Torkel Bjørnskau
Mattias Gripsrud
Tonje Grunnan
Tore Leite
Dag Wiese Schartum
TØI rapport 914/2007

Transportøkonomisk institutt
Stiftelsen Norsk senter for samferdselsforskning

Security i transport og personvernets grenser

TØI rapport
914/2007

Security i transport og personvernets grenser

Torkel Bjørnskau
Mattias Gripsrud
Tonje Grunnan
Tore Leite
Dag Wiese Schartum

ISSN 0808-1190
ISBN 978-82-480-0799-9 Papirversjon
ISBN 978-82-480-0800-2 Elektronisk versjon
Oslo, desember 2007

Tittel: Security i transport og personvernets grenser

Forfatter(e): *Torkel Bjørnskau; Mattias Gripsrud; Tonje Grunnan; Tore Leite; Dag Wiese Schartum*

TØI rapport 914/2007
Oslo, 2007-12
108 sider
ISBN 978-82-480-0799-9 Papirversjon
ISBN 978-82-480-0800-2 Elektronisk versjon
ISSN 0808-1190

Finansieringskilde:
Norges forskningsråd - RISIT-programmet

Prosjekt: 3077 Sikkerhet, security og effektivitet: Personvernets grenser

Prosjektleder: Torkel Bjørnskau

Kvalitetsansvarlig: Marika Kolbenstvedt

Emneord:
Sikkerhet; Security; Personvern; Transport

Sammendrag:
Etter terrorangrepene 11. september 2001 har securitytiltakene i transportsektoren blitt mer omfattende, særlig i luftfart og sjøfart, som tradisjonelt har hatt fokus på security. Norske tiltak er i stor grad implementering av internasjonale regler. Personvern er i liten grad i fokus blant norske transportaktører, bortsett fra i luftfart. Det er også i luft- og sjøfart at terrorsikring er på dagsordenen. I andre transportgrener er man lite opptatt av terrorsikring, og personvern diskuteres primært i tilknytning til ordinære sikkerhetstiltak og med tanke på egne ansatte.

Security-tiltak har implikasjoner for personvern. Adgangskontroll og sikkerhetssjekk utfordrer integritetsvernet; overvåkning og registrering utfordrer personopplysningsvernet. Tiltakene kan være i strid med personvernet fordi enkeltpersoner ikke får anledning til å nekte registrering, og de får kun begrenset innsikt i og mulighet for å korrigere opplysninger som er lagret om dem. Det oppstår også rettsstatlige problemer knyttet til mangel på innsyn i det rettslige grunnlaget og hemmeligholdelse av grunnlaget for trusselvurderinger. Strengere prosedyreregler for gjennomføring av securitytiltak kan til en viss grad bøte på problemene.

Title: Transport security and the protection of privacy

Author(s): *Torkel Bjørnskau; Mattias Gripsrud; Tonje Grunnan; Tore Leite; Dag Wiese Schartum*

TØI report 914/2007
Oslo: 2007-12
108 pages
ISBN 978-82-480-0799-9 Paper version
ISBN 978-82-480-0800-2 Electronic version
ISSN 0808-1190

Financed by:
The Research Council of Norway

Project: 3077 Transport security and the protection of privacy

Project manager: Torkel Bjørnskau

Quality manager: Marika Kolbenstvedt

Key words:
Safety; Security; Privacy; Data protection; Transport

Summary:
The 9/11 terrorist attacks in the US have resulted in a number of new regulations and anti-terrorist measures in the transport sector, especially within aviation and sea transport. Countermeasures adopted in Norway are for the most part implementations of international regulations. Among Norwegian transport actors, privacy rights and data protection rights are not very high on the agenda, except in aviation, where privacy implications of security measures are acknowledged. In other transport modes, privacy issues are mainly discussed with reference to ordinary safety measures and with reference to the rights of own employees.

Most security measures have privacy implications. Access control and security checks challenge the right to privacy; surveillance and registration may violate people's data protection rights. Data may be registered without consent and without knowledge of the information collected, and without possibility for individuals to check the information collected about them. These issues are also problematic within our democratic legal tradition. Strong procedural regulations related to data collection and registration in this area may to some extent mitigate these problems.

Language of report: Norwegian

Rapporten kan bestilles fra:
Transportøkonomisk institutt, Biblioteket
Gaustadalleen 21, 0349 Oslo
Telefon 22 57 38 00 - www.toi.no

The report can be ordered from:
Institute of Transport Economics, The library
Gaustadalleen 21, NO 0349 Oslo, Norway
Telephone +47 22 57 38 00 - www.toi.no

Forord

Etter terrorangrepene mot USA 11. september 2001 er det innført en rekke security-tiltak i transportsektoren. Slike tiltak vil normalt ha implikasjoner for personvern, og den foreliggende rapporten er en gjennomgang av (i) hvilke slike tiltak som er innført og som er på trappene i Norge og i EU, (ii) hvilke personvernimplikasjoner tiltakene kan ha og (iii) hvordan norske beslutningstakere i transportsektorene vurderer forholdet mellom aktuelle security-tiltak og personvern. Prosjektet er finansiert av Norges forskningsråd innenfor programmet "Risiko og sikkerhet i transportsektoren (RISIT)".

Ved Transportøkonomisk institutt (TØI) var Inger-Anne Ravlum prosjektleder i første fase av prosjektet. Hun sluttet ved TØI sommeren 2006, og Torkel Bjørnskau overtok som prosjektleder. Ved TØI har også Tore Leite, Mattias Gripsrud og Tonje Grunnan vært involvert i prosjektet. Tore Leite har hatt ansvar for gjennomgangen av aktuelle tiltak og skrevet kapittel 2 sammen med Torkel Bjørnskau. Mattias Gripsrud og Tonje Grunnan har gjennomført intervjuene med norske beslutningstakere og skrevet kapittel 4. Gjennomgangen av personvernimplikasjoner av securitytilakene er gjort av Dag Wiese Schartum ved Avdeling for forvaltningsinformatikk ved Universitetet i Oslo. Schartum har også skrevet kapittel 3. Kapittel 1 og 5 er skrevet av Torkel Bjørnskau. Avdelingsleder Marika Kolbenstvedt har kvalitetssikret arbeidet. Trude Rømming har hatt ansvaret for den endelige utformingen av rapporten.

Oslo, desember 2007
Transportøkonomisk institutt

Lasse Fridstrøm
instituttsjef

Marika Kolbenstvedt
avdelingsleder

Innhold

Forkortelser

ADR	Accord européen relatif au transport international des marchandises dangereuses par route (Europeisk avtale om transport av farlig gods på veg)
Alkolås	Et pusteprøveapparat knyttet til kjøretøyets tenningslås
APNR	Automatic Number Plate Recognition
ATK	Automatisk trafikkontroll
AutoPASS	Norsk automatisert system for elektronisk betaling av bompenger (på vei)
CAPPS	Computer Assisted Passenger Prescreening System
CBRN	Chemical, Biological, Radiological, and Nuclear
CSI	Container Security Initiative
DNV	Det norske Veritas
DSB	Direktoratet for samfunnssikkerhet og beredskap
eCall	Automatisk nødanropssystem som skal sikre hurtig bistand ved trafikkulykker.
ECAC	European Civil Aviation Conference
ECMT	European Conference of Ministers of Transport
EMK	Den europeiske menneskerettighetskonvensjonen
EOS-utvalget	Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste
ESA	EFTA Surveillance Authority (kontrollerer at EFTA-landene følger EØS-reglene i EFTA-området)
Eurojust	EU-organ for å utveksle og koordinere juridisk kompetanse for å bekjempe internasjonal og organisert kriminalitet.
Europol	European Police Office
EVI	Electronic Vehicle Identification
EØS	Det europeiske økonomiske samarbeidsområde (opprettet gjennom EØS-avtalen mellom EU og EFTA 1. januar 1994)
FFI	Forsvarets forskningsinstitutt
GALILEO	Global Navigation Satellite System
GPS	Global Positioning System
HMS	Helse, miljø, sikkerhet
ICAO	International Civil Aviation Organization
IKT	Informasjons- og kommunikasjonsteknologi
IMO	International Maritime Organisation
IRA	Irish Republican Army
ISPS-koden	International Ship and Port Facility Security Code

ITS	Intelligent Transport System(s)
NHD	Nærings- og handelsdepartementet
NSB	Norges statsbaner
NSM	Nasjonal sikkerhetsmyndighet
PFSO	Port Facility Security Officer
PIA	Privacy impact assessment
OECD	Organisation for Economic Co-operation and Development
PNR	Passenger Name Record
PPBM	Positive Passenger-Bag Matching
PSO	Port Security Officer
PST	Politiets sikkerhetstjeneste
RER	Réseau Express Régional (metro + forstadsbaner i Paris)
RFID	Radio-frequency identification
ROS	Risiko og sårbarhet
RSO	Recognized Security Organisations
Schengen	Avtale om forenklet intern grensekontroll og felles ytre grensekontroll i Europa
SMS	Short Message Service
TEN-T	Trans-European Transport Network

TØI-rapport 914/2007
Forfattere: Torkel Bjørnskau, Mattias Gripsrud,
Tonje Grunnan, Tore Leite, Dag Wiese Schartum
Oslo 2007, 108 sider

Sammendrag:

Security i transport og personvernets grenser

Intensivert security etter 11. september 2001

Særlig i luftfart og sjøfart er det innført en rekke nye bestemmelser og tiltak som følge av terrorangrepene i USA 11. september 2001. Også terroraksjonene mot jernbanen i Madrid i 2004 og mot kollektivtrafikken i London i 2005 samt avsløringene av planlagte terrorangrep mot transatlantiske flygninger sommeren 2006 har gitt økt fokus på terrorsikring og vært bakgrunnen for nye tiltak. Noen av de viktigste tiltakene som er innført er:

- Intensivert security-sjekk av passasjerer og bagasje på internasjonale og nasjonale lufthavner
- Innføring av biometriske pass. Krav om biometriske pass for innreise til USA
- Utlevering av passasjerlister med personopplysninger fra flyselskapene til amerikanske myndigheter
- Forbudet mot å bringe væskebeholdere med over 1 dl væske om bord i fly
- Kroppsskannere for å undersøke passasjerer er innført som forsøksordning bl.a. på Schiphol lufthavn i Amsterdam
- Fingeravtrykkavleser som sikrer samsvar mellom person som sjekker inn bagasje og som går om bord i fly er innført av SASBraathens på Oslo Lufthavn
- Strengere krav til sikkerhet og terrorberedskap for skip, bl.a. terroralarm, besiktigelse og kontroll av skip, krav til sikringsplaner, sikkerhetsutstyr mv.
- Strengere regler for fysisk sikring av havneområder, med inngjerding, adgangskontroll mv.
- Strengere krav til identifikasjonsbevis for sjøfolk
- Strengere kontroll av hvem som ansattes i transportvirksomhet (kontroll av bakgrunn og vandel)
- Fysisk kontroll av containere, skanningsteknologi, utvikling av ”smarte” containere, radiofrekvensidentifikasjon, satellittbaserte sporingssystemer mv.
- Forsøk med passasjerkontroll på utvalgte T-banestasjoner på undergrunnen i London

Rapporten kan bestilles fra:
Transportøkonomisk institutt, Gaustadalleén 21, NO 0349 Oslo
Telefon: 22 57 38 00 Telefax: 22 60 92 00

Som det framgår av denne listen er det særlig i luftfart og sjøfart at security-arbeidet er intensivert. Dette er transportgrener der security har vært nokså sterkt fokusert også tidligere. Det ser m.a.o. ut til at den nye terrortrusselen først og fremst har ført til nye tiltak på områder der det allerede er et visst securityregime fra før, og i langt mindre grad at det er kommet securitytiltak på helt nye områder.

Det finnes imidlertid en rekke tiltak innenfor alle transportgrener som ikke har terrorsikring som primært formål, men som innebærer overvåking og registrering av personer/kjøretøy og som dermed har personvernimplikasjoner og som har vært brukt eller kan brukes til forebygging/oppklaring av terroraksjoner eller -planer.

Dette gjelder kameraovervåkning av terminaler, transportmidler, infrastruktur og stasjonsområder som særlig er utbredt i Storbritannia, men som også er blitt stadig mer vanlig i Norge. Videre finnes det automatiske systemer for å registrere kjøretøyers passeringer i bomstasjoner (AutoPass), elektroniske billetteringssystemer, automatiske satellittbaserte fartstilpasningssystemer (”Intelligent speed adaptatation” (ISA)) og systemer for automatisk varsling av ulykker (e-call), atferdsregistrator (”black box”) i bil, automatisk trafikkontroll. Dette er systemer som enten er innført eller som er på trappene og som innebærer overvåkning og registrering av personopplysninger. Særlig innenfor veitransport skjer det en voldsom utvikling når det gjelder å ta i bruk ny teknologi for å styre og overvåke trafikken.

Slike systemer har åpenbare implikasjoner for personvern – og dels av samme grunn – kan de utnyttes i arbeidet mot terror. Det britiske systemet med automatisk registrering av kjennemerker på passerende biler (”Automatic Plate Number Recgonition” (APNR)) ble for eksempel brukt til å spore opp en av de terrormistenkte bak bilbombeaksjonene i London og Glasgow sommeren 2006.

Terrorsikring i norsk transport – tilpasning til internasjonale avtaler

Terrorsikring i norske transportvirksomheter skjer nær sagt utelukkende ut fra internasjonale forpliktelser. Luftfart og sjøfart er de transportgrenene hvor det tradisjonelt har vært et omfattende internasjonalt regelverk gjennom ICAO, IMO og etter hvert EU, og det er også i disse transportgrenene at de fleste sikringstiltak mot terror er implementert i Norge, som i de fleste andre vestlige land.

Det er få selvstendige initiativ når det gjelder tiltak mot terror mot transportmidler eller infrastruktur i Norge. Det innføres riktignok securitytiltak i alle de fire transportgrenene ut fra egne initiativ, men disse er begrunnet ut fra ønsker om å forhindre vanlig kriminalitet som tagging, hærverk og vold.

To hovedprinsipper for terrorsikring

Sikring mot terrorhandlinger kan i prinsippet skje på to ulike måter. For det første kan man forsøke å sikre utvalgte objekter slik at potensielle terrorister enten avskrekkes fra å forsøke å angripe, eller slik at de vil bli avslørt før de får gjennomført angrepet. Dette har vært hovedprinsippet for sikring i luftfarten; alle

personer og all bagasje som skal om bord i fly må gå gjennom streng sikkerhetssjekk for å sikre at ulovlige og potensielt skadelig gjenstander ikke bringes om bord. Det innebærer imidlertid at også pilotene må gjennom sikkerhetskontrollen.

For det andre kan man forsøke å sikre seg gjennom spaning og overvåkning av potensielle terrorgrupper slik at man kan pågripe dem før de får anledning til å gjennomføre et angrep. En slik strategi basert på politimetoder, spaning, registrering og etterretning dreier seg ikke om å sikre bestemte objekter, men å slå til mot potensielle terrorister før de aksjonerer, uavhengig av hva slags mål de måtte ha for en aksjon.

Konflikt mellom personvern og terrorsikring

Begrepet personvern er knyttet til demokratiske verdier som rettssikkerhet og borgerrettigheter, blant annet retten til en privatsfære og til personlig integritet. Retten til personvern er nedfelt i Den europeiske menneskerettighetskonvensjonen av 1950 og i EUs personverndirektiv.

Personvern kan noe forenklet sies å bestå av vern av personers *integritet* og vern av *opplysninger* om enkeltpersoner. Integritetsvern tilsvarer det engelske begrepet *privacy protection*, mens opplysningsvern tilsvarer begrepet *data protection*.

Opprinnelig var begrepet personvern i stor grad assosiert med integritetsvern dvs. vern mot innsyn i privatlivet/privatsfæren. Etter hvert som elektroniske datalagringssystemer ble utbredt utover på 1970-tallet ble begrepet personvern i økende grad brukt i betydningen personopplysingsvern, dvs. i forhold til innsamling, registrering og bruk av personopplysninger i elektroniske systemer.

Objektkontroll utfordrer primært integritetsvernet

Begge strategier for sikring mot terror som er beskrevet har personvernimplikasjoner, men på forskjellige måter. Sikring av objekter gjennom passasjerskanning og lignende har først og fremst implikasjoner for integritetsvernet. Fysisk kontroll av passasjerer skal sikre ingen bringer inn ulovlige og farlige objekter. Kontrollen gjelder uansett, og det spiller i prinsippet ingen rolle hvem personen er. Objektkontroll er derfor i utgangspunkt uavhengig av personregistre og personopplysninger, og utfordrer dermed heller ikke personvernet i betydningen personopplysningsvernet.

Forebygging av terror utfordrer primært opplysningsvernet

Motsatt gjelder for forebyggingsstrategien som innebærer overvåkning og registrering av enkeltpersoner og grupper som av en eller annen grunn kan mistenkes for å utgjøre en terrortrussel. Det ligger i sakens natur at en slik strategi baseres på at man må samle inn og lagre en stor mengde opplysninger om en rekke personer som så danner grunnlag for eventuell tettere oppfølging gjennom spaning, avlytting osv. Denne strategien utfordrer dermed først og fremst personopplysningsvernet i og med at en mengde opplysninger om enkeltpersoner

innhentes og lagres. Strategien utfordrer også integritetsvernet, men først og fremst når det gjelder personer som blir underkastet detaljert oppfølging i form av avlytting osv. Folk som ikke blir fulgt opp slik opplever trolig i liten grad at registrerings- og overvåkningssystemer strider mot integritetsvernet.

I den grad objektkontrollen skjer ved hjelp av elektronisk apparatur eller det på annen måte registreres opplysninger med utgangspunkt i slik kontroll, er det grunn til å se integritetsvern og opplysningsvern i sammenheng. Bruk av biometriske metoder og forsøk med kroppsskannere tyder på at en slik sammenkopling av de to aspektene ved personvernet kan bli stadig viktigere.

Avveining mellom personvern og sikring

Personverninteressene

Personvernspørsmål blir i faglitteraturen ofte diskutert med referanse til den såkalte "interesseteorien". Denne teorien er et forsøk på å systematisere og konkretisere hva som skal forstås med personvern. I følge interesseteorien består personvernet av en rekke "enkelt-interesser" som til sammen kan antas å representere våre interesser når det gjelder personvern. I følge interesseteorien har vi følgende hovedkategorier av interesser knyttet til personvernet:

a) Interesse i å bestemme over opplysninger om egen person

b) Interesse i innsyn og kunnskap

c) Interesse i opplysnings- og behandlingskvalitet

d) Interesse i forholdsmessig kontroll

e) Interesse i brukervennlig behandling

f) Interesse i personvernanalyse

Punkt (a) innebærer at man ønsker å bestemme hvilke opplysninger om egen person som skal lagres og være tilgjengelig for myndigheter og andre. I svært mange sammenhenger ivaretas denne interessen av kravet om at individer må samtykke i at opplysninger om dem blir registrert. Punkt (b) innebærer at man skal ha innsyn og kunnskap om hvilke opplysninger om egen person som er registrert. Punkt (c) innebærer at man er interessert i at det ikke er ukorrekte opplysninger som er lagret, og at eventuelle feil blir rettet. Punkt (d) dreier seg blant annet om at det må være en forholdsmessighet mellom graden av informasjon om egen person som registreres og det formål opplysningene innhentes for. Det kan også dreie seg om at en form for kontroll skal nøye vurderes i forhold til andre mulige kontrollformer. Punkt (e) om interesse i brukervennlig behandling, innebærer at informasjon om registre, lagringsprosedyrer osv. skal være lett tilgjengelig og at reglene som regulerer dette skal være forståelige.

Punkt (f) "Interesse i personvernanalyse" er føyet til i denne framstillingen som en presisering av interesseteorien, med spesiell relevans for securitytiltak i transport. Dette dreier seg om at hensynet til personvernet skal være nøye vurdert når ulike tiltak, som for eksempel securitytiltak i transportsektoren planlegges og

implementeres. Det innebærer for eksempel at ordinære krav til utredning av konsekvenser bør gjennomføres ved implementering av securitytiltak, at tiltakene skal være underlagt løpende kontroll, og at slike tiltak bør evalueres både med hensyn til effekt og kost/nytte, både på individ- og samfunnsnivå.

Terrorsikring truer personverninteressene

Det er nokså innlysende at alle punktene (a)-(f) i mange tilfeller ikke oppfylles når det gjelder securitytiltak. Som nevnt vil særlig overvåkningsstrategien måtte innebære hemmelig registrering av personopplysninger. Det innebærer registrering uten samtykke og med svært begrensete muligheter for å få innsyn i hvilke opplysninger som er registrert om egen person. Det innebærer også at interessen i opplysnings- og behandlingskvalitet rammes. Dersom enkeltpersoner ikke selv får anledning til å kontrollere hvilke opplysninger om dem som er registrert, vil mulighetene for å rette opp feil også bli svært mye dårligere.

Vilkårene for å imøtekomme interessen i forholdsmessig kontroll blir også nokså magre når hver enkelt ikke vet hvilke opplysninger som er registrert. Når formålet med overvåkning er å forebygge mulige terroraksjoner, blir også behovet for informasjon åpent; det er nesten umulig på forhånd å vite hvilken informasjon som vil være relevant. Da blir det også omtrent umulig å bestemme om informasjonsinnhentingen står i et balansert forhold til formålet.

Brukervennlig behandling er også svært vanskelig å imøtekomme når det gjelder securitytiltak. Som nevnt er det meste av som skjer på denne fronten i Norge implementering av internasjonale bestemmelser. For eksempel er de internasjonale reglene når det gjelder forebygging av anslag mot sikkerhet i luftfarten nedfelt i en egen forskrift til luftfartsloven. Denne forskriften peker til fem EU-forordninger og gir supplerende bestemmelser til disse. Flere av disse forordningene er blitt endret en rekke ganger, samtidig som flere av dem har vedlegg som er klassifiserte og unndratt offentligheten.

Hemmelighold og begrensede innsynsrettigheter bryter på grunnleggende måter med den ideologi som ellers har vært lagt til grunn på personvernområdet. Det som trer inn i stedet er en forhåpning om at myndigheter og ulike kontrollaktører opptrer innenfor rammene av grunnleggende menneskerettigheter og i samsvar med gjeldende nasjonale rettsregler. Tillit uten grunnlag for å etterprøve tilliten på grunn av hemmelighold er imidlertid problematisk i en demokratisk rettsstat.

Gjennomgangen av interesseteorien viser at tiltakene som iverksettes mot mulige terrorangrep både i transportsektoren og på andre områder, omtrent uten unntak kommer i konflikt med prinsippene om personvern. Det er imidlertid til en viss grad mulig å kompensere for dette gjennom forsterkede rettssikkerhetsgarantier.

Mye av rettsreguleringen når det gjelder personvern og sikring er prosedyreorientert til forskjell fra misbruksorientert. Det betyr at lovgivningen som for eksempel personverndirektivet, angir hvilke framgangsmåter som skal følges. En detaljert konkretisering av for eksempel hvilke personopplysninger som kan innhentes, brukes og registreres i tilknytning til kontroll av personer i for eksempel transportsektoren, vil gjøre kontrollen mer forutsigbar og mer etterprøvbar, og slik sett blir kontrollregimet mer akseptabelt i forhold til personvernhensyn og rettssikkerhet.

Et annet aspekt ved en slik prosedyreorientert tilnærming innebærer å ta i bruk teknologi og metoder som i størst mulig grad anonymiserer eller pseudonymiserer kontrollobjektene. Sikkerhetskontroll bør med andre ord i størst mulig grad skje uten at personers (virkelige) identitet avsløres. Ut fra hensynet til personvern kan maskinell tilgang til personopplysninger være å foretrekke framfor manuell tilgang. Årsaken er at personvernet kan sies å være mest krenket når personopplysninger kommer til menneskers kunnskap.

Det ligger i sakens natur at tiltak mot terror dels må baseres på hemmelig overvåkning og registrering. For å kompensere for dette kan man stille skjerpede regler både til framgangsmåte, behandling og lagring av slike opplysninger. Det kan for eksempel tenkes forbud mot at transportselskaper innhenter og bruker opplysninger i vandelsattester som er eldre enn fem år; krav om at visse minimumsbetingelser når det gjelder identifisering og autentisering må være oppfylt for å kunne legge noe frem som en personopplysning i en sak; rett til å få uavhengig sakkyndig granskning av informasjonssystemer som har generert ufordelaktige personopplysninger og klarlegging av straffeansvar for ulovlig innhenting og bruka av personopplysninger.

Norske transportaktørers syn på sikring og personvern

Representanter fra de fire transportgrenene samt fra relevante myndighetsorganer ble stilt en rekke spørsmål om securitytiltak som er gjennomført i ulike virksomheter. Det ble spurt om personvernimplikasjoner av securitytiltakene, om hvordan hensyn til personvern og security balanseres og hvordan arbeidet med security er forankret i organisasjonen.

Representanter fra følgende instanser/virksomheter ble intevjuet: Oslo T-banedrift, Oslo Havn, E18 Bjørvika, Datatilsynet, Nasjonal sikkerhetsmyndighet, Kystdirektoratet, Jernbaneverket, NSB, Luftfartstilsynet og Vegdirektoratet.

Særtrekk ved transportgrenene bestemmer security-nivået

Respondentene ga klart uttrykk for at særtrekk ved de ulike transportgrenene har avgjørende betydning for hvor mye fokus en har på terrorsikring. Et moment som ble trukket fram er at massetransportmidler i storbyområder har så mange passasjerer, avganger og holdeplasser at det er praktisk umulig å innføre et securityregime slik man har i luftfart. Også de rene bedriftsøkonomiske kostnadene ved dette vil være langt større enn hva man kan klare.

Det er også avgjørende forskjeller mellom transportnettverkene som de ulike transportgrenene opererer i. Luftfart er kjennetegnet av sentralisert punkt-til-punkt trafikk, der lufthavnene er plassert utenfor øvrige knutepunkter og dermed lettere å skjerme rent fysisk enn for eksempel jernbane og T-bane. Veitrafikk kjennetegnes ved en eksterm grad av åpenhet og det er omtrent umulig å tenke seg adgangskontroll for å delta i veitrafikken.

Et annet og beslektet element dreier seg om hvor integrert transportsystemene er med øvrig samfunnsliv og hverdagsliv. At hyppige trikkeavganger gis betegnelsen ”rullende fortau” illustrerer hvordan trikk (buss og T-bane) oppleves som en

integrert del av bysamfunnet. Massiv sikkerhetssjekk av passasjerer oppleves som uforenlig med et levende bysamfunn.

Flere informanter peker også på at det er store forskjeller i risikoaksept mellom transportgrener. Luftfart skiller seg ut med ekstremt lav risikoaksept og med tilsvarende høye security-kostnader. Flere peker på at sikkerheten for samfunnet som helhet ville øke om man flyttet ressurser fra securitytiltak i luftfarten over til ordinære trafikksikkerhetstiltak i veisektoren.

Mange peker også på at de forskjellige transportgrenenes institusjonelle forankring og regelverk i stor grad påvirker hvilket spillerom virksomhetene i de ulike transportgrenene har i valg og utforming av security-tiltak. Særlig sjøfart og luftfart er kjennetegnet av at de enkelte virksomheter må implementere internasjonalt regelverk.

Personvernimplikasjoner for egne ansatte og for trafikanter

Aktørene har ulike oppfatninger både når det gjelder *om* tiltakene de har gjennomført har personvernimplikasjoner og *hvem* de har implikasjoner for. Særlig i veisektoren oppleves personvernspørsmål i større grad å være en aktuell problemstilling når det gjelder egne ansatte enn når det gjelder trafikantene. I luftfart er oppfatningen at det er passasjerenes personvern som berøres av security-tiltakene.

Datatilsynet opplever at man i luftfart er svært bevisst spørsmål om personvernimplikasjoner av ulike tiltak, men at dette ikke gjelder i de andre transportgrenene. I luftfart er det særlig sikkerhetskontrollen av passasjerer som har personvernimplikasjoner. T-banen gir uttrykk for at de tradisjonelt er meget forsiktige når det gjelder tiltak med personvernimplikasjoner og at de følger myndighetenes krav. For Oslo Havn er hovedfokus å innføre internasjonale bestemmelser når det gjelder sikring, og personvern er ikke spesielt fokusert. Statens vegvesen er først og fremst opptatt av personvernspørsmål knyttet til trafikksikkerhetstiltak som innebærer overvåkning, og da særlig såkalt ”streknings-ATK”. I arbeidet med senketunnelen i Bjørvika i Oslo er det innført adgangskontroll og andre sikringstiltak, men personvernspørsmål har fått lite oppmerksomhet. Jernbaneverket forvalter infrastruktur og er i den forbindelse i liten grad involvert i spørsmål med personvernimplikasjoner, men opplever at slike spørsmål er relevante når det gjelder egne ansatte i forbindelse med sikkerhetsklarering av medarbeidere. NSB er klar over personvernimplikasjonene av kameraovervåkning og har bevisst valgt teknologi og prosedyrer for å minimere personvernimplikasjonene. Også i NSB er personvernspørsmål i stor grad rettet mot vern av ansatte.

Det generelle inntrykket er at personvern ikke er gjenstand for stor oppmerksomhet i norske transportvirksomheter, men at de ulike aktørene har vurdert personvernimplikasjoner av tiltak i egen virksomhet. Ingen mente at avveining mellom personvern og security var noe stort problemområde. Datatilsynet har stanset en del tiltak, men dette har i første rekke vært tiltak som har hatt andre formål enn terrorsikring.

Oppfatninger av security og safety i dag og i framtiden

Distinksjonen mellom safety og security er kjent i norske transportvirksomheter. Mange inkluderer sikring mot ordinær kriminalitet som hærverk, tagging, tyveri osv. i security-begrepet. Mange opplever også at det er tett sammenheng mellom safety og security; securitytiltak kan ha positive sideeffekter for safety. I forbindelse med beredskapsplaner oppleves distinksjonen safety/security som lite hensiktsmessig. Hvis en brann bryter ut må man ha beredskap til evakuering/slokking uavhengig av hva årsaken til brannen er.

De viktigste security-tiltakene med implikasjoner for personvern som er gjennomført blant norske transportvirksomheter er: kameraovervåkning av transportmidler og infrastruktur, informasjonstiltak og opplæring, adgangskontroll for passasjerer og ansatte og inspeksjoner og fysisk sikring av transportmidler og infrastruktur. Alle nevner også nær kontakt med politiet gjennom PST. Avanserte overvåkningssystemer som automatisk ansiktsgjenkjennelse, avanserte røntgenløsninger osv. ble opplevd som lite relevante, bortsett fra i luftfart der løsninger basert på biometri trekkes fram.

Organisatorisk er security plassert i tradisjonelle safety-avdelinger i T-banen, i Jernbaneverket, i NSB og Vegdirektoratet. Også i Kystdirektoratet og i havnevesenet er security og safety integrert i de samme enhetene. I Luftfartstilsynet er imidlertid dette delt der en egen avdeling arbeider med security, atskilt fra safety-spørsmål.

Alle transportgrenene arbeider systematisk med sikkerhetsspørsmål blant annet gjennom å utarbeide Risiko- og sårbarhetsanalyser (ROS). Terrortrusselen inngår som en del av trusselbildet. Tiltak mot terrortrusselen har som positiv sideeffekt at også ordinær kriminalitet blir redusert.

De fleste aktørene ser et behov for bedre koordinering av securitytiltak mellom transportgrener, men ikke behov for et felles regelverk på security-feltet. De fleste mener overvåkningen vil tilta i årene som kommer, men ser ikke for seg at ”flyplasslignende tilstander” vil komme i andre transportgrener, bortsett fra når det gjelder sjøtransport/havnesikring.

Security, effektivitet og rettssikkerhet

Det er begrenset fokus på terror og personvern i norsk transport. Det meste av terrorsikringen skjer som følge av internasjonale forpliktelser, og det er i de transportgrenene som tradisjonelt har vært regulert gjennom internasjonale avtaler – luftfart og sjøfart – hvor også security-tiltakene er innskjerpet og utvidet de senere år. Sikkerhetssjekken på flyplasser er for eksempel blitt betydelig skjerpet.

Ansvaret for security-tiltak er i stor grad organisasjonsmessig plassert i de samme enhetene som har ansvaret for ordinære sikkerhetstiltak (safety), og det er i stor grad den samme type hendelsesbaserte sikkerhetstenkningen som benyttes i utformingen av tiltakt mot terror. Det innebærer imidlertid at man overser at terroraksjoner gjennomføres at personer som tilpasser angrepet til de sikringstiltakene som gjennomføres, og som vil velge å angripe der man minst venter det. Det innebærer igjen at hendelsesbasert sikkerhetstenkning er av svært

begrenset relevans når man står overfor mulige terroraksjoner. Og det betyr at ytterligere sikring av objekter som alt er godt sikret ikke har særlig effekt.

Fra et samfunnsmessig synspunkt virker det nokså åpenbart at det ikke er en rasjonell balanse mellom tiltakene som settes i verk i luftfarten og mangelen på tiltak i andre transportgrener. Det fremstår i dag som litt av et tankekors at man ikke kan ta med vannflasker om bord i fly, mens det ikke foregår noen som helst kontroll passasjerer eller bagasje på tog og T-bane.

Objektsikring er derfor i beste fall ”lokalt” rasjonelt og kan bidra til å flytte risikoen til andre objekter som er dårligere sikret. For samfunnet vil imidlertid en strategi basert på objektsikring både være kostbar og lite effektiv. For mange transportvirksomheter – særlig veitrafikk og kollektivtransport i storbyene – er det ikke mulig å sikre seg mot terrorangrep gjennom tradisjonelle objektsikringstiltak. Erfaringer fra andre land viser også at i den grad man har lyktes i antiterrorarbeidet, så er det særlig gjennom forebygging av terrorangrep gjennom spaning og overvåkning at dette har skjedd.

Sikkerhetssjekk for å sikre bestemte områder eller objekter, slik man har i sikkerhetssjekken på flyplasser, har klare implikasjoner for personvernet i betydningen integritetsvern. Kroppsskanning og kroppsvisitasjon vil lett oppleves som inngrep i den enkeltes private sfære. Terrorsikring gjennom overvåkning og registrering av mistenkelige personer vil imidlertid kunne ha enda mer alvorlige konsekvenser for personvernet. Ikke bare vil slik overvåkning og registrering kunne omfatte veldig mange personer, registrering av informasjon innebærer også lagring i databaser med en rekke muligheter for å kobling av informasjon, for lekkasjer, for feilregistreringer mv. Fordi objektsikring bare er realistisk å gjennomføre innen luftfart og sjøfart, kan omfattende overvåking og registrering tenkes som strategi for å kompensere for manglende kontroll med reisende på tog, T-bane og buss mv. Et slikt valg vil ha store og alvorlige implikasjoner for personvernet.

Dersom vi gir kontrollører vide fullmakter til å gjennomføre kontroller som krenker personvernet, oppstår det også viktige spørsmål vedrørende tilstrekkelig kontroll med kontrollørene. Det er lett å tenke seg at det vil kunne utvikle seg egeninteresser knyttet til trusselnivået som vil være spesielt problematiske fordi det i stor grad er de samme enhetene som til enhver tid bestemmer trusselnivået, som også får tilført ekstra ressurser når trusselnivået øker. Det er godt mulig at dette til nå ikke har vært noe problem, men uansett er konstellasjonen uheldig; det er lett å mistenke at for eksempel sikkerhetstjenesten kan se seg tjent med å gi uttrykk for at terrortrusselen er høyere enn den faktisk er.

Dette er ikke bare utfordringer for personvernet, men for hele vår demokratiske rettstradisjon. Hemmelig politi med utvidete fullmakter og monopol på informasjon om trusler er noe vi ikke assosierer med rettsstaten. Spørsmålet som må stilles er om truslene vi står overfor kan forsvare slike brudd på demokratiske rettsstatsprinsipper.

TØI report 914/2007
Authors: Torkel Bjørnskau, Mattias Gripsrud Tonje Grunnan
Tore Leite Dag Wiese Schartum
Oslo 2007, 108 pages Norwegian language

Summary:

Transport security and the protection of privacy

Security increase after 9/11 2001

The 9/11 terrorist attacks in the US have resulted in a number of new regulations and anti-terrorist measures in the transport sector. The added effects of subsequent attacks, against the railway in Madrid in 2004 and against bus and underground transport in London in 2005, together with revelations of terrorist bomb plans, such as those against transatlantic flights in 2006, have put security high on the agenda and resulted in a number of new anti-terrorist measures. Some of the most important of these are:

- intensified security checks of passengers and baggage at both international and national airports;
- introduction of biometric passports (mandatory for entry to the US);
- obligatory handover from airlines to American authorities of passenger lists with personal information;
- regulations and checks to prohibit the carrying on-board of more than 10 ml liquid (including bottled water) from outside the airport;
- testing of invasive whole-body scanners to check passengers (for instance at Chisholm airport, Amsterdam);
- introduction of fingerprint registration to check consistency between the those passengers boarding planes and those checking in baggage;
- intensified security demands for ships and ports including terrorist alarms, on-site checks, obligatory security plans and security equipment;
- stricter demands on securing ports and port areas by measures such as fences or admittance checks (the ISPS-code);
- stricter identity-card requirements for ship and port workers;
- security checks of employees in transport companies (control of personal history);
- security control of containers, scanning techniques, development of smart containers (RFID-marking), satellite based tracking systems and so on; and
- attempts at airport-style security checks on the London underground.

The report can be ordered from:
Institute of Transport Economics, Gaustadalleén 21, NO 0349 Oslo
Telephone: +47 22 57 38 00 Telefax: +47 22 60 92 00

Such measures imply that increased security efforts have been focused mainly within aviation and shipping, the two main transport modes in which security has been high on the agenda for a long time. It seems that the new terrorist threat has been given most attention in domains where there already existed high-profile security efforts, and that the threats have been countered to a lesser extent in those modes of transport in which security has traditionally had a less elevated profile.

Across all four main transport modes efforts exist whose primary aim is not to secure against terrorist attacks, but which nevertheless can be used to help unravel terrorist plans and prevent terrorist acts. One example of this is the use by British police of the system known as Automatic Plate Number Recognition (APNR) to track down one of the suspects of the car bombs at airport terminals in London and Glasgow in the summer of 2006. Other measures open to exploitation by the authorities for use in anti-terrorist activity include surveillance or registration of persons or vehicles, where the primary aim is to enforce speed limits and avoid petty crime; camera surveilance of terminals, vehicles, infrastructure and station areas (camera surveillance of public places is particularly widespread in Great Britain, but it has increased also in Norway over later years); automatic registration systems that register vehicle passes on toll spots (AutoPass); electronic tickets; intelligent speed adaptation (ISA); systems that automatically alert ambulance and police of road accidents (e-call); and automatic trip recorders in cars ("black boxes"). In Norway, there are plans to introduce automatic speed control over longer stretches of roads, using two or more speed cameras to estimate average speeds over the distances. In fact, within road traffic there are lots of new technological devices being developed and introduced to guide and control traffic, and it is not difficult to envisage their potential use in anti-terrorism efforts.

In light of this, these latter measures and systems can be considered alongside those more direct anti-terrorist measures as having obvious and important implications concerning the protection of privacy and data.

Anti-terrorism security in Norwegian transport – adaptation to international regulations

Security measures against terrorist acts in Norwegian transport are almost exclusively implemented as a consequence of international regulations. Aviation and shipping are the transport modes with the most comprehensive international regulations administered by ICAO, IMO and, increasingly, the EU, and it is within these transport modes that security efforts against terrorism have been intensified in Norway and most other western countries.

There are few independent Norwegian initiatives on anti-terrorist security measures in transport. The main aim of any security efforts that are implemented is to reduce ordinary crime, like vandalism and violence, and not to secure against terrorist acts.

Two main strategies for anti-terrorism security

There are two main strategies for security against terrorist acts. The first is that one can try to secure threatened objects and thus deter or prevent terrorist attacks. This is the main security principle in aviation, where all persons and all baggage must pass strict security checks in order to make sure that illegal and potentially harmful objects are not brought on-board planes. This strategy is very restrictive, however, meaning that even pilots must pass the security checks.

The second strategy involves securing against terrorist attacks by way of police methods such as surveillance of potential terrorist groups. The aim here is to take action against potential terrorists before they are able to attack. Such a strategy is more general in that it does not aim at securing specific objects, but rather at arresting the terrorists regardless of the object they plan to attack.

Conflict between security and the protection of privacy

The notion of the protection of privacy is associated with core democratic values such as civil rights and legal protection. It is concerned with the right to personal privacy and integrity, as stated in the Euorpean Convention on Civil Rights and in the EU's Directive on the protection of personal data.

The term "privacy protection" is normally associated with the protection of personal integrity, whereas the term "data protection" connotes the protection of information of individuals. Originally, the focus was mainly on privacy protection, but with the introduction of computers and data storing facilities during the 1970s, data protection came increasingly into focus.

