors must be taken into account:

1. The purpose of the initiative.
2. The nature of the surveillance involved, including whether the surveillance is personal or mechanical
3. The nature of the data generated, including whether it can be anonym zed
4. Who will have access to the data generated, including government agencies, police, other private parties or family

Among other initiatives, the report recommends, that a “code of conduct” is established, formalizing the procedure in which the above mentioned factors are taken into account in the decision-making process and outlining some general principles for the use of ITS.

Among these guiding principles could be, that:

1. The least radical mean possible should always be chosen in order to further a certain goal.
2. The technology should be used as openly as possible, as long as this is not in conflict with the purpose of the system as such.
3. The use of the data generated should be minimized, also, of course, taking the purpose of the surveillance into account.
4. A strict discipline in the generation and use of the data must be secured, ensuring correctness in registration and use.

Based on this "code of conduct" and practical experiences, a set of "best practices" might be developed. These initiatives would ensure a better flow of information to decision makers and operators of the systems. Thus the possibilities of handling conflicts in the early stages of the design of ITS systems would be enhanced.

Taking into account that many of the ITS-systems are international in nature and are used cross borderline, it would be an advantage if the suggested code of conduct could be established in a joint Nordic context. A possible fist step might be arranging a line of seminars like this one in Oslo, where practitioners and decision makers can exchange ideas and experiences.

Vedlegg 1: De juridiske rammene for personvern og konsumentrettigheter i transport

Førsteamanuensis dr. juris Lee A. Bygrave, Institutt for privatrett, Universitetet i Oslo

Notater for Nordisk ministerråds seminar om utvikling av retningslinjer for personvern og forbrukerrettigheter i transport. Oslo 15. november 2004

1: Hovedregelverk på det internasjonale planet av betydning for seminarets formål

Europarådet

- Den Europeiske Menneskerettighetskonvensjon (1950)[2] artikkel 8:

  «1. Everyone has the right to respect for his private and family life, his home and correspondence.

  2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.»

- Konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger (1981)[3]

EU

- Direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av sådanne opplysninger.[4]

---

[2] *European Convention for the Protection of Human Rights and Fundamental Freedoms*, vedtatt 4. november 1950; i kraft 3. september 1953.

[3] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (E.T.S. No. 108), vedtatt 28. januar 1981, i kraft 1. oktober 1985.

- Traktat om innføring av en europeisk grunnlov (*draft Treaty establishing a Constitution for Europe*, Brussel, 18. juni 2004, CIG 86/04) artikkel I-50.
- EUs charter om grunnleggende rettigheter (*Charter of Fundamental Rights*, vedtatt 7. desember 2000) artikkel 7, 8.
- Direktiv 93/13/EF om urimelige kontraktvilkår i forbrukeravtaler.[5]
- Direktiv 97/7/EF om forbrukervern i forbindelse med avtaler vedrørende fjernsalg.[6]
    - NB. unntak for avtaler om transport etter artikkel 3(2).
    - Merk særlig artikkel 10.
- Direktiv 90/314/EF om pakkereiser.[7]

2: Hoved(personvern)rettslige instrumenter i de nordiske land

Danmark

- Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.

Finland

- Henkilötietolaki / Personuppgiftslag (FFS 523/99).
- Suomen perustuslaki / Finlands grundlag (FFS 731/1999) § 10.

Island

- Lög nr. 77 23. mai 2000 um persónvernd og medferd persónuupplýsninga.

Norge

- Lov om behandling av personopplysninger av 14. april 2000 nr. 31

Sverige

- Personuppgiftslagen (SFS 1998:204).
- Regeringsformen (SFS 1974:152) kap. 2 § 3.

---

[4] *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (O.J. L 281, 23. november 1995, s. 31), vedtatt 24. oktober 1995.

[5] *Directive 93/13/EEC on unfair terms in consumer contracts* (O.J. L 095, 21. april 1993, s. 29), vedtatt 5. april 1993.

[6] *Directive 97/7/EC on the protection of consumers in respect of distance contracts* (O.J. L 144, 4. juni 1997, s. 19), vedtatt 20. mai 1997.

[7] *Directive 90/314/EEC on package travel, package holidays and package tours* (O.J. L 158, 23. juni 1990, s. 59), vedtatt 13. juni 1990.

3: Europakommisjonen

- Decision 520/2000/EC of 26th July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (O.J. L 215, 28. august 2000, s. 7).
- Decision of 14th May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (C(2004) 1914) (O.J. L 235, 6. juli 2004, s. 11).

4: EUs arbeidsgruppe om personopplysningsvern (Working Party on the Protection of Individuals with regard to the Processing of Personal Data)

- Working Document on IATA Recommended Practice 1774 Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo (vedtatt 14. september 2001).
- Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines (vedtatt 16. januar 2004).
- Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines (vedtatt 11. februar 2004).
- Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (vedtatt 22. juni 2004).
- Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America (vedtatt 30. september 2004).