Security checks challenge personal integrity

The two security strategies mentioned above have different implications for privacy protection. Objects are secured by way of admittance control through physical scanning or inspection to prevent people from bringing in weapons or other illegal objects into a secure area. Such security checks threaten the protection of privacy mainly by challenging personal integrity. Physical checks or the use of scanning technology may be perceived as an invasion of privacy.

On the other hand, because security checks apply to all (it does not matter who the persons are), the strategy of securing objects by way of security checks is independent of person information and person registers. Thus, data protection rights are not challenged by security checks.

Surveillance and registration challenge data protection rights

It is clear that regstration and surveillance of people considered to be a security threat can violate their data protection rights. Such a security strategy must be based on the collection and processing of vast amounts of data that may lead to closer scrutiny of persons and groups by way of surveillance, stakeout and so on.

This strategy challenges mainly data protection rights in that a lot of personal information is collected, processed and stored. The right to personal integrity might also be considered violated for people subjected to closer scrutiny, but the majority of people, who are not examined closely, would probably not consider the surveillance and registration systems as a threat to their personal integrity.

To the extent that object control is accomplished by use of electronic equipment, or there are other types of information collection during security checks, data protection rights and personal integrity rights should be considered together. The use of for instance biometric methods and body scanners suggests that there will be closer links between these two aspects of personal privacy issues in the future.

Balancing security with the protection of privacy

The interest in privacy protection

Questions about privacy protection in the scientific literature often refer to the so-called ”Theory of interests”. This theory is an attempt to systematise and delineate the notion of privacy protection. The theory of interests consists of a number of specific interests that, when considered together, are assumed to represent our interest in the protection of our privacy. According to the theory of interests we have the following main categories of interests:

a) The interest in deciding about information concerning oneself.

b) The interest in inspection and knowledge.

c) The interest concerning the quality of information and information treatment.

d) The interest in balanced control.

e) The interest in user-friendly treatments.

f) The interest in person privacy analysis.

Point (a) implies that we have an interest in deciding what type of information about ourselves is going to be available to the authorities and others. In many respects this interest is looked after by the obligatory demand that people must consent to having their personal information collected and stored. Point (b) implies that individuals must have access to and knowledge about any of their personal information collected and stored. Point (c) states that as individuals it is also in our interest that the quality of the information collected and the treatment of this information is good. This also implies that it is possible to correct errors in the information collected. Point (d) maintains that there must be a balance between the type and amount of information collected and the purpose of the data collection. This point also implies that alternative and less thorough registration and control should always be considered.

Point (e) about user-friendly treatment implies that information about relevant registers, about procedures for data collection and data storage, about the governing rules and legislation should all be easily accessible and intelligible.

Point (f) ”Interest in privacy analysis” is added here as a specification of the interest theory with particular relevance to security measures in transport. This implies that considerations of privacy should be closely addressed when measures (such as security measures in the transport sector) are planned and adopted. It follows for instance that traditional impact assessment studies should be carried out when security measures are adopted, that the measures should be subject to consecutive control, and that cost/utility studies of the counter-measures should be carried out.

Security measures against terrorist attacks may threaten privacy rights

It seems rather obvious that in many cases points (a)-(f) are violated when anti-terrorism security measures are adopted. As noted, the surveillance strategy in particular requires secret registration, which is registration without consent and without any opportunity for the person being registered to gain knowledge about the information collected. Secret registration implies violation of not only data protection rights but also the interest in the quality of information and information treatment. When the persons themselves are not allowed to check the information collected, they cannot of course correct it for mistakes and errors.

The likelihood of achieving balanced control is also rather slim when one does not know what information is collected and stored. This is a particular problem when the aim is to secure against terrorist attacks where it is almost impossible to know beforehand what information might become relevant. Consequently, it is impossible to decide whether the informtion gathered is in balance with the aim of the registration.

User-friendly treatment is also hard to achieve where security measures are concerned. As noted, most security measures adopted in Norway are implementations of international regulations. The international regulations to prevent terrorist attacks against civil aviation were adopted through amendment to the Norwegian Aviation Act. This amendment addresses five different EU decrees and gives supplementary rules to these. Several of the decrees have been altered repeatedly and several have appendices that have been classified as closed to the public.

Secrecy and limits to insight violate fundamentally the principles that otherwise dominate the areas of data and privacy protection. What replaces them is merely the hope or expectation that authorities and control actors will behave according to human rights principles and according to national law. However, to trust actors to behave according to the law without being able to check their actions because of secrecy is a severe problem within a democratic constitutional state.

The comments on the theory of interests presented above clearly show that the security measures adopted within the transport sector, and within other areas, almost without exception violate the principles of personal privacy and data protection. It is, however, to some extent possible to compensate for this by strengthening legal protection.

Much of the law concerning privacy and data protection rights already comes in the form of procedural rules and principles that describe the proper way to collect

personal data. Modification of these regulations to effect a very specific description of what personal information can be collected, used and registered in order to conduct security checks for instance in the transport sector would make the control process more predictable and easier to check, and thus make the control regime more acceptable according to privacy and data protection rights.

An added advantage of such a procedural approach is that it implies the utilisation of technology to the greatest extent possible to make the control objects anonymous or pseudonymous. Security checks should accordingly to the greatest extent possible be carried out without revealing a person's (real) identity. From the perspective of personal privacy one may argue that personal data should be collected electronically and/or automatically rather than manually. The reason is that privacy rights are better fulfilled when the information is not available to other persons.

Naturally, security measures against terrorist attacks must at least partly be based on secret surveillance and registration. In compensation one may adopt stricter rules concerning the procedures, the treatments and the storage of person information. For instance, one can possibly ban the use of certificates of conduct older than five years, adopt minimum standards of identification and authentication when a case is brought to trial, guarantee independent expert scrutiny of information systems that have provided unfavourable information, and identify legal responsibilities for unlawful collection of person information.

Views of Norwegian transport actors on security and the protection of privacy

Representatives from the four major transport modes, together with representatives from relevant authorities, were interviewed about security measures adopted in the transport sector. They were asked about possible implications for personal privacy and data protection, how they weigh security and privacy issues against each other and how security issues are founded in their organisation.

Representatives from the following organisations/bodies were interviewed: Oslo T-banedrift (The Oslo Underground), Oslo Havn (Oslo Port), E18 Bjørvika, (Project organisation within the National Road Administration being responsible for the construction of the subsea Bjørvika-tunnel in Oslo), Datatilsynet (The Data Inspectorate) Nasjonal sikkerhetsmyndighet (The Norwegian National Security Authority), Kystverket (The Norwegian Coastal Administration), Jernbaneverket (The Norwegian National Rail Administration), NSB (The Norwegian State Railways), Luftfartstilsynet (The Civil Aviation Authority) and Vegdirektoratet (The Directorate of Public Roads/National Roads Administration).

Differences between transport modes determine security efforts

The respondents were of the opinion that differences between the transport modes were of great importance for the level of security attention. One aspect mentioned was that urban mass transport has so many passengers, departures and stops/stations that it is practically impossible to adopt an aviation-style security

regime. Such a regime would also be far too costly for most urban transport companies.

Profound differences were observed between the transport networks that the different transport modes operate in. Aviation is characterised by centralised point-to-point traffic, where airports are placed outside of central junctions and thus much more easy to secure physically than, for instance, railways and underground systems. Road traffic is characterised by very open access and it is almost impossible to imagine security checks and control of access to the road system.

A related aspect concerns the level of integration of the transport system with society and everyday life. Tram lines with frequent departures in Oslo are called ”rolling pavements” which illustrate how trams (and buses/underground) are perceived as an integrated part of city life. Massive security checks of passengers is something that is perceived as incompatible with a vital city life.

Several respondents also pointed out that there are huge differences in risk acceptance between transport modes. Aviation deviates from the other modes in its very low level of risk acceptance and consequent high security costs. Several respondents argued that safety for society as a whole would increase if resources were transferred from security measures in aviation to ordinary safety measures in road traffic.

Several respondents also maintained that the institutional basis and governing rules of different transport modes influenced to a very large degree the scope for instigating and adopting security measures. For instance, aviation and sea transport are heavily regulated by international agreements and the different transport companies and infrastructure administrations have no choice but to comply with these international rules.

Privacy implications for employees and transport users

The respondents have different perceptions both regarding *whether* the measures implemented have privacy implications, and for *whom* they have implications. Within road transport privacy questions are perceived as more relevant to employees than to road users. Within aviation, however, privacy issues in association with security measures are perceived as something mainly affecting the passengers.

The impression of The Data Inspectorate is that actors within aviation are very much concerned about questions regarding personal privacy when implementing safety and security measures. Similar concerns do not seem to be present within the other transport modes. It is of course mainly the security checks at airports that have privacy implications.

The Oslo Underground maintain that they are traditionally cautious when it comes to measures with implications for personal privacy, and that they abide by the rules. For Oslo Port, however, the main focus is to implement international regulations concerning port and ship security and questions regarding personal privacy are not much discussed.

The Norwegian Road Administration is mainly concerned with privacy issues regarding road safety measures where some kind of traffic surveillance is involved. This is particularly relevant to current 'hot' issue of speed enforcement by use of speed cameras calculating average speeds for single drivers over a specific stretch of road. The sub-sea tunnel project in Oslo has introduced access control to the site, and other security measures, but privacy issues have not been addressed to any large extent.

The Norwegian National Rail Administration (Jernbaneverket) manages infrastructure and is in that respect not much involved in privacy related issues. They nevertheless feel that such questions are relevant when it comes to security clearance of employees.

In the Norwegian State Railways (NSB) one is aware of the privacy implications of camera surveillance and has deliberately chosen equipment and procedures in order to avoid violations of privacy protection and data protection rights. Nevertheless, privacy issues are for the most part seen as relevant to their own employees.

The general impression is that privacy issues are not high on the agenda in Norwegian transport companies, but that actors have considered privacy implications of measures within their own organisation. No respondent felt that balancing privacy rights and security needs was a particularly big problem. The Data Inspectorate has intervened to prevent the use of some measures, but these measures have mainly been directed towards threats other than possible terrorist acts.

Perceptions of security and safety today and in the future

Norwegian transport companies are familiar with the distinction between safety and security. Some include measures against ordinary crime, such as vandalism, tagging (graffiti) and theft, in the security concept. Many feel that there is a close connection between safety and security, that security measures can have positive effects on safety. As regards emergency and evacuation plans, the distinction between safety and security is irrelevant: if fire starts one needs to have staff and equipment to put it out regardless of its cause.

The most important security measures with privacy implications that have been implemented are: camera surveillance of transport means and infrastructure, information measures, training, access control of passengers and employees, and inspection and physical protection of transport means and infrastructure. Everyone also mentioned close contact with the secret police service (PST). Advanced security measures like automatic face recognition systems, advanced x-ray equipment etc. were perceived as not very relevant, apart from in aviation, where respondents argued that security measures based on biometrics are of high interest.

Administratively, security is organized within traditional safety units both in Oslo Underground (T-banen), in the Norwegian National Rail Administration (Jernbaneverket), in the Norwegian State Railways (NSB) and in the Directorate of National Roads (Vegdirektoratet). Within the Norwegian Coastal Administration (Kystverket) and the Port Authorities (Havnevesenet), security

and safety are also placed together within the same units. However, in the Civil Aviation Authority, these issues are separated with a special unit responsible for security issues.

Within all transport modes, safety is systematically and continuously dealt with, for instance by use of risk and vulnerability studies. Possible terrorist attacks are a part of the threat scenario. Counter-measures against terrorist attacks have had the favourable side-effect of reducing ordinary crime.

Most actors identify the need for better coordination of security measures across transport modes, but they do not see the need for common intermodal regulations in this field. Most actors expect surveillance to increase in the years to come, but they do not envisage ”airport-like” security systems implemented in other transport areas, with the exception of sea transport and port security.

Security, effectiveness and legal rights

Terrorist threats and privacy protection issues are not high on the agenda in Norwegian transport. Most anti-terrorism security measures are implemented as part of adherence to international regulations, and transport modes that traditionally have been characterized by a lot of international regulations – aviation and sea transport – are also the ones where security measures have been most intensified and expanded recently.

Responsibility for security measures is to a large extent placed administratively in the same units that deal with ordinary safety issues. Further, these units carry out to a very large degree the sort of incident-based (i.e. after-the-event) counter-measures that are typical of ordinary safety work. These sorts of measures dominate security planning against terrorist attacks. Consequently, one ignores the fact that terrorists may select the targets where security is poorest. Incident-based security policies will normally have limited relevance when faced with possible terrorist attacks. Furthermore, it follows that strengthening security to already protected objects will have only a limited effect.

From a societal view it seems rather obvious that the heavy security regimes in aviation are out of proportion to the almost total lack of security efforts in other transport modes. It is a paradox that you cannot bring ordinary water bottles on planes and at the same time there is no security check, either of passengers or baggage, on the train or underground.

To secure specific objects against terrorist attacks is at best only “locally” rational. It may in other words merely transfer the risk to other objects less well secured. To society at large a strategy based on object protection will be both costly and of limited effect. In some transport modes, especially road traffic and public transport in urban areas, it will not be possible to protect the public effectively with such a strategy. Furthermore experiences from abroad indicate that effective counter-terror policies must be based on police methods like surveillance if terrorist attacks are to be prevented.

Security checks to protect specific areas or objects, such as security checks at airports, have obvious privacy implications. Body scanners, and body searches may be experienced as a violation to personal integrity. However, security

policies based on surveillance and registration of potential terrorists may have even more severe implications to privacy and data protection. Surveillance and registration will not only include data collection of a huge number of persons but implies data storage in data bases with the potential to link data from different sources, to leak information to unauthorized persons, to make incorrect registrations etc.

Securing specific areas or objects by access control and security checks is only a realistic option within aviation and sea transport. To secure other transport areas a comprehensive surveillance strategy may be envisaged. Such a choice, will however, have severe implications to privacy and data protection.

Giving controllers wide authorisation to collect and check information about us raises questions about how to control the controllers. One can easily imagine that controllers may see a certain level of terrorist threat to be in their own interest, in that more resources may be allocated to security as a consequence. While we have not experienced such problems to date, the situation is clearly far from ideal. It is easy to suspect that the security services overstate the terrorist threats.

These are not only challenges to privacy and data protection but rather to our democratic legal tradition. Secret police with wide authority and a monopoly on the information about terrorist threats, is something we do not associate with democratic legal states. Thus we must ask whether the actual threats we face can justify severe violations of privacy, data protection and legal rights.

1 Innledning

1.1 Bakgrunn

I luftfarten og til dels også for transport til sjøs, har overvåkning, kontroll og behandling av personopplysninger vært en del av det internasjonale sikkerhets-regimet i lang tid. Også på jernbane- og T-banestasjoner har kameraovervåkning etter hvert blitt ganske vanlig for å forebygge hærverk og vold. Alle slike tiltak, som er innført for å øke sikkerheten for mennesker og materiell, innebærer samtidig at en mengde personopplysninger registreres og lagres noe som kan være en trussel mot personvernet. Retten til personvern er nedfelt i den europeiske Menneskerettighetskonvensjonen av 1950, og i EUs personverndirektiv.

Etter terroranslaget mot USA 11. september 2001 er tiltak mot terror betydelig skjerpet, og det er innført omfattende sikkerhetstiltak i ulike deler av transportsektoren, særlig innen luftfart og i sjøfart. Eksempler på dette er overføring av opplysninger om europeiske flypassasjerer til USA og innføring av identifikasjonskrav for sjøfolk. Terroraksjonene i Madrid 11. mars 2004 og i London 7. juli 2005 viste at også andre deler av transportsektoren er svært følsomme for sabotasje og terroraksjoner. Hendelsene har ført til en allmenn oppfatning om at det er behov for økte sikkerhetstiltak i transport også i Norge (DSB 2004). Terroraksjonen mot T-banen i London var for eksempel den direkte foranledningen til den omfattende terrorøvelsen i Oslo høsten 2006.

For luft- og sjøfarten kan ytterligere innskjerping av sikkerhetskravene ses på som en skjerping av de tiltakene som allerede er gjennomført i nasjonal og internasjonal lovgivning. Nye tiltak innen veitransport, jernbane og kollektiv-trafikk kan bli vurdert innført etter de samme prinsippene for transportsikring som i sjø- og lufttransport (derStandard 2005). Økte sikkerhetskrav innen disse transportgrenene vil kunne innebære omfattende utvidelser av overvåkning, kontroll og behandling av personopplysninger. Sikringstiltak som hver for seg kan begrunnes ut fra de enkelte transportgrenenes sikkerhetskrav, kan i sum medføre omfattende endringer av personvernets stilling i de europeiske landene.

Det vil være en utfordring for transportmyndighetene å imøtekomme krav om sikring av transportsektoren og samtidig ivareta sentrale personvernhensyn. Denne utfordringen reiser en rekke viktige spørsmål. Er det for eksempel grunnleggende forskjeller mellom luft- og sjøtransport og de øvrige transportgrenene som tilsier at personverninteressene bør tillegges ulik vekt? Kan et tilstrekkelig sikkerhetsnivå i transportsektoren dekkes med tiltak som ikke kommer i konflikt med personvernsinteressene? I hvilken grad utgjør hemmelighold av tiltak et problem for personvern og rettsikkerhet? Hvordan sikre tilstrekkelig demokratisk kontroll over kontrollørene?

Diskusjonen om skjerpede sikkerhetskrav foregår i alle europeiske land, i internasjonale organisasjoner og i EU. I denne rapporten vil vi beskrive aktuelle tiltak for økt sikring av transportsektoren i europeiske land, på EU-nivå og som følge av andre internasjonale overenskomster. Vi beskriver aktuelle sikringstiltak innen alle de fire transportgrenene: Luft, sjø, vei og bane. I tillegg blir de aktuelle tiltakene og problemstillinger vedrørende personvern drøftet i forhold til

gjeldende rett både i Norge og internasjonalt. Vi har også gjennomført personlige intervjuer med en rekke beslutningstakere innenfor norske myndighetsorganer og transportvirksomheter for å få innblikk i hvordan personvern og security-tiltak vurderes konkret i de ulike sektorer og virksomheter.

Utformingen og gjennomføringen av nye tiltak for økt sikkerhet mot ulovlige handlinger innen transport er fremdeles i støpeskjeen. Denne kartleggingen vil derfor først og fremst gi et tidsbilde av det nasjonale og internasjonale arbeidet med sikkerhet og vise til tendenser og muligheter for tiltak innen de ulike transportgrenene. Drøftingen av personvernimplikasjonene vil forhåpentligvis ha relevans på noe lengre sikt. Det er all grunn til å vente at nye og skjerpede tiltak mot terror kan bli lansert med vesentlige implikasjoner for personvernet.

1.2 Rapportens innhold

Rapporten gjengir resultatene fra forskningsprosjektet ”Security i transport – personvernets grenser” som er gjennomført innenfor Norges forskningsråds program ”Risiko og sikkerhet i transport” (RISIT). Prosjektet har bestått av tre deloppgaver:

1) En gjennomgang av aktuelle security-tiltak i de ulike transportgrenene
2) En juridisk gjennomgang av regelverk og drøfting av mulige konflikter mellom personverninteresser og security-tiltak
3) En empirisk undersøkelse av beslutningstakeres vurderinger av forholdet mellom security-tiltak og personvern.

Rapporten følger strukturen i prosjektet i den forstand av hver deloppgave er presentert i hvert sitt kapittel. Kapittel 2 innholder en oversikt over security-tiltak som er innført eller som er på trappene i de forskjellige transportgrenene. Kapittel 3 gjengir den juridiske drøftingen av forholdet mellom personvern og tiltak, og kapittel 4 gjengir resultatene fra den empiriske studien av beslutningstakeres vurderinger.[1] I kapittel 5 følger en oppsummering av hovedfunn samt en drøfting av mulige implikasjoner av resultatene. I vedlegg 1 er intervjuguiden som ble benyttet presentert. I vedlegg 2 presenteres en oversikt over lov- og regelverk som det henvises til i rapporten.

1.3 Begrepsavklaring og avgrensing

1.3.1 Personvern

Begrepet personvern er knyttet til demokratiske verdier som rettsikkerhet og borgerrettigheter, blant annet retten til en privatsfære og til personlig integritet (*privacy protection*). Retten til personvern er nedfelt i den europeiske menneskerettighetskonvensjonen av 1950.

[1] Hver deloppgave er også dokumentert noe mer detaljert i hhv. Leite (2006), Schartum (2007) og Gripsrud og Grunnan (2007).

Opprinnelig var begrepet personvern i stor grad assosiert med vern mot innsyn i privatlivet/privatsfæren. Etter hvert som elektroniske datalagringssystemer ble utbredt utover på 1970-tallet ble begrepet personvern i økende grad brukt i forhold til innsamling, registrering og bruk av personopplysninger i elektroniske systemer. Personverndiskusjonen har derfor etter hver blitt dominert av diskusjonen om personopplysningsvernets stilling i datasamfunnet.

Schartum og Bygrave (2004) definerer personopplysningsvern som en underkategori av personvern som ”*omhandler normer for behandling av personopplysninger med sikte på å verne om personlig integritet, herunder anonymitet og privatlivets fred*” (Schartum og Bygrave 2004: 14). Dette begrepet tilsvarer det engelske begrepet *data protection*.

Denne rapporten omhandler ikke bare sikringstiltak som innebærer registrering, lagring og bruk av personopplysninger, men alle tiltak som på ulik måte og i ulik grad kan krenke personenes integritet – som for eksempel kameraovervåkning og visse former for skanning.

1.3.2 Safety og security

Det norske begrepet ”sikkerhet” dekker de to engelske begrepene *safety* og *security*. Det tradisjonelle sikkerhetsarbeidet i transportsektoren rettet mot å unngå ulykker og skader er i tiltak for å øke sikkerheten i betydningen ”*safety*”.

Med *security* menes tiltak for å beskytte transportsektoren mot ulovlige *intenderte* (”*man made*”) handlinger. Disse handlingene kan spenne fra tilfeldig volds-utøvelse og spontan vandalisme til organiserte og planlagte sabotasje- eller terror-aksjoner. I det følgende vil vi også bruke det norske begrepet *transportsikring* som betegnelse for *security i transport*.[2] Vi vil imidlertid i de fleste sammenhenger benytte den engelske betegnelsen *security* som også er nokså vanlig i den norske faglitteraturen.

1.3.3 Aktive og passive tiltak

Tiltak for å bedre safety og security i transport er i prinsippet av to typer; ”aktive” og ”passive”. *Aktive tiltak* er tiltak som skal forhindre at en ulykke eller en sabotasje- eller terrorhandling skal skje. Politiovervåkning, enten manuelt eller ved hjelp av tekniske hjelpemidler, er et eksempel på aktivt, forbyggende tiltak. Politiovervåkning kan både gi økt ”safety” (konvensjonell trafikkovervåkning reduserer ulykker) og gi økt ”security” (spaning med på terrormistenkte). Overvåkning kan true personvernet, og det er dermed også klart at hensynet til personvern kan komme i konflikt med både safety- og security-tiltak.

Passive tiltak er tiltak som skal redusere skadeomfanget dersom en ulykke eller sabotasje- eller terrorhandling skjer. Slike tiltak omfatter en rekke forhold, fra f.

[2] Etter en språklig utredning valgte Infrastrukturutvalget (NOU 2006: 6) å benytte begrepet ”sikkerhet” til å dekke både *safety* og *security* og å benytte uttrykket ”sikkerhet mot uønskede utilsiktede hendelser” for å beskrive *safety*, og tilsvarende ”sikkerhet mot uønskede tilsiktede hendelser” for å beskrive *security*.

eks. påbud om bruk av sikkerhetsbelter i private biler og i passasjerfly til krav brannslukningsapparater på T-banen og rømningsveier i tunneler.

I en rapport fra en arbeidsgruppe om objektsikkerhet, nedsatt av Forsvarsdepartementet, brukes det en alternativ inndeling av sikringstiltak: Sikringstiltakene kan være *barrierer* mot en ytre trussel, for eksempel i form av en fysisk eller elektronisk barriere. *Deteksjonsmekanismer* vil kunne avdekke et forsøk på å overvinne disse barrierene gjennom et angrep. *Reaksjonstiltak* vil være nødvendige tiltak for å kunne reagere på et angrep (Forsvarsdepartementet 2002: 37).

1.3.4 Risiko

En vurdering av behovet for tiltak for økt transportsikkerhet eller -sikring vil være knyttet til *risikoen* for at en ulykke eller en ulovlig hendelse skal skje. Risiko defineres som en funksjon av sannsynlighet for at en hendelse skal inntreffe og hvor alvorlige konsekvenser hendelsen vil ha. Risiko er dermed noe annet enn *trussel*. En trussel kan forstås som en ytre fare som kan skade oss; en risiko er et samlet (og ofte kvantifisert) uttrykk for hvor sannsynlig den aktuelle faren er og hvor store negative konsekvenser den kan påføre oss. Risikostyring er dermed et forsøk på rasjonelt å håndtere trusler eller farer (Schneier 2004).

En analyse av risiko skal danne grunnlaget for å vurdere behovet for forbyggende handlinger. I veitrafikken vil man i mange tilfeller ha historiske ulykkesdata som kan benyttes til å gi gode estimater på hvor stor risikoen for ulykke er. I andre transportgrener, der ulykker er sjeldne, vil dette være langt vanskeligere. Når det gjelder risikoen for sabotasje eller terror, er det naturligvis vanskelig eller umulig å basere seg på historiske data. I svært mange tilfeller må derfor risikovurderinger gjøres uten at man har erfaringsdata å støtte seg til.[3]

Sårbarhetsutvalget (NOU 2000: 24) tar utgangspunkt i erfaringer med storulykker i Norge. Utvalget peker på at utviklingen i samfunnet gir nye former for risiko og sårbarhet som krever årvåkenhet og stadig tilpasning av sikkerhetstiltak og beredskap fra den øverste administrative og politiske ledelses side (NOU 2000: 24). Utredningen, som kom før 11. september 2001, fokuserer på risiko for ulykker på grunnlag av erfaringer med årsaker til tidligere ulykker (se Jernbaneverket 2005). Ingen storulykker i Norge har til nå vært knyttet til forhold som har med terror og sabotasje å gjøre.[4] Statistisk sett er risikoen for å dø i en storulykke langt lavere enn i en ”vanlig” trafikkulykke.

[3] Innenfor beslutningsteori benyttes ofte begrepet ”beslutninger under usikkerhet” når man ikke kan tilordne sannsynligheter til de ulike utfall. I praksis vil dette langt på vei være situasjonen når det gjelder mulighetene for alvorlige hendelser som terroranslag og lignende. Slike problemer er forsøkt løst ved hjelp av såkalt Bayesiansk oppdatering av sannsynligheter, jf. f. eks. Aven (2003).

[4] Direktoratet for samfunnssikkerhet og beredskap peker på at det er en stor utfordring å dimensjonere et planverk for beredskap som tar høyde for hendelser med liten sannsynlighet, men som kan ha meget omfattende konsekvenser (DSB 2004: 17).

Infrastrukturutvalget (NOU 2006: 6) poengterer at i en samfunnsmessig tilnærming til risiko vil fokus i sterkere grad være på *konsekvensen* av uønskede hendelser enn på *sannsynligheten*. Utvalget peker på at for kritisk infrastruktur, som transport, og kritiske samfunnsfunksjoner, vil samfunnet .. "iverksette defensive sikkerhetstiltak på grunnlag av den samfunnsmessige verdien, ikke på grunnlag av sannsynligheten for at en hendelse skal skje" (NOU 2006:6, s. 35).

1.3.5 Transportsikring

Med transportsikring forstås i dette dokumentet aktive tiltak som har som formål å forhindre ulovlige handlinger. Tiltakene omfatter ikke tiltak for beredskap og sårbarhetsreduserende tiltak og må avgrenses mot disse:

1. Beredskapstiltak er tiltak som primært retter seg mot å minimere skadeomfanget ved en terrorhendelse eller en ulykke – for eksempel prosedyrer for brannvern og evakuering av tunneler og terminaler.
2. Sårbarhetsreduserende tiltak er tiltak som forebygger en terrorhandlings evne til å lamme sentrale samfunnsfunksjoner (NOU 2000: 24).

Terrorangrepene i New York, Madrid og London har hatt stor betydning for strategier og tiltak som er utviklet de senere år. Sikringsstrategier som beskrives i dette dokumentet vil særlig være rettet mot tiltak som har som formål å forhindre terrorangrep og sabotasje og særlig være knyttet til en for Norge "ny" terrortrussel som oppsto gjennom religiøse ekstremistiske gruppers reaksjon på krigen i Irak (NOU 2004: 6).

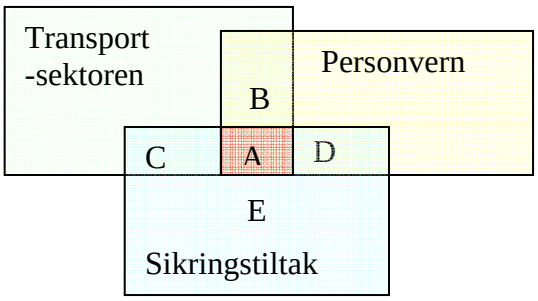
Et hovedsiktemål i rapporten har vært å kartlegge hvordan terrorhendelsene i New York, Madrid og London har påvirket utviklingen av en mer bevisst sikringspolitikk i transportsektoren og i hvilken grad sikringstiltakene utfordrer hensynet til personvern.

2 Sikring av transportsektoren

I dette kapitlet vil vi omtale hvilke tiltak som er i bruk og som kan bli aktuelle for å sikre transportsektoren mot terrorangrep og andre uønskede hendelser. Det betyr at vi ser på tiltak som er spesielt rettet mot ulovlige handlinger og hvor transportsektoren er et *mål* eller blir brukt som et *middel*. Generelle sikringstiltak mot andre *mål* som offentlige bygninger eller kjøpesentre vil ikke bli omtalt. Det samme gjelder i utgangspunktet for generelle tiltak som er rettet mot å forhindre og oppklare ulovlige handlinger og som ikke er knyttet til transportsektoren spesielt, slik som preventiv etterforskning. I avsnitt 2.3 har vi likevel sett på muligheten for bruk av personopplysninger i preventiv etterforskning i tilfeller der data er hentet fra transportsektoren som for eksempel bruk av passasjerlister i etterforskningsøyemed.

Den offentlige diskusjonen om personvern og sikring dreier seg ofte om tiltak hvor personopplysninger brukes til kriminalitetsbekjempelse. Et eksempel på slike tiltak er EU-direktivet om lagring av kommunikasjonsdata fra telefoner og e-post fra 2006.[5] Disse tiltakene er ikke spesifikt rettet mot transportsektoren, men er iverksatt for å forebygge terrorhandlinger generelt, og er også blitt kritisert for å bidra til en generell overvåkning av samfunnet (European Parliament 2005).

Andre tiltak, som kameraovervåkning av stasjonsområder, er spesifikke tiltak i transportsektoren, men som også kan benyttes i forbindelse med spaning og etterforskning av annen kriminalitet. I tillegg har mange av de person-opplysningene som blir innhentet og registrert i de ulike transportgrenene andre formål enn transportsikring, f. eks. til passasjerstatistikk osv. I figur 2.1 er forholdet mellom transportsektoren, personvern og sikring forsøkt illustrert.



Kilde: TØI rapport 914/2007

Figur 2.1 Modell for sammenheng mellom transportsektoren, personvern og sikringstiltak.

[5] Direktiv 2006/24/EF

Figuren angir ulik grad av overlapp mellom de tre områdene. De ulike kombinasjonene er gitt bokstavkoder og innebærer følgende:

A. Tiltak innen transportsektoren som har implikasjoner for personvern og som har sikring som formål for eksempel adgangskontroll og skanning av bagasje på flyplasser.

B. Tiltak i transportsektoren som har implikasjoner for personvern, men som har andre formål enn sikring som for eksempel betaling av bompenger ved bruk av AutoPASS-brikker.

C. Sikringstiltak i transportsektoren som ikke har personvernimplikasjoner, som for eksempel fysisk inspeksjon av fly før avgang.

D. Sikringstiltak utenfor transportsektoren som har implikasjon for personvernet som for eksempel sikringstiltak overfor ambassader eller kameraovervåkning av kjøpesentre.

E. Sikringstiltak utenfor transportsektoren som ikke har personvernimplikasjoner.

I denne framstillingen av sikringstiltak vil vi primært begrense oss til tiltak som befinner seg i feltene A og C, det vil si sikringstiltak i transport som enten kommer eller som ikke kommer i konflikt med hensynet til personvern. I tillegg vil vi vurdere i hvilken grad tiltak i kategori B vil kunne brukes til sikringsformål (se avsnitt 2.3).

2.1 Endret trusselbilde gir økt fokus på sikring

I EUs forordning om sikkerhet i sivil luftfart[6] slås det fast at terrorhendelsen 11. september 2001 viser at terrorisme er en av de største truslene mot den Europeiske Unions felles idealer og verdigrunnlag; demokrati, frihet og fred. Etter terror-aksjonen i Madrid vedtok det Europeiske Rådet på toppmøtet i Brussel i mars 2004 en deklarasjon om terrorbekjempelse (European Council 2004). Deklarasjonen gir klart uttrykk for medlemslandenes ønske og forpliktelse til felles og samordnete tiltak mot terrorisme, bl.a. med henvisning til solidaritetsbestemmelsen i Artikkel 42 i Traktaten for den Europeiske Union. Deklarasjonen omhandler tiltak med personvernsrettslige implikasjoner som lagring av telekommunikasjonsdata og innføring av biometriske pass.

Også i norske beslutningsdokumenter omtales terroraksjoner som den nye store utfordringen for samfunnssikkerheten. I Stortingsmelding nr. 39 (2003-2004) om samfunnssikkerhet og sivilt-militært samarbeid heter det: ”*Framveksten av internasjonale terrornettverk og trusler om bruk av masseødeleggelsesmidler er blitt en viktig del av dagens trusselbilde og har særlig relevans for det sivil-militære samarbeidet*” (St.meld. nr. 39 (2003-2004):6).

Politimetodeutvalget legger vekt på at terrorangrepene mot USA den 11. september 2001 utgjør en ny type sikkerhetsutfordring ved at omfanget er større og at trusselen i større grad er global. Flertallet i utvalget viser til at den

[6] Forordning 2320/2002/EF

organiserte kriminaliteten blir stadig mer uoversiktlig og at faren for terrorvirksomhet har økt (NOU 2004: 6). Nasjonal Sikkerhetsmyndighet viser også til terror som ny trussel mot rikets sikkerhet og peker på *"et endret trusselbilde hvor en forsøker å bekjempe såkalte asymmetriske aktører, det vil si terrorister, langt unna statsterritoriet til de land som kanskje er hovedmålet for terrorhandlingene"* (NSM 2005a: 1).

Når terror står høyt på den politiske dagsorden, får arbeidet med sikring høy legitimitet. I hvilken grad nye og strengere sikringstiltak iverksettes, vil imidlertid være avhengig av institusjonell kapasitet, tilgjengelige ressurser og vurderingen av behovet for tiltak i de enkelte sektorene. En vurdering av trusselbildet for Norge blir viktig for å balansere mellom hensynet til sikring og personvern og for å kunne velge adekvate tiltak. I avsnittene nedenfor vil vi derfor gi et overblikk over aktuelle vurderinger av trusselbildet og av transportsektoren som mål for terrorisme.

2.1.1 Internasjonale avtaler om sikkerhet i transport

Dagens terrortrussel er transnasjonal. Riktignok har de mest spektakulære terroraksjonene mot transportmidler de senere år skjedd mot innenlandske transporter, men det skyldes trolig først og fremst at innenlandsk transport er dårligere sikret enn internasjonal transport. De skjerpede tiltakene som ble innført på flyplasser fra august 2006 (væskeforbudet) ble innført nettopp fordi man mente å ha avslørt terrorplaner mot internasjonal luftfart.

Arbeidet med sikring mot terror foregår derfor i utstrakt grad i form av internasjonalt politisamarbeid og implementering av felles regler og tiltak på tvers av landegrenser. Dette er verken nytt eller overraskende. Krav til sikkerhet innen transport har tradisjonelt vært regulert gjennom godt etablerte internasjonale avtaler.[7] Særlig for luftfart og sjøfart finnes det en rekke avtaler som er relevante for sikring mot ulovlige hendelser

Konvensjonen om internasjonal sivil luftfart ble vedtatt i 1944 (ICAO 2000). Konvensjonen til bekjempelse av ulovlige handlinger mot sikkerheten i sivil luftfart ble undertegnet i Montreal 23. september 1971. En protokoll til denne konvensjonen trådte i kraft i 1991 og omfatter bekjempelse av ulovlige voldelige handlinger ved lufthavner som betjener internasjonal sivil luftfart. Konvensjon om merking av eksplosiver fra 1998 er en annen relevant avtale.

FNs regelverk om farlig gods danner grunnlaget for den europeiske avtalen om internasjonal veitransport av farlig gods – ADR-avtalen[8]. Transport av farlig gods er også regulert av DIREKTIV 94/55/EF og den norske forskriften om transport av farlig gods på vei og jernbane fra 1990. FN signaliserte i 2003 at de ønsker å inkludere terrorfaren i regelverket om farlig gods (Hagen m.fl. 2003: 29).

Etter terrorhendelsen i New York har naturlig nok tiltak mot terrorhendelser og internasjonal kriminalitet fått økt fokus innenfor disse regelverkene. Det

[7] For eksempel ble den europeiske avtalen om internasjonal vegtransport av farlig avfall inngått i 1957.

[8] Accord européen relatif au transport international des marchandises dangereuses par route

tydeligste eksempelet her er den Internasjonale sjøfartsorganisasjonens (IMOs) skjerpede regler for krav til sikring av skip og havneanlegg.

2.1.2 Sikring mot terror i EU/EØS-området

EUs antiterrorarbeid har de senere år særlig hatt fokus på styrket politi- og justissamarbeid, støtte til internasjonale konvensjoner og styrking av en felles sikkerhets- og utenrikspolitikk, hvor EU skal spille en mer aktiv rolle for å forhindre og stabilisere regionale konflikter.

EU-kommisjonen foreslo i 2003 en rekke tiltak for transportsikring som ble anbefalt innført i medlemsstatene (European Commision 2003). Tiltakene burde ifølge EU-kommisjonen særlig rettes mot viktig infrastruktur innen det transeuropeiske transportnettverket (TEN-T). Behovet for tiltak også innen nasjonale transportnettverk ble illustrert ved terrorangrepene i Madrid og London kort tid etter.

De fleste av tiltakene Kommisjonen anbefalte var knyttet til utarbeidelse av sikringsprosedyrer og oppfølging av sikringsstrategier. Kommisjonen nevner her at medlemslandene bør:

1. Utarbeide risikoanalyser (”Security Risk Assessment”).
2. Utarbeide sikringsplaner som inkluderer en årlig handlingsplan for å bøte på svakheter som er blitt identifisert i risikoanalysen.
3. Utpeke en ansvarlig kontakt og en ansvarlig institusjon for sikring av infrastruktur.
4. Gjennomføre årlig evaluering av sikringsplanen.

Sentralt i sikringsstrategien er utarbeidelsen av en risikoanalyse. I 2005 publiserte ECMT og OECD en felles rapport om sikring i intermodal transport med vekt på farer for terroranslag i containertransport (ECMT 2005). Utredningen legger vekt på at transportmyndighetene må kjenne transportkjedens svakeste ledd, gjennomføre mer spesifikke vurderinger av risiko, tilpasse seg den konkrete trusselen og spille en rolle i å øke sikkerheten på alle ledd i transportkjeden. I følge ECMT (2005: 38) bør slike risikoanalyser blant annet inneholde en vurdering av:

1. Trusselbildet i forhold til hendelser nasjonalt og internasjonalt som indikerer økt risiko for terrorangrep.
2. Sårbarhet og svakheter i infrastruktur og prosesser som kan bli utnyttet av terrorister.
3. Hvor sannsynlig et angrep med kjemiske, biologiske, radioaktive eller nukleære (CBRN) våpen er, og hvor alvorlige konsekvensene kan bli.
4. Mulige mottiltak for å redusere risiko

Dette er momenter som inngår i såkalte risiko- og sårbarhetsanalyser (ROS). ROS-analyser benyttes for å vurdere sannsynlighet og konsekvens av ulike trusler mot kritiske objekter eller funksjoner som grunnlag for å prioritere tiltak. En såkalt ROS-matrise blir ofte benyttet for å veie sammen sannsynlighet og konsekvens av trusler mot enkelte objekter/funksjoner, jf. Figur 2.2.

Probability of occurrence	Severity level			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A – Frequent	IA	IIA	IIIA	IVA
B – Probable	IB	IIB	IIIB	IVB
C – Occasional	IC	IIC	IIIC	IVC
D – Remote	ID	IID	IIID	IVD
E – Improbable	IE	IIE	IIIE	IVE

Figur 2.2 Eksempel på ROS-matrise hentet fra ECMT (2005).

Figur 2.2 viser en matrise over ulik klassifisering av risiko og sårbarhet brukt i en studie fra ECMT/OECD (ECMT 2005). Matrisen angir kombinasjoner av sannsynlighet og konsekvens og viser generelt at trusler som kan plasseres oppe og til venstre i matrisen er viktige å sikre seg mot, mens trusler nede og til høyre kan ignoreres.

EU har også arbeidet aktivt med tiltak direkte rettet mot transportsektoren.[9] Deklarasjonen om terrorbekjempelse viser for eksempel til direktiv om krav til transportører om å informere om passasjerdata. Det Europeiske Rådet har også bedt EU-kommisjonen om å utarbeide et forslag for felles regler om bruk av passasjerdata for å øke grense- og flysikkerheten (European Council 2004). En videre oppfølging av EUs antiterrorstrategi er det pågående arbeidet med felles regler for økt sikring av vei og jernbane med særlig fokus på godstransporten (se avsnitt 2.2.3).

For sikring av skip og havneanlegg gir EU omfattende bestemmelser[10] som bygger på IMOs nye krav til sikring innen internasjonal sjøfart. EUs regler har som formål å sikre felles bestemmelser og bedre sikring av skip og havneanlegg i EU/EØS-området. I forhold til IMOs regelverk har EU valgt å utvide anvendelsesområdet og gjøre flere av regelverkets veiledende råd obligatoriske innenfor EU.

EUs antiterrorstrategi har klare føringer for norsk politikk for sikring av transportsektoren. Norge er gjennom EØS forpliktet til å gjennomføre skjerpede krav til sikring av sivil luftfart og sjøfart. Luft- og sjøfart er derfor de transportgrenene der vi i dag ser de mest konkrete tiltakene for økt sikring i Norge (se avsnitt 2.2). Norge vil også tilpasse seg og delta i EUs politi- og justissamarbeid og samarbeid mellom etterretningstjenester.

EU har som nevnt valgt å gjøre flere av de veiledende bestemmelsene i IMOs regelverk obligatoriske. Dette gjelder blant annet:

- Obligatorisk revisjon av skipenes sikringsplaner og sårbarhetsvurdering av havnene, samt at disse må behandles fortrolig

[9] For transportsektoren viser Det Europeiske Rådet til Forordning om sikkerhet i luftfarten (FOR 2320/2002/EF) og Forordning om bedre sikring av skip og havnefasiliteter (FOR 725/2004/EF).

[10] FORORDNING 725/2004/EF

- Bruk av anerkjente sikringsorganisasjoner og garanti for deres uavhengighet
- Bruk av minstestandarder for vurdering av sikringsorganisasjon, sikringsstandard, sårbarhet og havnenes sikringsplaner
- Sikkerhetsøvelser og sikringsutdannelse for skipsbesetning og sikringssansvarlige i rederier, om bord i skipene og i havneanleggene

Bombeaksjonen i Madrid 2004 viste at pendeltransport inn til store europeiske byer er sårbart for terrorangrep, noe som har aktualisert spørsmålet om strengere sikringstiltak for tog- og ferjetransport. Dette har imidlertid kun blitt gjennomført for spesielle traséer når det gjelder jernbane, slik som for toglinjen gjennom kanaltunnelen, der det er tilrettelagt for flyplasslignende sikkerhetstiltak (UK ICO 2005). Grunnen er at det er svært vanskelig og meget kostbart å gjennomføre slike sikringstiltak for pendel- og nærtrafikk i storbyområder.[11]

Også landbasert godstransport har vært fokusert i EUs antiterrorarbeid i transportsektoren. I følge EU-kommisjonen finnes det ingen felles (minimums)standard for sikring hos internasjonale speditører og transportører. Kommisjonen har anbefalt at alle transportører skal følge internasjonale sikringsstandarder, og har sett behovet for koordinering og harmonisering av praksis gjennom et felles regelverk for transportbransjen (European Commission 2003: 10). EU-kommisjonen anbefaler at tiltak for økt sikring i godstransport både bør omfatte viktig infrastruktur og de enkelte transportører. Kravene til sikring av godtransporten skal utformes som minimumsstandarder og gjelde for transportører, terminaloperatører, jernbaneselskap, parkeringsplasser og rørledninger (European Commission 2003: 2).

I følge EU-kommisjonen er det et betydelig kunnskapsbehov på feltet både med hensyn til avveining av risiko for kriminalitet og terrorisme og til kostnadene knyttet til tiltak (European Commission 2003: 4).

EU-kommisjonen peker på at veitransporten er særlig sårbar og trenger spesiell oppmerksomhet: Den består av flere tusen aktører som beveger seg meget fritt innenfor EUs grenser. I følge EU-kommisjonen er det behov for å utvikle en sikringsstrategi som omfatter hele transportkjeden, også veitransport (European Commission 2003: 3).

Tollmyndigheter og grensekontroll har naturlig nok en viktig rolle i den økte fokus på transportsikring i EU/EØS-området. Fra og med desember 2006 er det innført endringer i regelverket om toll og sikring av eksterne grenser. Det nye regelverket inneholder bestemmelser om elektronisk utveksling av informasjon om eksport mellom tollmyndighetene i de ulike land (export control system), forhåndsvarsling til tollmyndighetene om gods som skal transporteres inn til eller ut fra EU og sertifisering av pålitelige transportører (”Authorised Economic Operator” (AEO)) som gis forenklet tollbehandling. De nye reglene innføres gradvis f.o.m. 1.7.2007.[12]

---

[11] I Storbritannia er det som en forsøksordning innført adgangskontroller på Paddington station i London.

[12] FORORDNING 648/2005

2.1.3 Trusselvurderingen i Norge og tilpasning til EU

Nasjonal Sikkerhetsmyndighet (NSM) peker på at antall potensielle terrormål er stort og variert og omfatter symbolske, militære, statlige og private mål. Målene for terroraksjoner har som oftest vært knyttet til konfliktområder og vært rettet mot symbolske mål og mål med stort potensial for massedrap (Lia 2003).[13]

I en rapport fra Forsvarets forskningsinstitutt (FFI) hevdes det at mangelen på erfaring med overvåkning, infiltrering og opprulling av internasjonale nettverk kan gjøre Norge til et mer attraktivt mål for terrorister enn landet ellers ville ha vært (Hagen m.fl. 2003). Transportsektoren antas å være den delen av sivil infrastruktur som er mest utsatt for terrorangrep ved siden av spesifikke amerikanske og israelske mål. Transportsektoren kan også være en velegnet arena for terroraksjoner ved at den er enkel å angripe og at det er mulig å gjøre stor skade med enkle terrormidler. Aksjoner mot transportsektoren er også egnet til å spre frykt i befolkningen (Hagen m.fl. 2003, Stortingsmelding nr. 39 (2003-2004)).[14]

Norske strategier for terrorsikring i transportsektoren har fram til nå vært preget av implementering av EUs regelverk om sikkerhet for sivil luftfart og implementering av IMOs regelverk for sjøfart gjennom EUs krav. Arbeidet med sikring av særlig luftfarten og sjøfarten i Norge kan derfor beskrives som en rettslig tilpasning til EU-forordninger og EU-direktiv. Norske tiltak for sikring i transportsektoren innebærer først og fremst at EUs regelverk implementeres i Norge; det er svært få egne norske tiltak. Som et ledd i arbeidet mot terror har imidlertid norske myndigheter også satt større fokus på beredskap og sårbarhet. For eksempel ble det gjennomført en omfattende beredskapsøvelse ved Nationaltheatret stasjon høsten 2006.

2.2 Sikringstiltak i transportsektoren

Økt fokus på sikring mot terror i transport kan i prinsippet skje langs to dimensjoner. For det første kan selve omfanget og tyngden i tiltakene øke innenfor transportgrener som tradisjonelt sett har hatt en bevisst strategi for sikring – da særlig luftfart og sjøfart. For det andre kan sikringstiltakene og sikringsmetodene bre seg til nye transportgrener. Vi kan, som nevnt, få ”flyplass-lignende tilstander” i andre deler av transportsektoren, som veitransport og jernbane (Adey 2004), selv om det er komplisert og dyrt å innføre.

---

[13] I en risikovurdering etter bombeaksjonen i London skrev NSM at flere aksjoner fra radikale, islamistiske terrornettverk har vært planlagt og avslørt i Europa de siste fem årene. Dette og aksjonene i Madrid og London, gjorde at Europa ble oppfattet som et aktuelt mål for slike terrorhandlinger, men NSM var av den oppfatning at det ikke er grunn til å endre det konkrete trusselnivået i Norge (NSM 2005b).

[14] Stortingsmelding nr. 39 (2003-2004) beskriver tiltak mot terror og sabotasje mot luftfarten som sikkerhetskontroll av passasjerer, bagasje, frakt, post og ansatte. Fysisk sikring av lufthavnene er også et av tiltakene som nevnes i Stortingsmeldingen (St.meld. nr. 39 (2003-2004): 52). Regjeringen viser også til det nye IMO-regelverket som beskriver tiltak for sjøfart og for havneanlegg. ”*Det er i dag økende bevissthet om at skip, havner og maritime installasjoner kan være potensielle mål for terrorangrep, og at skip vil kunne bli brukt som middel for terroraksjoner og til transport av masseødeleggelsesvåpen*” (St.meld. nr. 39 (2003-2004): 53)

Foreløpig er det først og fremst *omfanget* av sikringstiltak innen luft- og sjøfart som har økt, og det har i liten grad foregått en overføring av sikkerhetstenkningen og systemene fra luft og sjø til bane og vei. I Storbritannia har det imidlertid som nevnt vært gjort noen forsøk i denne retning.[15]

I dette avsnittet skal vi beskrive arbeidet med sikring innen de enkelte transportgrenene. Vi vil gjøre rede for det juridiske grunnlaget for sikringstiltakene, hvilke tiltak som er satt ut i livet eller som diskuteres, hva disse tiltakene omfatter og hva slags sikringstiltak som er mulige å gjennomføre i de ulike transportgrenene.

For å strukturere presentasjonen, gir vi først en kort oversikt over det juridiske grunnlaget og deretter presenteres tiltakene i henhold til EUs forordning om sikkerhet i sivil luftfart.[16] Forordningen systematiserer tiltak for transportsikring som følger:

1. Sikringsplaner, prosedyrer og opplæring.
2. Utforming av terminal og fysisk sikring av forskjellige sikkerhetsbeskyttede områder.
3. Kontroll av personale.
4. Kontroll av passasjerer og bagasje ved ombordstigning av transportmiddel og terminaler.
5. Overvåkning av passasjer, bagasje og frakt.
6. Kontroll/sjekk av transportmidlene.

Norske særlover og forskrifter for de forskjellige transportgrenene inneholder i ulik grad bestemmelser om sikring mot ulovlige handlinger. For luftfarten og sjøfarten er sikringsarbeidet klart hjemlet i særlovene for disse sektorene. Dette betyr også at det institusjonelle ansvaret for sikringsarbeidet innenfor disse sektorene er klart definert. For transport av gods og personer på vei og bane er bestemmelser om krav til sikring fordelt på flere lover og hjemmelsgrunnlaget er ikke klart. For sikring av visse objekter kan også sikkerhetsloven hjemle tiltak for sikring.

Gjennomgangen av særlovene i dette kapitlet er gjort med sikte på å beskrive krav og muligheter for iverksetting av tiltak for økt sikring av transportsektoren. Dette regelverket vil som regel ikke gi hjemmel til registrering, lagring og bruk av personopplysninger, men denne behandlingen vil måtte hjemles særskilt i personvernlovningen eller i særlov (Schartum 2007, Schartum & Bygrave 2004). Flere av de konkrete tiltakene som beskrives nedenfor vil med andre ord kreve en lovhjemmel utover regelverket for sikring av de ulike transportsektorene.

---

[15] Som nevnt er det gjennomført forsøk med adgangskontroll for passasjerer på Paddington stasjon i London. I Storbritannia er også kameraovervåkning av veitrafikken etter hvert blitt omfattende, og systemet med "Automatic Number Plate Recognition" (APNR) gir muligheter for å identifisere og spore stjålne biler, mistenkelige personer m.v.

[16] FORORDNING 2320/2002/EF

2.2.1 Luftfart

Lover og forskrifter

Som eier av nasjonale og regionale lufthavner har Avinor ansvar for å gjennomføre kravene til sikring i EUs forordning om sikkerhet i sivil luftfart. EU-regelverket gjelder nå for alle regionale flyplasser i Norge. Dette innebærer kontroll av alle passasjerer og all bagasje på norske lufthavner. I Avinors årsrapport for 2004 ble kostnadene ved å implementere forordningen anslått til ca. 400 millioner kroner (Avinor 2005: 49).

Den sentrale særloven for norsk luftfart er Lov om luftfart fra 1993. Luftfart kan bare finne sted når den er i samsvar med loven og forskrifter gitt med hjemmel i loven.[17] EUs forordning om sikkerhet i sivil luftfart er grunnlagt på hjemler gitt i luftfartsloven og gjort gjeldende ved Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten.[18]

Luftfartstilsynet har et todelt ansvar for oppfølging av EUs forordning. For det første er det ansvarlig for å godkjenne organisasjoner som utdanner sikkerhetskontrollører og sikkerhetsvakter på sikkerhetsbeskyttede områder. For det andre skal det føre tilsyn med lufthavnenes sikring. Luftfartstilsynet har organisert dette arbeidet i en egen security-seksjon i Lufthavn- og utdanningsavdelingen.

Tiltak for økt sikring i luftfarten tar utgangspunkt i henstillinger fra den Europeiske Konferansen om Sivil Luftfart (ECAC), Dokument 30, som er inkludert i EUs forordning om sikkerhet i sivil luftfart (ECAC 2006).

Sikringsplaner, prosedyrer og opplæring

Det er omfattende regler for hvilke prosedyrer som må følges for å sikre luftfarten mot ulovlige handlinger og strenge krav til opplæring og utdanning av personell. Reglene gjelder også alt servicepersonale (luftfartsselskap eller kontrahenter) som har adgang til sikkerhetsbeskyttede områder. Virksomhetene skal peke ut sikkerhetsansvarlige og følge rutiner for forsvarlig avlåsing, forsegling og fysisk sikring av utstyr og kjøretøy.

Nasjonale utdannelsesprogrammer skal sørge for tilstrekkelig kompetanse på sikringstiltak og sikringsprosedyrer. Det skal gjennomføres ett program for sikkerhet for flybesetning og ett program for lufthavnpersonell (basis/ etterutdannelse). I Norge er det Luftfartstilsynet som godkjenner utdannelsesorganisasjoner.[19]

---

[17] Hjemmel for forskrifter om sikkerhetskontroll er gitt i lovens § 7-24 og § 7-25. Samferdselsdepartementet kan med denne hjemmelen regulere ferdselen på landingsplassen og vedta forskrifter for kontroll av personer, reisegods og fraktgods. § 7-25, annet ledd gir departementet fullmakt til å stille krav om utarbeidelse og gjennomføring av sikkerhetsinstrukser for Avinor, flyselskaper, fraktagenter og andre som driver virksomhet knyttet til lufthavnen. Luftfartslovens § 16-1 gir regjeringen fullmakt til å vedta forskrifter om gjennomføring av EØS-avtalen på luftfartens område.

[18] Forskrift 2004-04-30 nr. 715: Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten (BSL A 2-1) definerer Luftfartstilsynet som "vedkommende myndighet" i forhold til FORORDNING 2320/2002/EF. Forskriften gir Luftfartstilsynet myndighet til å treffe vedtak om ytterlige sikkerhetstiltak i særlige tilfeller og etter samråd med Sikkerhetsrådet for luftfarten.

[19] En oversikt over godkjente utdanningsorganisasjoner finnes på www.luftfartstilsynet.no

Fysisk sikring av flyplasser

EU setter krav til fysisk planlegging av lufthavner for å sikre effektiv adgangskontroll og effektiv bruk av sikringsutstyr innenfor sikkerhetsbeskyttede områder. Det gjøres her et skille mellom flysiden og landsiden. Flysiden er ferdselsområdet i en lufthavn og tilstøtende områder og bygninger. Kjøretøy som brukes på flysiden skal i så stor grad som mulig forbli på flysiden. Landsiden er området som ligger utenfor flysiden og som omfatter alle områder som er tilgjengelige for allmennheten uten at det er foretatt en adgangskontroll.

EU-regelverket gir generelle bestemmelser om at terminalområder og andre områder med adgang for allmennheten skal overvåkes. Arealer som ligger nært opp til sikkerhetsbeskyttede områder skal overvåkes med patruljer, med videokamera eller på andre måter. Det skal i tillegg defineres kritiske soner i det sikkerhetsbeskyttede området. Disse områdene skal patruljeres, og passasjerer og andre personer skal holdes under overvåkning av sikkerhetspersonalet. En viktig del av den fysiske planleggingen er også å sikre at passasjerer som reiser ut fra lufthavnen holdes atskilt fra passasjerer som ankommer lufthavnen eller er i transitt.

Reglene for fysisk planlegging og sikring av lufthavnene gjør det mulig å gjennomføre effektiv adgangskontroll, og fysiske barrierer gjør det vanskeligere for uautoriserte personer å trenge inn på sikkerhetsbeskyttede områder.

Kontroll av personale

Både personale og servicekjøretøy, herunder også flybesetning og medbrakte gjenstander, skal undersøkes/skannes før de får adgang til beskyttede områder. Hvis en slik kontroll ikke er mulig, kan myndighetene bestemme at det skal gjennomføres kontinuerlige stikkprøver.

Kontroll av personale gjøres også i forbindelse med ansettelse i luftfartens servicefunksjoner som catering, forsyning og rengjøring. Luftfartstilsynet har ansvaret for å gjennomføre vandelskontroll ved utstedelsen av ID-kort for personale som skal ha adgang til flysiden på en lufthavn.[20] I henhold Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten, er kravene til plettfri vandel særlig knyttet til opplysninger om forelegg og dom for forbrytelser.

Kontroll av passasjerer, bagasje og frakt

EUs regelverk stiller krav om adgangskontroll av passasjerer, bagasje, frakt og gods. Regelverket skal sikre omfattende kontroll av alle personer, all bagasje og all frakt. Bestemmelsene om sikkerhetskontroll stiller imidlertid ikke krav om at en bestemt teknologi for skanning eller kontroll skal benyttes. Det vil derfor være mulig å innfri kravene til kontroll av bagasje og passasjerer ved å bruke tradisjonelt utstyr som konvensjonell røntgen, metalldetektorer og manuelle undersøkelser.

Kontroll av innsjekket bagasje omfatter blant annet merking, identifikasjon (bagasje og person på flyet) og skanning. Hvis det kun benyttes konvensjonelt røntgenutstyr, skal minst ti prosent av bagasjen bli undersøkt ytterligere (manuelt

[20] Bilag til FORORDNING 2320/2002/EF

eller ved hjelp av andre teknikker). Innsjekket bagasje skal også sikres mot uautorisert adgang. All frakt, kurerpost og ekspresspakker skal undersøkes for å sikre at de ikke innholder ulovelige gjenstander. Det er også regler for sikkerhetskontroll av flypost, ekspresspost og luftselskapenes forsendelse av egen post og eget materiale.

Sikkerheten på norske og internasjonale lufthavner vil kunne øke ved innfasing av ny teknologi for passasjerkontroll og bagasjekontroll.[21] Flere av disse teknologiene vil kunne ha implikasjoner for personvernet. Dette gjelder særlig nyere avansert teknologier som kan brukes til skanning av personer.[22] Felles for disse er at de kan framstille konstruerte digitale bilder av personer som gir inntrykk av at de er nakne. Teknologien er egnet til å avsløre skjulte objekter som kniver, pistoler etc. (UK ICO 2005). Personvernsimplikasjoner er knyttet til personlig integritet ved at de reisene kan føle seg "avkledt".[23] En spørreundersøkelse tyder på at publikum er skeptisk til slik skanning (UK ICO 2005). Avinor har ønsket å ta bruk skanning-teknologi på norske flyplasser, men etter oppslag og debatt i media er dette blitt utsatt på ubestemt tid (Aftenposten 2007b). Ny teknologi for skanning kan imidlertid også anvendes for å kontrollere reisebagasje og håndbagasje. Slik skanning av bagasje vil trolig skape mindre motstand (Adey 2004: 503).

En annen viktig del av sikkerhetskontrollen i luftfart er knyttet til sikker identifikasjon av passasjerer. Her gir bruk av biometriske pass nye teknologiske muligheter. Biometriske kjennetegn i passene vil gjøre det vanskelig å reise med falsk identitet, og biometriske data i maskinlesbare pass kan hindre bruk av falske og stjålne pass. USA har satt krav om innføring av biometriske pass etter terrorhendelsen i New York. ICAO har på sin side særlig lagt vekt på innføringen av maskinlesbare pass for å sikre en effektiv kontroll av passasjerer og samtidig innfri kravene om økt sikkerhet i luftfarten (Abeyratne 2004: 9).

Ved lagring av personopplysninger i et smartkort kan klareringen av passasjerer ved flyplassen skje raskere. Dette tiltaket går under betegnelser *Simplified Passenger Travel* (SPT). *Advanced Passenger Information* (API) innebærer en forhåndsutveksling av registrerte data til toll- og immigrasjonsmyndighetene i et land for å kunne sikre raskere klaringer av passasjerer. Dette beskrives som et tiltak for å hindre forsinkelser for lavrisiko-passasjerer når økte krav til sikring fører til kapasitetsproblemer for toll- og immigrasjonsmyndighetene (Abeyratne 2004: 7ff).[24]

---

[21] SASBraathens fikk i mai 2007 tillatelse av Datatilsynet til å innføre et system for å registrere fingeravtrykk for å kontrollere samsvar mellom den som sjekker inn bagasje og den som går på flyet.

[22] "X-ray backscatter (XTB) technology" er en røntgenteknologi som gir skarpe bilder av material med forskjellige tetthet. Millimetre Wave Scanning (MWS) er en radiobølgeteknologi som drar nytte av materialenes ulike refleksjon av naturlig strålning. Teknologien har vært testet i kanaltunnelen (Calais) og ved Gatwick lufthavn i 2002.

[23] I forsøk med slik skanning ved Heathrow flyplass ble passasjerene tilbudt en alternativ kontroll. Personen som kontrollerer bildene kan ikke se personene som skannes og vil være av samme kjønn som denne. Bildene blir slettet umiddelbart. Metropolitan Police har brukt teknologien blant annet til å skanne større folkemengder. (UK ICO 2005)

[24] USA har innført systemer for overvåkning av passasjerer som går under betegnelser Computer Assisted Passenger Presrcreening System (CAPPS) og Positive Passenger-Bag Matching (PPBM).

I luftfarten er lagring av passasjeropplysninger gjeldende praksis. Som et ledd i bekjempelsen av illegal innvandring er det foreslått nye regler om rapporteringsplikt for personer som reiser innenfor Schengen-området (Datatilsynet 2004a: 22). Også passasjeropplysninger innhentet av reisebyråer legges i sentrale databaser. Reiselivet har utarbeidet retningslinjer for håndtering av passasjerlister/kundelister (Datatilsynet 2004a: 23). Lister med passasjerdata ("Passenger Name Record" (PNR)) må nå utleveres av alle selskap på flyvinger til og fra USA. Her lagres dataene i egne databaser og kan sammenlignes med personopplysninger fra andre databaser. Avtalen ble erklært ugyldig av EU-domstolen sommeren 2006. I en ny avtale som ble undertegnet i juli 2007 sikres amerikanske myndigheter tilgang til passasjerdata, men nasjonale myndigheter gis rett til å suspendere overføringer av opplysninger dersom gjeldende beskyttelsesnormer overtres (Schartum 2007).

Kontroll av luftfartøy

EU-regelverket omfatter sikkerhetskontroll av fly før de tas i bruk (når de kjøres inn eller umiddelbart etter de er kjørt inn i sikkerhetsbeskyttede områder) og sikkerhetssjekk for fly som er i bruk. Kontroll og sjekk skal gjennomføres etter at alle serviceleverandører har forlatt fartøyet og disse skal ikke ha tilgang til flyet etter denne sjekken. Alle fly som er i bruk skal overvåkes, mens fly som ikke er i bruk skal sikres på en forvarlig måte. Blant annet skal kabindører holdes lukket, luftbroer og trapper skal være trukket tilbake, og dører skal være forseglet.

2.2.2 Sjøfart

Lover og forskrifter

Som for luftfarten er det omfattende internasjonale regelverket for sikring av sjøfarten mot ulovlige handlinger implementert i Norge gjennom tilpasningen til EUs regler på området. EUs forordning for sikring av sjøfarten[25] er tatt inn i norsk rett gjennom Forskrift om sikkerhet og terrorberedskap om bord på skip og flytende boreinnretninger.[26] Denne gjelder for skip over 500 tonn bruttotonnasje og stiller krav om:

- Dokumentasjon for skip som ankommer norsk sjøterritorium om at de følger gjeldende internasjonale krav om sikring (lovens § 3a)
- Særskilte sikkerhetssertifikater og prosedyrer for besiktigelse og kontroll, samt nærmere bestemmelser om dokumentasjon og utstedelse av slike sertifikat (lovens § 41a)

Slike systemer har som formål å identifisere passasjerer som trenger utvidet sikkerhetskontroll (National Research Council 1999). CAPPS identifiserer passasjerer og velger ut personer som antas å utgjøre en sikkerhetsrisiko for utvidete undersøkelser bl.a. av bagasje. Flere av terroristene som gjennomførte terroraksjonen 11. september 2001 ble identifisert og sjekket gjennom dette systemet. En oppfølging under betegnelsen CAPPS II har vært drøftet, men er trukket tilbake etter press fra personverninteresser mv. En videreføring av CAPPS vil trolig implementeres i 2010 under betegnelsen "Secure Flight".

[25] FORORDNING 725/2004/EF

[26] Forskriften er hjemlet i Skipssikkerhetsloven (LOV 2007-02-16 nr 09: Lov om skipssikkerhet).

- Sikkerhetsutstyr (lovens § 42)

Nærings- og handelsdepartementet (NHD) har overordnet ansvar for skipstrafikk og havner, mens Sjøfartsdirektoratet har oppfølgingsansvar for den delen av regelverket som retter seg mot de enkelte skip. Kystverket har ansvaret for det konkrete arbeidet som knytter seg til oppfølging av sikkerhetstiltak i havnene. (St.meld. nr. 31 (2003-2004): 64).

NHD anslår at ca. 1000 norske passasjer- og lasteskip omfattes av regelverket. Det er også anslått at kostnadene ved implementering ligger på rundt 100.000 kroner per skip. Kystverket har ansvaret for det konkrete arbeidet som knytter seg oppfølging av sikringstiltak i havnene. For de største havneanleggene er kostnadene anslått til et sted mellom 3 og 10 millioner kroner (St.meld. nr. 31 (2003-2004): 64). [27]

Sikringsplaner, prosedyrer og opplæring

EU-regelverket pålegger skipsførere og havneansvarlige å fastlegge sikringsnivåer for de enkelte skip og havneanlegg.[28] Sikringsplanene skal inneholde retningslinjer for beskyttelse mot sikkerhetsrelaterte hendelser for hvert av disse nivåene.

Det skal være utarbeidet en godkjent sikringsplan for hvert enkelt skip og disse skal ta hensyn til ulike sikringsnivåer. Planen kan kontrolleres og godkjennes av en anerkjent sikkerhetsorganisasjon. Sikringsplanen skal minimum omfatte tiltak for å:

- Sikre mot uautorisert adgang til skipet
- Utpeke områder med adgangsbegrensninger
- Utarbeide prosedyrer for å møte sikkerhetstrusler og brudd på sikringsreglene, evakuering, evaluering av sikringsaktiviteter, opplæring og øving og dessuten prosedyrer for inspeksjon og kontroll av sikringsutstyr
- Utarbeide prosedyre for anvendelse og kontroll av skipenes alarmsystemer

---

[27] Stortingsmeldingen (St.meld. 31 (2003-2004)) legger også vekt på at det har vært betydelig fokus på maritim transport innenfor "Initiativet for spredningssikkerhet" ("The Proliferation Security Initiative" (PSI)) og at initiativet forventes å berøre norsk skipsfart. Norge er blant de 14 landene som deltar i den såkalte kjernegruppen i PSI. Blant tiltak som vurderes er inngåelse av bilaterale bordingsavtaler og deltagelse i øvelsesaktiviteter. Det er etablert en interdepartemental kontaktgruppe for koordinering og nasjonal oppfølging av initiativet. Et annet viktig forum for internasjonalt samarbeid er den juridiske komiteen som skal sluttføre revisjonen av konvensjonen "Suppression of Unlawful Acts against the Safety of Maritime Navigation" (SUA-konvensjonen) innen 2005. Dette arbeidet medfører at SUA-konvensjonen vil være oppdatert i forhold til det nye trusselbildet (St.meld. nr. 31 (2003-2004): 66).

[28] FORORDNING 725/2004/EF bruker betegnelsen sikringsnivå, mens det i Forskrift FOR 2004-06-22 nr. 972 brukes betegnelsen beredskapsnivå.

Skipenes sikringsansvarlige (sikkerhetsoffiserer) har ansvar for å gjennomføre inspeksjoner, oppdatere sikringsplaner, sørge for gjennomføring av sikringsplanenes bestemmelser og underrette rederiets sikringssansvarlige om eventuelle mangler.

Rederienes sikringsansvarlige har spesielt ansvar for å informere om skipenes risiko og andre relevante opplysninger. De har også ansvar for at det gjøres sårbarhetsvurderinger og utarbeides sikringsplaner. Rederiets sikkerhetsoffiserer har et overordnet ansvar for å sikre tilstrekkelig opplæring på skipene og sørge for effektiv kommunikasjon mellom skipenes sikkerhetsoffiserer og havnenes sikringssansvarlige.

Sikringsansvarlig for havneanleggene har tilsvarende ansvar for å gjennomføre sikkerhetsundersøkelser, lage sikringsplaner og følge opp og foreslå endringer av disse for havneanlegget. Den ansvarlige har særlig ansvar for opplæring, rapportering av hendelser til myndighetene og sørge for koordinering med sikringstjenesten.

Kontroll av personale

Kontroll av sjøfolk er regulert i den Internasjonale arbeidstakerorganisasjonen (ILO) sin konvensjon om sjøfolks identitetsbevis.[29] Disse skal blant annet inneholde biometriske opplysninger (fingeravtrykk), et digitalt bilde og en maskinlesbar sone. Opplysninger om utstedte, suspenderte eller tilbaketrukne identitetsbevis skal lagres i en elektronisk database i hvert medlemsland (St.meld. nr. 10 (2004-2005)).

I Norge er Sjøfartsdirektoratet ansvarlig for gjennomføringen av ILO-konvensjonen. Direktoratet innførte nytt ID-kort for sjøfolk i 2004 (SID) som har lettet verifisering av sjøfolks identitet i mange havner og grenseoverganger som dekkes av IMO-regelverkets ISPS-kode[30] (Sjøfartsdirektoratet 2004a).

Kontroll ved ombordstigning

Sikring av skip skjer ved gjennomføring av en rekke tiltak som blant annet omfatter kontroll med hvem som skal ha adgangstillatelse, kontroll med om bord-stigning, tilsyn med håndtering av last og lagerrom og beskyttelse av sikringsrelaterte kommunikasjonsinnretninger. For havneanleggene kreves det tilsvarende tiltak.

---

[29] ILO-konvensjon 185 inneholder nye krav til identifikasjon av sjøfolk. Norge støttet den nye konvensjonen som trådte i kraft den 9. februar 2005. Konvensjonen inneholder krav om at det landet der vedkommende er statsborger skal utstede identitetsbevis for denne (St.meld. nr. 10 (2004-2005)).

[30] International Ship and Port Facility Security Code (ISPS-koden) er IMOs internasjonale regelverk for sikring av skip og havner. Koden gjelder for alle de 148 statene som er part i SOLAS-konvensjonen (Safety of Life at Sea Convention). Regelverket omfatter lasteskip over 500 tonn bruttotonnasje og passasjerskip i utenriksfart (samt flyttbare boreplattformer) og havner som betjener slike skip.

Sikringstiltakene som er beskrevet ovenfor gjelder ved ”Sikringsnivå 1”. Ved høyere sikringsnivåer (2 og 3), vil det i tillegg kreves supplerende beskyttelsestiltak som er beskrevet i sikringsplanene for skipene og havneanleggene.

Kontroll av frakt

Transportkjeden for maritime containere er kompleks, samtidig som det mangler en ansvarlig instans som kan kontrollere hele kjeden. Dette gjør transportkjeden sårbar (ECMT 2005: 36). De tradisjonelle sikringstiltakene for sjøtransport av containere har vært knyttet til tyveri og bruk av containere til smugling og innføring av ulovlige gjenstander:

- Kontroll og overvåkning av landgangen på skip fra land (*Gangway security*). Denne kontrollen bør være kontinuerlig fra skipet legger til kai til det forlater havnen og omfatte en liste over ombordstigninger og en oversikt over alle personer om bord. Kontrollen omfatter også overvåkning for å hindre uautorisert ombordstigning eller bording (Elliot 1990: 30)
- Systematisk planlegging ved lasting på skip som gjør det mulig å identifisere sårbare containere og øke informasjonssikkerheten for EDB-systemene (*Cargo security*). Disse tiltakenes hovedformål har vært å hindre tyveri fra lasten (Elliot 1990: 32).
- Tiltak på ferger og ”*Roll-on-roll-off*-fartøy” har vært rettet mot kontroll av tyveri fra lastbiler på dekk under overfart (Elliot 1990).

Sikring av containere i intermodal transport er nærmere beskrevet i avsnitt 2.2.3.

Kontroll av skip og havneanlegg

Kontroll og overvåkning av skip og havneanlegg skjer gjennom overvåkning av områder med adgangsbegrensning, overvåkning av dekkareal og områder rundt skipet samt overvåkning av selve skipet gjennom terroralarm.

IMOs regelverk krever at alle skip skal ha terroralarm. Alle skip bygget etter 1. juli 2004, alle passasjerskip og alle skip med spesiallast (oljetankere, kjemikalietankskip, mobile oljerigger m.m.) skal ha installert et alarmsystem før første tilsyn etter juli 2004. For andre skip skal alarmsystemet være installert ved første kontroll etter den 1. juli 2006.

Terroralarmen er knyttet til et automatisk identifikasjonssystem og baseres på et posisjonsbasert system for overvåkning av skip. Regelverket inneholder flere krav til alarmsystemet. For det første skal alarmen være stille og kun sendes til en kompetent myndighet i flaggstaten og altså ikke til andre skip. I Norge er terroralarm koblet direkte til hovedredningssentralen på Sola (St.meld. nr. 31 (2003-2004):65). Sikringsalarmen skal fortsette inntil den avbrytes eller nullstilles. Alarmen skal kunne aktiveres fra broen og fra minst et annet sted på skipet. Den skal være beskyttet på en slik måte at den ikke skal kunne utløses ved en feiltakelse.

Ansvaret for inspeksjon og kontroll av at skipene overholder de internasjonale kravene til sikring av sjøtransporten tilligger de nasjonale myndigheter der skipet befinner seg. I en sikkerhetsmelding fra Sjøfartsdirektoratet gjengis resultatene fra en inspeksjon om bord på et norskregistrert skip som ble gjennomført av den nordamerikanske kystvakten i 2004. Rapporten fra kystvakten viser til flere mangler og utilstrekkelig kjennskap til ISPS-koden. Blant annet var det ingen adgangskontroll og fartøyets sikkerhetsoffiser var ikke kjent med sine sikringsoppgaver (Sjøfartsdirektoratet 2004b). En konsekvens av dårlig oppfølging av krav til sikring vil være at skipene nektes anløp.

2.2.3 Intermodal godstransport på vei og jernbane

Lover og forskrifter

Relevante hjemler i Norge for sikring av intermodal godstransport på vei og bane vil særlig være Lov om yrkestransport med motorvogn og fartøy (yrkestransportloven) og Jernbaneloven med tilhørende forskrifter. Jernbanelovens § 5 stiller særskilte krav til sikkerhetsreglement og til personell med sikkerhetsansvar. Utenlandske transportører (som GreenCargo) må ha sikkerhetssertifikat utstedt av Jernbanetilsynet. Yrkestransportlovens § 5 gir bestemmelser om tillatelse til å drive godstransport på vei.[31] Yrkestransportloven fastslår at egentransport av gods kan drives uten tillatelse.[32]

Sikringsplaner, prosedyrer og opplæring

For transportørene har sikringstiltak for godstransport i stor grad handlet om å redusere risiko for tyveri og narkotikasmugling. Speditørene har utarbeidet egne planer og gjennomført tiltak i egen regi både for å unngå økonomiske tap og for å motvirke dårlig rykte i bransjen. Prosedyrer for fysisk sikring av omlastningsplasser og terminaler har vært viktig og omfatter blant annet tiltak i containerhavner, i godsterminaler, men også på parkeringsplasser for lastebiler og ved varehus.

ECMT og OECD har ønsket å rette fokus på containertransport fordi den er spesiell sårbarhet og fordi containere kan brukes til transport av eksplosiver mv. (ECMT 2005). Det pekes også på at terroristnettverk i dag bruker containere som et ”*logistic support system*” mer enn et ”*weapon delivery system*” (ECMT 2005: 19). EU-kommisjonen påpeker at veitransporten er særlig sårbar og trenger spesiell oppmerksomhet: Den består av flere tusen aktører med busser og lastebiler og som beveger seg innenfor EUs grenser (European Commission 2003).

---

[31] Nærmere regulering av krav til speditører er gitt i Forskrift om yrkestransport innenlands med motorvogn og fartøy (Yrkestransportforskriften) og setter krav om politiattest for utøver av en transporttjeneste. Forskriftens § 14 gir hjemmel for et løyveregister som inneholder informasjon om alle utstedte tillatelser.

[32] Krav til utførelse av sikkerhetsbestemmelser for egentransport må derfor gis i forskrifts form. Krav til fysiske sikringstiltak for omlastningsplasser for gods vil kunne gis i forbindelse med behandling av reguleringsplan etter Plan- og bygningslovens § 25 nr. 3 om offentlige trafikkområder i forbindelse med § 26 om reguleringsbestemmelser.

Tiltak for å øke sikkerheten vil ha ulik virkning avhengig av om terroristene bruker metodene ”kidnapping” eller ”trojansk hest” (ECMT 2005). De fleste tiltakene for sikring av gods vil kunne forhindre plassering av ulovlig last i containere. I forhold til en ”falsk” handelsidentitet er det kun fysisk inspeksjon, kontroll av dokumenter og selskapsinformasjon, samt preventiv etterretning som vil kunne forhindre et anslag (ECMT 2005: 46f).

Det er særlig posisjonsbasert overvåkning (GALILEO) og bakgrunnskontroll av ansatte i bransjen som vil kunne få konsekvenser for personvern, mens mer klassiske sikringssystemer som låsing og sikker lasting vil ha færre implikasjoner.

Fysisk sikring av omlastnings- og lagringsplasser

Containere er mer utsatt for manipulasjon og plassering av ulovlige gjenstander ved lagring på omlastningsplasser, hvor containerne kan være uten oppsikt over lengre tid. Særlig utsatt er jernbaneanlegg og parkeringsplasser (ECMT 2005: 61). I følge ECMT (2005: 58) er sikringsnivåene ved grenseoverganger innenfor EU/EØS svært forskjellige med hensyn til bruk av EDB-systemer, røntgen og bemanning. ECMT påpeker betydning av fysisk sikring av lagerplasser og sikkerhetssjekk av ansatte for å øke beskyttelsesnivået (ECMT 2005: 61). Også EU-kommisjonen foreslår at transportørene bør gjennomføre fysiske sikringstiltak og sikring av IT-systemer (European Commission 2003: 8).

Kontroll av personell

I rapporten fra ECMT og OECD konkluderes det med at behovet for å sikre containerne er stort, men at hele lasteprosessen må sees under ett for å nå et økt beskyttelsesnivå: ”*Any container seal is only as good as the container stuffing and sealing process in which it is involved*” (ECMT 2005: 57). ECMT legger derfor vekt på at det har stor betydning for beskyttelsesnivået hvem som ansettes i transportvirksomhetene (ECMT 2005: 61).

Også EU-kommisjonen foreslår at det skal innføres grunnleggende sikringstiltak rettet mot de ansatte i transportbransjen slik som innføring av egne identitetskort og kontroll av de ansattes vandel og bakgrunn.