5: EF-domstolen

- Dom av 20. mai 2003 i sak 465/00, *Rechnungshof* mot *Österreichischer Rundfunk m fl* og forente saker 138/01 og 139/01, *Neukomm og Lauermann* mot *Österreichischer Rundfunk*.
- Dom av 6. november 2003 i sak 101/01, *Bodil Lindqvist* mot *Åklagarkammaren i Jönköping*.

6. Begrepet «personopplysning» («personal data» / «personal information»)

Direktiv 95/46/EF

- «Personal data» = «any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.» Jf. artikkel 2(a).
- «to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.» Jf. fortalen nr. 26.

7. Grunnleggende personvernprinsipper

Rettferdighet og rettmessighet

- Personopplysninger skal behandles på rettferdig og rettmessig vis («fairly and lawfully»), jf. direktiv 95/46/EF artikkel 6(1)(a).
    - Implisitt: Den behandlingsansvarlige skal ta i betraktning og ha respekt for de registrertes interesser og rimelige forventninger; inngrep som behandlingen medfører, skal ikke være uforholdsmessige; den registrerte skal ikke utilbørlig tvinges til å avgi opplysninger om seg selv eller til å godta at allerede innsamlede opplysninger brukes til visse formål; behandlingen skal dessuten være gjennomsiktig og forståelig for den registrerte.

Minimalitet

- Mengden av innsamlede personopplysninger skal begrenses til det som er nødvendig for å realisere formålet ved innsamling og den videre behandlingen av opplysningene, jf. direktiv 95/46/EF artikkel 6(1)(c) – (e), 7, 8.
    - Implisitt: Så snart allerede innsamlede personopplysninger ikke lenge er nødvendige å beholde utfra innsamlings-/bruksformålet, skal de slettes eller anonymiseres; det skal legges til rette for at enkeltindivider kan forbli anonyme ved inngåelse av transaksjoner med ulike organisasjoner.

Formålsbestemthet

- Personopplysninger skal behandles til uttrykkelig angitte, legitime formål og kun brukes i samsvar med disse formål, jf. direktiv 95/46/EF artikkel 6(1)(b).
    - Implisitt: formålet skal angis på en rimelig presis måte; formålet skal som et minimum være i samsvar med den behandlingsansvarliges ordinære, lovlige virksomhet; formålet bør muligens også være i samsvar med mer generelle etiske (og ikke bare rettslige) samfunnsnormer.

Opplysningskvalitet

- Personopplysninger skal være korrekte i forhold til det de er ment å representere, og skal være relevante, adekvate og fullstendige i forhold til deres bruksformål, jf. direktiv 95/46/EF artikkel 6(1)(c) – (d).
    - Implisitt: behandlingsansvarlige skal etablere tiltak for å sjekke opplysningskvaliteten.

Medbestemmelse

- Den registrerte skal kunne delta i og ha en viss mulighet til å påvirke andres behandling av opplysninger om seg selv, jf. direktiv 95/46/EF artikkel 7, 8, 10, 11, 12, 14, 15.
    - Implisitt: Behandlingsansvarlige skal sørge for at sine behandlingsoperasjoner er kjente, transparente og forståelige for de registrerte; behandlingsansvarlige skal videre så langt som mulig samle opplysninger direkte fra vedkommende person; personer skal i utgangspunktet selv kunne bestemme hvorvidt opplysninger om dem skal kunne samles inn av andre, og hva opplysningene skal kunne brukes til etter innsamling; personer skal kunne motsette seg visse typer behandlingsoperasjoner, og de skal kunne kreve at registrerte opplysninger om dem rettes eller slettes når disse er uriktige, ufullstendige eller ulovlige å registrere.

Informasjonssikkerhet

- Behandlingsansvarlige skal etablere tiltak for å sikre personopplysninger mot uautorisert eller utilsiktet tilgang, videregivelse, endring og/eller sletting, jf. direktiv 95/46/EF artikkel 17.

Sensitivitet

- Behandling av visse personopplysninger (i hovedsak om personers helse, seksualitet, rase eller etnisk bakgrunn, politiske, religiøse eller filosofiske oppfatninger, eller fagforeningsmedlemskap) skal – p.g.a. deres antatt sensitivitet – underkastes strengere regulering enn hva som gjelder for andre personopplysninger, jf. direktiv 95/46/EF artikkel 8.

Øvrige (og forholdsvis nye) prinsipper

- **Anonymitet:** teknologiske og organisatoriske forhold skal legges til rette for at en person kan forbli anonym ved inngåelse av transaksjoner med ulike organisasjoner. Hvis anonymitet ikke er mulig, skal transaksjonene kunne fullføres ved bruk av pseudonymer som gjør det vanskelig å identifisere personen, jf. f.eks. den tyske *Bundesdatenschutzgesetz* (1990) § 3a, jf. også artikkel 29 arbeidsgruppens rekommendasjon 3/97 (vedtatt 3. desember 1997).
- **Helautomatiserte beslutninger:** Helautomatiserte vurderinger av en persons personlige egenskaper skal ikke kunne utgjøre det eneste grunnlaget for beslutninger som griper inn i personens liv, jf. direktiv 95/46/EF artikkel 15.