EU-kommisjonen viser til konseptet ”*secure actor*” og hevder at identifikasjon av skippere og flyførere kan øke sikringsnivået. Det forslås derfor å utvide dette konseptet til andre transportgrener. Dette vil gi brukerne sikker informasjon om sikringsstandarden til transportørene slik at de kan ta hensyn til dette når det velger speditør. Bruk av ”registrerte” transportører vil da både kunne redusere risiko og føre til færre kontroller og forsinkelser (European Commission 2003: 9). De enkelte medlemslandene vil være ansvarlig for revisjoner og inspeksjoner, hvis ”secure actor”-konseptet gjennomføres i EU. Kommisjonen legger vekt på at det vil være nødvendig med tilstrekkelige kontroller for å nå det ønskede målet om forbedret sikring av godstransporten.

Kontroll og overvåkning av containere

For godstransporten vil en adgangskontroll innebære screening av containere som betingelse for at disse gis ”adgang til transportnettet”. Dette betyr i praksis kontroll av gods ved omlastningsplasser og bruk av bestemte sikringsklarerte containere for visse transportkjeder. Adgangskontroll av containere vil være nært knyttet til overvåkning, særlig gjennom overvåkning av containere og lastebiler i transportsluser.

Rapporten fra ECMT viser til at fysisk inspeksjon av innholdet i en container vil være det klart mest effektive tiltaket, men også et meget kostbart og tidkrevende tiltak. Slike sikringstiltak kan derfor komme i konflikt med kravet om en rask og billig transport av gods i et felles europeisk marked. Ved kontroll av containere skilles det mellom kontroll (fysisk inspeksjon eller skanning) og vurdering av hvilke containere som har høy risiko (ECMT 2005: 47).

I USA har containersikring være sterkt fokusert de senere år. Det amerikanske konseptet ”*Container Security Initiative*” (CSI) inneholder flere elementer:

- Informasjonsutveksling om gods: Informasjon om last til USA skal oversendes 24 timer før containeren lastes på skip som skal til havn i USA
- Etablering av kriterier for å kunne identifisere containere med høy risiko
- Bruk av teknologi for rask vurdering/sjekking
- Utvikling av sikre og ”smarte” containere

For å forhindre terrorisme vil det være nødvendig å kunne spore containere gjennom hele transportkjeden, både for å identifisere containere med høy risiko og for å spore opp containere på avveier. Dette kan både skje ved registrering av containere ved ”sluser” i transportkjeden eller ved permanent overvåkning ved hjelp av satellittovervåkning (GPS) (ECMT 2005: 61). ECMT-rapporten anbefaler registrering ved ”sluser” i transportkjeden, men viser til at transportørene i første omgang må få hjelp til å forbedre interne sporingssystemer. Disse dataene kan gi nøyaktig informasjon om hvor containerne befinner seg på et bestemt tidspunkt. Myndighetene og transportindustrien kan samarbeide om å samle denne informasjonen i et sporingssystem (ECMT 2005: 63).

EU-kommisjonen foreslår økt bruk av avanserte elektroniske informasjons-systemer for visse laster. Et system for posisjonsbasert informasjonsformidling vil kunne brukes til å identifisere mistenkelige laster og være til nytte i forbindelse med krisehåndtering. For visse laster og/eller transportkorridorer vil et slikt informasjonssystem kunne gjøres obligatorisk og informasjonen vil da kunne formidles mellom medlemstater ved behov (European Commission 2003: 9) Slike informasjonssystemer vil også kunne bidra til en mer effektiv logistikk.

Kontroll av transportmidlene

Tiltak for å kontrollere transportmidlene vil ofte være knyttet til fysisk og elektronisk sikring. Elektronisk forsegling kombinerer fysisk sikring med informasjon om status. Avanserte systemer vil kunne formilde en rekke typer av informasjon (for eksempel om radioaktivitet, CO_2, biologiske data) og kan kombineres med globale posisjoneringssystemer. Avanserte låsesystemer kan

imidlertid også gi en falsk trygghet og en ulovlig "ettermontering" kan i verste fall gjøre det lettere for en container å ferdes med illegal last (ECMT 2005: 53f).

Undersøkelser foretatt av *US Cargo Handling Co-operative Program* viser at teknologien for elektronisk sikring er klar for kommersialisering, men at det kreves internasjonale standarder (ISO) for at dette skal kunne implementeres. Rapporten viser til flere muligheter for å gjøre containeren "smartere" – for eksempel en kombinasjon av en passiv RFID containermerking[33] , semi-passiv elektronisk lås på container og aktiv cargo-identifikasjonsmerke (ECMT 2005: 58).

2.2.4 Persontransport på vei og bane

Lover og forskrifter

Også for sikring av persontransporter vil Lov om yrkestransport med motorvogn og fartøy (Yrkestransportloven) og Jernbaneloven med tilhørende forskrifter inneholde relevante regler. Vilkårene for å drive persontransport er de samme som for godstransport og omfatter blant annet politiattest for personell som har sikringsansvar og utarbeidelse av egne sikkerhetsreglementer. Andre tiltak for å øke sikring i persontransporten er ikke hjemlet i særlover på området.

I transportselskaper organisert som aksjeselskap har styret ansvar for forsvarlig organisering av virksomheten. Virksomheten vil da ha et selvstendig ansvar for å tilby sine kunder en transporttjeneste med høy grad av sikkerhet. Det er imidlertid usikkert hvor langt ansvaret går i forhold til å iverksette tiltak mot ulovlige handlinger som tar sikte på å skade passasjerer og/eller infrastruktur. Internt sikringsarbeid kan også være fordelt på flere virksomheter og datterselskap.

Sikringsplaner, prosedyrer og opplæring

Prosedyrer for sikkerhet og opplæring av personell er en del av transportvirksomhetenes interne rutiner. Opplæringsforskriften gjelder for jernbane, herunder sporvogn, tunnelbane og forstadsbane. Forskriften setter krav om opplæring av personell som jobber med oppgaver som er relevante for sikkerheten (safety). Det stilles ingen krav om opplæring relatert til sikringstiltak mot ulovlige handlinger.

Fysisk sikring av infrastruktur

Fysisk sikring av vei og bane kan gjelde for eksempel anlegg uten tilgang for allmennheten slik som verksteder, vedlikeholdsanlegg og parkeringsplasser for busser og togmateriell. Sikring av slike områder vil kunne hindre sabotasjehandlinger fra inntrengere og ordinært hærverk. Oslo Sporveier har de senere år avdekket flere tilfeller av mulig sabotasje mot vognmateriell på verkstedet på Ryen.

---

[33] RFID står for Radio Frequency Identification. Et RFID-system består av en server, en sender og en mottaker. RFID-merking av en container innebærer at containeren utstyres med en "tag" med informasjon om identitet, innhold, posisjon osv.

Fysisk sikring kan også omfatte tiltak for å beskytte jernbanetraseer, broer og andre infrastrukturanlegg. Mulige tiltak kan være adgangsbegrensninger, overvåkning og varslingssystemer. Tiltak som gjelder fysisk planlegging av verksteder, parkeringsanlegg og servicestasjoner vil i stor grad være sammenfallende med tiltak som beskrevet i avsnitt 2.2.3 om intermodal transport av gods.

Kontroll av passasjerer

Det er få tiltak som er rettet spesielt mot sikring av persontransport på vei og bane. Fram til nå er det ikke vært innført flyplasslignende sikringstiltak for disse transportgrenene som økt kontroll av passasjerer og bagasje. Det vanligste (og mest omdiskuterte) tiltaket som hittil er tatt i bruk er kameraovervåkning og registrering av data som innhentes fra en slik overvåkning.

Terroraksjonene i London og Madrid viser at tog og T-bane er meget sårbare. Samtidig vil det være praktisk vanskelig og meget kostbart å kontrollere alle adgangsmuligheter til slike kollektive transportsystemer. Disse transportmidlene frakter et meget stort antall mennesker, og muligheten for fysisk adgangskontroll til terminaler, perronger eller til selve transportmidlet er begrenset. En talsmann for EU-kommisjonen illustrerer problemet med en altomfattende sikring av forstadsbaner: "*RER in Paris carries three million people a day. You can not scan three million people*" (EUPolitix 2004).

I London er det utarbeidet nye sikringstiltak for å bedre sikringsnivået på sentrale jernbanestasjoner. Blant disse tiltakene er skanning av passasjerer som på en flyplass. Som nevnt er dette tiltaket gjennomført som et forsøk på Paddington stasjon i London (EurActiv 2005, derStandard 2005).

En annen mulighet for passasjerkontroll er ved hjelp av elektroniske betalingskort. Ved bruk av slike billettsystemer vil det være mulig å koble informasjon fra kundekonto med data for påstigning og avstigning på det kollektive transportsystemet. Slike data kan blant annet brukes i etterforskingsøyemed, se avsnitt 2.3.

I Nederland brukes elektronisk betalingskort i Rotterdam-regionen, og systemet skal utvides til å gjelde kollektivtransport i hele Nederland. Selv om formålet med innføring av elektroniske betalingssystemer primært er å effektivisere betalingen og redusere muligheten for sniking, kan slike systemer også brukes til overvåkning og sporing av passasjerer.

Personlige, elektroniske reisebevis vil bli tatt i bruk i stadig større omfang også i Norge. Elektroniske billetter brukes i mange fylker/transportselskap i dag (Datatilsynet 2004a: 19). For Oslo-regionen har Oslo Sporveier i lang tid hatt planer om å innføre et nytt billett- og betalingssystem i samarbeid med Stor-Oslo Lokaltrafikk (SL) og Norges Statsbaner (NSB). Dette systemet vil sammen med fysiske sperreporter for T-banen, føre til bedre kontroll med betalingen. Systemet medfører at alle passasjerer må være i besittelse av et smartkort med RFID-teknologi. Elektroniske billetter kan både utstedes som et personlig smartkort med foto og som et upersonlig overførbart betalingsmiddel (Oslo Sporveier 2004, SL 2002).

Økt bruk av elektronisk billettering vil kunne gi muligheter for økt sikkerhets-kontroll og overvåkning av den enkelte reisende. Hvis et slikt tiltak skal være effektivt i forhold til planlagte ulovlige handlinger, vil imidlertid registreringen måtte være meget omfattende. I kollektivtransporten vil slik registrering kunne skje gjennom obligatorisk bruk av personlige elektroniske billetter. For veitransporten er det mulig å tenke seg adgangskontroll til veinettet basert på elektronisk systemer for gjenkjenning av registreringsnumre, eller satelittbasert overvåkning, for eksempel i forbindelse med innføring av veiprising som ikke tillater anonym ferdsel. For en vurdering av mulighetene for økt registrering av personopplysninger til andre formål enn sikring, se avsnitt 2.3.

Kontroll av bagasje

Generelt er det lite eller ingen kontroll av de reisenes bagasje på bane eller buss. Det er mulig å skanne bagasje for eksempel ved inngang til togperronger eller bussterminaler. Et slik tiltak vil imidlertid være svært kostnadskrevende hvis det skal gjennomføres i stort omfang (og nokså meningsløst om det gjennomføres i lite omfang). Skanning av bagasje er derfor foreløpig bare vurdert i forbindelse med spesielle traseer som for eksempel kanaltunnelen mellom Storbritannia og Frankrike. Denne banen har få stasjoner for på- og avstigning og dermed gode muligheter for effektiv adgangskontroll (Clutterbuck 1994 og UK ICO 2005). Skanning av bagasje kan også være aktuelt for oppbevaring av bagasje i oppbevaringsbokser på jernbanestasjoner og andre transportterminaler, men det er svært få steder der dette gjøres.

Problemstillingen rundt bagasjesjekk på tog ble særlig aktualisert etter at to bomber i etterlatt bagasje ble funnet i Tyskland sommeren 2006. Muligheten for å skanne all bagasje ble imidlertid raskt avvist:

"We have between 4.5 million and 4.7 million travellers at 5400 stops and train stations every day. You cannot put millions of people and their luggage through a metal detector every day."
(Talsperson for tysk jernbane til Reuter,
http://www.rmtbristol.org.uk/2006/08/rail_security_questioned_after.html)

Kontroll av transportmidlene.

Det er i prinsippet mulig å utarbeide et tilpasset regelverk for sikringsrelatert kontroll av kjøretøy for offentlig persontransport som bygger på metodikken for kontroll av luftfartøy (jfr. avsnitt 2.2.1). En slik kontroll vil innebære at busser og tog gjennomsøkes regelmessig i forholdt til mulige plassering av bomber eller andre ulovlige gjenstander før det settes i drift etter opphold på rutebilstasjon eller terminal. For skinnegående transport og transport med buss vil det imidlertid være mulig å plassere ulovlige gjenstander i transportmidlet når det er i (rute)drift. For å forhindre slike muligheter måtte man innføre et system med skanning av passasjerer og bagasje før ombordstigning for å sikre transportmiddelet. Som kjent gjøres dette i luftfarten, men for kollektvitransport med buss og bane vil dette være svært kostbart og praktisk meget vanskelig. Det ville trolig også føre til at mange ville velge alternative transportmidler.

Overvåkning med kamera og posisjoneringssystemer

I forbindelse med bombefunnene i Tyskland tok flere politikere til orde for kraftig økning av kameraovervåkning i jernbane og annen kollektivtrafikk (http://www.rmtbristol.org.uk/2006/08/rail_security_questioned_after.html).

Kameraovervåkning brukes i stadig større grad for å sikre områder der allmennheten har tilgang, ikke minst på kollektivknutepunkter som jernbane- og T-banestasjoner. Kameraovervåkning er også blant de mest diskuterte tiltakene for sikring av offentlige transportmidler og jernbanestasjoner. Det har vært flere forsøk med kameraovervåkning i ulike transportmidler i Europa, blant annet i Berlin, Oslo, Brussel og Wien (Hempel & Töpfer 2002: 6f). Slik overvåkning har særlig vært begrunnet med kriminalitetsbekjempelse og dermed økt sikkerhet for allmennheten.

Kameraovervåkning av stasjonsområder og transportmidler i Norge er hjemlet i Personopplysningsloven, og lovens regler for meldeplikt kommer til anvendelse (Schartum og Bygrave 2004: 166).[34]

Kameraovervåkning vil også kunne øke muligheten for sosial kontroll. Leon og Töpfer (2002) gir eksempler på at kameraer for overvåkning av trafikken har vært brukt til andre formål, bl.a. til filming av demonstrasjoner (Leon og Töpfer 2002: 9). Heidi Mork Lomell konkluderer i sin doktorgradsavhandling med at private vektere bruker kameraovervåkning for å holde uønskede personer vekk fra det overvåkede området (Graven 2005).

Omfanget av kameraovervåkning har økt betydelig de senere år. I Datatilsynets årsmelding for 2006 var 8 prosent av over 9000 telefonhenvendelser spørsmål om kameraovervåkning (St.meld. nr. 5 (2007-2008)). Datatilsynet er av den oppfatning at det meste av økningen i kameroverv̊åkning skyldes at teknologien er blitt billigere og lettere tilgjengelig, og dermed tas mer i bruk. Datatilsynet mener at omfanget av ulovlig kameraovervåkning dermed også har økt St.meld. nr. 5 (2007-2008); 23. I følge Wiecek og Sætnan (2002) var om lag 5 prosent av spørsmålene om kameraovervåkning som Datatilsynet hadde til behandling i 2001 knyttet til transport og samferdsel. De fleste sakene som Datatilsynet behandler når det gjelder kameraovervåkning dreier seg følgelig ikke om virksomheter relatert til transport og samferdsel. Økningen de senere år har i særlig grad vært i forbindelse med overvåkning av kunder og ansatte i butikk, og sivil/privat overvåkning (nabolag, borettslag og lignende) (St.meld. nr. 5 (2007-2008).

Datatilsynet fremhever imidlertid samferdsel som et område der mange nye initiativer for elektronisk og annen overvåkning er på trappene, og advarer spesielt mot streknings-ATK. Dette er et system for å måle gjennomsnittsfart mellom to punkter på en veistrekning, og det innebærer at alle kjøretøyer som

---

[34] Hjemmel for en generell kameraovervåkning av offentlige steder kan være Personopplysningslovens § 8d som setter vilkår for når kameraovervåkning skal være tillatt dersom overvåkningen er nødvendig for å utføre en oppgave av allmenn interesse. Kameraovervåkning av steder hvor en begrenset krets av personer ferdes jevnlig, er bare tillatt hvis det ut fra virksomheten er et særskilt behov for overvåkningen (personopplysningslovens § 38). Konsesjonsplikten etter § 33 i Personopplysningsloven gjelder kun når billedopptak fra kameraovervåkning lagres på en måte som gjør det mulig å finne igjen opplysninger om en bestemt person (Personopplysningslovens § 37).

passerer det første punktet fotograferes og bildet lagres inntil kjøretøyet har passert det andre punktet hvor gjennomsnittsfart beregnes. Dersom farten har vært for høy, overføres opplysningene til politiet. Datatilsynet uttaler:

"Ved å ta i bruk en systemteknologi som tar bilde av alle biler, er en helt ny infrastruktur for omfattende overvåkning blitt etablert."

(St.meld. nr. 5 (2007-2008); 28)

Det er store forskjeller i holdninger til bruk av kameraovervåkning i de europeiske landene, men i de senere år har slik overvåkning på offentlige steder fått generelt høy aksept (Wiecek og Sætnan 2002, Sætnan, Lomell & Wiecek 2004, Ravlum 2005). I en spørreundersøkelse Opinion gjennomførte for NSB i 2005 svarte åtte av ti at de var positive til kameraovervåkning i buss, tog, trikk og T-bane (Bergens Tidende 2005). Tilsvarende resultater gjenfinnes i en undersøkelse Norstat gjennomførte for Teknologirådet i mai 2007. Tre av fire mente det bør tillates mer overvåkning i samfunnet dersom det gjør hverdagen tryggere (Teknologirådet 2007b). Folk er imidlertid mer skeptiske dersom overvåkning innebærer overvåkning av personer som ikke har gjort noe galt. Sætnan m.fl. (2004) fant også at folk var mer skeptiske til kameraovervåkning hvis overvåkningsområdet ble oppfattet som privat og/eller intimt. Et klart flertall var i mot kameraovervåkning i den gaten de selv bodde.

Storbritannia er blant de landene med størst erfaring med bruk av kameraovervåkning i offentlige rom. I 1991 gjennomførte IRA bombeeksplosjoner på Paddington og Victoria Station i London noe som førte til innføringen av en rekke sikringstiltak på jernbaneterminaler i London. Tiltakene omfattet kameraovervåkning, økt belysning, patruljering av stasjonsområder og toaletter samt fjerning av søppelkasser (Dwyer 2003: 128).

I Sverige ga Länsrätten i 1998 AB Stor-Stockholms Lokaltrafik rett til å bruke kameraovervåkning for å øke sikkerheten, mens svenske taxiselskaper har fått avslag på tilsvarende søknader om å installere kameraer i motsetning til taxiselskaper i Norge, Danmark, Storbritannia og Tyskland (Lindkvist m.fl. 2002).

Videoopptak fra kameraer på forstads- og bybaner har blitt brukt som bevismateriale i kriminalsaker i Danmark og Sverige, og dette har ført til økt aksept for slik overvåkning. Etter en domsavgjørelse i Regeringsrätten i 2000 er det blitt lettere å sette opp overvåkningskameraer på offentlige plasser i Sverige. I Malmø ble det gitt tillatelse til et prøveprosjekt hvor kameraene styres av politiet og der politiet kan gå inn og zoome manuelt. Justisdepartementet i Sverige var imidlertid skeptisk til denne utviklingen (Lindkvist m.fl. 2002).

I Tyskland ble det første systemet for kameraovervåkning av offentlig plasser installert i Leipzig i 1996. I 2000 anbefalte ministerne for de føderale innenriksdepartementene bruk av kameraovervåkning på kriminalitetsutsatte områder. I en høring til en rapport fra innenrikskomiteen i det tyske parlamentet (Bundestag) definerte ekspertene imidlertid kameraovervåkning som et inngrep i borgernes privatsfære og de mente at et slikt inngrep trengte lovhjemmel. Mot slutten av 2001 hadde alle føderalstater bortsett fra Berlin vedtatt lovhjemler for kameraovervåkning (Hempel & Töpfer 2002).

Under de olympiske leker i Athen i 2004 ble et meget avansert overvåkningssystem utprøvd. Systemet innebar bl.a. lagring av data fra over 1000 høyoppløselige overvåkningskameraer, automatisk lesning av e-post, av internettrafikk, telefonsamtaler og SMS-utveksling samt lyddata fra mikrofoner som var montert på overvåkningskameraene. Bilder og lyd ble elektronisk behandlet av programvare for å tolke hendelsesforløp og mønstergjenkjenning (Ström 2006a).

Det foregår en rivende utvikling når det gjelder intelligente transportsystemer (ITS) med store potensialer for overvåkning og styring av trafikk. Det er for eksempel teknisk mulig å overvåke veitransporten ved hjelp av satellittovervåkning av kjøretøyer ved hjelp av geografiske posisjoneringssystemer GPS og Galileo. Slike systemer vil kunne brukes til å spore opp enkeltkjøretøy, til å registrere posisjon og fart og de kan koples mot andre systemer som f.eks. eCall. eCall er et system for automatisk varsling av ulykker, som vil bli obligatorisk i alle nye biler i Norge og en rekke andre land fra og med september 2009. eCall er basert på satellittposisjonering av kjøretøy og varsler automatisk politi og ambulansetjeneste ved ulykker.

I Storbritannia har man gått langt i retning av teknologisk trafikkovervåkning og registrering. Her er det innført et omfattende system med automatisk fotografering og lagring av bilenes nummerskilt (”Automatic Number Plate Recognition” (APNR)). Systemet benyttes primært til å identifisere stjålne kjøretøy, men har også blitt utnyttet for å spore annen kriminalitet (Ström 2006b). I Storbritannia er det også prøvet ut et system med forsikringsrabatt til bilister som installerer atferdsregistrator i bilen (Teknologirådet 2007a), og et lignende forsøk er i gang blant unge bilførere på Karmøy (Nettavisen 2007).

2.3 Bruk av opplysninger til andre formål

Elektronisk databehandling av person-, steds- og tidsbestemte data vil kunne bli betydelig ettersom det utvikles ny teknologi som gjør det mulig å registrere og lagre data i stort omfang. Selv om det er knyttet en betydelig samfunnsmessig interesse til transportsikring, er dette i liten grad begrunnelsen for å innføre elektronisk registrering og behandling av data. Ny teknologi som innebærer behandling av personopplysinger brukes primært for å effektivisere betalingssystemene i transportsektoren.[35]

Alle tiltakene som beskrives i dette kapitlet er tiltak som gjennomføres i transportsektoren og som har implikasjoner for personvernet, men med et annet formål enn sikring (kategori B i figur 2.1). Ved formålsendring vil disse tiltakene imidlertid kunne brukes til økt transportsikring – da særlig i forhold til preventiv etterforskning av alvorlige kriminelle handlinger.

[35] Oslo Sporveier påpeker i sin årsrapport for 2004 at innføringen av nytt billett- og betalingssystem vil være bedriftsøkonomisk lønnsomt på grunn av mer effektiv betaling og mindre sniking (Oslo Sporveier 2005).

2.3.1 Økt registrering av personopplysninger i transportsektoren

I transportsektoren registreres store mengder data. Registreringsnummer for kjøretøy brukes blant annet til kontroll av trafikk og trafikanter, for eksempel ved passering av bomstasjoner, ved fartskontroller og for å bestemme om reglene om kjøre- og hviletid overholdes.

Et sentralt register er førerkortregisteret (Autosys). Utlevering fra dette registeret er begrenset til myndigheter med hjemmel. Innhenting av opplysninger fra motorvognregisteret blir regulert gjennom offentlighetsloven. Også private aktører som parkeringsselskap får tilgang til personopplysninger (navn, adresse) via registreringsnummer for å kunne sende faktura. Andre viktige registre i veisektoren er det sentrale registeret over prikkbelastninger, verkstedregisteret, løyveregister for yrkestransport, kjøreskoleregisteret og ulykkesregisteret (Datatilsynet 2004a: 14f). Annen registrering knyttet til biltrafikk er ferdskrivere og elektronisk kjøretøyidentifikasjon (EVI).

Trafikkovervåkning kan foregå uten å samle inn personopplysninger, men flere tiltak forutsetter innhenting og lagring av slike opplysninger. Automatisk trafikkontroll (ATK) gjennomføres som punktkontroll og ved å bruke stillbilder av registreringsnummer og førers ansikt. Disse dataene kan kobles sammen med opplysninger som hentes fra det sentrale motorvognregisteret. Statens vegvesen har ønsket å ta i bruk systemet med streknings-ATK i lang tid, men dette er blitt stanset fordi det innebærer lagring av opplysninger om personer som ikke har brutt loven (i motsetning til tradisjonell ATK).

Datatilsynet har nylig påklaget at alle biler som passerer bomstasjonene med bruk av AutoPASS-brikke blir avfotografert til tross for at dette ikke er i overensstemmelse med AutoPASS' kravspesifikasjon. Dette er det heller ikke blitt informert om til publikum eller til Datatilsynet (Datatilsynet 2007).

I de helautomatiske bomstasjonene som prøves ut i Tønsberg, Bergen og Gjesdal skjer betalingen ved elektronisk registrering og avregning fra kundekonto eller ved etterfakturering på grunnlag av kameraopptak. Innføring av helautomatiske bomstasjoner fører til økt registrering av personopplysninger. For de ulike betalingsformene er det innført regler og rutiner for registrering, lagring, bruk og utlevering av personopplysninger som skal sikre samsvar med personopplysningsloven. Passeringsdata som innhentes i forbindelse med veiavgifter lagres for et bestemt tidsrom, slik at kundene kan kontrollere at fakturaene er riktig. På bakgrunn av erfaringene med forsøksordningene, har Statens vegvesen fått konsesjon til et nytt betalingsalternativ, hvor passeringsopplysninger anonymiseres og slettes etter kort tid (Statens vegvesen 2006).

På bakgrunn av erfaringene med forsøksordningene, har Statens vegvesen foreslått et nytt betalingsalternativ, sporingsfri avtale, hvor passeringsopplysninger anonymiseres og slettes etter kort tid (Statens vegvesen 2006).

Personopplysningsloven inneholder regler om at opplysninger fra for eksempel bompengestasjoner, ikke kan leveres til utenforstående uten at det finnes et selvstendig behandlingsgrunnlag for dette. Utlevering av kameraopptak til politiet kan skje ved etterforsking av straffbare handlinger eller ulykker. For utlevering av

andre personopplysninger kreves det selvstendig behandlingsgrunnlag, som regel rettslig kjennelse for utlevering. Sporfrie alternativ vil føre til at politiet i mindre grad kan hente ut relevante data fra bompengeselskapene til slike formål.

Satellittnavigasjonssystemet GALILEO skal legge til rette for et harmonisert elektronisk avregningssystem (Europäische Kommission 2001: 84f). I 2004 ble det vedtatt et direktiv som skal sikre samsvar i systemene for innkreving av veiavgifter mellom i de ulike medlemslandene.[36] Direktivet tillater registreringssystemer som bygger på mobil kommunikasjon (GSM), satellittnavigasjon (GPS/GALILEO) og mikrobølgeteknologi som i det norske AutoPASS-systemet. Det tas imidlertid sikte på at nye systemer skal bruke GPS-teknologi nettopp for å kunne åpne for flere telematikktjenester gjennom samme system.[37] Datatilsynet viser til at GALILEO legger til rett for applikasjoner og tjenester som innebærer kontinuerlig registrering. Disse systemene kan innføres frivillig for så senere å bli obligatorisk gjennom krav fra myndighetene (Datatilsynet 2004a: 8). Datatilsynet nevner flåtestyring av taxier fra taxisentraler som eksempler på GPS-løsninger som kan forventes å få personverns-implikasjoner (Datatilsynet 2004a: 16f).

Datatilsynet viser til at også elektroniske betalingssystemer for kollektivtrafikk medfører betydelig registrering og lagring av personopplysninger. Elektroniske billetter innebærer at informasjon om kundedata, reisebevis og reisedata ligger lagret i elektronisk form. Reisedata omfatter informasjon som tidspunkt for reiser, transportmiddel, takstsone med mer. Datatilsynet poengterer at det bør finnes likeverdige anonyme alternativer, som for eksempel systemer basert på RFID-teknologi der elektroniske billetter kan fylles opp i kortautomater uten at korteier identifiseres (Datatilsynet 2004a: 19).

2.3.2 Personopplysninger fra transportsektoren kan brukes til andre formål

Det er gjort en rekke utredninger som berører bruk av informasjons- og kommunikasjonsteknologi (IKT) i transportsektoren. Vegdirektoratets etatsprosjekt ”ITS på veg” inngår som en del av Vegvesenets oppfølging av Samferdselsdepartementets vektlegging av og satsing på *intelligent transport systems* (ITS). Etatsprosjektet tar ikke opp sikring og personvern som tema, men prosjektet er forankret i målsetninger om effektiv transport, trafikksikkerhet og miljø (Statens vegvesen 2002). Statens vegvesen, Vegdirektoratet har nylig opprettet et nytt etatsprosjekt ”Personvern og trafikk” der slike problemstillinger blant annet skal behandles.

Flere utredninger om bruk av IKT berører forholdet til personvern (Teknologirådet 2005, Ravlum 2004, Lindkvist m.fl. 2002), men ser ikke på hvilken betydning IKT kan få for transportsikring og bruk av elektroniske data til preventiv og oppklarende etterforsking.

Erfaringer fra Storbritannia viser imidlertid i noen grad hva slags potensial som ligger i slike systemer. Som nevnt har APNR-teknologien også blitt brukt i

[36] DIREKTIV 2004/52/EF

[37] DIREKTIV 2004/52/EF, betraktning (2)

etterforskning av ordinær kriminalitet, og nylig også brukt for å etterforske terrorhandlinger. En av de mistenkte bak bilbombene i Glasgow og London i juni/juli 2007 ble identifisert ved hjelp av APNR-teknologien og stanset og arrestert på motorveien M6.

Økt bruk av elektronisk registrering av data gir et stort teknisk potensial for å bruke personopplysninger til andre formål enn det dataene ble innhentet for. Dette omfatter også muligheten for å sammenstille informasjon fra ulike registre (Teknologirådet 2005: 89). Det vil i utgangspunktet stride mot prinsippet om formålsbestemthet i personopplysningsloven (Personopplysningslovens § 11b). Allmenne interesser av stor betydning vil imidlertid kunne gi en begrunnelse for å gjøre unntak fra formålsregelen, for eksempel i forbindelse med politietterforskning (Schartum 2007). En slik bruk av dataene vil imidlertid kreve en egen hjemmel. Ved bruk av en selvstendig hjemmel vil det også være mulig å knytte et nytt formål til datainnsamlingen (Schartum og Bygrave 2004: 137).

2.3.3 Terror som begrunnelse for økt generell overvåkning

Terrorbekjempelse er et formål som generelt har stor legitimitet. Store terrorhendelser kan derfor påvirke beslutningstakernes holdninger til behovet for sikring mot slike hendelser og gi økt aksept for tiltak som har implikasjoner for personvernet. Interesseorganisasjonen Statewatch[38] kritiserer EUs tiltak for kriminalitetsbekjempelse som er foreslått av det Europeiske Rådet etter bombeaksjonen i Madrid 2004. Statewatch hevder at tiltakene har lite eller ingenting å gjøre med håndtering av terrorisme, men mer med generell kriminalitetsbekjempelse og overvåkning og at disse kan misbrukes til politisk og sosial kontroll. Statewatch nevner spesielt lagring av kommunikasjonsdata, formidling av passasjerlister til preventiv etterforsking og bruk av biometriske pass (Statewatch 2004). EUs strategi for terrorbekjempelse åpner for iverksettelse av en samordnet etterforskning og bruk av utvidede politimetoder innenfor EU-området. Disse tiltakene er imidlertid blitt karakterisert som uforholdsmessige av politiske beslutningstakere (European Parliament 2005).

Store terrorhendelser påvirker i stor grad beslutningstakernes holdninger til behovet for sikring og hvilke interesseavveininger som gjøres i forhold til personvernet. De fleste strategier som er foreslått for å bekjempe terror og annen alvorlig kriminalitet vil ha implikasjoner for personvernet. Valg av hjemmelsgrunnlag vil ha betydning for hvilke kriterier som vektlegges i utarbeidelsen av lovhjemmel for sikringstiltakene. Det kan ha betydning for interesseavveiningen mellom transportsikring og personvern, hvorvidt tiltakene begrunnes og hjemles ut fra lover som dekker politi- og sikkerhetsarbeidet, eller om disse tar utgangspunkt i personvernlovgivningen.[39]

---

[38] Statewatch er en frivillig organisasjon grunnlagt i 1991. Organisasjonene består av advokater, akademikere, journalister, forskere og aktivister. Et av hovedformålene for Statewatch er å påvirke debatten om sivile rettigheter og demokratisk åpenhet. (http://www.statewatch.org/)

[39] Amerikanske myndigheter satte i gang et omfattende overvåkningsprogram i kjølvannet av terrorangrepene 11. september 2001. Programmet består blant annet i elektronisk overvåkning av telefonsamtaler med utlandet og e-post. Justiskomiteen i Senatet har kommet med ni formelle henvendelse om tilgang til dokumenter som beskriver overvåkningsprogrammet og stevnet i juni

For EUs institusjoner har det vært viktig å reagere raskt og målrettet på terrorhendelsene etter 2001. De tilgjengelige virkemidlene (policy instruments) som EU rår over er i hovedsak relatert til generell kriminalitetsbekjempelse. Dette kan være en forklaring på hvorfor EUs arbeid med terrorbekjempelse har hatt fokus på etterforsking og tiltak relatert mot forebygging av kriminalitet.

Også i Norge har hensynet til terrorbekjempelse åpnet for en økt aksept for utvidede etterforskningsmetoder som kommer i konflikt med personvernet. Truslene fra organisert kriminalitet og terror var bakgrunnen for at Politimetodeutvalget ble nedsatt i juli 2001. Utvalget leverte sin utredning i 2004 (NOU 2004: 6). Flertallet i utvalget viste til at den organiserte kriminaliteten er blitt stadig mer uoversiktlig og at faren for terrorvirksomhet har økt. De mente derfor at politiet har et generelt behov for å kunne ta i bruk utvidede metoder. De viste til at det er få lovhjemler som åpner for inngripende metoder for å forebygge kriminalitet (NOU 2004: 6, s. 18). Mindretallet var kritisk til slike utvidede metoder og viste til at forebyggende politimetoder har klare betenkelige sider. Dette gjelder da særlig forberedelse av straffbare handlinger. Mindretallet var likevel "*.. enige med flertallet i at det* er *behov for selvstendige forebyggende metoder for Politiets sikkerhetstjeneste*" (NOU 2004: 6: 19).

I september 2006 ble fire personer arrestert og siktet for planlagte terrorhandlinger mot den amerikanske og den israelske ambassaden. Politiet hadde for første gang benyttet spionmikrofoner i en bil for å avsløre planene (Dagbladet 2006). Denne etterforskningen med bruk av skjulte mikrofoner for å forebygge terrorhandlinger er en konsekvens av endringer i straffeprosessloven som følge av forslag fra Politmetodeutvalget (NOU 2004: 6).

2.4 Sikring mot terror er en ny utfordring for transportsektoren

Ansvaret for sikring i forhold til "dagligdagse" hendelser i transportsektoren er lagt til de ulike virksomhetene. Dette følger av at virksomhetene har et selvstendig

---

2007 Presidenten for å få tilgang til dokumentene. President Bush har hele tiden hevdet at han i følge grunnloven har rett til å godkjenne overvåkning i krigstid uten rettens godkjennelse. Sommeren 2007 ble det vedtatt en ny lov "The Protect American Act" som stadfester myndighetenes rett til elektronisk overvåkning av e-post og telefonsamtaler med utlandet uten krave rettslig godkjenning (Aftenposten 2007a)

I EU vil hjemmelgrunnlaget for et direktivforslag være avhengig av hvilke traktatbestemmelser som direktivet referer til. Dette har betydning blant annet for hvilke bestemmelsesprosedyrer som velges og hvilke utvalg i det Europeiske Parlamentet som får ansvar for rapportering. Denne konflikten er blitt tydelig i diskusjonene om det Europeiske Rådets forslag til rammedirektiv om lagring av kommunikasjonsdata. Hjemmelsgrunnlaget for direktivforslaget var her bestemmelsene om felles handlinger for å bekjempe kriminalitet i Traktaten om den Europeiske Unionen. Direktiv om disse bestemmelsene treffes etter samrådsprosedyren. Europaparlamentets komité for borgerrettigheter viste til at bestemmelser om lagring av kommunikasjonsdata måtte hjemles i gjeldene personvernslovning og at det foreliggende direktivforslaget ville være i konflikt med gjeldene europeisk regelverk om personvern. Utvalget var derfor av den oppfatning av bestemmelsene måtte hjemles i Artikkel 47 i Traktaten. Regler om lagring av kommunikasjonsdata måtte derfor ifølge komiteen for borgerrettigheter treffes etter medbestemmelsesregelen som gir det Europeiske Parlamentet større innflytelse (European Parliament 2005).

ansvar for å følge de lover og forskrifter som gjelder for de ulike transportgrenene. Herunder følger også at de enkelte virksomhetene har et selvstendig ansvar for å sikre tilstrekkelig sikkerhet ved ytelse av transporttjenester.

Forebyggende tiltak for å forhindre terror er et "nytt problem" for de norske institusjonene utenfor luftfarten. Det kan derfor være rimelig å anta at institusjonelle tradisjoner for sikkerhetsarbeid i Norge påvirker utforming, implementeringen og organisering av sikringsarbeidet i transportsektoren. Organiseringen av trafikksikkerhet og sikring mot ulovlige handlinger er tredelt:

1. For nasjonal sikkerhet har institusjonene og myndighetenes arbeid vært rettet om sikring av objekter som er viktige for at samfunnet skal kunne fungere godt i en krisesituasjon. Strategien til norske sikkerhets-myndigheter vil være særlig rettet mot sikringsverdige objekter og sårbarhetsreduserende tiltak. Direktoratet for samfunnssikkerhet og beredskap (DSB) har på sin side ikke noen spesiell rolle eller kompetanse på forebyggende tiltak, men har ansvaret for å sikre en god beredskap som kan redusere konsekvensene av en eventuell storulykke eller terror-hendelse.
2. Forbyggende tiltak for å sikre transportsektoren mot ulovlige handlinger kan også omfatte etterforskning av mulige terrorgrupperinger som kan ha transportsektoren som mål for sine aksjoner. Politiets sikkerhetstjeneste (PST) har en relativ stor frihet til å vurdere bruk av utvidede etter-forskningsmetoder som vil ha betydelige implikasjoner for personvernet og kreve en særskilt interesseavveining. I Politimetodeutvalget var det bred enighet om at terrorbekjempelse bør åpne for annen og utvidet bruk av preventive etterforskningsmetoder (NOU 2004: 6).[40]
3. Transportsektoren har på sin side sikkerhetstiltak som en integrert del av sine institusjonelle oppgaver. I luftfart og til dels sjøfart er security en integrert del av sikkerhetsarbeidet. I vei- og banetransport er sikkerhetstiltak først og fremst knyttet til tradisjonelt trafikksikkerhetsarbeid (*safety*) og har lite til felles med tiltak som er rettet mot sikring mot ulovlige handlinger (*security*). vei.

For luftfarten og sjøfarten stiller regelverket klare krav til og gir hjemmel for arbeidet med sikring. Mye av sikringsarbeidet på vei og bane foregår i dag uten klare nasjonale føringer eller hjemmel. Det betyr at sikringsarbeidet er en del i det interne sikkerhetsarbeidet i transportbedriftene, og at de enkelte virksomhetene i liten grad er forpliktet til å rapportere eller å informere myndigheter og offentligheten om sitt arbeid med sikring mot ulovlige handlinger.[41]

---

[40] Instruks for Politiets sikkerhetstjeneste inneholder bestemmelser om behandling av personopplysninger ved forebyggende etterforskning (Kgl. res. 2005-18-04).

[41] For transportbedrifter med sikringsverdige objekter eller som forvalter sikkerhetsgraderte informasjoner gir sikkerhetslovens § 5 generelle plikter som blant annet omfatter utarbeidelse av en intern sikkerhetsinstruks. Samtidig skriver Nasjonal Sikkerhetsmyndighets i sin risikovurdering for 2006 at det er mangler i sentrale deler av sivil forvalting med hensyn til sikkerhets-administrasjon. Dette omfatter sikkerhetsorganisering, rapporteringsrutiner, instrukser, ansvarsforhold og metodiske krav til risikovurdering (NSM 2006: 6f).

2.5 Transportsikring som en del av nasjonalt sikkerhetsarbeid

Sikring av transportsektoren mot terrorhandlinger kan også tenkes forankret i det nasjonale sikkerhets- og etterretningsarbeidet. I Stortingsmelding nr. 39 (2003-2004) om samfunnssikkerhet og sivilt-militært samarbeid vises det til at det er nødvendig med preventiv etterforskning av terrornettverk: *"I kampen mot terrorisme er det viktigste tiltaket å forebygge terrorangrep ved å avdekke og stoppe terrornettverk før de er i stand til å gjennomføre angrep*." (St.meld. nr. 39 (2003-2004): 6)

I Stortingsmelding nr. 39 (2003-2004) legges det vekt at framveksten av internasjonal terror gjør det nødvendig å revurdere organiseringen av samarbeidet mellom sivilt beredskap og militæret. I meldingen heter det således: *"Framveksten av internasjonale terrornettverk og trusler om bruk av masseødeleggelsesmidler er blitt en viktig del av dagens trusselbilde og har særlig relevans for det sivil-militære samarbeidet*" (St.meld. nr. 39 (2003-2004): 6).

Stortingsmeldingen gjennomgår samfunnssikkerhet i ulike sektorer og dens organisering. Det vises til at Justisdepartementets samordningsrolle for samfunnets sivile sikkerhet er tydeliggjort og styrket. Meldingen viser blant annet til:

- Etableringen av Direktoratet for samfunnssikkerhet og beredskap (DSB)
- Nasjonal sikkerhetsmyndighet (NSM) har fått faglig ansvarslinje til Justisdepartementet for det som gjelder den sivile sektoren
- Permanent sekretariat for Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene
- Omorganisering av Sivilforsvaret
- Kontaktgruppe for forebygging av terrorhandlinger under ledelse av Politiets sikkerhetstjeneste (PST)

Meldingen legger vekt på å beskrive det sivilt-militære samarbeidet som en konsekvens av endringene i trusselbildet og en omfattende omstilling i Forsvaret (St.meld. nr. 39 (2003-2004): 5).

Nasjonal sikkerhetsmyndighet (NSM) ble opprettet i 2003. Myndighetens oppgaver er knyttet til forebyggende sikkerhetsarbeid. Lovgrunnlaget for NSM sitt arbeid er sikkerhetsloven fra 1998 som har som formål *"å sikre skjermingsverdig informasjon og skjermingsverdige objekter mot sikkerhetstruende virksomhet som spionasje, sabotasje og terrorhandlinger. Det er informasjon og objekter med betydning for rikets selvstendighet og sikkerhet som i denne sammenheng regnes som skjermingsverdige*" (www.nsm.stat.no).

Private og offentlige virksomheter med sikringsverdig informasjon eller sikringsverdige objekter er ansvarlig for det konkrete sikringsarbeidet, mens NSM koordinerer dette arbeidet som fagmyndighet. Blant oppgavene er sikkerhetsklareringer og vurdering av trusselbilde. Hvorvidt det nasjonale sikkerhetsarbeidet er relevant for transportsektoren vil være avhengig av om transportvirksomhetene besitter sikringsverdige objekter eller ikke.

Ved å beskrive terror som ny trussel for Norge, gis en begrunnelse for hvorfor nye metoder må vurderes i politiarbeidet. Disse blir sett på som viktige i arbeidet med å bekjempe alvorlige anslag mot demokratiet og menneskerettighetene. ”*Spesielt når det gjelder forbygging og bekjempelse av terror skal relevante faglige og politiske innspill vurderes*” (St.meld. nr. 39 (2003-2004): 6). Bruk av nye virkemidler innenfor preventiv etterforskning skal ifølge Regjeringen veies opp mot ønsket om et åpent demokratisk samfunn (St.meld. nr. 39 (2003-2004): 6).

3 Personvern og transportsikring – personverninteresser og nasjonale og internasjonale rettskilder

3.1 Innledning og oversikt

3.1.1 Problemstillinger

Ambisjonen i denne delen av prosjektet var å

- "Analysere hvordan sikkerhetstiltakene forholder seg til personverninteressene (interesseteorien) og til relevante norske og europeiske rettskilder. Hva er rettstilstanden i Norge og hvordan vil denne kunne påvirkes av de internasjonale utviklingstrekkene?"

Med "personverninteressene" sikter en her til den interesseteorien som har vært utviklet i Norge siden tidlig på 1970-tallet og som har ligget til grunn for mye av norske lovarbeider på personvernområdet, herunder ved forberedelse av personregisterloven (1978) og personopplysningsloven (2000). Interesseteorien representerer en tilnærming til personvernet med klart rettslig preg. Formuleringen av interesser er basert på analyser av aktuelle saker som har vært behandlet ved domstolene og i Datatilsynet mv., og som kan sies å gjelde personvern. Et annet viktig grunnlag er debatter i media om personvern.

Personverninteressene representerer primært en systematisering av fremførte relevante argumenter i personvernsaker og -debatter, og sier intet om hvilken vekt det enkelte argument skal ha. Tvert i mot forutsetter interesseteorien at det skal skje en avveining (på samfunnsnivå eller individuelt nivå) der andre argumenter – for eksempel vedrørende security i transport – kan gi som resultat at personvernet i en viss grad må vike. Avveiningene må likevel skje innenfor rammene av bestemmelsene i Den europeiske menneskerettighetskonvensjonen (EMK) art. 8 som gir grunnleggende beskyttelse for personvern.

En viktig del av denne deloppgaven har vært å gjennomgå og klargjøre denne interesseteorien, herunder vurdere om teorien slik den har vært formulert er adekvat i forhold til de problemstillinger som security i transport reiser.

Interesseteorien er bl.a. vurdert opp i mot aktuelle sikkerhetstiltak. Det har imidlertid ikke ligget innenfor rammene av denne deloppgaven å gjennomføre empiriske undersøkelser av de faktiske tiltakene. I stedet er interesseteorien vurdert opp i mot de sikkerhetstiltak som det er gitt hjemmel for i lov og forskrift. Security-tiltak vil normalt innebære så inngripende regulering i forhold til enkeltpersoner og virksomheter at *legalitetsprinsippet* i norsk rett innebærer at det må kreves at tiltaket har hjemmel i lov eller i forskrift i medhold av lov. Prosjektet er med andre ord basert på en forutsetning om at den aktuelle

kontrollen har lovlig hjemmel. Vi tror dette er en rimelig forutsetning, men kan imidlertid ikke påstå med sikkerhet at det ikke skjer kontroll som savner den nødvendige rettslige forankringen.

Interesseteorien er også vurdert opp mot norske og europeiske rettskilder som kan sies å være relevante for spørsmål vedrørende security i transport. Prosjektet har vært begrenset til undersøkelse av aktuell lovgivning mv. og europeisk regulering i form av forordninger, direktiver og utkast til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler. Domspraksis er ikke undersøkt. Den rettslige beskrivelsen har ikke tatt sikte på å gå i dybden på enkeltspørsmål (slik domsavgjørelser ofte gjør), men har hatt som ambisjon å tegne et helhetlig bilde av hvorledes rettstilstanden og rettsutviklingen på dette feltet er i Norge, sett i en europeisk kontekst.

Store deler av det aktuelle regelverket gjelder regler som er av direkte betydning for fysisk kontroll av personer og for behandling av personopplysninger (jf. "personopplysningsvern"). Viktige deler av dette regelverket er oversiktlig og greit å avgrense. Dette gjelder særlig regelverk som eksplisitt enten gjelder behandling av personopplysninger eller fysiske sikkerhetstiltak innen en transportgren (og som derfor kan ha betydning for personvernet). Undersøkelsen dekker imidlertid ikke alle transportgrener, men legger størst vekt på luftfart og tog/skinnegående transport.

Innenfor rammene av prosjektets tid og budsjett har det vært vanskelig å fange opp de mange spredte bestemmelser som finnes i prosesslovgivning og annen særlovgivning som kan ha betydning for bedømmelsen av personvern. Dette gjelder spesielt de regler som gjelder for politi, påtalemyndigheter og domstoler; nasjonalt og internasjonalt. Det ville også ha vært av interesse å kartlegge tilsvarende regler for tollmyndigheter.

Samtidig har det vært viktig å dekke denne delen av norsk og europeisk rett i et visst omfang, fordi slike myndigheter i stor grad får tilgang til personopplysninger; enten gjennom egen direkte informasjonsinnsamling eller fordi det skjer innsamling av personopplysninger i sivil sektor for securityformål som tilflyter politi mv. Denne utfordringen er håndtert ved at det er gjennomført analyser av foreliggende utkast til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler (European Commission 2005). Denne rammebeslutningen er ment å utgjøre den felles europeiske reguleringen på området og vil derfor trolig ha stor betydning for den fremtidige rettstilstanden i Norge og Europa i årene fremover.

Opplegget vi har valgt innebærer at får frem forskjeller i vernenivå mellom personopplysningsvernet etter personverndirektivet og lov om behandling av personopplysninger på den ene side og foreslåtte regler for personvern innen politi og domstoler mv. på den annen side. Vi får imidlertid ikke beskrevet forskjellen mellom personopplysningsvern innen politi- og domstoler i Norge i dag og det mulige fremtidige vernenivået som kan bli resultatet av EUs rammebeslutning.

I tillegg til regelverk som direkte gjelder personvern og sikring av transportmidler har vi inkludert enkelte andre regelverk i studien som åpenbart har stor betydning for problemområdet. Dette gjelder primært datalagringsdirektivet som i april 2007 ennå ikke var gjennomført i norsk rett, og enkelte bestemmelser i

sikkerhetsloven.[42] Det er mulig at også annet regelverk burde vært med, og det kan også være at sikkerhetsloven burde ha vært behandlet i større omfang. Spørsmålene knyttet til utvalg av regelverk viser imidlertid hvor vanskelig det er å formulere relevanskriterier som gir en håndterlig avgrensing av problemområdet. Problemet uttrykker en generell innsikt, nemlig at security i transport i sin ytterste konsekvens gjelder informasjonsbehandling og kontroll med personer i et åpent samfunn. I dette ligger det en forutsetning om at et meget stort antall kilder for informasjon kan være aktuelle, og at kontroll med personer kan være aktuelt i mange situasjoner og på mange ulike steder. Et meget vidt kontrollfelt gir tilsvarende vid og vanskelig avgrensning av aktuelle lover og regelverk.

3.1.2 Metode

Forskningsmetodikken som er benyttet i denne juridiske gjennomgangen har vært markert forskjellig for de ulike delene av arbeidet. Arbeidet med interesseteorien har bestått i aktiviteter som – isolert sett – ligger på grensen av det som av mange kan karakteriseres som forskning. Her har oppgaven langt på vei vært å aktualisere foreliggende beskrivelser av interesseteorien i forhold til security i transport. Den ansvarlige forskeren (Dag Wiese Schartum) er, sammen med Lee A. Bygrave, selv forfatter av den siste og i dag mest anvendte fremstillingen av personvernteorien (Schartum og Bygrave 2004). Et viktig element av dette arbeidet har derfor vært å formidle eksisterende resultater fra tidligere juridisk forskning. I tillegg er det gitt supplerende vurderinger og tillegg til den etablerte interesseteorien ut fra særlige trekk ved den kontrollvirksomhet som er aktuell for ivaretakelse av security i transport. Dette er primært basert på en normativ-deskriptiv analyse av de personverninteresser og det security-arbeidet som allerede er etablert.

Interesseteorien er bygget opp ved hjelp av fem "personverninteresser" der hver interesse konkretiseres i spesifikke "krav" som må anses å være realisert for at interessen skal kunne anses å være varetatt. De normative-deskriptive analysene i dette arbeidet resulterer i forslag til presiseringer eller nye kravformuleringer.

Når det gjelder utvalg og analyse av aktuelle lover, forskrifter, direktiver, forordninger mv., kan forskningsmetoden beskrives som en modifisert rettsdogmatisk metode. Modifiseringen innebærer at prosjektet ikke har gjort bruk av hele spekteret av rettskilder, men primært er basert på ulike typer regelverk og forarbeider til disse. Årsaken er ønsket om å tegne "det store bildet" og få frem "horisontale" sammenhenger i eksisterende regler, snarere enn å gå i dybden på enkelte rettsspørsmål slik et tradisjonelt rettsdogmatisk arbeid ville gjøre. Denne tilnærmingen innebærer at resultatet fra prosjektet ikke kan hevdes å si noe sikkert om den detaljerte rettslige forståelsen av de aktuelle regelverkene, og konklusjonene kan derfor vanskelig brukes direkte i argumentasjonen vedrørende konkrete saker. Styrken ved denne tilnærmingen er at det for politikkutvikling, valg av fremtidige regeltekniske løsninger mv. er lettere å se viktige mønstre og sammenhenger. Man unngår med andre ord å "ikke se skogen for bare trær"!

---

[42] Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) av 20. mars 1998 nr.10.

Problemområdet ”security i transport” er spesielt utfordrende fordi det er i stadig og rask endring. Underveis i arbeidet har det vært gjort viktige vedtak av EU-forordninger, og det har vært omfattende og skiftende diskusjoner av den kommende rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler.

Samtidig som rettsutviklingen er betydelig og rask er deler av disse endringsprosessene lukkede, noe som gjør det vanskelig å følge med i utviklingen. Et annet vesentlig problem i studien av de rettslige reguleringene har vært et ikke ubetydelig hemmelighold av rettsregler. Flere av EUs forordninger samt nasjonale dokumenter vedrørende flysikkerhet er hemmelige og har derfor ikke kunnet inngå i analysene i prosjektet. Som ledd i siste delen av arbeidet fikk prosjektansvarlige tilbud fra Luftfartstilsynet om tilgang til Nasjonalt Sikkerhetsprogram mot å undertegne taushetsplikterklæring. I den aktuelle fasen av arbeidet ble tilbudet ikke benyttet for å unngå en mulig situasjon der innholdet av plandokumentet kunne gjøre det vanskelig å publisere antagelser som allerede var gjort i det foreliggende utkastet til grunnlagsrapport i prosjektet.

3.1.3 Oversikt over kapitlet og type resultater

Arbeidet i deloppgave 2 har primært tre typer resultater. For det første er det særlig med utgangspunkt i teorien om personverninteresser søkt å utvikle generelle forståelser av hva forholdet mellom security i transport og personvern kan sies å handle om, og konkret hvilke mulige interessemotsetninger som kan tenkes å oppstå. Hovedvekt har blitt lagt på å utforske personvernet, dels ved å se på sammenhenger mellom personvern i fysisk forstand (jf. kontroll av personalet og av reisende mv.) og personopplysningsvern, og dels ved å vurdere interesse-teorien i lys av security i transport.

Den andre type resultater fra deloppgave 2 er en oversikt over og vurdering av regelverk som direkte kan sies å ha innvirkning på ivaretakelsen av personvern i tilknytning til arbeidet med security i transport. Denne gjennomgangen viser – ikke overraskende – at personvern får mindre gjennomslag på dette området enn etter den generelle lovgivningen. I grunnlagsrapporten fra deloppgave 2 (Schartum 2007), som dette kapitlet bygger direkte på, kommer dette særlig til uttrykk i den sammenlignende gjennomgangen av reglene i personverndirektivet og utkast til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler (kapittel 14), samt av gjennomgangen av datalagringsdirektivet (kapittel 15) og reglene for sikkerhet i luftfarten (kapittel 16), herunder regler vedrørende tilgang til opplysninger fra plassreservasjonssystemer (avsnitt 16.2.4).

Det kan også være grunn til å anta at de hemmelige reglene vedrørende flysikkerhet kan inneholde bestemmelser der hensynet til personvern har fått lite gjennomslag. Det alt vesentlige av denne delen av rettsutviklingen skjer med utgangspunkt i europeiske og andre internasjonale initiativ. I denne sluttrapporten har vi søkt å presentere nevnte hovedresultater ved å ta utgangspunkt i interesse-teorien og knytte spørsmål vedrørende gjeldende regelverk til den enkelte interesse, se avsnitt 3.3. En viktig del av resultatet fra denne delen av arbeidet består imidlertid av konkrete gjennomganger av sammenheng mellom regelverk og regelinnhold som det ikke er mulig å redegjøre for i denne sluttrapporten. For disse delene viser vi derfor til grunnlagsrapporten (Schartum 2007).

Den tredje typen resultat fra denne delen av arbeidet er det en kan betegne som generelle innsikter vedrørende personvern og security i transport. Dette er resultater som ikke direkte er knyttet til konkrete regelverk eller til interesseteorien, men som er av mer generell karakter. I denne sluttrapporten har vi søkt å presentere slike hovedresultater ved delvis å knytte dem til de europeiske personvernprinsippene (avsnitt 3.4) Andre generelle innsikter blir diskutert uavhengig av denne referanserammen (avsnittene 3.5-3.7).

3.2 Kontroll med personer i et åpent samfunn

Et viktig utgangspunktet for den rettslige undersøkelsen i dette prosjektet er at sikkerhet i transport må forutsettes å kreve innsamling og videre behandling av personopplysninger vedrørende passasjerer og ansatte som er knyttet til transporttjenestene. Det primære formålet med slik informasjonsbehandling er å forhindre anslag og andre sikkerhetshendelser. Også rask og sikker oppklaring av forsøk på eller gjennomføring av anslag er et viktig hensyn.

Forebygging gjelder i forhold til en trussel som i utgangspunktet ikke kan avgrenses til en bestemt persongruppe eller et klart avgrenset miljø. Enhver passasjer, ansatt og annen person som kan komme i kontakt med transportsystemet kan således *i utgangspunktet* utgjøre en trussel. I regelverket søker en bl.a. å takle denne åpne trusselsituasjonen ved å definere visse fysiske rammer der det kan være mulig å skaffe seg nær fullstendig fysisk kontroll over potensielle trusler. Sikkerhetssonene på lufthavner er et godt eksempel. Innen slike rammer er det for eksempel mulig å kontrollere passasjerer bagasje og ansatte før de får tilgang til flysiden i en lufthavn. Kontrollen kan gjelde etablering av personenes identitet, relevante opplysninger om vandel, samt full fysisk kontroll med hva personene bringer med seg av gjenstander som kan tenkes anvendt til å utsette transportmiddelet for fare, jf. også kapittel 2, avsnitt 2.2.1.

Som omtalt i kapittel 2 kan tilsvarende kontrollregime langt på vei anlegges for skip der en har gjennomført egne krav til sikring av havneterminaler for passasjerskip og store lasteskip mv. i internasjonal fart.[43] For tog er det også teoretisk mulig å skille ut internasjonal trafikk eller lignende og etablere egne terminaler som kan sikres på tilsvarende måte, men dette ville åpenbart være så dyrt og begrensende på togtransporten at det er lite aktuelt. For skinnegående transport som trikk, T-bane og lokaltog vil det, som påpekt i kapittel 2, ikke være gjennomførbart med omfattende fysisk kontroll av passasjerer. Dette vil være alt for tidkrevende i forhold til reisetid og forventet effektivitet i transporten. Samtidig kan sikkerhetstruslene mot slik lokal passasjertransport trolig – tidvis – være like store som mot for eksempel flytransport. Sikkerhetstrusselen i disse transportsystemene må derfor trolig i hovedsak møtes på en annen måte enn i luftfart og internasjonal skipsfart.

En annen forskjell mellom transportgrenene dreier seg om sårbarhet underveis, mellom terminaler. Luftfartøy er for eksempel lite sårbare overfor anslag under transport *mellom* lufthavnene fordi det kreves store ressurser og/eller spesiell

[43] Se forskrift FOR 2007-07-03 nr 825: Forskrift om sikring av havner og havneterminaler mot terrorhandlinger mv.

kompetanse for å kunne rette anslag utenfra mot et fly som er i luften. Det er derfor grunn til å tro at full oppmerksomhet om sikkerheten i lufthavner vil gi en effektiv beskyttelse av denne transporten. Skip underveis er mer sårbare, og et tog eller lignende som hele tiden beveger seg på bakken er mye mer sårbart enn både luftfartøy og skip. Derfor gir det forholdsvis lite mening for den totale sikkerheten å stille strenge krav til sikkerhet av stasjonsområder for T-bane og tog mv.

Disse ganske markerte og åpenbare forskjellene mellom de kollektive transportgrenene legger sterke begrensninger på valget av strategier i transportsikringsarbeidet. Slike forskjeller har trolig også stor innvirkning på hvorledes sikringstiltakene påvirker ivaretakelsen av personvernet. I tilfeller der det langt på vei kan etableres områder der alle personer kan kontrolleres fysisk for å få tilgang til området, er det grunn til å anta at behovet for å sikre gjennom *innsamling av personopplysninger* er forholdsvis lite. Motsatt vil manglende mulighet for å etablere fysisk kontroll med mennesker som kan utgjøre en trussel mot sikker transport, gjøre det desto viktigere å innsamle informasjon som kan sette myndigheter i stand til å fange opp og forhindre personer å gjennomføre anslag mv.

Fordi potensielle terrorister er ukjente, og fordi truende planer/intensjoner kan gi seg så mange utslag, blir behovet for tilgang til personopplysninger vidt og ubestemt. Det innebærer at det er vanskelig på forhånd å ta stilling til hvilke opplysninger som vil kunne være interessante. Selv om bare et meget lite utvalg av innsamlet personinformasjon faktisk vil komme til nytte, er det problematisk dersom en på forhånd må binde seg til å bruke visse opplysningstyper på bestemte måter. Informasjonsbehovet kan derfor grunnleggende sett sies å være åpent og dermed uavgrenset.

Dersom forutsetningen om et åpent og – i prinsippet – uavgrenset informasjonsbehov er riktig, innebærer det behov for informasjonsinnsamling fra en lang rekke kilder innen ulike sektorer. Gjennomgangen av regelverket vedrørende behandling av personopplysninger illustrerer hvorledes ulike rettslige reguleringer kommer til anvendelse avhengig av samfunnsområde. Hovedskillet går mellom i) behandling av personopplysninger innen det vanlige sivile samfunn (generell lovgivning og særlovgivning), ii) behandling av personopplysninger innen politi, domstoler mv., og iii) behandling av personopplysninger for rent private/personlige formål.

Behandling av personopplysninger i det sivile samfunn som skjer for rent private og personlige formål er stort sett bare omfattet av enkelte bestemmelser i straffeloven. Øvrig behandling av personopplysninger i sivil sektor er omfattet av personopplysningsloven, og særlige regler kan gjelde for enkelte sektorer. Det er imidlertid ikke vedtatt andre særlige regler vedrørende personopplysninger i transportsektoren enn bestemmelser vedrørende identifisering og vandel. Når det gjelder det rettslige regimet for behandling av personopplysninger for politi og domstoler, er dette fragmentert og vanskelig å få fullgod oversikt over. I denne rapporten er dette regelverket ikke gjennomgått. I stedet er EUs forslag til rammebeslutning for behandling av personopplysninger i denne sektoren omfattet.

Gjennomgangen viser et gjennomgående lavere nivå for personvernet dersom rammebeslutningen blir gjennomført. Det hersker imidlertid stor usikkerhet både

med hensyn til det endelige innholdet av rammebeslutningen og hvorledes denne vil komme til å bli gjennomført i norsk rett.

Poenget her er at det åpne og uavgrensede informasjonsbehovet, som særlig er knyttet til security i transport når det ikke er praktisk mulig å etablere fysisk kontroll med mennesker og medbrakte gjentander, skaper situasjoner der personopplysninger vil måtte innhentes fra mange kilder. Dermed vil det oppstå informasjonsflyt som innebærer at opplysningene krysser grensene mellom ulike rettslige regimer. De rettslige reguleringene innen de ulike rettslige regimene er til dels omfattende og kompliserte og står ikke alltid i et avklart forhold til hverandre. Situasjonen er derfor lite tilfredsstillende når det gjelder regelverk som kan få betydning for personvern i samband med security i transport.

Det er mulig at det tilsynelatende skarpe skillet mellom områder som er under sterk fysisk kontroll (lufthavner, havneterminaler) og åpne miljøer (gater, T-banestasjoner mv.) er lite reelt. Kontrollen ved lufthavner er primært egnet til å hindre flykapring mv. (jf. et stor antall flykapringer f.o.m. slutten av 1960-tallet), sprengning av luftfartøy (Lockerby-ulykken) og bruk av fly som angrepsmiddel (11.9.2001). Likevel er det generelt sett ikke grunn til å tro at terrortrusler kan begrenses til denne typen anslag. Et anslag mot køen for sikkerhetskontroll i en lufthavn, mot et parkeringshus, bagasjeutlevering mv. vil også ramme transportsystemet på avgjørende måte, og ha stor effekt og nyhetsverdi; noe som kan gjøre det attraktivt for anslag.[44] Dette er deler av transportsystemet som er langt dårligere sikret enn flysiden fordi de er deler av det åpne samfunnet på samme måte som jernbanestasjoner mv.

Spørsmålet er videre om det er grunn til å tro at security i transport på vesentlige måter avviker fra sikkerhetsspørsmål på andre livsområder. I utgangspunktet kan det være grunn til å tro at det er ansamling av et stort antall personer, kombinert med symboltunge steder, funksjoner eller tidspunkt som vil være avgjørende for om noe kan ses som terrormål eller ikke. Det kan derfor være grunn til å se anslag mot teatre,[45] skoler[46] og idrettsarenaer[47] som like aktuelle som anslag mot fly, tog og busser mv. Dersom en legger dette perspektivet til grunn, er det sikkerhets-utfordringen knyttet til det åpne sosiale liv (gater, restauranter, T-banestasjoner mv.) som representerer den reelle utfordringen, fordi det handler om sikring mot terror mv. *i et åpent samfunn*, dvs. utenfor områder der det kan etableres full fysisk kontroll med mennesker, bygninger og gjenstander.

Arbeid for å avdekke forberedelser til terroranslag mv. på ethvert sted til enhver tid trekker ytterligere i retning av uavgrensbare behov for informasjon. Forberedelseshandlinger kan skje hvor som helst og i et langt tidsrom forut for det eventuelle anslaget. Dersom forutsetningen om at det kan være mange mulige mål (også annet enn transportmidler) er holdbar, bidrar dette til at det oppstår

---

[44] Et eksempel er anslaget mot terminalbygget i Glasgow sommeren 2007, omtalt i kapittel 2.

[45] Jf. anslaget mot Dubrovka-teateret i Moskva, 2002.

[46] Jf. anslaget mot skole 1 i Beslan i Nord-Ossetia, 2004.

[47] Jf. anslag mot OL i München i 1972 og bomben i Centennial Olympic Park under Atlanta-OL i 1996. Jf også bombeangrepet mot feirende fotballsupportere etter Iraks seier i semifinalen i Asia-mesterskapet i juli 2007 (Dagbladet 25.7.2007).

uavgrensede behov for informasjon. Store deler av disse opplysningene vil være personopplysninger, og skaper således potensialer for at informasjonsinnsamlingen skaper alvorlige personvernproblemer.

3.3 Interesseteorien: undersøkelse av personvernbegrepet

3.3.1 Generelt

Interesseteorien innebærer en detaljering og konkretisering av hva som kan anses å være personvernspørsmål, særlig i tilknytning til behandling av personopplysninger. Utgangspunktet her har vært den etablerte interesseteorien slik den kommer til uttrykk i Schartum og Bygrave (2004). Denne fremstillingen bygger igjen på tidligere fremstillinger fra flere ulike forfattere, skrevet fra og med diskusjonen knyttet til personregistre tok fart tidlig i 1970-årene. Her skal vi nøye oss med å angi hovedpunktene i den systematikken som ble anvendt i dette prosjektet. Punkter i fet kursiv er tillegg som er tatt inn i tilknytning til diskusjonen om security i transport:

- Interessen i å bestemme over opplysninger om egen person.
  - ***Krav om minimalitet og beskyttelse av identitet***
  - Krav om konfidensialitet
  - Krav om beskyttet privatliv
  - Krav om vern av individets identitetsbilde
  - Krav om etablert tillitsforhold
- Interessen i innsyn og kunnskap
  - Krav om rettsinformasjon
  - Krav om generelt innsyn
  - Krav om individuelt innsyn
  - Krav om begrunnelse
- Interessen i opplysnings- og behandlingskvalitet.
  - Krav til opplysningskvalitet
  - Krav til behandlingskvalitet
- Interessen i forholdsmessig kontroll.
  - Krav til forholdsmessighet mellom veiledning og kontroll
  - ***Krav til forholdsmessighet mellom kontrollgrupper***
  - Krav til forholdsmessighet mellom forhåndskontroll og etterkontroll
  - Krav til forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst
  - Krav til forholdsmessighet ekstern og intern kontroll
- Interessen i brukervennlig behandling
  - Krav om lydhørhet
  - Krav om forståelighet
  - Krav om uhindret dialog
  - Krav om driftsstabilitet

- ***Interessen i personvernanalyse***
  - Krav om konsekvensanalyse
  - Krav om løpende kontroll
  - Krav om evaluering

Under "interessen i å bestemme over opplysninger om egen person" er det i samband med dette prosjektet tatt inn en kravformulering vedrørende "minimalitet og beskyttelse av identitet". Dette er en understreking av at forutsetningen for at det overhodet skal oppstå konflikter med personopplysningsvern er at det behandles personopplysninger. Dersom en minimaliserer bruken av slike opplysninger og/eller beskytter identiteten til personene som opplysningene beskriver, vil diskusjonen om personvern kunne bli langt lettere å håndtere. Kravformuleringen er nært knyttet til to av personvernprinsippene i europeisk lovgivning, og inviterer bl.a. til diskusjoner vedrørende bruk av pseudonymer, avidentifisering og endog anonymisering. Enkelte av disse og beslektede spørsmål kommer vi tilbake til i avsnitt 3.6.

I diskusjonen om forholdsmessig kontroll er det tatt inn en kravformulering vedrørende "forholdsmessighet mellom kontrollgrupper". Formuleringen er sterkt inspirert av Karanja (2006) og erkjennelsen av at personvern tradisjonelt har vært beskrevet som en interesse for individer uten at en i særlig grad har vurdert vernebehov knyttet til *grupper* av slike individer. Særlig kan det være grunn til å vurdere gruppevern for sosiale grupper som utgjør en minoritet, er underpriviligerte og/eller er under en eller annen type sosialt press. Ved kontroll av passasjerer kan ytre tegn på religiøs (klær, krav til mat mv.) eller politisk tilhørighet, etnisitet eller nasjonalitet være forhold som kontrollørene vektlegger og der slikt gruppevern kan være aktuelt å vurdere. Tilnærmingen begrunner selvsagt ikke fravær av kontroll med slike grupper, men er en påpeking av at kontrollen i alle henseender bør være forholdsmessig, dvs. stå i et begrunnet forhold til kontrollen med andre grupper/de alminnelige reisende.

Som ledd i dette arbeidet er det også formulert en "interesse i personvernanalyse" med "krav om konsekvensanalyse", "krav om løpende kontroll" og "krav om evaluering". Heller ikke disse formuleringene representerer noe egentlig nytt i den generelle diskusjonen om personvern, men bidrar primært til å tydeliggjøre elementer i den løpende diskusjonen, jf. for eksempel spørsmål om "privacy assessment".[48]

De tre kravformuleringene representerer tre tidsperspektiv på analysen: "Konsekvensanalyse" representerer en proaktiv tilnærming, "løpende kontroll" gjelder analyser som bør skje parallelt med potensielt personvernkrenkende praksis, mens "evaluering" er tilbakeskuende og reaktiv. Det generelle bakenforliggende perspektivet er en "jo-jo-regel":[49] Jo mer krenkende security-tiltak er i forhold til personvern, jo større vekt må det legges på å analysere om tiltakene virker på tilfredsstillende måte. Antakelsen er dessuten at security-tiltak

[48] Se presentasjon av Privacy impact assessment (PIA) hos Office of the Privacy Commissioner of Canada; http://www.privcom.gc.ca/speech/2004/sp-d_040310_e.asp.

[49] Fritt etter professor Erik Boe ved Det juridiske fakultetet i Oslo!

ofte vil være av klart krenkende karakter og at det derfor må være en forventning om at personverneffekten av security-tiltak innen transportsektoren er gjenstand for grundige analyser. I utgangspunktet bør bare krenkelser som en kan dokumentere virkninger av beholdes, og evalueringskriteriene bør fastsettes som en del av vedtaket vedrørende fastsettelse av security-tiltaket.

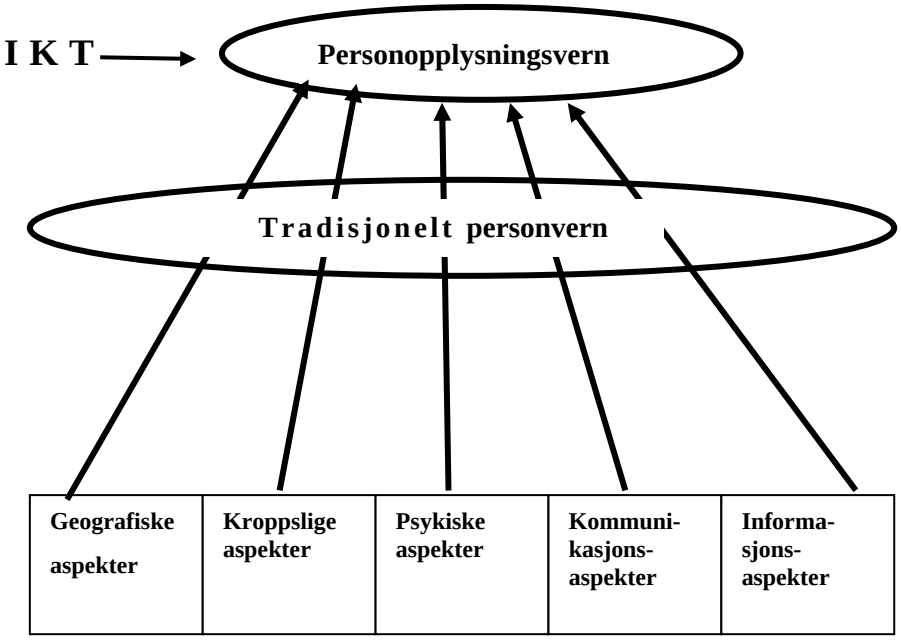
3.3.2 Forholdet mellom personopplysningsvern og personvern for øvrig

Personvern har vært diskutert i mange tiår, men innhold og vektlegging i diskusjonene har variert i ganske betydelig grad. Før datamaskinens gjennombrudd i 1960-årene var "personlighetens rettsvern" en betegnelse på grunnleggende vern av fysiske personer og med privatliv og vern om privat og personlig informasjon som del av en bred og forholdsvis helhetlig tilnærming. Da datamaskinteknologien ble tatt i bruk, fikk vi en klar vektlegging mot spørsmål vedrørende personregistre, dvs. mot spørsmål knyttet til personopplysninger som var organisert slik at det lettet gjenfinning og sammenstilling av opplysninger om den enkelte. Dette perspektivet ble befestet og styrket ved innføringen av personregisterloven i 1978. Samtidig ble det forholdsvis liten interesse for spørsmål som kun var knyttet til personvern i fysisk forstand.

Personopplysningsloven fra 2000 bygget blant annet på en erkjennelse av at personverntruslene ikke lenger på en hensiktsmessig måte kunne knyttes til organiseringen av personopplysninger i "registre", fordi det ikke lenger var mulig å forutsette en bestemt organisering av opplysningene. Derfor ble enhver "behandling av personopplysninger" regulert uavhengig av om det forelå et register eller ikke.

Personregistrene inneholdt primært tekst. Overgangen fra "personregistre" til "behandling av personopplysninger" i kombinasjon med den teknologiske utviklingen, gjorde at den nye lovgivningen også regulerer behandling av personopplysninger uansett om disse kommer til uttrykk som tekst, bilde, lyd, kroppssensorer eller annet. Teknologi for opptak av bilde og lyd og teknologi som gjør bruk av biometriske teknikker (dvs. som måler kroppens egenskaper og tilstander), gir grunn til fornyet oppmerksomhet om forholdet mellom personvern knyttet til opplysninger ("personopplysningsvern") og personvern i mer fysisk forstand. Dette gjelder ikke minst i tilknytning til sikkerhetstiltak i transportsektoren med kameraovervåkning og fingeravtrykklesere som en del av sikkerhetsutrustningen. Her smelter behandlingen av personopplysninger og behandlingen av fysiske personer sammen til et sammenhengende problemområde. Selv om det ikke anvendes biometrisk apparatur direkte mot kroppen, vil ransakelse av person og bagasje faktisk kunne oppleves som en del av tilknyttede (potensielt) krenkende tiltak. Dersom inngående ransaking for eksempel skjer på grunnlag av informasjon om vedkommende person, er det nødvendig å se behandlingen av opplysninger og ransakingen i sammenheng – i alle fall dersom den samlede personvernkrenkelsen skal kunne beskrives.

Interesseteorien er ensidig rettet mot spørsmål vedrørende informasjonsbehandling og er i mindre grad formulert ut i fra personvern i fysisk forstand. Likevel vil mange av interesse- og kravformuleringene ha klar relevans også for personvern i mer fysisk forstand, se figur 3.1.



Figur 3.1: Forholdet mellom tradisjonelt personvern og personopplysningsvern.

Bilde fra Rapiscan Secure Body Scanner produsert av OSI Systems, Inc, Kilde: American Civil Liberty Union (aclu.org)

I grunnlagsrapporten fra deloppgave 2 (Schartum 2007) er det presentert en enkel modell som beskriver denne sammenhengen mellom personvern på de to nivåene. Dersom en kombinerer denne modellen med interessemodellen, vil en få en tett systematikk for kartlegging av mulige personvernproblem uavhengig av om problemene kan sies å være knyttet til informasjonsbehandlingen eller mer tradisjonelle aspekter (kroppslige, geografiske mv.) jf. figur 3.2.

I modellen ses de geografiske, kroppslige, psykiske, kommunikasjonsmessige og informasjonsmessige aspektene som grunnelementer i personvernet *generelt* sett. Bruk av informasjons- og kommunikasjonsteknologi (IKT) kan anvendes for behandling av informasjon vedrørende alle disse grunnelementene. Både fysisk ransaking av person og bruk av "kroppsskanner" (se bilde) kan for eksempel sies å gjelde "kroppslige aspekter" ved personvern. Fordi bruk av skanner som avbilder eventuelle objekter på naken kropp genererer personopplysninger, kan tilknyttede spørsmål sies å gjelde "personopplysningsvern". Ransaking foretatt av en person gir ikke slike opplysninger (direkte), og kan derfor sies å handle om personvern i en mer

tradisjonell, fysisk forstand. Tilsvarende vil både manuell gjennomlesing av reisedokumenter mv. og registrering av elektroniske pass gjelde "informasjonsaspekter".

For å gjennomføre "tette" personvernanalyser kan dette perspektivet kombineres med interesseteorien i en enkel matrise for helhetlig vurdering av personvernspørsmål jf. figur 3.2.

Aspekter / Interesse	Geografiske	Kroppslige	Psykiske	Kommunikasjonsmessige	Informasjons-messige
Selv-bestemmelse					
Innsyn og kunnskap					
Kvalitet					
Kontroll					
Bruker-vennlig					
Personvern-analyse					

Kilde: Schartum 2007

Figur 3.2 Matrise (forenklet) for helhetlig vurdering av personvern

Inn under "Interesser" kommer de ulike kravformuleringene, se listen i avsnitt 3.3.1. Modellen er helhetlig i den forstand at den tar opp i seg interesseteorien som er en "fullstendig" systematisk beskrivelse av elementer som kan hevdes å inngå i personvernet, samtidig som den er satt i kombinasjon med grunnelementer i beskrivelsen av personvern i fysisk/konkret forstand. I mange situasjoner vil det trolig være for omfattende å bruke hele matrisen, og det kan derfor være aktuelt å gjøre et utvalg. I større/viktige politikkdiskusjoner bør matrisen imidlertid kunne være grunnlag for systematiske og helhetlige gjennomganger der en ikke legger avgjørende vekt på om personvernkrenkelsen er knyttet til IKT eller ikke.

Skillet mellom tradisjonelt (fysisk mv.) personvern og personvern knyttet til opplysninger og IKT, setter i stor grad også sitt preg på lovgivningen. Den mest omfattende rettslige reguleringen finner vi således innen vernet av person-opplysninger. I grunnlagsrapporten (Schartum 2007) blir det hevdet at det er behov for endring av lovgivningen for å oppnå en mer helhetlig/sammenhengende regulering av personvernspørsmål, se også avsnitt 3.5 under.

3.3.3 Interessen i å bestemme over opplysninger om egen person

Interessen i å bestemme over opplysninger om egen person kan sies å bygge på en forutsetning om det foreligger en valgfrihet for den enkelte. I praktiseringen av personopplysningsloven er den registrertes samtykke ansett å være det ideologiske utgangspunktet.[50]

Stilt overfor tiltak som skal fremme security i transport kan en forutsetning om valgfrihet svikte på minst to måter. For det første kan valgfriheten være eliminert eller begrenset fordi det er truffet bindende vedtak om plikt for den enkelte til å medvirke til og/eller tåle at det blir behandlet personopplysninger om dem. Det er for eksempel ikke frivillig å ha et fødselsnummer,[51] og dette nummeret er sentralt for å kunne sammenstille opplysninger fra mange kilder, for eksempel som ledd i arbeidet med security i transport.