Vedlegg 2: Deltakerliste

Abelvik, Astrid	Transportøkonomisk institutt	NO	asa@toi.no
Andelius, Camilla	Vägverket	SE	camilla.andelius@vv.se
Andersen, Annegret	Vegdirektoratet	NO	annegret.andersen@vegvesen.no
Appel, Kristian	Traficon ltd / NETs temagruppe	FI	kristian.appel@traficon.fi
Asmussen, Tine	Datatilsynet	DK	ta@datattilsynet.dk
Bygrave, Lee	Institutt for privatrett	NO	l.a.bygrave@jus.uio.no
Bäckström, Rolf	Sjöfartsverket	FI	rolf.backstrom@fma.fi
Christiansen, Jan	NSB BA	NO	jan.christiansen@nsb.no
Dagslet, Beate S.	Datatilsynet	NO	b.s.dagslet@datatilsynet.no
Fernquist, Catharina	Datainspektionen	SE	datainspektionen@datainspektionen.se
Guðjónsson, Rúnar	Min.Transport, Tourism and Telecommunications	IS	runar.gudjonsson@sam.stjr.is
Hasselgren, Kjell	Vegdirektoratet	NO	kjell.hasselgren@vegvesen.no
Holm Petersen, Mads	Vejdirektoratet	DK	mho@vd.dk
Haaheim, Jan Kåre	Avinor	NO	jan.kare.haaheim@avinor.no
Jørgensen, Thomas	Trafikministeriet / NETs temagruppe	DK	tjo@TRM.dk
Kaspersen, Knut-Brede	Datatilsynet	NO	k.b.kaspersen@datailsynet.no
Kjellerup, Ulf	COWI A/S	DK	ukj@cowi.dk
Negård, Gry	Forbrukerombudet	NO	gn@forbrukerombudet.no
Norberg, Bernt	Luftfartsverket	SE	bernt.norberg@hk.lfv.se
Ottesen, Rasmus	Nordisk ministerråds sekretariat	DK	Ro@norden.org
Ravlum, Inger-Anne	Transportøkonomisk institutt	NO	iar@toi.no
Roll-Hansen, Trygve	Samferdselsdepartementet / NETs temagruppe	NO	trygve.roll-hansen@sd.dep.no
Stener, Malin	Konsumentverket	SE	malin.stener@konsumentverket.se
Stenström, Olle	Luftfartsverket	SE	olle.stenstrom@hk.lfv.se
Storhaug, Haakon	Sjøfartsdirektoratet	NO	haakon.storhaug@sjofartsdir.no
Öörni, Seppo	NETs temagruppe	FI	seppo.oorni@mintc.fi

Sist utgitte TØI publikasjoner

Tittel	TØI Publikasjon
Behov for grunnlagsdata for videreutvikling av godsmodellsystemet i Norge	731/2004
Endring av fartsgrenser. Effekt på kjørefart og ulykker	729/2004
Sovning bak rattet: Medvirkende faktorer, omfang og konsekvenser	728/2004
Regionale virkninger av OL i Tromsø	726/2004
Virkninger av økte satser for gebyr og forenklet forelegg på lovlydighet i trafikken.	725/2004
Evaluering av "Sei ifrå " kampanjen i Telemark.	722/2004
Transportytelser i Norge 1946 - 2003	721/2004
Transportytelser for små godsbiler	720/2004
Samfunnsmessige trender - betydning for mobilitet og transport i storbysamfunnet	718/2004
Lokale næringsøkonomiske virkninger av vegutbygging	717/2004
Hva koster et skipsanløp ?	716/2004
Delvis brukerbetalt utbygging av transportsystemet i Oslo og Akershus - Evaluering av Oslopakke 1 og 2	714/2004
Overlevelse eller avvik? En modell for bilføreres atferd. Sluttrapport.	666/2003
Fordeling av turistovernattinger på fylker - grunnlagsberegninger for satelittregnskap for reiseliv på fylkesnivå	589/2002
Review of the Tanzania Road Sector Programme TAN 045 - Final Report	571/2002

Transportøkonomisk institutt

Stiftelsen Norsk senter for samferdselsforskning

- utfører forskning til nytte for samfunn og næringsliv
- har rundt 70 forskere med høy, flerfaglig samferdselskompetanse
- samarbeider med en rekke samfunns-institusjoner, forsknings- og under-visningssteder i Norge og i utlandet
- gjennomfører forsknings- og utrednings-oppdrag av høy kvalitet innen områder som trafikksikkerhet, kollektivtransport, miljø, reisevaner, reiseliv, planlegging, beslutningsprosesser, transportøkonomi og næringslivets transporter
- driver aktiv forskningsformidling gjennom TØI-rapporter, internett, tidsskriftet Samferdsel og andre nasjonale og internasjonale tidsskrifter

Transportøkonomisk institutt
Stiftelsen Norsk senter
for samferdselsforskning
P.b. 6110 Etterstad
0602 Oslo

Telefon 22 57 38 00
www.toi.no