For det andre kan det være at den enkelte ikke formelt sett er fratatt selvbestemmelsesretten, samtidig som det reelt sett foreligger liten grad av valgfrihet. Dersom en vil reise med fly, er det obligatorisk å la seg undersøke i samsvar med luftfartsloven med forskrifter (inkludert EU-forordninger og ICAOs[52] regelverk). Dersom reisens mål er det amerikanske kontinentet finnes det knapt noe alternativ når utgangspunktet er Oslo. Skal en derimot reise til Trondheim, kan både tog og buss være reelle alternativ. Reelt sett vil det med andre ord foreligge en varierende grad av valgfrihet som i noen tilfelle er helt illusorisk. På lignende måte kan det i prinsippet være mulig å unngå kameraovervåkning på tog og buss, men i praksis vil monopoler og konkurrerende selskaper som inneretter seg likt, gjøre valgfriheten lite reell. Selv om det derfor formelt sett foreligger en valgfrihet kan det derfor ofte – reelt sett – foreligge en "faktisk tvang". Der reell valgmulighet mangler, kan mye tale for å innrette transporttjenesten og reguleringen av den ut i fra en erkjennelse om den faktiske tvangssituasjonen. En eventuell uvilje mot kameraovervåkning på buss, bør med andre ord ikke møtes med argumentet om valgfrihet, dersom det ikke finnes alternativ kollektiv transport uten overvåkning.

3.3.4 Interessen i innsyn og kunnskap

Ivaretakelsen av interessen i innsyn og kunnskap er spesielt problematisk for security i transport fordi en del tiltak krever hemmelighold. Behovet for hemmelighold gjelder primært informasjonssystemene hos politi- og påtalemyndigheter. I den grad politiet også gjør systematisk eller gjentatt bruk av sivile informasjonssystemer, for eksempel systemer knyttet til transportmidler og stasjonsområder, kan behovet for å begrense innsyn smitte over på deler av sivil sektor.

---

[50] Se Personvernnemndas avgjørelse i klagesak 2004 nr. 1 der nemnda etablerer hensynet til den enkeltes autonomi som et hovedprinsipp etter personopplysningsloven.

[51] Jf. lov om folkeregistrering av 16. januar 1970 nr.1 som i § 4 bestemmer at " For enhver som er bosatt i Norge, fastsettes et fødselsnummer. …"

[52] International Civil Aviation Organization

I forslaget til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler er innsynsrettighetene knyttet til i) generelle beskrivelser av informasjonssystemene og ii) personinformasjon om en selv betydelig redusert i forhold til det som ellers gjelder i henhold til personverndirektivet og personopplysningsloven. Slikt hemmelighold vil langt på vei komme til å stenge den enkeltes mulighet for å ivareta egne personverninteresser, og innsyn og kunnskap må anses å være en forutsetning for å gjøre bruk også av andre rettigheter. Samlet sett vil dette svekke den enkeltes autonome stilling og mulighet til selvstendig og aktivt å forfølge egne interesser.

Hemmelighold og meget begrensede innsynsrettigheter bryter således på grunnleggende måter med den ideologi som ellers har vært lagt til grunn på personvernområdet. Det som trer inn i stedet er en forhåpning om at myndigheter og ulike kontrollaktører opptrer innenfor rammene av grunnleggende menneskerettigheter og i samsvar med gjeldende nasjonale rettsregler. Tillit uten grunnlag for å etterprøve grunnlaget for tilliten pga hemmelighold, er imidlertid problematisk i en demokratisk rettsstat.

I tillegg til begrensninger i innsynsrettigheter mv. kommer manglende tilgang til enkelte gjeldende rettsregler. Flere av de detaljregler som gjelder for reisende innen luftfarten er vedtatt som forskrifter men unntatt offentlighet. Dette innebærer at de er unntatt fra høring, kunngjøring og demokratisk menings-utveksling. Også hemmelige regler er svært problematisk å akseptere i en demokratisk rettsstat.

3.3.5 Interessen i opplysnings- og behandlingskvalitet

Personvern kan begrunne at det ikke skal samles inn og behandles personopplysninger. Ikke sjelden vil imidlertid slike hensyn måtte vike og personopplysninger vil således bli behandlet i stort omfang og på intensive måter innenfor rammene av avanserte IKT-baserte informasjonssystemer. Med slik behandling av personopplysninger som utgangspunkt, er spørsmål om opplysnings- og behandlingskvalitet helt sentrale for ivaretakelsen av personvern. Personvernet begrunner høy kvalitet og dermed forutsigbarhet og sikkerhet mht bruken av opplysningene.

Med få, enkle og enkeltstående informasjonssystemer kan det være en forholdsvis lett oppgave å sikre kvaliteten av opplysningene. Jo flere opplysningstyper et informasjonssystem inneholder, jo mer avansert databehandling som ligger bak tilblivelsen av hver opplysning, og jo flere andre informasjonssystemer et system skal samvirke med, desto mer utfordrende er det å sikre tilstrekkelig kvalitet.

Kvalitetsspørsmålene kan deles inn i "opplysningskvalitet" og "behandlingskvalitet".[53] Kravet til opplysningskvalitet gjelder særlig:

- Forholdet/samsvaret mellom en opplysning og den person opplysningene er ment å representere/beskrive.

[53] Se nærmere om dette i Bygrave (1996).

- Forholdet mellom en personopplysning og bruksformålet for denne opplysningen.

Kravet til behandlingskvalitet gjelder særlig:

- Forholdet mellom de forskjellige personopplysningene som inngår i behandlingen i et informasjonssystem (konsistens, fortolkbarhet mv.).
- Overordnede forhold knyttet til systemløsningen (krav til konfigurasjon, integrasjon med andre systemløsninger, driftssikkerhet mv.).

Arbeidet med security i transport må antas å skape behov for informasjonsinnsamling fra flere kilder, for eksempel fra flere kameraovervåkningssystemer, billettsystemer, telekommunikasjonssystemer mv. I den grad informasjonsbehandlingen er planlagt, for eksempel for å drive etterretning og forhindre anslag mot transportmidler, har en anledning til å ta hensyn til kvalitetsspørsmålene. I mange andre tilfeller, for eksempel når det oppstår en akutt trussel eller en hendelse skal etterforskes, kan kvalitetsproblemene være langt vanskeligere å håndtere. Særlig alvorlige problemer knyttet til kvaliteten av personopplysninger oppstår i situasjoner der politiet mener å ha grunn til å gripe inn umiddelbart for å forhindre et anslag, for eksempel på bakgrunn av (tilsynelatende) gjenkjennelse av etterlyst terrormistenkt med stor ryggsekk på vei ned mot et stasjonsområde.[54]

I situasjoner som ikke er akutte, for eksempel ved etterforskning i påvente av rettssak og bevisvurdering, kan spørsmål vedrørende kvaliteten av personopplysninger være lettere å håndtere. Utgangspunktet for å dømme noen til straff er at det straffbare forholdet kan bevises utover enhver rimelig tvil. Dette innebærer at kravene til opplysningskvalitet ved domstolsbehandlingen gjennomgående er høye.

Det at kvaliteten av personopplysninger lett kan bli stridens kjerne, gjør at spørsmål om innsyn og kunnskap (jf. avsnitt 3.3.4, ovenfor) blir viktig ved bedømmelsen av kvalitet. Individuelt innsyn vil for eksempel være viktig for å avdekke om en opplysning det er strid om er konsistent med andre opplysninger i samme informasjonssystem eller i andre informasjonssystemer. Innsyn i andre opplysninger enn de det står direkte strid om, for å påvise kvalitetsbrister der, kan dessuten være en viktig strategi for å angripe opplysninger som for eksempel er avgjørende for bedømmelsen av skyldspørsmål i en etterfølgende straffesak.

For å kunne bedømme kvaliteten av en personopplysning blir det derfor viktig å ha kunnskap om hvilke andre informasjonssystemer som inneholder opplysninger som er egnet for å teste om den omstridte personopplysningen har tilstrekkelig kvalitet. Det kan dessuten være viktig å ha kjennskap til hvilke tekniske eller andre svakheter ved informasjonssystemene som personopplysningene er hentet fra. I grunnlagsrapporten for dette arbeidet (Schartum 2007) blir det imidlertid vist hvorledes tilgang til slik viktig kunnskap kan bli sterkt begrenset som et resultat av EUs utkast til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler. Hemmeligholdet svekker med andre ord også muligheten til å granske kvaliteten av personopplysningene.

---

[54] Britisk politi gjorde for eksempel en fatal feil da de mistok en brasiliansk mann på vei til arbeid for å være en potensiell selvmordsbomber på undergrunnen i London i juli 2005. Mannen ble skutt og drept.

Spørsmål om rettssikkerhet er primært knyttet til offentlige myndigheters inngripende beslutninger og bruk av makt, mens personvern er generelt knyttet til behandling av personopplysninger. Når personopplysninger benyttes som beslutningsgrunnlag, er det vanskelig å skjelne mellom rettssikkerhet og personvern. Manglende innsyn mv. som svekker muligheten for å bedømme kvaliteten av "personopplysningsbevis" er derfor både et alvorlig rettssikkerhetsproblem og et alvorlig personvernproblem.

I den grad innsynet begrenses, må dette i utgangspunktet søkes kompensert slik at det totale vernenivået av den enkelte ikke reduseres. Slike mulige tiltak diskuteres ikke i denne rapporten, men vi nevner kort tre tiltaksområder som kan være aktuelle:

a) Tiltak for å sertifisere/godkjenne enkeltstående og samvirkende informasjonssystemer som skal inngå i arbeid med etterretning og/eller etterforskning.

b) Etablering av uavhengige tilsyns-/kontrollinstanser som ettergår bruken og kvaliteten av informasjonssystemer som brukes i etterretning og etterforskning vedrørende terrorvirksomhet mv.

c) Etablering av nye regler for vurdering av personopplysningsbevis, dvs. for opplysninger fra IKT-baserte informasjonssystemer om enkeltpersoner når disse legges frem som bevis i en straffesak. Det bør herunder være aktuelt å vurdere om det er grunn til å gjøre enkelte avvik fra prinsippet om domstolenes frie bevisvurdering.

3.3.6 Interessen i forholdsmessig kontroll

Uansett hva resultatet av avveiningen mellom security i transport og personvern er, vil avveiningene ofte legitimere ulike typer kontrolltiltak med/av fysiske personer og/eller av opplysninger om personene. Derfor kan personverninteressen i forholdsmessig kontroll forventes å være relevant i mange situasjoner der security-tiltak skal fastsettes. Med "forholdsmessighet" siktes det ikke til balanse, men til at forholdet mellom ulike kontrollstrategier skal være vel begrunnet, dvs. stå i et velbegrunnet forhold til hverandre. Dette innebærer at én kontrollstrategi bør være nøye vurdert opp mot alternative kontrollstrategier.

En underliggende antagelse er at man med slike veloverveide kontrollstrategier kan få et generelt lavere kontrollnivå i samfunnet enn uten fordi kravet til forholdsmessighet stimulerer til å prøve om behovet for kontrolltiltak er reellt. Nedenfor vil vi kort referere fem aktuelle vurderinger av forholdsmessighet, men også andre vurderinger kan tenkes.

1. Krav til forholdsmessighet mellom veiledning og kontroll

Kravet tilsier at den som ønsker å iverksette nye kontrolltiltak alltid bør vurdere om det er iverksatt tilstrekkelig veiledningstiltak mv. Dersom det er udekkede veilednings- eller informasjonsbehov, innebærer denne tilnærmingen at kontrolltiltakene utsettes eller reduseres. "Veiledning" forutsettes her å kunne omfatte enhver skriftlig, muntlig og praktisk kommunikasjon.

Med "praktisk kommunikasjon" menes fysiske innretninger som kan virke atferdsregulerende. På flyplasser er det for eksempel ikke uvanlig å sette opp fysiske sperrer som gjør det umulig eller uforholdsmessig vanskelig å ta med bagasjetraller forbi sperrene. Håndtering av ryggsekker mv. som spesialbagasje og strevet med å måtte benytte egen skranke, stå i flere køer mv., kan likeledes redusere antallet personer som har med bagasje som anses å være uønsket og som det antas å være knyttet særlige kontrollbehov til. Slik praktisk veiledning kan tenkes å være så effektiv at det langt på vei kan likestilles med et formelt forbud.

I tillegg til praktisk veiledning er det alltid grunn til å vurdere om skriftlig og muntlig informasjon (generell og/eller individuell) til reisende og ansatte er tilstrekkelig og hensiktsmessig. Videre er det grunn til å vurdere vektleggingen mellom ulike veiledningstiltak, og om endret vektlegging kan øke effektiviteten av veiledningsvirksomheten. Når veiledningsvirksomheten er gjennomgått og forbedret, blir neste spørsmål om det (fortsatt) er behov for å øke kontrollen. Uansett kontrolltiltak kan det være aktuelt å vurdere de følgende kravene til forholdsmessighet, jf. nedenfor.

2. Krav til saklighet og forholdsmessighet mellom kontrollinnsats mot persongrupper

I diskusjonen knyttet til terroraksjonene i London i 2005, gjaldt ett av spørsmålene hvordan ulike befolkningsgrupper kan bli berørt av kontrolltiltak på ulike måter på grunn av hudfarge, religiøse symboler mv. Krav til forholdsmessighet mellom persongrupper er grunnlagt på en forutsetning om at kontrollstrategier ofte vil bygge på felles kjennetegn ved personer, noe som innebærer at en etablerer grupper av kontrollobjekter.[55] Dette kan skje ut fra nasjonalitet, religion, etnisitet, utseende ellers (for eksempel om en er pent kledd eller ikke), alder, språk, oppførsel osv.

Kjennetegnene blir brukt som indikasjon på økt risiko for at en sikkerhetstruende hendelse eller handling skal inntreffe. For eksempel kan noen mene at nasjonalitet kan indikere en forhøyet risiko for terror, og mange vil mene at beruselse kan innebære en økt sikkerhetsrisiko for flypassasjerer. Bruk av slike ytre kjennetegn for å anslå risiko, spenner fra de helt usaklige til det som er klart saklig begrunnet. Samtidig er det legitimt å gjøre utvalg som gir en så virkningsfull kontrollinnsats som mulig, slik at å skjelne mellom grupper kan begrunnes ut fra en risiko-/sannsynelighetsvurdering.

Ut fra et personvernhensyn kan det imidlertid stilles krav om at i) kontrolltiltak rettet mot spesielle grupper skal være *saklig* begrunnet og ii) at det skal være *forholdsmessighet* mellom kontrolltiltak rettet mot ulike grupper.

Saklighetskravet innebærer at en i størst mulig grad skal kunne vise til et empirisk grunnlag og logisk holdbare resonnementer. Dette kan igjen være argument for at den som foretar vurderingen i størst mulig grad skal benytte anerkjente metoder og empiri som er innhentet ut fra strenge krav til kvalitet (f. eks. vitenskapelige krav). Krav til empiri og metode/vurderingsmåte/resonnement innebærer også økt

---

55 Denne kravformuleringen er basert på Karanja (2006).

mulighet for å kunne kommunisere informasjon om kontrollen, og for å skaffe aksept for at kontrolltiltaket er saklig begrunnet og dermed legitimt og akseptabelt, jf. avsnitt 3.4 (nedenfor) og personvernprinsippet om rettferdig og rettmessig behandling av personopplysninger.

Det neste elementet er et krav om forholdsmessighet mellom ulike persongrupper som er plukket ut for kontroll. La oss si at det er saklig grunnlag for å intensivere kontroll overfor personer som bærer bagasje og personer med vide klær, fordi begge grupper kan skjule eksplosiver. Kravet til forholdsmessighet vil da innebære at begge grupper behandles ut fra den saklig begrunnede økte risikoen. Dette fører med andre ord til at en ikke bør kontrollere personer med vide klær mer enn en kontrollerer folk med bagasje, uten at det kan dokumenteres en forskjell i risiko. Lik risiko knyttet til persongrupper, bør med andre ord alltid lede til likt kontrollnivå mellom gruppene.

3. Krav til forholdsmessighet mellom proaktiv og reaktiv kontroll

Kontroll kan utøves før eller etter at en uønsket handling utøves eller en hendelse inntrer.[56] Betegnelsene "proaktiv" og "reaktiv" viser til en todeling av et tidsforløp. Hensynet til den enkeltes sikkerhet kan ofte tilsi at en i størst mulig grad velger en proaktiv kontrollstrategi fordi dette kan redusere muligheten for at handlinger/hendelser rammer transportmidler og passasjerer.

I forhold til personopplysningsvern, er det ikke mulig generelt å si at proaktiv kontroll av passasjerer er mer eller mindre inngripende enn reaktiv kontroll. Det kan derfor i utgangspunktet argumenteres for at proaktiv kontroll bør kunne velges uten at det normalt vil fremkomme sterke personvernmessige motforestillinger.

Proaktiv og reaktiv kontroll kan imidlertid langt på vei tilsvare skillet mellom etterretning og etterforskning. I den grad etterretning er mindre målrettet enn etterforskning og derfor omfatter flere (uskyldige) mennesker enn etterforskningen, kan personvern derfor være et argument mot å velge en proaktiv tilnærming til behandling av personopplysninger.

Som en del av interesseteorien kan det formuleres et krav om forholdsmessighet mellom proaktiv og reaktiv kontroll. Dette betyr at det alltid bør være bevissthet om nye tiltak innebærer forhåndskontroll og/eller kontroll i ettertid. For hvert slikt tilfelle bør det skje en vurdering av om det kan velges en "motsatt" kontrollstrategi, og det bør vurderes hva som er best sett ut fra hensynet til personvern. Dersom en planlegger et nytt tiltak med proaktiv kontroll, blir spørsmålet om balansen i forhold til mulige reaktive kontrolltiltak er godt begrunnet. Spørsmålet blir for eksempel om proaktiv kontroll kan skje ved å nekte personer adgang til et transportmiddel ut fra en vurdering av rus og oppførsel.

---

[56] Ved formulering av interesseteori har en tidligere gjort bruk av et skille mellom "forhåndskontroll" og "etterkontroll". Her velger vi i tråd med kritikk i Karanja (2006, s. 176) å formulere dette som krav til forholdsmessighet mellom "proaktiv" og "reaktiv" kontroll. Denne betegnelsen innebærer den en indirekte henvisning til litteratur vedrørende "proactive law", som generelt er relevant i informasjonssikkerhetssammenheng. Se om proactive law, Wahlgren (ed.) (2006).

Reaktiv kontroll kan skje ved videoopptak for å dokumentere hendelser der voldelige/truende berusede personer opptrer, direkte alarm til politi mv.

4. Krav til forholdsmessighet mellom kontroll til de registrertes gunst og til deres ugunst

Spørsmålet her er om følgen av kontroll vil bli opplevet som en negativ sanksjon eller ikke. Kontroll som ikke leder til negative sanksjonstiltak vil kunne være lettere å akseptere enn annen kontroll. Denne tilnærmingen peker i retning av krav til vurdering av forholdsmessigheten mellom kontrolltiltak som gir "negative" og "positive" resultater for den som blir kontrollert. Kontroll for å fremme transportsikkerhet vil ofte være knyttet til reaksjoner med negative elementer. Resultater av kontroll vil for eksempel kunne anses å være "positive" fordi de er konstruktive, samtidig som andre elementer oppfattes som negative (f.eks. fordi de inneholde atferdsregulerende elementer). En truende person kan for eksempel anholdes, settes på glattcelle og bøtelegges, eller kan holdes tilbake og pålegges samtale med terapeut med tanke på mulig behov for senere oppfølging. Dersom en sjåfør anses å være en sikkerhetsrisiko pga. sitt temperament, kan dette kravet til forholdsmessighet tilsi at en for eksempel vurderer opplæring/terapi fremfor overvåkning av hvorledes sjåføren utfører jobben.

5. Krav til forholdsmessighet ekstern og intern kontroll

Dette kravet gjelder forholdsmessighet mellom tiltak rettet mot de som planlegger eller gjennomfører kontrollen og eksterne aktører, og er helt sentralt når personvern og security i transport skal vurderes. Et intuitivt utgangspunkt kan være at det er nærliggende å anse at "de andre" representerer problemer som det må rettes tiltak mot, og at kontrolltiltakene derfor primært vil bli rettet mot eksterne aktører.

Forholdsmessighet mellom ekstern og intern kontroll innebærer at en ved planlegging av tiltak rettet mot mennesker utenfor egen organisasjon, alltid bør vurdere om dette står i et rimelig forhold til kontroll som er rettet mot egen organisasjon.

Intern kontroll kan for eksempel innebære at en påser at egne ansatte følger de sikkerhetsrutiner som er etablert i bedriften, og ikke har en atferd som kan øke muligheten for sikkerhetstruende hendelser. Slik kontroll kan for eksempel avdekke at sjåfører ikke takler visse situasjoner som kan utvikle seg til et problem for sikkerheten ("har lett for å bli sint og krangle med berusede personer"). Resultatene av slik kontroll behøver ikke å være en sanksjon, men kan like gjerne være assistanse til og tilrettelegging for vedkommende person, for eksempel opplæring og/eller endring av arbeidstider mv.

En lignende tilnærming er aktuell for å vurdere forholdet mellom kontrollørene og de kontrollerte. Kravet til forholdsmessighet innebærer da at kontrollen med kontrollørene skal stå i et rimelig forhold til den makt og myndighet mv. som disse kan utøve i egen kontrollvirksomhet mot passasjerer og ansatte mv. Jo videre og mer inngripende fullmakter kontrollører har, desto sterkere er grunnene for å kontrollere kontrollørene. I forhold til manglende innsyn og hemmelige

rettsregler med vide fullmakter til kontrollører på flyplasser, kan det for eksempel stilles spørsmål om det er etablert tilstrekkelige kontrollfunksjoner overfor kontrollørene. I grunnlagsrapporten for dette arbeidet tenderer vi å svare nei på dette spørsmålet, se Schartum (2007, avsnitt 17.3).

3.3.7 Interessen i brukervennlig behandling

Også i forhold til interessen i brukervennlig behandling er behovet for hemmelighold av regelverk, systemløsninger og registrering av personopplysninger et problem. Kort sagt innebærer hemmeligholdet en hindring for kommunikasjonen mellom myndigheter og de personer som er gjenstand for kontrolltiltak.

På de fleste områder er det imidlertid vanlig åpenhet som gjelder, dvs. aktuelle regler er kunngjorte og tilgjengelige, enhver har krav på innsyn i visse opplysninger som beskriver de aktuelle systemløsningene og den enkelte har innsyn i opplysninger om seg selv. Også i slike tilfelle er det imidlertid tilfeller der det åpenbart er vanskelig å lykkes med en brukervennlig behandling. Dette skyldes primært regelverkets kompleksitet og struktur som gjør det vanskelig forståelig for andre enn eksperter.

Særlig oppstår det problemer når security-arbeidet er regulert ved hjelp av forordninger som etter EØS-avtalen skal gjennomføres i norsk rett direkte, ord for ord.[57] Det mest problematiske eksempelet som blir trukket frem i grunnlagsrapporten (Schartum 2007) er reguleringen av forebyggelse av anslag mot sikkerheten i luftfarten der utgangspunktet er en bestemmelse i luftfartsloven § 7-25. Til bestemmelsen er det gitt en forskrift (BSL A 2-1) som dels peker til fem forordninger og dels gir supplerende bestemmelser til disse. Flere av forordningene er endret, og en av de mest sentrale forordningene er endret 9 ganger. I Lovdatas forskriftsbase er det kun gjort tilgjengelig en "foreløpig norsk versjon av tekst under oversettelse", og i denne versjonen er ingen av endringene innarbeidet. Til forordningene følger det vedlegg og flere av disse er klassifisert som "Begrenset" og ikke offentlig tilgjengelig.

Betenkeligheter vedrørende hemmelig regelverk er tidligere kommentert i avsnitt 3.3.4. I tillegg til momentene nevnt der er det også et problem at viktige deler av det regelverket som er åpent og tilgjengelig har en så vanskelig struktur at det er meget krevende for interesserte personer å sette seg inn i hvilke regler som gjelder. Dessuten er EUs forordninger forfattet innenfor en annen rettstradisjon enn den norske som kan være vanskelig å sette seg inn i for personer som kun har kjennskap til norsk rett. Samlet sett innebærer dette stor avhengighet av at norske myndigheter etablerer og vedlikeholder utfyllende og god informasjon til befolkningen.

---

[57] Se LOV 1992-11-27 nr 109: Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven), artikkel 7.

3.3.8 Interessen i personvernanalyse

Interessen i personvernanalyse er føyet til i denne fremstillingen som en presisering av interesseteorien. Interessen er formulert på bakgrunn av den allmenne debatten om personvern, og er ikke direkte knyttet til erfaringer i konkrete saker. Samtidig uttrykker denne interessen mer generelle trekk ved samfunnsstyringen, og kan sies å være i slekt med andre spørsmål knyttet til risikohåndtering, kvalitetssikring mv. innen områder med store krav til sikkerhet (miljøskadelig produksjon, drift av infrastrukturer mv.).

For å tydeliggjøre noen enkle underliggende strukturer, er det formulere tre underliggende krav som må oppfylles for å kunne hevde at interessen fullt ut er ivaretatt:

1) Krav om konsekvensanalyse
2) Krav om løpende kontroll
3) Krav om evaluering

De tre kravene til personvernanalyse kan tenkes benyttet på minst tre nivåer:

a. *Lovgivningen* mv., dvs. vedrørende generelle, politisk fastsatte regler for behandling av personopplysninger.
b. *Systemnivået*, dvs. vedrørende hvorledes lovgivning er implementert i eller rammer for informasjonssystemer som behandler personopplysninger.
c. *Individuelt nivå*, dvs. vedrørende hvorledes enkeltsaker blir behandlet som et resultat av de to overordnede nivåene.[58]

Krav om konsekvensanalyse

Endring i lovgivning som vedrører personvern, endring av informasjonssystemer der personopplysninger inngår, og endringer av formell organisering med ny kompetanse- og oppgavefordeling, vil ha konsekvenser for personvernet. Ofte vil det imidlertid være vanskelige å forutsi presist hva konsekvensene vil være, og dersom en skal ha et rimelig sikkert bilde av mulige effekter, krever det en nærmere analyse.[59]

Slike analyser kan også ses som et spørsmål om å skaffe et tilstrekkelig og forsvarlig beslutningsgrunnlag for vedtak og andre disposisjoner som kan ha betydning for personvernet. Poenget er primært at en i størst mulig grad skal kunne forutse konsekvensene for personvernet. På den måten kan en også tydeliggjøre prioriteringer og valg; for eksempel slik at en tydelig angir at visse personvernhensyn må vike for å ivareta transportsikkerhet, hvilke konsekvenser tilsidesettelsen kan tenkes å få og hva som kan gjøres for å begrense mulige

[58] Det individuelle nivået tilsvarer ulike aspekter ved enkeltsaksbehandling, dvs. særlig saksutredning og kontroll med opplysninger i enkeltsaker, men vil ikke bli viet mer oppmerksomhet her. Konsentrasjonen vil i stedet gjelde de overordnede nivåene, dvs. der vurderingene har effekt for mange mennesker.

[59] Slike analyser blir også kalt "privacy impact assessments" og anvendes av flere lands myndigheter, se f.eks. presentasjon av Privacy impact assessment (PIA) hos Office of the Privacy Commissioner of Canada; http://www.privcom.gc.ca/speech/2004/sp-d_040310_e.asp.

skadevirkninger. Slik kan konsekvensanalyser også gi beslutninger og andre disposisjoner legitimitet samtidig som de gir et klart grunnlag for å vurdere politisk og faglig ansvar i tilfelle konsekvensene avviker fra det som er forutsatt.

I følge utredningsinstruksen[60] skal man forhåndsvurdere økonomiske, administrative og andre vesentlige konsekvenser av et utredningsarbeid, se instruksen punkt 2.2. Under "andre vesentlige konsekvenser" hører konsekvenser for personvernet. Det er imidlertid ikke utformet noen veileder for understøttelse av slike vurderinger.

Selv om det kommer generelle retningslinjer om dette, kan det være det grunn til å vurdere om det ikke i tillegg bør gis egne retningslinjer for vurdering av personvernvirkninger av security-tiltak i transportsektoren (og ellers). Særlige utfordringer vedrørende hemmelige regler, begrenset innsyn og tett internasjonalt samarbeid kan anføres blant slike grunner som tilsier er særskilt vurdering. Konsekvensutredninger bør særlig skje i samband med endringer i lovgivning og regelverk vedrørende transport og transportsikkerhet og ved utforming av det enkelte informasjonssystem innen sektoren.

Krav om løpende kontroll

Kravet om løpende kontroll, innebærer først og fremst krav om lovlighetskontroll, dvs. kontroll med at behandling av personopplysninger er i samsvar med lover, forskrifter, avtaler og andre bindende disposisjoner.[61] At behandlingen skal være i overensstemmelse med avtaler, innebærer bl.a. krav om overensstemmelse med avtaler som er inngått med registrerte personer, for eksempel transport-/passasjeravtaler med tilhørende standard avtalevilkår/vedtekter.

Krav om løpende kontroll gjelder ikke bare i forhold til spørsmålet om lovlighet og rettsanvendelse, men også kontroll med at skjønnsutøvelsen utøves konsekvent, forsvarlig og innenfor de rettslige, politiske og etiske rammer som den behandlingsansvarlige er bundet av eller har gitt sin tilslutning til. Løpende kontroll med skjønnsutøvelsen innebærer et krav om å undersøke om endrede faktiske, politiske, rettslige og andre forhold kan foranledige endret skjønnsutøvelse.

Langt på vei følger det av selve rettssystemet at det enkelte rettssubjekt, herunder den enkelte behandlingsansvarlige, har en plikt til å påse at ens egen opptreden er i samsvar med lov, avtaler og andre bindende bestemmelser. Personopplysnings-loven § 14 om internkontroll er direkte utslag av en slik tanke, og innebærer dessuten krav til fremgangsmåter for å sikre samsvar med gyldige reguleringer.

Som en del av interesseteorien bør imidlertid kravet om løpende kontroll neppe begrenses til rettssystemet, men også knyttes til etiske standarder, personvern-politikk mv. Personverninteressene kan med andre ord begrunne at den enkelte som forestår behandling av personopplysninger bør ha et gjennomtenkt forhold til

---

[60] Instruks om utredning av konsekvenser, foreleggelse og høring ved arbeidet med offentlige utredninger, forskrifter, proposisjoner og meldinger til Stortinget, fastsatt ved kongelig resolusjon 18. februar 2000, revidert ved kongelig resolusjon 24. juni 2005 (FOR-2005-06-24 nr. 692).

[61] Her overlapper interessen i forholdsmessig kontroll delvis med interessen i personvernanalyse.

personvern, og disponere overveiet og i samsvar med prinsipielle holdninger til personvern. Dersom en innenfor rammene av de rettslige reguleringene fastsetter høyere standarder for ivaretakelse av personvern, innebærer kravet om løpende kontroll at en også tar stilling til om praksis er i samsvar med disse standardene.

Krav om evaluering

Kravet om evaluering innebærer at tiltak som antas å ha effekt på personvernet (jf. konsekvensutredninger), skal evalueres for derved å ta stilling til om effektene faktisk ligger innenfor det som i henhold til konsekvensanalysen ble ansett å være akseptabelt. Særlig viktig er kravet om evaluering i forhold til regelendringer, nye informasjonssystemer, omorganisering mv. som kan innebære en svekkelse av personvernet.

Det enkle resonnementet bak et slikt krav er at tiltak som ikke har (tilstrekkelig) effekt, ofte ikke bør videreføres, men må justeres eller termineres. Evaluering kan tenkes å dekke spennet fra de helt skjønnsmessige vurderingene av virkninger av regelendringer, tekniske tiltak mv., til prøving i henhold til stringente, vitenskapelige evalueringskriterier. En forutsetning for reell evaluering, er trolig at evalueringskriteriene tar utgangspunkt i relevante konsekvensutredninger, dvs. at kriteriene fastlegges på forhånd.

Det vil i denne sammenheng særlig være lov- og systemnivåene som er aktuelle for evaluering. På lovnivået er uttrykket "etterkontroll av lover og forskrifter" anvendt, se ”Veiledning om lov- og forskriftsarbeid” fra Justis- og politidepartementets lovavdeling (Justis- og politidepartementet 2000, s 209). Det gjelder imidlertid ingen faste krav til omfang og metode for slik etterkontroll, og spørsmålet er ikke spesielt belyst i forhold til personvern.

I forhold til omstridte tiltak som har security i transport som begrunnelse, og som innebærer en nedprioritering av personvern, er kravet til evaluering særdeles viktig. I en slik situasjon vil evalueringen gjelde to aspekter; i) om de positive effektene for transportsikkerhet som ble forventet er realisert eller ikke, og ii) om de personvernmessige konsekvensene er som forventet. Manglende positive effekter av sikkerhetstiltak, kombinert med negative personverneffekter av tiltaket, kan for eksempel begrunne endret politikk.

3.4 Personvernprinsippene i europeisk rett

3.4.1 Generelt

Personvernprinsippene betegner et sett generelle normer som ligger til grunn for europeisk rettslig regulering av personvernspørsmål. Prinsippene er grunnlag for og kan utledes av EUs personverndirektiv.[62] Prinsippene gir uttrykk for hovedlinjene i tenkningen rundt personvern innen et geografisk område som minst dekker EØS-området, dvs. 30 land.

[62] Direktiv 95/46/EF

Betegnelsen "prinsipp" gir inntrykk av noe som er temmelig fast formulert og med et klart innhold. Dette er sant på den måten at det skal forholdsvis mye til for at det skal kunne hevdes at et prinsipp eksisterer. Et etablert prinsipp innebærer imidlertid primært etablering av et rettslig utgangspunkt, og det kan ikke utelukkes at det kan skje avvik fra prinsippene. Prinsippene er med andre ord ikke unntaksfrie og har ikke bestandig gjennomslagskraft i forhold til andre, motstående interesser, for eksempel i tilknytning til security i transport mv.

Prinsippenes karakter av (kun) å være utgangspunkter for regulering vises klart i den pågående diskusjonen om EUs rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler der prinsippene ser ut til å få vesentlig mindre gjennomslag enn i personverndirektivet, jf. diskusjonen nedenfor.

Det må også understrekes at personvernprinsippene ikke alltid er klart formulerte, men fremstår snarere som retningslinjer enn som klart definerte regler. Hvert prinsipp kan derfor ikke sies å determinere konkrete løsninger, men leder en snarere i retning av visse typer løsninger. Personvernprinsippene sier noe om hovedtrekkene i den eksisterende rettslige reguleringen, men kan ikke sies å gi dekkende uttrykk for alle fellestrekk innen personopplysningsvernet.

I kontrast til dette står interesseteorien (jf. avsnitt 3.3, ovenfor) som tar sikte på å dekke alle vesentlige aspekter innen problemområdet. Det følgende er en kortfattet diskusjon av viktige, utvalgte personvernprinsipper vurdert i forhold til security i transport. Grunnlaget for diskusjonen er gjennomgangen av den viktigste europeiske og norske rettslige reguleringen på området; EUs utkast til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler, samt meningsmålinger om personvern (se også Schartum 2007).

3.4.2 Gjennomslaget for prinsippet om rettferdig og rettmessig behandling av personopplysninger

Enkelte personvernprinsipper står trolig sterkere enn andre, i den betydning at lite gjennomslag for visse prinsipper er mer problematisk enn for andre. Prinsippet om rettferdig og rettmessig behandling av personopplysninger, må både sies å være grunnleggende og sterkt. Prinsippet innebærer at sikringstiltak innen transport-sektoren og ellers skal oppfattes som rettferdige og legitime i befolkningen.

Meningsmålinger innen EU som ble gjennomført i 2003, dvs. forholdsvis kort tid etter terroranslagene mot New York og Washington, viste at en stor del av respondentene (ca 70%) mente at telefoner og Internett enten ikke burde overvåkes for å bekjempe terrorisme i det hele tatt (European Opinion Research Group 2003)[63] eller at slik overvåkning burde begrenses til personer som var mistenkt for terrorhandlinger ("suspected of terrorist activities").[64] Disse tallene gir ikke annet enn en liten indikasjon på folks holdninger på et tidspunkt i historien. Det kan imidlertid være grunn til å merke seg at rundt 40% kun var

[63] Gjennomsnittlig 33% for telefon (spennvidden mellom landene i svarene; 25-48%) og 25% for Internett (spennvidden mellom landene i svarene; 20-41%).

[64] Gjennomsnittlig 40% for telefon (spennvidden mellom landene i svarene; 25-48%) og 40% for Internett (spennvidden mellom landene i svarene; 28-58%), se spørsmål 36a og 36b i undersøkelsen.

villige til å godta overvåkning av telefon og Internett i kampen mot terrorisme dersom overvåkningen kun gjaldt personer som var *mistenkt* for terror. En meningsmåling som Teknologirådet fikk utført i Norge i juni 2007 viste at 57 % mente at det var ubehagelig å bli overvåket dersom man ikke hadde gjort noe galt (Teknologirådet 2007b).

For å forhindre anslag mot transportmidler mv. er det nettopp behov for å drive informasjonsbehandling for å *etablere* mistanke. Da må overvåkningen omfatte et stort flertall av mennesker som er langt unna enhver mistanke om terror.

Myndigheter kan med andre ord ha oppfatninger om et kontrollbehov med tilhørende behov for behandling av personopplysninger, som ligger langt utenfor det store deler av befolkningen (i dag) kan akseptere. En slik utvikling vil derfor kunne komme i strid med prinsippet om rettferdig og rettmessig behandling av personopplysninger, dvs. med det grunnleggende prinsippet for den rettslige reguleringen som ble etablert i og med Europarådskonvensjonen i 1981 og EU-direktivet om personvern i 1995. De refererte tallene gir grunn til å følge nøye med på om dagens regimer og forslag til endringer av aktuelle rettslige reguleringer har oppslutning i befolkningen eller ikke.

Problemene vedrørende legitimiteten av omfattende kontroll ved hjelp av personopplysninger blir spesielt vanskelige fordi tiltakene i mange tilfeller ikke kan diskuteres i full åpenhet og med full informasjon til befolkningen. Forslag om sterkt reduserte innsynsrettigheter i utkastet til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler illustrerer dette problemet. For det første kan hensynet til effektiv etterretning og etterforskning tilsi tilbakeholdenhet med informasjon om trusselsituasjonen og myndighetenes metoder. For det andre kan det være ønske om å unngå opphetede debatter om bruk av personopplysninger i kontrollarbeidet, fordi dette kan skape uheldig motstand. Oppfatninger om at slik bruk av personopplysninger er strengt nødvendig, kombinert med holdninger om at "det du ikke vet har du ikke vondt av" og "den som har rent mel i posen har intet å frykte", kan komme til å begrunne et ønske om lav profil og liten kunnskap i befolkningen om myndighetenes praksis på området.

Mangelen på åpenhet er ytterligere problematisk fordi den kombineres med hemmelige generelle regler.[65] Det faktum at deler av EUs forordninger er hemmelige og at disse er/blir vedtatt som forskrifter til luftfartsloven, strider mot en grunnleggende rettsstatsidé om at lovgivningen skal publiseres, jf. prinsippet om "publicatio legis".[66] Et slikt hemmelighold er med andre ord ikke bare i strid med personvernprinsipper, men også med et vesentlig element i selve grunnlaget for en demokratisk rettsstat.

Hemmeligholdet kan ha noe mindre alvorlige konsekvenser dersom det formelt er utpekt én eller flere kontrollmyndigheter med stor legitimitet, autoritet og tilstrekkelig arbeidskapasitet som har som klart definert oppgave å kontrollere innholdet av og praksisen med slike hemmelige regelverk. Datatilsynet er trolig ikke aktuelt for en slik rolle uten særlig regulering, jf. unntak for Datatilsynets og Personvernnemndas kompetanse når det skjer behandling av personopplysninger

---

[65] Se avsnitt 1.2.4 (ovenfor).

[66] Se Bing (1982) s. 202-209.

som er nødvendig av hensynet til rikets sikkerhet eller de alliertes sikkerhet, forholdet til fremmede makter og andre vitale nasjonale sikkerhetsinteresser.

Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) er kontrollinstans for sikkerhetsarbeid som hører inn under sikkerhetsloven.[67] Forordningene vedrørende flysikkerhet blir også behandlet i Stortingets konsultasjonsorgan for EØS-saker (EØS-utvalget), men det er neppe grunn til å legge stor vekt på den mulige kontrollfunksjonen som er knyttet til denne saksbehandlingen.[68] Det er også mulig at det felles tilsynsorganet som er foreslått i utkastet til rammebeslutning vedrørende personvern i kriminalsaker innen politi og domstoler kan ha en rolle på det nasjonale planet.

Generelt er det et behov for å klarlegge hvilke(n) kontrollmyndighet(er) som skal ha ansvaret for å ha tilsyn med regler og praksis vedrørende personvernkrenkende tiltak, og spesielt med de hemmelige delene av flysikkerhetsarbeidet. Slike myndigheter bør kontrollere kontrollørene og også gi innspill til diskusjon og eventuell endring av uakseptable tiltak på området. Målet må være å sikre at befolkningen ser tiltakene vedrørende security i transport som rettferdige og rettmessige.

3.4.3 Prinsippet om formålsbestemthet

Prinsippet om formålsbestemthet innebærer at enhver behandling av personopplysninger skal være knyttet til ett eller flere bestemte formål. Prinsippet er problematisk å realisere i en situasjon der behovet for informasjonsbehandling ikke kan begrenses til bestemte og avgrensede kilder og metoder for videre behandling av personopplysningene. Riktignok er det slik at det fra politiets side kan være meningsfullt å snakke om begrensning til et formål, for eksempel til terrorbekjempelse, men i forhold til alle mulige kilder som politiet og andre myndigheter vil gjøre bruk av, blir en slik formålsbegrensning problematisk. En mulighet er generelt å definere terrorbekjempelse og transportsikring som et formål knyttet til behandling av personopplysninger i transportsektoren og andre aktuelle sektorer.

Imidlertid vil slik introduksjon av "standard formål" om terrorbekjempelse for mange ulike behandlinger av personopplysninger komme i strid med det som må antas å være en grunnleggende idé bak prinsippet; nemlig å legge begrensninger på spredning og bruk av personopplysninger. Dessuten vil en tydelig formålsangivelse vedrørende bekjempelse av anslag mot transportmidler mv. være positiv fordi den forutsetter en viss grad av åpenhet om den faktiske informasjons-bruken. Behovet for hemmelighold og begrensning av informasjon om konkrete rutiner og systemer som brukes i terrorbekjempelse, kan imidlertid gjøre det uønsket å opplyse om at ulike informasjonssystemer har terrorbekjempelse som et av sine formål.

---

[67] Jf. også Sikkerhetsloven § 30 og instruksen for EOS-utvalget § 11.

[68] I tillegg behandles EØS-saker i EØS-komitéen og EØS-rådet på vanlig måte, jf. EØS-avtalen art. 89 og 92.

3.4.4 Prinsippet om minimalitet

Prinsippet om minimalitet innebærer at det ikke skal brukes flere personopplysninger enn formålet for behandlingen tilsier. Både i etterretnings- og etterforskningsformål er metoden ofte å sette sammen et puslespill av opplysninger fra mange kilder til et helhetlig bilde. Dersom den underliggende antagelsen i underlagsrapporten (Schartum 2007) om et åpent og ubegrenset informasjonsbehov er holdbar, innebærer dette at minimalitetsprinsippet ikke kan etterleves i arbeidet med security.

Prinsippet om minimalitet kan også knyttes til spørsmålet om anonymitet. Det er eksempler på lovgivning og rekommandasjoner der det kreves at det legges til rette for anonym informasjonsbehandling, dvs. for å hindre at det oppstår "personopplysninger" med tilhørende behov for personopplysningsvern. Et forholdsvis ferskt eksempel på en klar sammenkopling mellom minimalitetsprinsippet og spørsmålet om anonymitet, finnes i en anbefaling fra en gruppe nasjonale og regionale datatilsynsmyndigheter, der det heter at "2. The Conference resolves that developing an international privacy standard must be based on the fair information practices *as well as the concepts of data scarcity*, *minimisation and anonymity*." (min kursiv).[69] Det foreligger imidlertid kun anbefalinger i retning av å legge til rette for anonymitet, og det kan derfor neppe konkluderes med at det er etablert et prinsipp om anonymitet.

I grunnlagsrapporten for dette prosjektet (Schartum 2007) er det referert til diskusjonen i artikkel 29-gruppen i EU.[70] Gruppen legger også vekt på pseudonymitet, dvs. ikke på anonymitet, men en form for beskyttet identitet. Poenget kan derfor være at det ikke skal være åpne personidentiteter, men at disse skal beskyttes, for eksempel ved hjelp av pseudonymisering, avidentifisering, kryptering eller – i siste instans – anonymisering. Flere slike teknikker for å beskytte personidentiteter kan være aktuelle å gjøre bruk av også i arbeidet med security i transport. Skjulte identiteter kan for eksempel tenkes benyttet som del av de rettssikkerhetsgarantier som kan være knyttet til politiets bruk av personopplysninger. En kan for eksempel tenke seg at virkelige identiteter ble tilgjengelige for politiet etter en rettslig kjennelse, dvs. slik at domstolene fikk myndighet til å tillate tilgang til identifiserbare opplysninger som danner mistenkelige mønstre, og som derfor bør undersøkes på personnivå.

3.4.5 Prinsippet om opplysningskvalitet

Også prinsippet om opplysningskvalitet kan være problematisk å håndtere i informasjonsbehandling for å forebygge anslag mot transportmidler mv. Dette gjelder i alle fall forberedende informasjonsbehandling, dvs. informasjonsbehandling som ligger forut for påtalemessige beslutninger, domstolsavgjørelser mv. Etterretnings- og etterforskningsarbeid må nødvendigvis i stor grad gå ut på å samle inn og analysere store informasjonsmengder der

---

[69] Se Conference of International Data Protection Commissioners, Wroclaw, 14. September 2004 Resolutions on a Draft ISO Privacy Framework Standard, tilgjengelig fra http://www.bfd.bund.de/EN/Home/homepage.

[70] Dvs. gruppen som er nedsatt i henhold til art. 29 i EUs personverndirektiv (Direktiv 95/46/EF).

opplysningskvaliteten er veldig varierende. Særlig gjelder dette *vurderinger*, dvs. opplysninger som tilkjennegir subjektive oppfatninger. Her vil opplysningene lett kunne være uriktige eller ufullstendige, samtidig som de kan være vanskelige å verifisere. Problemet er mindre når informasjonskilden er tekniske systemer, for eksempel epostlogger mv. Slike opplysninger kan imidlertid manipuleres, og det kan også være stor usikkerhet mht. hvem opplysningene i loggene faktisk gjelder.

Utfordringene knyttet til opplysningskvalitet gjelder ikke spesielt for terrorbekjempelse, men kjennetegner mye politiarbeid. Arbeidet går nettopp ut på å ta utgangspunkt i sann og usann informasjon for så gradvis å verifisere og bevise sanne opplysninger om handlinger, årsaksforhold, motiver mv. I sluttbehandlingen innen påtalemyndighet og domstoler er med andre ord kravene til opplysningskvalitet og sannhet meget høye. Jo større og mer mangfoldig informasjonstilfanget er i utgangspunktet, desto lenger vei kan det antas å være frem mot en tilstrekkelig informasjonskvalitet. Store deler av politiets forberedende behandling av personopplysninger vil med andre ord ofte være problematisk vurdert opp mot prinsippet om opplysningskvalitet. Ivaretakelse av personvern og rettssikkerhet kan nettopp tenkes å skje ved at det stilles krav til kvaliteten av opplysninger før de kan anvendes på måter som får konsekvenser for enkeltpersoner.

3.4.6 Prinsippet om informasjonssikkerhet

Prinsippet om informasjonssikkerhet er trolig det prinsippet som skaper minst problemer i forhold til behandling av personopplysninger for å forhindre terroranslag. Her vil politiet og andre myndigheter ha selvstendige motiver for å gjennomføre tilfredsstillende sikring, fordi etterretning og etterforskning både krever tiltak for å sikre konfidensialitet, integritet og tilgjengelighet.

3.4.7 Et samlet bilde

Oppsummert kan det sies at det er klare problemer med å etterleve de europeiske personvernprinsippene i en situasjon med omfattende bruk av personopplysninger for å bekjempe anslag mot transportmidler (og andre samfunnsinstitusjoner). I hvilken grad gjennomslaget av prinsippene konkret vil bli svekket gjenstår å se, men diskusjonen frem til utkast av rammebeslutning vedrørende ivaretakelse av personvern innen kriminalsektoren mv., [71] viser hvordan hensynet til bekjempelse av organisert kriminalitet og terror systematisk begrunner svekkelse av personvernet i forhold til det generelle regimet i personverndirektivet og personopplysningsloven.

Det kan stilles spørsmål ved hvor lite gjennomslag et prinsipp kan få før det opphører å være et prinsipp. I rettsteknisk forstand kan det være grunn til å endre prinsippet dersom unntakene blir så viktige eller mange at prinsippet ikke lenger gir et hensiktsmessig utgangspunkt. Med et ideologisk utgangspunkt kan det imidlertid være grunn til å holde på prinsipper som midlertidig i en gitt historisk

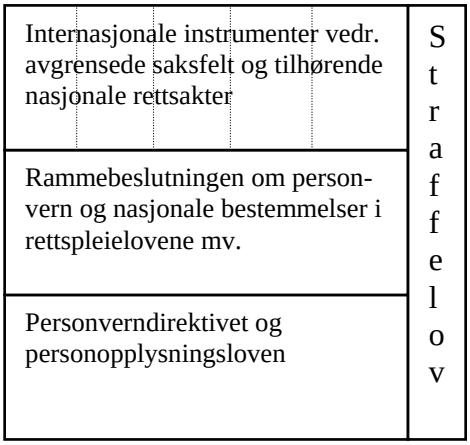
[71] Jf. diskusjonene i kapittel 14 vedrørende hovedpunkter i utkast til rammebeslutning art 1 (3) i Council of the European Union, 7315/07, Brussels, 13. Mars 2007.

situasjon har svakt gjennomslag, fordi en mener at denne situasjonen prinsipielt sett er uheldig. Dersom det (retts)politiske målet er å reetablere prinsipper som faktisk bærende, kan det derfor være grunn til å omtale normer som "prinsipper" selv om gjennomslaget er svakt.

Konklusjonen på denne lille gjennomgangen av personvernprinsippene bør etter min mening ikke være at prinsippene bør omformuleres selv om de på security-området kan bli svakere enn det som ideelt sett er ønskelig. Svekkelsen av prinsipper bør tvert i mot grunngi en intensivert diskusjon om hvert prinsipp. Diskusjonene bør særlig gjelde behovet/muligheten for å kompensere for manglende gjennomslag av prinsippene ved hjelp av forsterkede rettssikkerhetsgarantier, se avsnitt 3.6 og 3.7.

3.5 Spørsmål vedrørende lovgivningsteknikk

Grunnlagsrapporten viser at det i hovedsak kan sies å være fire rettslige regimer som har direkte betydning for behandling av personopplysninger vedrørende security i transport (Schartum 2007). Mest sentralt står et felles EØS-regime som omfatter de fleste virksomheter utenfor politi og rettsvesen, dvs. virksomheter innen det alminnelige sivile samfunn (offentlig og privat sektor). [72] Dette regimet omfatter en felles EU-rettslig regulering (personverndirektivet), personopplysningsloven og forskrifter til denne. I utgangspunktet hører alle transportselskaper mv. inn under dette alminnelige regimet, og bortsett fra regler vedrørende vandelsattester mv., eksisterer det i liten grad særlige regler om behandling av personopplysninger i transportsektoren.



Kilde: Schartum 2007

Figur 3.3 Illustrasjon av forholdet mellom ulike rettslige regimer vedrørende ivaretakelsen av personvern.

Det andre regimet gjelder behandling av personopplysninger innen forebygging, etterforskning, oppdagelse og rettsforfølgelse av straffbare handlinger og gjennomføring av straff. Også her vil det bli tale om en felles europeisk regulering (rammebeslutning), men høsten 2007 var denne ikke endelig behandlet og vedtatt. Det er uklart hvorledes rammebeslutningen vil bli gjennomført i norsk rett. Rammebeslutningen følger imidlertid langt på vei skiller som allerede finnes i norsk personopplysningslovgivning, jf. unntaket fra personopplysningsloven vedrørende saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvistemålsloven, tvangsfullbyrdelsesloven mv.).[73]

[72] Også enkeltpersoner kommer inn under dette regimet, men virksomheter er langt viktigere når det gjelder sikkerhet i transport.

[73] Jf. unntakene i personopplysningsforskriften § 1-3.

Det tredje regimet er ikke et enhetlig sett av reguleringer, men likevel et viktig systematisk trekk ved den samlede reguleringen. Dette er tilfeller av særregulering for avgrensede saksfelt, for eksempel for Europol, Eurojust, toll, Schengen og luftfart og tilbakeholdelse av trafikkdata vedrørende elektronisk kommunikasjon. Deler av særreguleringen inneholder rettsregler som spesielt skal ivareta personopplysningsvern innen hvert sitt begrensede område, mens særreglene innen transportsektoren (luftfart) i liten grad inneholder slike regler, men regulerer andre aspekter ved sikkerhet i lufttransport. I tilfelle av motstrid mellom spesielle og generelle regler, vil særlovgivningen normalt gå foran de generelle reguleringene, jf. de to foregående regimene nevnt over.

Det fjerde og siste regimet er nasjonale regler som kriminaliserer visse handlinger som kan anses å være skadelig for personvernet. Straffebestemmelser som skal beskytte ære, privatlivets fred, private brevsendinger og annen kommunikasjon, hemmelige lydopptak der en selv ikke deltar mv. gjelder generelt, men har spesielt stor betydning for enkeltpersoner som er unntatt fra personopplysningsloven. Dessuten tydeliggjør slike bestemmelser grensene for hva myndigheter, transportbedrifter mv. kan foreta seg uten konkrete hjemler.

De fire regimene kan også grupperes i henhold til hovedtrekk ved den regulatoriske strategien som er valgt. Personverndirektivet, rammebeslutningen og i stor grad også særreguleringer er prosedyreorienterte, dvs. rettsreglene angir i (forholdsvis) stor detalj hvilke *fremgangsmåter* som skal følges og hvilken kompetanse de ulike aktørene skal ha. Til forskjell følger straffelovgivningen en misbruksorientering, dvs. lovgivningen angir *negativ atferd* som krenker personvernet og som derfor er rettsstridig og belagt med straff.[74]

Mens en misbruksorientering i stor grad gjenspeiler allmenne sosiale normer, inneholder prosedyreorienterte regelverk anvisninger på fremgangsmåter som skal følges for å sikre den balanse mellom motstridende hensyn som vedtaksorganet har ansett å være riktig. Det er grunn til sterkt å understreke betydningen av slik prosedyreorientering. Samtidig er det imidlertid grunn til å argumentere mot at slike prosedyrer blir beskrevet på et helt overordnet nivå. I stedet bør de være så konkrete at de beskriver praktiske og gjenkjennelige situasjoner for den som ønsker å sette seg inn i hvilke regler som gjelder. Regler for kontroll av ansatte og passasjerer i lufthavner bør med andre ord konkret angi hvilke personopplysninger som kan innhentes, brukes og registreres i tilknytning til kontrollen, hvilke selvbestemmelsesrett den enkelte har, hvilke integritetskrenkelser som må tolereres, og hvilke fremgangsmåter som skal følges ved fysisk kontroll av person.

Detaljert regulering vil som nevnt langt på vei innebære stor grad av politisk involvering fordi direktiver, forordninger og nasjonale lover springer ut av politiske prosesser.[75] En slik detaljert tilnærming kan dessuten hevdes å være i god overensstemmelse med demokratiske idealer, bl.a. fordi den konkrete

[74] Også brudd på flere bestemmelser i prosedyreorientert lovgivning er belagt med straff. Poenget ved å skille mellom prosedyre- og misbruksorientert regulering er således ikke bruken av straff men innholdet av de øvrige reglene.

[75] Selvsagt springer også straffelovgivningen ut av politiske prosesser, men reguleringen er langt mindre omfattende.

avveiningen mellom security i transport og personvern direkte utføres av personer som står til valg og/eller på annen måte kan gjøres direkte politisk ansvarlig. Detaljert og konkret prosedyreorientert regulering vil også gi størst forutsigbarhet for den enkelte. På den annen side vil slik regulering gi mindre grad av fleksibilitet ved utførelsen av kontrollarbeidet, noe som kan kreve hyppigere regelendringer enn med mer generelt formulerte bestemmelser. Hensynet til personvern og rettssikkerhet taler for detaljerte og konkrete regelverk som både beskriver den enkeltes rettigheter samt innholdet av og grensene for myndighetsutøvelse.

Det er viktig å gjøre bruk av prosedyreorienterte regelverk for å uttrykke den til enhver tid fremforhandlede balansen mellom security i transport (beskyttelse av liv og helse) og personvern/rettssikkerhet. Samtidig er det imidlertid grunn til å ha et tydelig samspill mellom slikt regelverk og regler i straffeloven som angir tilfeller av straffverdige brudd på individuelle rettigheter og myndigheters plikter i forhold til personvernet. Det er herunder grunn til å vurdere om det er behov for å vedta flere/endrede straffebud som "grensestolper" for å markere grensene mellom det akseptable og det uakseptable. Selv om hovedinnsatsen bør gjøres innen det prosedyreorienterte regelverket, bør dette m.a.o. ses i sammenheng med bestemmelser i straffeloven mv. som (bl.a.) beskytter personvern.

Særlig kan det være grunn til å vurdere nærmere hensiktsmessigheten av bestemmelsene i straffelovens kapittel 11 om "Forbrydelser i den offentlige Tjeneste." Det kan for eksempel stilles spørsmål om bestemmelsene i § 121 om brudd på taushetsplikt og § 122 om brevbrudd er fyllestgjørende og hensiktsmessige i forhold til situasjoner der offentlige myndigheter innhenter og behandler personopplysninger elektronisk, i stort omfang, fra en rekke kilder og innen en internasjonal ramme. Jo større endringer som blir gjort i myndigheters adgang til å behandle personopplysninger for å bekjempe anslag mot transportsystemer mv., desto viktigere er det at det blir satt opp nye grensestolper som viser at det fortsatt er klare grenser for myndighetsutøvelsen, og som kan bidra til å øke bevisstheten om hvor disse grensene går.

Gjennomgang av regelverket i grunnlagsrapporten (Schartum 2007) viste en omfattende og kompleks rettslig regulering. Det er grunn til å tro at omfanget og kompleksiteten av denne reguleringen vil øke. For det første er det enda ikke gitt regler vedrørende security innen landtransport. For det andre er det grunn til å tro at det vil bli behov for regler som presiserer/konkretiserer en del av de generelle bestemmelsene som i dag gjelder. Både hensynet til effektiv myndighetsutøvelse og bedre beskyttelse av den enkelte kan begrunne slike tillegg. Det er imidlertid ikke slik at økt omfang og detaljeringsgrad i regelverket automatisk gir et bedre vern.

Det er ikke her anledning til å gå nærmere inn på de omfattende og vanskelige spørsmål som er knyttet til kvalitet av regelverk. Likevel er det god grunn til å understreke betydningen av særlig god regelteknikk innen områder som direkte berører beskyttelse for folks liv, helse og friheter. Innen regelverk vedrørende terrorbekjempelse mv. (i transport og ellers) kan det derfor være grunn til å følge særskilt grundige rutiner for lovteknisk assistanse og gjennomgang, for eksempel i regi av Justisdepartementets Lovavdeling.

3.6 På hvilket nivå skal personopplysninger vernes?

Dagens regulering av personopplysningsvern har som utgangspunkt at vernebehovet er like stort for opplysninger som *kan* knyttes til enkeltpersoner (selv om dette ikke har skjedd) som for opplysninger som faktisk og sikkert er knyttet til en person. Videre er opplysninger som kun finnes registrert i et datamaskinsystem likestilt med opplysninger som mennesker faktisk tilegner seg og får kunnskap om.

Med dette som utgangspunkt kan det være grunn til å spørre om den nest beste formen for personvern vedrørende sikkerhet i transport vil være 1) i minst mulig grad etablere identiteter, 2) hvis identifisering har skjedd; i størst mulig grad skjule virkelige identiteter og 3) i størst mulig grad hindre at personer tilegner seg kunnskap om fullt identifiserbare personopplysninger. Høyt automatiseringsnivå for behandlingen av personopplysninger kan forhindre at mennesker får slik kunnskap. I tabellen nedenfor er det illustrert hvorledes de tre nevnte elementene kan ses i sammenheng.

		Maskinell tilgang	Manuell tilgang
Mulig ID	Vanskelig	1	2
	Lett	3	4
Etablert ID	Skjult	5	6
	Åpen	7	8

Kilde: Schartum 2007

Tabell 3.1 Mulige kombinasjoner av mulig og etablert identitet og maskinell versus manuell informasjonstilgang.

I tabellen blir det skjelnet mellom tilfeller der identifikasjon er mulig men ikke er utført, og tilfeller der identiteten er brakt på det rene. Når det er mulig å identifisere, kan slik identifikasjon være mer eller mindre vanskelig å foreta. I tabellen er det markert to ytterpunkter for å beskrive vanskelighetsgraden.

Identifikasjon av personer fra et videoopptak i det offentlige rom vil for eksempel normalt anses å være vanskelig (mulig ID, vanskelig), mens identifikasjon av personer fra opptak gjort på ansattes pauserom vil normalt være lett (mulig ID, lett). En åpen identitet i tabellen er tilfeller der personen er identifisert med fullt personnavn mv., mens skjult identitet vil være fødselsnummer, kundenummer mv.

Det er ikke her anledning til å gå inn på en detaljert diskusjon av de åtte kategoriene som fremkommer i tabellen. Det generelle poenget er imidlertid at (bare) maskinell tilgang til personopplysninger kan anses å være mindre krenkende enn manuell tilgang, dvs. krenkelsen av personvernet kan anses å være mindre dersom opplysningene kun er gjenstand for maskinell behandling og ikke kommer til noen personers kunnskap.

Tilsvarende kan en hevde at ikke etablerte, men mulige identiteter gir mindre negative effekter for personvernet enn tilfeller der identiteten er etablert. Videre er det i utgangspunktet mindre alvorlig å behandle opplysninger der identiteter er

vanskelige å etablere enn tilfelle der dette er enkelt. Blant de etablerte identitetene er det dessuten grunn til å skjelne mellom tilfeller der identiteten er skjult (jf. pseudonymisering, kryptering av ID og avidentifisering), og tilfeller der identiteten er åpen. Førstnevnte situasjon må normalt anses å være mer gunstig for personopplysningsvernet enn situasjoner med åpen identitet.

Samlet sett vil denne tilnærmingen i utgangspunktet klassifisere personvern-truslene som lavest i kategori 1 i tabellen ovenfor og størst i kategori 8. Denne rangeringen er imidlertid bare et utgangspunkt. Hva som konkret kan anses å være den typiske rekkefølgen mellom kategoriene i tabellen vurdert etter alvorlighetsgrad mht personopplysningsvern, vil vi ikke her ha veldig bestemte oppfatninger om. Det er imidlertid nærliggende å tro at slik gradering ofte kan sies å følge nummereringen i tabellen. En viktig faktor, som ikke er del av oppsettet i tabellen, er imidlertid mengden opplysninger. Muligheten for å behandle langt større mengder personopplysninger ved automatisert behandling enn ved manuell behandling vil for eksempel kunne gjøre at kategori 7 kan bli vurdert som mer krenkende enn kategori 8.

Tabellen kan gi grunnlag for minst to konklusjoner. For det første kan den gi grunnlag for å gi generelle retningslinjer for planlegging av aktuelle informasjonssystemer og -rutiner. Det kan for eksempel være grunn til å pålegge virksomheter som behandler personopplysninger minst mulig direkte identifisering og mest mulig automatisert behandling. For det andre kan kategoriene i tabellen være et utgangspunkt for å fastsette (nye) rettssikkerhetsgarantier, dvs. regler for å sikre at personopplysningene blir behandlet på en måte som beskytter mot uberettiget rettsforfølgelse mv. Det kan for eksempel tenkes regler om domstolskontroll med manuell tilgang til personopplysninger innen politi- og påtalemyndigheter, og pålegg om logging og kontroll fra tilsynsorgan med automatisert behandling av personopplysninger i kategoriene 3,5 og 7.

3.7 Forholdet mellom personvern og rettssikkerhet

Personopplysningsvern gjelder vernet av personopplysninger generelt og er i utgangspunktet uavhengig av hvilken bruk av opplysningene som skjer. I litteraturen er det vanlig å anlegge et "beslutningsperspektiv" på personopplysningsvernet. Dette kan gjelde situasjoner der personopplysningene utgjør beslutningsgrunnlag for offentlige myndigheter, for eksempel dersom det tas beslutning om å innlede etterforskning eller avvise en person fra et offentlig transportmiddel.

Krenkelser av personopplysningsvernet er imidlertid ikke avhengig av at opplysningene anvendes som beslutningsgrunnlag, og ulovlig spredning av personopplysninger kan være en alvorlig krenkelse i seg selv. Der offentlige myndigheter bruker personopplysninger som grunnlag for avgjørelser som innebærer påbud, forbud eller begrensning av rettigheter for den enkelte, blir imidlertid personvernspørsmålene alltid alvorlige og langt på vei sammenfallende med spørsmålene om rettssikkerhet. Når personopplysninger for eksempel blir lagt fram som bevis i en straffesak, er det åpenbart av betydning hvorvidt disse er lovlig innhentet og hvilken kvalitet opplysningene har. Domfellelse på uriktig

grunnlag er åpenbart et rettssikkerhetsspørsmål. I beslutningssituasjonene møtes med andre ord hensynet til personvern og rettssikkerhet på en måte som gjør at det ikke alltid er lett å skjelne disse tilnærmingene fra hverandre – og det er heller ikke alltid fruktbart og ønskelig å gjøre det. På tiltakssiden kan det derfor være grunn til å se på personvern- og rettssikkerhetsgarantier som to sider av samme sak.

I samband med transportsikkerhet og personvern kan det være grunn til å legge vekt på følgende beslutningssituasjoner:

- Domstolenes dommer og kjennelser.
- Enkeltvedtak og prosessledende avgjørelser hos offentlig forvaltningsmyndighet.
- Enkeltavgjørelser hos transportvirksomheter mv. vedrørende adgang til og vilkår for transporttjenester.

Selv om offentlig myndighetsutøvelse i domstoler og offentlig forvaltning må anses som de mest sentrale aktørene, indikerer det siste kulepunktet at også enkelte private beslutninger på lignende måte bør ses i samme rettssikkerhets-belysning.

Utgangspunktet er at lovgiver kan finne grunn til å endre på balansen mellom ivaretakelse av transportsikkerhet/security og personvern, ved for eksempel i større grad enn tidligere å tillate innsamling, utveksling og analyse av personopplysninger for om mulig å avdekke planer om terrorhandlinger mot transportmidler mv. Dette er i seg selv en svekkelse av personvernet, men behandling av personopplysninger leder ikke nødvendigvis til andre negative konsekvenser.

Det kan følgelig være grunn til å fremheve situasjoner der personopplysningene nettopp brukes til å treffe tiltak som for den enkelte har negative konsekvenser (påbud, forbud, innskrenkning av rettigheter osv.). Spennet er stort mht hva slags negative resultater det her kan være tale om, men frihetsstraff, erstatningsplikt, utestenging fra transporttjenester, forbud mot opphold på bestemte steder til bestemte tider (stasjonsområder mv.) og bortvisning mv. er noen viktige eksempler.

Poenget er at et svekket personopplysningsvern i tilknytning til beslutninger om de personene opplysningene gjelder, så langt som mulig bør kompenseres i form av skjerpede regler knyttet til *bruken av personopplysningene.* Jo mer negativ og inngripende den mulige beslutningen er, desto viktigere blir det å kompensere for et svekket personopplysningsvern. Kompensasjon kan særlig på følgende måter:

- Skjerpe kravene til lovlig adgang til å fremlegge personopplysninger som beslutningsgrunnlag/bevis i en sak.
- Skjerpe kravene for at opplysningene kan få (avgjørende) effekt, for eksempel i form av nærmere retningslinjer, eventuelt regler om beviskrav mv. for at opplysningene kan legges til grunn for negative beslutninger.
- Styrke den enkeltes rettigheter og muligheter til å forsvare egne rettigheter.

- Tydeliggjøre kravene til og grensene for offentlige tjenestemenn som de må forholde seg til ved utøvelse av beslutningsmyndigheten.[76]

Det kan for eksempel tenkes forbud mot at transportselskaper innhenter og bruker opplysninger i vandelsattester som er eldre enn 5 år; krav om at visse minimumskrav til identifisering og autentisering må være oppfylt for å kunne legge noe frem som en personopplysning i en sak; rett til å få uavhengig sakkyndig granskning av informasjonssystemer som har generert ufordelaktige personopplysninger i en sak; og klarlegging av straffeansvar for ulovlig innhenting av personopplysninger.

Poenget er med andre ord å forbedre vernet mot at behandling av personopplysninger skal få ukorrekte belastende/inngripende konsekvenser. Spørsmålet om det nærmere innhold av slike tiltak vil ikke bli drøftet som del av dette arbeidet. Samtidig må det innrømmes at slik kompensering for svekket personopplysningsvern i form av styrket rettssikkerhet vil gi en rekke vanskelige avveininger av til dels prinsipiell karakter, og er således ikke alltid enkelt å gjennomføre.[77]

[76] Jf. for eksempel straffelovens kapittel 11 om "Forbrydelser i den offentlige Tjeneste".

[77] Det ville for eksempel være prinsipielt og kontroversielt med "bevisregler" som begrenser domstolens frie bevisbedømmelse.

4 Intervjuer om security og personvern

4.1 Design og gjennomføring

Formålet med den empiriske undersøkelsen var å få informasjon om vurderinger av sikringstiltak og personvern både fra representanter i transportgrenene og fra relevante myndighetsorganer. Dette lyktes, med unntak av luftfartssektoren hvor det viste seg praktisk umulig å få i stand et møte med operativ virksomhet/ lufthavn. Intervjuene ble gjennomført i perioden 8. februar - 30. mars 2007.

Mange detaljer rundt tiltak og planverk er konfidensielle. Dette betyr i praksis at vi ikke har fått tilgang på all informasjon. Vi mener likevel at problemstillinger rundt personvern ble belyst i tilstrekkelig grad.

Formålet med intervjuene var å kartlegge hvilke security-tiltak som er gjennomført i virksomhetene, hvilke personvernimplikasjoner de enkelte tiltakene har, hvordan hensynet til personvern og security avveies og hvordan arbeidet med security er forankret i organisasjonen. Det ble utarbeidet en felles intervjuguide med noe individuell tilpasning til hver enkelt virksomhet.

Representanter fra følgende instanser/virksomheter ble intervjuet:

- Oslo T-banedrift
- Oslo Havn
- E18 Bjørvika-prosjektet
- Datatilsynet
- Nasjonal sikkerhetsmyndighet
- Kystdirektoratet
- Jernbaneverket
- NSB AS
- Luftfartstilsynet (telefonintervju)
- Vegdirektoratet

I og med at kapitlet bygger på intervjuer der aktørenes egne synspunkter og oppfatninger presenteres, har vi valgt å beholde den muntlige framstillingsformen fra intervjusituasjonene. Opplysningene som kom fram i intervjuene kan ikke betraktes som utfyllende, men må forstås som momenter som aktørene selv valgte å legge vekt på i intervjuene. En del av informasjonen vi ønsket å få er

konfidensiell, og av den grunn vil noe informasjon være utelatt. På bakgrunn av dette fant vi det dessuten mest korrekt ikke å bruke opptaksutstyr under intervjuene og brukte ”live” transkribering.

Vi har videre valgt å strukturere kapitlet ut fra noen dimensjoner vi mente representerte de viktigste funnene fra intervjuene. Dimensjonene er et forsøk på en tolkning og sammenfatning av viktige tema og problemstillinger som kom fram under intervjuet. Dimensjonene vi har valgt er:

- Særtrekk ved transportgrenene
- Security-tiltak
- Aktørenes oppfatning av personvernimplikasjoner
- Organisatorisk forankring av security-arbeid
- Trusselvurderinger, risiko og sårbarhet
- Behov for koordinering
- Framtidsutvikling

4.2 Særtrekk ved transportgrenene

Utgangspunktet for denne dimensjonen er representantenes egen oppfatning av hva som særpreger transportgrenene. En samlet gjennomgang av intervjuene viste at dette framsto som vesentlig for flere av aktørene. De trakk fram særtrekk ved sin sektor som var viktige i forhold til hvilke security-tiltak som kunne gjennomføres i sektoren. Intervjuene viste at det er vesentlige forskjeller mellom transportgrenene som har betydning for synet på security og personvern. Disse forskjellene dreier seg om:

a) Grad av massetransport og ulikhet i transportøkonomi
b) Transportmidler som nettverk
c) Grad av integrasjon i øvrige systemer og hverdagsliv
d) Samfunnets risikoaksept overfor de ulike transportgrenene
e) Ulikheter i institusjonell forankring og regelverk

4.2.1 Massetransport og transportøkonomi

Kollektivtransportmidler som T-banelinjer i Oslo har typisk avgang hvert 15. minutt. Et T-banesett kan i rushtrafikken frakte opp til 900 passasjerer og har 4-5 stasjoner med større trafikk enn Gardermoen.

Siden security-tiltak koster penger, er også omfanget av security-tiltakene begrenset av rene transportøkonomiske hensyn. I intervjuene kom det fram at kostnadene til security-tiltakene i sivil luftfart beløper seg til om lag 40 kroner per passasjer per reise. Dette er mellom to og tre ganger så mye som billettprisen ved offentlig transport i sentrale byområder. Svært omfattende sikringstiltak, slik de vi finner i luftfart, vil bli for kostbare i de fleste andre transportgrener. De grunnleggende økonomiske betingelsene for mange kollektivtransportselskaper vil derfor være et hinder for å gjennomføre den type sikkerhetsregime som i dag

eksisterer i luftfarten. Dette var en oppfatning som kom til uttrykk fra flere av aktørene.

4.2.2 Transportmidler som nettverk

Transportgrenene er svært ulike når det gjelder hva slags nettverk de opererer i. Ekstremt sentraliserte transportmidler, som fly, konsentrerer seg først og fremst om punkt-til-punkt-trafikk mellom knutepunkter/lufthavner som ofte er plassert et godt stykke unna øvrige samferdselsknutepunkter. En slik struktur legger godt til rette for overvåkning og skjerming av flyplasser. Kollektivtransport i byområder, som buss, trikk og T-bane er derimot en integrert del av bybildet og dermed svært vanskelig å skjerme på tilsvarende måter. Det samme gjelder ekstremt desentraliserte transportformer, som biltrafikk. Biltrafikken foregår på et omfattende og spredt veinett med et enormt antall kjøreruter og et bortimot uendelig antall på- og avstigningspunkter. Adgangen til både transportmiddel og trafikknettet er under individuell kontroll.

Dette er antakelig en viktig grunn til at rene security-tiltak i veisektoren oppfattes som vanskelige å gjennomføre, og det kan også være problematisk å identifisere konkrete behov for denne type tiltak. Tiltakene i kollektivtransport og på vei vil også nødvendigvis måtte være av en annen art enn i luftfart, og kan kun unntaksvis være basert på f. eks. systematiske massekontroller av alle passasjerer slik vi kjenner det fra luftfart.

4.2.3 Integrasjon i systemer og hverdagsliv

Integrasjon i systemer og hverdagsliv dreier seg om hvor tett innvevd transportgrenene er i passasjerenes hverdagslige rutiner som daglige reiser til jobb, til daglige fritidsaktiviteter etc. Kollektivtrafikk som T-bane blir beskrevet som en integrert del av byen, med drift over hele byen og til nesten alle døgnets tider. Passasjertoleransen for forsinkelser og opphold i forbindelse med eventuelle security-tiltak er dermed sterkt begrenset. Den kan derimot være stor for forsinkelser som skyldes enkelthendelser dersom dette blir godt kommunisert til publikum. NSB har hatt episoder hvor tog og stasjonsområder må tømmes for publikum ved mistanke om trusler og lignende. NSB har derfor satset sterkt på varsling og kommunikasjon med passasjerer ved slike hendelser og mener dette er gode security-tiltak.

4.2.4 Risikoaksept i ulike transportgrener

Flere av informantene pekte på at det er forskjellig grad av aksept for risiko og ulykker innen de forskjellige transportgrenene, og at dette selvsagt også påvirker security-tiltak innen transport. Luftfarten skiller seg særlig ut med stort ressursbruk (per passasjer per reise). Informanter både fra bane- og veisektoren pekte på at det ville være gevinster i liv og helse ved å flytte ressurser fra security-tiltak i flysektoren til eksempelvis safety-tiltak i veisektoren, og at tiltakene ikke burde være så *hendelsesstyrt* som de faktisk er. Dette henger også sammen med at de mange små ulykker i eksempelvis veisektoren vies mye mindre oppmerksomhet enn de få store samferdselsulykkene. Slik noen av informantene

så det var årsakene til dette i stor grad knyttet til mekanismer i en mediestyrt offentlighet og politikk, slik at en rent rasjonell nytte-kostnads-tankegang har vanskelig for å få gjennomslag. Et moment som ble nevnt som et argument mot en slik nytte-kostnadsbasert tankegang er at terroranslag kan tenkes å ha en sterkt demoraliserende virkning på den allmenne tilliten som eksisterer til transportsystemene, på en helt annen måte enn rene ulykker og lignende episoder har. Begrunnelsene for security-tiltak vil dermed ikke være identiske med begrunnelsene for safety-tiltak.

4.2.5 Ulikheter i institusjonell forankring og regelverk

De forskjellige transportgrenenes institusjonelle forankring og regleverk knyttet til transporten påvirker i stor grad hvilket spillerom virksomhetene i de forskjellige transportgrenene har i valg og utforming av security-tiltak. Her er det store forskjeller mellom aktørene. Spesielt informantene fra sjøfartsmyndigheter og luftfart oppfatter i stor grad security-tiltakene som implementering av internasjonalt regelverk, fra både EU og internasjonale organisasjoner som IMO. Andre transportgrener som eksempelvis jernbane, T-bane og vei står mye friere til å velge både tilnærmingsmåte og virkemidler innen security-feltet. Samtidig oppgir de aller fleste transportgrenener at de i økende grad opplever forventninger og føringer fra offentlige myndigheter når det gjelder security-tiltak. Dette gjelder særlig fra Samferdselsdepartementet, men også fra Kyst- og fiskeridepartementet og Næringsdepartementet. Sjøtransporten (sjø, kyst og havn) sorterer under alle de tre nevnte departementene.

Mange av aktørene, spesielt innen kollektivtransport, medgir at de er sårbare på mange punkter. Vårt inntrykk er likevel at de fleste informantene ikke finner det påkrevd med større grad av formalisering og mer enhetlig regelverk innen security. Aktørene i kollektivtransporten opplever at det delegerte ansvaret fungerer godt. Det tillater hurtigere læring og mer selvstendige tilpasninger, og dermed mer målrettede og hensiktsmessige tiltak enn det mer sentraliserte beslutningssystemer vil kunne legge til rette for: ”Vi vet selv best hvor skoen trykker”.

4.3 Aktørenes oppfattelse av personvernimplikasjoner ved security-tiltak

Hovedhensikten med intervjuene var å finne ut hvordan personvern er integrert i arbeidet med security-tiltak i de ulike transportgrenene. Sentrale spørsmål har vært om tiltakene har personvernimplikasjoner og om hensyn til personvern har kommet i konflikt med tiltak for økt security.

Aktørene i bransjen har noe ulik oppfatning av om tiltakene de har gjennomført har personvernimplikasjoner, og de skiller gjerne mellom implikasjoner tiltakene har for de ansatte og for publikum. I Vegdirektoratet oppleves personvern i hovedsak å være knyttet til tiltak for de ansatte i etaten; i Luftfartstilsynet er oppfatningen at det først og fremst er passasjerenes personvern som berøres av security-tiltak. Enkelte virksomheter, som T-banen og NSB, uttaler seg også om hvordan de oppfatter publikums syn på innføring av security-tiltak som kan ha implikasjoner for personvernet.

Intervjuet med Datatilsynet ga innblikk i en rekke ulike aspekter ved personvernlovgivning som har betydning for avveiningen mellom personvern og security-tiltak som kameraovervåkning, adgangskontroll, flåtestyring og biometri. Datatilsynets inntrykk er at aktørene i transportsektoren jevnt over tenker lite rundt hvilke personvernimplikasjoner innføring av ulike security-tiltak kan få. Unntaket er luftfarten hvor personsikkerhet og personvern går veldig mye hånd i hånd. Det er lite motstridende interesser, formålet er reell sikkerhet. Dersom formålet er økonomiske innsparinger kan det fortere bli konflikt.

Datatilsynet prøver å skape en offentlig debatt rundt personvern. Datatilsynets syn er at i den grad det er implikasjoner når det gjelder personvern, er det viktig å ta bevisste valg. I det faktiske valget taper man noe og oppnår noe annet. Stortinget skal bestemme, og de må ha et skikkelig grunnlag. Datatilsynet ga noen eksempler på tiltak med overvåkningskameraer som de mente tok de nødvendige personvernhensyn. Det er eksempelvis greit med plassering av kamera ved utgang/inngang i buss. Da blir både personvern og sikkerhet tatt vare på i forsvarlig grad. Taxiløsningen, med filming de første fem sekundene når passasjeren går inn i bilen, fungerer også greit i følge Datatilsynet. Oslo Sporveier har ønsket å filme hele bussen, noe Datatilsynet har vært motstander av. Vedtaket ble imidlertid klaget inn til Personvernnemnda, og Oslo Sporveier fikk medhold i at det var i orden å filme hele bussen.

Bransjen har selv utført publikumsundersøkelser om holdninger til personverninngripende tiltak som Datatilsynet mener var noe fargelagt av oppdragsgiver og formuleringer. Datatilsynets holdning er at kameraovervåkning i mange tilfeller er greit, men at det brukes litt for lettvint i mange sammenhenger. Mange aktører har et litt for ureflektert syn på dette; det viser seg at kameraovervåkning i mange tilfeller egentlig ikke er et hensiktsmessig tiltak. I tillegg hender det at mange ønsker å ”legge til litt til” etter at man har innført et tiltak som kan ha personvernimplikasjoner, og da beveger jo systemet seg vekk fra de opprinnelige og mer begrensede hensiktene.

T-banen har tradisjonelt hatt en forsiktig tilnærming til overvåkning og har med vilje valgt å holde tilbake enkelte virkemidler, eksempelvis ved ikke å ha høydefinerte kameraer, og ikke rette kameraene mot personene som går mot billettautomatene, men mot selve automatene etc. T-banen følger ellers myndighetenes krav i forhold til personvern og forholder seg til gjeldende lovverk. Datatilsynet har aldri stoppet T-banen når det gjelder tiltak. Personvern for T-banen er å følge myndighetenes krav. I følge T-banen er kundene i stor grad positive til kameraene. Passasjerene på T-banen er isolerte fra føreren i motsetning til på bussen, og kamera vil kunne gi en større følelse av trygghet. I følge T-banen ønsker publikum trygghet og er villig til å inngå kompromisser.

For Oslo havn er ikke personvern noen stor sak, først og fremst fordi det ikke er så mye publikum på havneområdet. Når det gjelder personvernimplikasjoner av security-tiltak, ble det referert til kroppsvisitering. Slik det er i dag kan ingen tvinges til å bli kroppsvisitert, men hvis en ikke ønsker å underlegges kontroll, blir en bortvist fra området. I den nye forskriften prøver en å hjemle visiteringen i Havne- og farvannsloven. Når det gjelder de ansatte signerer de en sikkerhetserklæring/taushetserklæring.

Oslo Havn prøver i den grad det er mulig å samkjøre arbeidet med sikkerhet og security. Etter innføringen av ISPS (International Ship and Port Facility Security Code) har tyveri og øvrig kriminalitet gått ned. Dette er en gunstig bieffekt. Mindre populært er permanent og periodevis avstengning av kaiområder, da noen av disse områdene også brukes til ferdsel og rekreasjon. Det finnes personer som har fisket på kaia i alle år og som nå er forhindret i dette på grunn av inngjerding av kaiområdet. Enkelte politikere har også engasjert seg mot å stenge havneområder for publikum. Det er i og for seg ikke er personvernproblem, men et eksempel på et security-tiltak som er til hinder for fri ferdsel blant publikum.

Kystverket viste til at det er havnene som må søke om tillatelse for å drive kameraovervåkning og regner med at havnene sørger for dette og søker Datatilsynet.[78] Det har mye å si om kameraene identifiserer personer. Man har ellers ikke gjort seg så mange tanker rundt tiltakene og personvern, men det er tenkt på personvern i forhold til prosessen rundt sikkerhetsklarering av personell hvor man må ivareta deres person- og rettssikkerhet.

Samtalene med Vegdirektoratet viste at hensyn til personvern er integrert i arbeidet med trafikksikkerhetstiltak, som for eksempel punkt- og streknings-ATK (automatisk trafikkontroll), og trafikkstyrings- og bompengesystemet AutoPASS m.m. Direktoratet har imidlertid i liten grad erfaringer når det gjelder forholdet mellom personvern og security-tiltak, i og med at veisektoren ikke har iverksatt konkrete security-tiltak utover interne tiltak rettet mot de ansatte. Det kan komme tiltak ved heving av trusselnivået som eksempelvis å kanalisere trafikk og utføre kontroll på ferjer. Personvernhensyn er mer aktuelt for interne forhold. Sikringstiltakene til Vegdirektoratet (grunnsikringen) består av fysisk sikring og informasjonsbehandling. Direktoratet prøver å beskytte personvernet i behandlingen av informasjonen de forvalter.

I E18-Bjørvika-prosjektet har det heller ikke vært tenkt mye rundt personvern, men prosjektledelsen er klar over at slike implikasjoner kan oppstå. De følger retningslinjene fra Vegtrafikksentralen. Det ble gjort en omfattende registrering av bygninger før prosjektet ble satt i gang dersom erstatning skulle bli aktuelt. De bruker egne firmaer som har tillatelse fra Datatilsynet til å utføre jobben og oppbevare disse opptakene. Under byggefasen gjennomføres adgangskontroll og andre sikkerhetstiltak, men det er lite uttalt fokus på personvern i forhold til dette.

Jernbaneverket er infrastrukturforvalter og i den rollen i liten grad involvert i spørsmål knyttet til personvern. Som arbeidsgiver er imidlertid personvernspørsmål aktuelle for Jernbaneverket, og dette gjelder særlig overfor ansatte i IT-funksjoner. Når det gjelder personvernimplikasjoner av security-tiltak, innhentes det stort sett tillatelse fra Datatilsynet. Eksempler på tiltak med personvernimplikasjoner er tilgangskontroll, som er relativt streng, på alle

[78] Datatilsynets årsmelding for 2006 viser at dette ikke alltid er tilfellet. Mandal havnevesen planla en storstilt kameraovervåkning av småbåthavner med høyoppløselige "doom-kameraer". Dette er fjernstyrte kameraer med 360 graders dekningsområde og som regel også med zoom-funksjon for å sikre havner mot ordinær kriminalitet (tyveri av/fra båter osv.). Dette ble innklaget til Datatilsynet som konkluderte med at dette var i strid med personvernlovgivningen. Det ble gitt råd om en løsning som vil tilfredsstille personopplysningslovens krav, blant annet med maskering av privat eiendom, låsing av kameraposisjon og begrenset tilgang til overvåkningsbildene (St.meld. nr. 5 (2007-2008, s. 39).

jernbaneverkets lokasjoner, og krav om sikkerhetsklarering for medarbeidere. Kameraovervåkning skal kun brukes for å avdekke ulovlig virksomhet.

I NSB er man bevisste på at security-tiltak kan ha implikasjoner for personvernet. Kameraovervåkning er det tiltaket hvor en kommer tettest inn på mennesker. NSB mener likevel at det ikke har særlige følger for personvernet med den teknikken de har valgt å bruke. Det er for eksempel ikke snakk om "live" overvåkning. Det har vært en del diskusjoner rundt dette. I kravene til risikoanalyse står det ingenting om personvern. Det kommer opp som tema likevel, i første instans overfor de ansatte ettersom verneapparatet er med i arbeidet og engasjerer seg for deres personvern. Alle ansatte skal være kundenes ambassadør, og da går også tankene med en gang til kundenes personvern. Temaet personvern har også dukket opp i forbindelse med økt bruk av elektronisk billettering. Dette er imidlertid ikke et tiltak rettet mot security, men nevnes likevel som et eksempel i forhold til personvernimplikasjoner. Med dette systemet kan man spore opp hvor reisen er kjøpt, men det stopper der. NSB har ikke et system hvor en kan følge med og identifisere tidligere passasjerer på nye reiser. Informasjonen om billettkjøp blir slettet. De bruker systemet til telling, men dette er anonymiserte data. Det er ikke noe ønske i selskapet om å misbruke billetteringssystemet til andre formål enn det som er tiltenkt.

I forbindelse med et prøveprosjekt med kameraovervåkning på tog, gjennomførte NSB en intervjuundersøkelse der 7000 kunder ble intervjuet angående kameraovervåkning. Tilbakemeldingene var positive. NSB fikk ros fordi de hadde begynt med kameraovervåkning. Kundene ga massiv støtte til tiltaket; sju prosent ga et nøytralt svar, og bare to prosent var negative til kameraovervåkning.

For luftfartssektoren er det sikkerhetskontrollen på flyplassene som har størst implikasjoner for personvernet. Det berører den enkelte passasjer som må ta av seg klær og gjenstander og eventuelt kroppsvisiteres. Dette kan føles vanskelig for mange. Luftfartstilsynet har lenge ønsket å innføre biometri som security-tiltak. Dette er i begrenset omfang nå innført i form av fingeravtrykkleser for å sammenligne innsjekket bagasje og passasjer, men Datatilsynet stilte en rekke betingelser for å godkjenne systemet.

Vårt generelle inntrykk fra intervjuene er at personvernhensyn ikke er svært høyt oppe på dagsorden i det daglige arbeidet, men samtlige aktører har likevel tenkt gjennom de sidene ved personvernet som oppleves relevante for egen virksomhet. Intervjuene viste stor variasjon i de ulike virksomhetenes oppfatninger av og interesse for personvernspørsmål. Flere uttrykte at de hadde stort fokus på personvern og var bevisste dette ved innføring av tiltak som kameraovervåkning, identitetskontroll m.m. Det skyldes også sterk kontroll av dette fra Datatilsynets side. Ingen mente at avveining av personverninteresser og innføring av security-tiltak var et stort problemfelt for virksomheten. Mange av respondentene kunne vise til eksempler på ulike tiltak som var blitt stoppet av Datatilsynet fordi de var i strid med personvernet, men dette var ikke tiltak som hadde sikring mot terror som formål.

4.4 Security-tiltak

Virksomhetene var godt kjent med security-begrepet, og alle virksomhetene vi snakket med hadde innført, eller var i ferd med å innføre, ulike virkemidler innen security-området. Det varierte derimot en del hva de ulike transportgrenene la i begrepet ”security”. De fleste, og særlig representantene for kollektivtrafikk som T-bane og tog, inkluderte vanlig hverdagskriminalitet som voldstrusler, hærverk, tyveri, tagging etc. i security-begrepet. Representanten fra T-banen forklarte dette med at T-banen var så tett integrert med samfunnet og hverdagen for øvrig, at alt som skjedde i samfunnet, skjedde også på T-banen.

I hvilket omfang security-tiltak var innført og konkret hva slags tiltak man hadde valgt, varierte en del mellom transportgrenene. Gjennom intervjuene kom det fram at dette både henger sammen med graden av institusjonell styring (regelverk etc.), og med aktørenes egne vurderinger av hva som er hensiktsmessige måter å løse security-problemer på. Et gjennomgående inntrykk var at flere av virksomhetene bestrebet seg på å bygge opp en ”security-kultur” på nivå med virksomhetens ”safety-kultur”. Representanten fra luftfartssektoren trakk spesielt fram dette. Det kom også fram fra de aller fleste at det hadde blitt lagt veldig stor vekt på dette aspektet etter 11. september 2001.

Et gjennomgående funn var at informantene oppfattet at det var nær sammenheng mellom tiltak innen security og safety. Tiltak som var rettet mot security kunne også ha positive virkinger på safety. I forbindelse med beredskapsplaner så flere av informantene heller ikke store forskjeller på om beredskapen var knyttet til security eller safety. Ved brann i tunnel vil det i praksis ikke være stor forskjell på om den skyldes en villet handling eller om den skyldes en ren ulykke. Representanten fra Luftfartstilsynet trakk fram at både tiltakene i safety og security har samme mål, selv om det var vanskelig entydig å dokumentere sammenhengen mellom safety og security i luftfarten.

Intervjuobjektene ble bedt om å beskrive security-tiltakene generelt i sin bransje, samt å nevne tre (hvis mulig) security-tiltak som de har gjennomført i sin virksomhet. Tiltakene som ble nevnt er delt inn i fem grupper og presenteres nedenfor. Virksomhetene kan selvsagt ha tiltak utover de som er nevnt her.

Overvåkning:

Her menes maskinelle og visuelle teknologier som f eks skanning og kamera.

Tiltak	Nevnt av
Radarovervåkning	Oslo havn
Skanning	Oslo havn, Luftfartstilsynet
Kameraovervåkning	T-banen, Kystdirektoratet, Jernbaneverket, NSB, Oslo havn

Informasjonstiltak:

Her menes kommunikasjon og informasjon til ansatte og publikum.

Tiltak	Nevnt av
Årvåkenhetsmelding til ansatte	Jernbaneverket
Opplæring av ansatte	NSB
Informasjonsskjerming	E18 Bjørvika, NSM, Vegdirektoratet
Informasjon til publikum/melding om bagasje over høyttaleranlegg	T-banen, Jernbaneverket

Tilgangskontroll

Her menes kontroll på regulær passasjerferdsel.

Tiltak	Nevnt av
Adgangskontroll	Oslo havn
Samsvarskontroll	Luftfartstilsynet
Sikkerhetskontroll	Luftfartstilsynet
Forbud mot å ta med konkrete gjenstander på transportmiddelet	Luftfartstilsynet

Inspeksjon og fysisk sikring

Her menes tiltak for å hindre irregulær adgang til transportmidler og områder.

Tiltak	Nevnt av
Manuell sjekk	Oslo havn
Sjekk med detektor	Oslo havn
Vektere (synlige og sivile)	T-banen, NSB
Billettkontrollører	T-banen
Sikring av førerhus mot innbrudd	T-banen
Montering av gjerder	Oslo havn, Kystdirektoratet
Låsbytte	NSB
Fysisk sikring av bygg og anlegg	Vegdirektoratet

Andre tiltak

Her nevnes andre tiltak som ble nevnt.

Tiltak	Nevnt av
Sårbarhetsanalyse	NSB
Etterretning og kontakt med politi	Alle
Øvelser i kriseledelse og krisekommunikasjon	Jernbaneverket

Enkelte interessante trekk kan leses ut av denne oversikten. NSB har for eksempel plukket ut opplæring og kursing av *ansatte* som et vesentlig security-tiltak for jernbane, noe som står i sterk kontrast til luftfartens fokus på *passasjerene*. Dette henger naturligvis sammen med at betingelsene for kontroll og styring av passasjerer er helt forskjellige i flysektoren og i jernbanesektoren. Det henger igjen sammen med internasjonale regleverk, med ulik aksept for security-tiltak blant passasjerer i ulike transportgrener, og med ressursene som står til rådighet. Det betyr imidlertid at det for eksempel ikke er noe i veien for å ha med et skytevåpen på tog, så lenge det er forskriftsmessig transportert. Kontrasten til flytrafikken er altså stor.

Et felles trekk er at nær sagt alle har kontakt med politiet gjennom PST. Hvor regelmessig denne kontakten er, varierer, men flere av virksomhetene får regelmessige oppdateringer fra PST. Denne kontakten oppleves gjennomgående som svært nyttig.

Systematisering av elektroniske spor (fra billetteringssystem) eller sammenkjeding av informasjon i security-sammenheng var lite utbredt. Noen av virksomhetene hadde for så vidt vurdert muligheten for det, men hadde av flere grunner ikke gått for denne løsningen. Dette gjaldt for eksempel ved T-banen i Oslo hvor man i utformingen av nytt elektronisk billettsystem bestemte seg for et system uten omfattende sporingskapasitet. Flere av representantene, for eksempel Datatilsynet, pekte ut veisektoren som den transportgrenen som hadde valgt løsninger med størst kapasitet for lagring av informasjon om reisende. Datatilsynets informant pekte også på at dette var et felt i sterk vekst og at det var sterkt teknologidrevet, ofte med utgangspunkt i forskningsprogrammer i EU. Et tankevekkende moment er at mange av de løsningene med sterkest implikasjoner for personvernet ikke er knyttet til security-tiltak, men er oftest knyttet til safety (potensielle automatisk ulykkesvarsling (”eCall”), alkolås m/varsling etc.) og betalingsløsninger (eksempelvis bompengeinformasjon i AutoPASS).

Det viste seg også å være beskjeden interesse for ulike høyteknologiske løsninger som automatisk ansiktsgjenkjennelse, avanserte røntgenløsninger etc. Flere av informantene var for så vidt godt kjent med slike løsninger, men anså disse som mindre egnede i en norsk sammenheng. Et unntak her var flysektoren hvor løsninger basert på *biometri* ble trukket fram. I veisektoren er det stor uvikling innen teknologiske løsninger, men det gjelder som nevnt på safetyområdet.

Et annet moment er at flere representanter fra kollektivtrafikken angir fysisk sikring av infrastrukturen (sikring av førerhus, avlåsing av utganger etc.) som et

security-tiltak. Slike tiltak vitner om at den økte bevisstheten rundt security er relativt ny i disse transportgrenene.

Enkelte virksomheter har en svært eksplisitt satsing på security, eksempelvis flysektoren. Andre sektorer, som veisektoren, har en mindre eksplisitt satsing på security-tiltak. Dette betyr ikke at security-aspekter ikke er vurdert, men at flere av de "typiske" security-tiltakene ikke er særlige hensiktsmessige i veisektoren. Et eksempel på dette er E18-Bjørvika-prosjektet hvor en etter en vurdering av trusselbildet har konsentrert seg om safety-tiltak uten å gjennomføre spesielle tiltak mot mulige terrortrusler. Trafikksikkerhetstiltakene er derimot omfattende, og flere av dem vil også virke positivt inn i en security-sammenheng, og ved en eventuell security-relatert hendelse. Tiltakene er kameraer med hendelses-detektering, fotobokser, telefoner, nødutganger, ventilasjonssystemer, automatisk trafikkstyring, infotavler m.m. Vegdirektoratet nevner safety-tiltak som automatisk trafikkontroll (ATK), alkolås, atferdsregistrator m.m. Security-tiltak er for veimyndighetene primært knyttet til interne forhold, men tiltak også for eksterne forhold kan bli aktuelt dersom trusselnivået skulle endre seg og det vil bli behov for spesielle tiltak.

Vår intervjurunde viser at security-tiltak er kommet inn på alle felt etter 11. september 2001. Tiltakene utformes relativt fritt av aktørene selv etter en vurdering av hensiktmessighet og forholdsmessighet, med unntak for havner og luftfart hvor det omfattende og detaljerte internasjonale regelverket gir mindre spillerom lokalt. Få av aktørene ser for seg at noen enkelt av transportgrenene skiller seg ut som et forbilde for andre.

4.5 Organisatorisk forankring av securityarbeid

Securityarbeidet er ulikt organisatorisk forankret i de virksomhetene vi har hatt samtaler med. Dette kan ha betydning for hvordan security vektlegges i organisasjonen og hvordan man tar personvernhensyn der det måtte være nødvendig. Intervjuene viste at enkelte virksomheter er organisert slik at de har egne avdelinger med ansatte som jobber med security. Andre virksomheter har ikke det, selv om de også jobber med security. Intervjuene viser også at det er ulik organisering av risiko-og sårbarhetsarbeidet. Virksomhetene er i ulik grad involvert i utarbeidelsen av ROS-analyser, og det er ulik praksis mht å trekke inn ekspertise utenfra.

T-banen har for eksempel hovedfokuset på trafikksikkerhet (safety), men securityaspektet har kommet mer og mer inn i dette arbeidet. T-banen har ingen egen avdeling som utelukkende jobber med security. I staben er det de samme personene som jobber med både sikkerhet og trygghet[79] (security), men operativt er dette delt. Det er ikke et skarpt skille, men i praksis tar for eksempel vektere seg av deler av securityarbeidet, mens førerne vier seg i større grad til trafikksikkerhet. T-banen utarbeider risikoanalyser selv basert på egne, interne analyser og på eksterne analyser de mottar fra for eksempel PST.

Jernbaneverket har en sikkerhetsdirektør som er rådgiver i forhold til Jernbaneverkets ledelse og ivaretar mange sentrale støttefunksjoner. Han skal

[79] T-banen har valgt å bruke begrepet "trygghet" om "security".

blant annet legge til rette for at den enkelte linjeleder kan ivareta ansvaret sitt og omsette alle lover og retningslinjer til praktiske gjennomførbare tiltak. Jernbaneverket har et desentralisert rådgivningssystem og har et nettverk av rådgivere innen både security og safety. Det er de samme som driver med sikkerhet som driver med safety. ROS-analyser utarbeides vanligvis av Jernbaneverket selv, men også i samarbeid med eksterne virksomheter, for eksempel Forsvarets Forskningsinstitutt (FFI), Det norske Veritas (DNV), Scandpower og Safetech. Jernbaneverket får bakgrunnsinformasjon fra blant annet Nasjonal sikkerhetsmyndighet (NSM) på IT-siden. Jernbaneverket har en securitygruppe for hele jernbane-Norge.

NSB AS har en sikkerhetssjef i driftsavdelingen. Det er også en sikkerhetsavdeling i konsernet. Disse to enhetene jobber tett innen security. Ulykkesberedskapen til NSB er utviklet sammen med SINTEF og DNV, og denne er i ferd med å bli utvidet til også å gjelde security på alle områder. Når det gjelder ROS-analyser får de hjelp av eksterne konsulenter. En konsulent vil hjelpe til med å sette kravspesifikasjoner; FFI bidrar med innspill når det gjelder terror og sabotasje, og SINTEF tar seg av safety.

Vegdirektoratet har tre årsverk i en stab som jobber med sikkerhet, beredskap og krisehåndtering. Lederen for staben er Vegdirektørens rådgiver i forhold til tiltak, informasjon, tredjemanns opplysninger som kan være sensitive, beredskapsplaner, hendelser utenfor drift m.m. Staben har nylig presentert et forslag til en overordnet ROS-analyse for hele sektoren. Analysen er basert på en rekke mindre ROS-analyser gjennomført i regionene og i Vegdirektoratet og er sydd sammen i et felles system. Denne sammensyingen gjøres av Vegdirektoratet/"sikkerhetsstaben".

E18 Bjørvika-prosjektet er en del av byutviklingsprosjektet Bjørvika. Målet med prosjektet er å legge om E18. Veien legges om ved å bygge en senketunnel og et nytt avviklingssystem for trafikken som går over Bispelokket i dag. Prosjektet er delt i to etapper, den første fram til 2010 og den andre fram til 2012.

Prosjektet har gjennomført en hendelses- og usikkerhetsanalyse. Analysene ble utført i egen regi, men man trakk inn også eksterne krefter. I første fase var også politiet og brann- og redningsetaten involvert. De var med på å definere og vurdere ulike scenarier for E18 Bjørvika. De så også på konsekvensene eventuelle ulykker ville ha. Analysene blir revidert to ganger i året, av prosjektet selv. Noen av konsulentene som har vært med på prosjekteringen av byggingen, deltar i disse revisjonene. Prosjektet har tatt opp spørsmålet rundt sikring av tilgang til tunneltegningene med Vegdirektoratet, men direktoratet har ikke noen spesiell policy på området. Det har vært opp til prosjektet selv å finne en hensiktsmessig løsning.

I Kystdirektoratet ligger krigs- og kriseberedskap og securityoppgaver i "Enhet for sjøtransport og havner", men det finnes også en beredskapsavdeling i direktoratet som ligger i Horten og som har ansvar for akutt forurensingsberedskap. Hvert havneanlegg skal gjøre en sårbarhetsvurdering, og på grunnlag av den nedfelles en handlingsplan. Det er viktig å poengtere at havnene ikke utarbeider sårbarhetsvurderingene selv; det gjørs av såkalte RSO (Recognized Security Organisations). RSO er selskaper som er funnet kompetente til å utføre denne jobben og som får autorisasjon fra Kystdirektoratet.

Sårbarhetsanalysen danner grunnlaget for Sikkerhetsplan m/tiltak. Sikkerhetsplanen kan utformes av havnene selv, men de fleste havner har imidlertid brukt samme RSO til å lage både sårbarhetsanalyse og sikkerhetsplan. I henhold til EU-direktiv 2005/65 kan man ikke lenger bruke samme RSO til begge deler. En RSO kan gjøre vurderingene, men havnen skal være med på deler av arbeidet og kvalitetssikre analysen til slutt.

Ved Oslo havn er havnedirektøren øverste sjef. Havnekapteinen er PSO (Port Security Officer) og sikringsansvarlig for hele Oslo havn. Det innebærer bl.a. myndighet til å bestemme heving og senking av sikkerhetsnivået. Oslo havn er delt inn i to distrikter, som hver har distriktssjefer som er assisterende PFSO (Port Facility Security Officer). Disse er også PFSO for cruiseanløp. Hvert distrikt har flere terminaler, og hver terminal har igjen en sikkerhetsansvarlig fra det rederiet som opererer terminalen. Color Line har for eksempel en sikkerhetsansvarlig på Hjortneskaia.

I Luftfartstilsynet er safety og security atskilt. Tilsynet har en egen securityavdeling som er direkte underlagt luftfartsdirektøren. Det har vært et ønske om å bygge en ”security-kultur” på samme måte som ”safety-kulturen” og luftfartsdirektøren har derfor løftet opp security til egen avdeling. Security kom som eget fagfelt etter 11. september og fikk også økt fokus ved flyttingen av tilsynet til Bodø. Fokuset er også styrket gjennom implementeringen av nye og strengere internasjonale regler for security på lufthavner. Det har alltid vært arbeidet med security, men det har ikke vært så klart skille mellom safety og security før. Tilsynet har ingen egen safetyavdeling, men har operativ avdeling og teknisk avdeling og begge disse har safety i seg. Det jobbes mot felles mål, men det er vanskelig å helt entydig kunne dokumentere sammenhengen mellom security og safety – hvilken konkret innvirkning på safety security-tiltakene har.

Security-fokuset til Luftfartstilsynet er knyttet til anslag mot terror. Security-avdelingen har blant annet ansvar for adgangskontroll og regelverksutvikling. Sju inspektører har ansvaret for å sjekke at alle aktører etterlever det felles europeiske regelverket. De driver stort sett inspeksjon i Norge, men noen har EU-sertifisering og inspiserer sammen med EU. Luftfartstilsynet har ikke gjennomført egen ROS-analyse, men samler inn kunnskap som grunnlag for å drive risikobasert tilsyn.

4.6 Trusselvurderinger, risiko og sårbarhet

I intervjuene stilte vi et spørsmål om virksomhetens trusseloppfatning og trusselvurdering, og som forventet var muligheten til å svare og åpenheten rundt svarene svært forskjellige. Enkelte virksomheter nevnte kriminalitet (hærverk, tyveri, fysiske trusler mot passasjerer m.m.) og terror som sentrale trusler for deres virksomhet. Andre ønsket ikke å svare på grunn av at det var gradert informasjon. Alle intervjuobjektene har oppgitt at virksomheten har en ROS-analyse, med unntak av Luftfartstilsynet. Dette er ikke et tegn på manglende fokus på risiko og sårbarhet i luftfart, men henger sammen med tilsynsrollens utforming i luftfarten. Tilsynet har et sterkt fokus på security og jobber etter forskrift om forebyggelse av terroranslag mot sivil luftfart.

Når det gjelder villede handlinger jobber T-banen mye med logger i forbindelse med materielle skader som tagging. Dette er hendelser hvor det er et stort

”volum” av historiske data som det jobbes med. Sammensetningen av dette volumet danner et risikobilde og kan si noe om punkter som mer utsatt enn andre. Eksempelvis hvor det tagges, når det tagges, hvilke banestrekninger og tidspunker som er mest belastet osv. Tagging er ansett som en av de store utfordringene og truslene T-banen til enhver tid står overfor.

T-banen har flere kanaler å benytte seg av i forbindelse med trusselvurderinger og har blant annet noe kontakt direkte med politiet og PST. T-banen har gjort risikoanalyser, og de inneholder i og for seg både safety og security. I arbeidet med ROS-analysene var en av konklusjonene at for utkommets og beredskapens del spiller det ikke alltid noen stor rolle om dette regnes som safety eller security, for eksempel om en person selv ramler eller blir dyttet foran T-banen. Konsekvensene og beredskapen vil uansett være de samme. I forhold til terror er selvsagt konsekvensene potensielt svært store, men sannsynligheten er så liten at det ikke er lett å treffe mer omfattende tiltak for slike potensielle hendelser.

T-banen oppdaterer trusselbildet løpende. T-banens risikovurderinger dokumenteres også i beredskapsplaner – det er et samspill mellom trusselnivå og tiltak. Oppsummert så bearbeider T-banen den informasjonen de mottar om sannsynlighet for terrorhandling, og de utarbeider analyser av egen sårbarhet.

I Kystdirektoratet er security-arbeidet fokusert på terror. Sikrer man seg mot terroranslag, får man også med gunstige bieffekter som nedgang i tyveri og øvrig kriminalitet. Det har man sett eksempel på etter innføring av ISPS-koden ved Oslo Havn. Oslo havn har gjennomført en ROS-analyse som omfatter både safety og security. Trusselbildet tar høyde for terror på en helt annen måte i dag. Før var planverket tilpasset kald krig, men nå er dette helt usannsynlig. Oslo Havn blir underrettet av PST hvis det oppstår noe av relevans. I tillegg er det nær kontakt med havnepolitiet som blir oppdatert av PST ukentlig. De har egne oppsynsbåter og har naturlig samarbeid mellom brannvesen, politi og Oslo kommune.

I Vegdirektoratet lages det som regel ROS-analyser for enkeltprosjekter. Det er i utgangspunktet mange typer ROS-analyser, for trafikksikkerhet, nyanlegg m.m. Vegdirektoratet har nylig presentert et forslag til en overordnet ROS for hele sektoren. Innholdet favner organisering, materiell, personell, infrastruktur etc. I alt 1000 ROS-analyser i hele sektoren er gjennomført som grunnlag, på region- og direktoratsnivå, og dekker hele spekteret fra hendelse i tunnel til ”sur eks-ansatt” som får sparken. Den største utfordringen har vært å ”lande” matrisene, de måtte inn i et felles system hvor sannsynlighet og konsekvens vurderes på en enhetlig måte. Hensikten med de overordnete ROS-analysene er å etablere en universell metodikk som kan brukes på alle fagområder slik at alt risikoarbeidet i Statens vegvesen lages etter samme mal. De som jobber med ROS-analyser ser ut til å ha problemer med å skape forståelse for dette i virksomheten og blir blant annet møtt av holdninger som ”security skaper bryderi”. Vegdirektoratet får trusselvurderinger fra PST og NSM og disse brukes i forebygging.

E18-Bjørvika-prosjektet har gjennomført en hendelses- og usikkerhetsanalyse hvor det ble lagt inn terrorscenarier. I tillegg har de en krisekommunikasjonsplan. De har et kostnadsestimat for prosjektet og skulle man hatt forebyggende terrortiltak ville det sterkt påvirket kostnadsestimatet. Terror ble derfor ikke lagt inn i dimensjoneringen av prosjektet.

Jernbaneverket har kategorisert sju mulige topphendelser som er aktuelle trusselscenarier og gjennomførte blant annet en øvelse i 2001 hvor de så på "Hva hvis vi var terrorister? – Hvordan ville vi gå fram for å skape noen av de sju hendelsene?" Det er mye man kan sikre seg mot, men noe som det er umulig å sikre seg mot. Det er derfor nødvendig å prioritere. Det foreligger en masse ROS-analyser i Jernbaneverket, både tradisjonelle safetyanalyser og strekningsanalyser. Det er avgjørende å se på hva som er mest kritisk akkurat nå og hvor vi er mest sårbare. For tiden er man veldig oppmerksom på eksempelvis klimaendringer; høyere temperaturer kan føre til flom eller større rasfare.

Trusseloppfatningene til NSB er knyttet til gjengproblematikk, tyveri, kjeltringstreker og terror. NSB er også utsatt for tagging, men ikke i den grad som Oslo Sporveier. Det finnes eksempler på dødsulykker i forbindelse med tagging. NSB har også opplevd trusler om bord i tog i form av at nattogene har vært utsatt for tyveri fra bander fra Øst-Europa. I følge NSB gjenspeiles samfunnets trusselbilde seg også i NSB. Det gjøres en del forebyggende tiltak, blant annet gjennom opplæring av personell. Terrortrusselen er med i ROS-arbeidet slik at ROS-analysen inneholder både safety og security. Beredskapsplanen skal oppdateres som en del av den omfattende oppdateringen av ROS-analysen, og denne skal nå utvides til security på mange områder. Det er ikke mer enn noen år siden NSB fikk security inn i arbeidet.

Luftfarten har som overordnet mål å øke flysikkerheten. Luftfartstilsynet har en egen forskrift i forhold til forebyggelse av terroranslag mot sivil luftfart og har dermed et klart uttrykt trusselbilde.[80] Security-avdelingen bygger sin aktivitet rundt dette reglementet. Tilsynet har som nevnt ikke gjennomført egen ROS-analyse, men samler inn kunnskaper for å ha grunnlag for risikobasert tilsyn.

Avslutningsvis kan det nevnes at Nasjonal sikkerhetsmyndighet (NSM) årlig produserer en gradert trusselvurdering som går til en engere krets. Det gis også ut en ugradert versjon. I følge NSM gir PST ut en trusselvurdering som har en kortere horisont. De ser på aktører, mens NSM ser på et overgripende bilde. Det er ingen innretting mot den enkelte sektor i dette dokumentet. Med hensyn til skjermingsverdige objekter sier NSM at det er objekteeiere som i utgangspunktet foreslår objekter. Eksempelvis kan togsentralen, styringsanlegg som gjør det lett å påvirke trafikken, knutepunkt etc. være et skjermingsverdig objekt. Det er altså objekteeierne som foreslår, men departementene har det siste ordet.

Objektsikkerhetsforskriftene tar nå i stor grad over nøkkelpunktdirektivet, som gir direktiv om å skaffe oversikt over objekter som skal beskyttes med militære styrker. Enkelte transportgrener er "mer hemmelige" enn andre. Spørsmålet er: Skal det være overlatt til den enkelte operatør å foreslå objekter, eller skal det være en minimumsstandard? Man trenger ikke legge lista helt der oppe.

[80] FOR 2004-04-30 nr.715: Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten (BSL A 2-1)

4.7 Behov for koordinering

De ulike transportgrenene er som nevnt tidligere ulike av natur. Security-tiltak i én sektor kan passe svært dårlig i en annen sektor. Enkelte sektorer, som luftfarten, har stort fokus på security og har mange tiltak og et strengt regelverk å følge, mens veisektoren er helt motsatt med et mye sterkere fokus på safety enn security. På grunn av de strukturelle forskjellene mellom transportgrenene og hvordan dette arter seg i form av ulik organisering og implementering av security-tiltak, stilte vi spørsmål om intervjuobjektene så behov for samlet koordinering av security-tiltakene på tvers av transportgrener. De fleste som svarte på spørsmålet mente det kunne være positivt med større grad av koordinering.

Virksomheten i Oslo havn har for eksempel i høyeste grad konsekvenser for lastebilnæring og omlastingsledd, og de har derfor et nært samarbeid med lastebil- og jernbanesektoren i forbindelse med omlossing. Oslo havn ser dermed behovet for koordinering med andre transportaktører.

Jernbaneverket mener at det opplagt er et behov for koordinering på tvers av grener. Det er viktig å vite hva som foregår i andre sektorer. Flåm stasjon ligger eksempelvis innenfor et havneområde.

NSB ser at transportsektorene kan ha flere fellesnevnere. Det er ikke noe forum for å utveksle erfaringer. Politiet er bindeleddet her og forteller NSB om andre bransjer. Det eksisterer en del uformelle møter, men NSB ville sett et forum som veldig positivt. Først må de imidlertid koordinere seg bedre innenfor jernbanebransjen.

Respondenten fra Luftfartstilsynet tror det er behov for koordinering av tiltak, og dette er noe de har tatt opp med EFTAs overvåkningsorgan (ESA). På havnesiden kan man for eksempel hente litt fra luftfartssektoren; det er ikke nødvendig å finne opp kruttet på nytt.

Vegdirektoratet ser det som en fordel med koordinering, men kan ikke se noe annet enn at det er slik at alle likevel opererer godt hver for seg. Det finnes dessuten allerede noe samarbeid, for eksempel beredskapsgruppen i Samferdselsdepartementet.

NSM mener at regelverket i transportsektoren er svært forskjellig. Hadde det vært en enhetlig tanke bak transportgrenene ville det vært likere regelverk i den grad terror retter seg mot der det er mye folk. Man kan stille seg spørsmålet om hvorfor regelverket er så forskjellig. Det bærer preg av å være hendelsesstyrt; innen flytrafikk har terroristene boltret seg i mange år. Det skal bare en hendelse til innen ferjetrafikk for eksempel. Det kan være bedre å ha et ytterst oppegående PST.

Aktørene føler ikke behov for et felles *regelverk* på security-feltet, til det er sektorene for grunnleggende forskjellige. De fleste aktørene ytrer derimot ønske om økt grad av samarbeid mellom transportgrenene, for slik å få innblikk i andre virksomheters tiltak og strategier og å kunne lære av hverandre, i forhold til ROS-analyser, tiltak, kriseplaner osv.

4.8 Framtidsutvikling – hvor er vi om 10 år?

I media har vi sett utsagn som at ”vi går mot flyplasslignende tilstander” i flere transportsektorer. Vi ønsket derfor å høre med intervjuobjektene hvordan de ser for seg utviklingen i sin sektor i et tiårs perspektiv. Fellesnevneren er at få av aktørene ser ut til å støtte påstanden om at ”flyplassliknende tilstander” vil utvikle seg på tvers av transportgrenene; til det er sektorene for ulike av natur. De fleste mener imidlertid at samfunnet utvilsomt vil bli preget av mer overvåkning i årene som kommer.

T-banen tror at framtiden vil innebære mye mer overvåkning, og slik sett vil personvernet kunne måtte vike for behov for trygghet. Publikum ønsker trygghet og er villig til å inngå kompromisser. Det er bra at det finnes et skikkelig regelverk og rutiner rundt praktiseringen av overvåkning. Uten et skikkelig regelverk og oppfølging av dette ville det vært svært mye ulovlig og ubegrunnet overvåkning i samfunnet.

Datatilsynet følger nøye med på utviklingen. I mange sektorer ser man en tendens til at det er ønske om å innføre nye teknologiske løsninger. Systemene hver for seg kan virke harmløse, men hvis man kobler flere sammen kan de få store konsekvenser. Dette er det viktig at Datatilsynet holder øye med.

Jernbaneverket ser ikke for seg en dramatisk endring, men forventer noe mer kontroll over kritisk infrastruktur og overvåkning.

For Luftfartstilsynet er fremtiden biometriske løsninger. Hvis de får lovhjemmel til å innføre biometri kan det bli en forbedring på noen områder innen security-arbeidet. I mai d.å. konkluderte Datatilsynet eksempelvis med at personopplysningsloven ikke er til hinder for at SASBraathens kan bruke fingeravtrykk i innsjekkingen av bagasje for å oppnå økt sikkerhet.

Oslo havn er en av de aktørene som har tro på en utvikling mot flyplasstilstander i årene som kommer. Spørsmålet er bare hvor lang tid det tar. Selv om arbeid med innføring av flere security-tiltak var i gang fra før, var det hendelsene i New York 11. september 2001 som satte fortgang i IMO. Deretter fikk vi terrorbombene i Madrid og London som også fikk betydning for regelverk og tiltak. Dersom det skjer en alvorlig hendelse i Skandinavia vil det trolig skape forandringer og security-tiltakene vil bli strengere.

5 Drøfting

5.1 Lite fokus på terror og personvern i norsk transport

Gjennomgangen av norske og europeiske security-tiltak har vist at norske tiltak for å sikre transportmidler og infrastruktur mot terrorhandlinger nesten utelukkende skjer som følge av internasjonale forpliktelser. Innsatsen for å sikre transportsektoren mot terrorangrep har økt de senere år, men først og fremst i form av ytterligere sikring i de sektorene som har tradisjoner for sikring; luft- og sjøfart. Både internasjonale organisasjoner som IMO, ICAO og nasjonale og internasjonale myndigheter (USA, EU) har satt i verk og intensivert en rekke tiltak knyttet til kontroll og overvåkning av passasjerer, frakt og infrastruktur. Norge er gjennom internasjonale avtaler forpliktet til å innføre lignende regimer.

Det er ikke så overraskende at det er få norske initiativ på dette området. Ingen personer har så langt mistet livet i terroraksjoner på norsk jord. Behovet for å sikre seg mot terror føles dermed heller ikke særlig påtrengende. De tiltakene som vurderes av norske transportvirksomheter og som har betydning for personvernet, er gjennomgående enten tradisjonelle safety-tiltak som for eksempel streknings-ATK, eller security-tiltak rettet mot hærverk, tagging og vold som kameraovervåkning på stasjonsområder og i transportmidlene.

Gjennomgangen av tiltak og lovverk i de foregående kapitlene har vist at det er enorme variasjoner mellom transportgrener når det gjelder omfanget av security-tiltak og dermed også når det gjelder personvernsimplikasjonene. I veisektoren oppleves terrortrusselen som bortimot totalt fraværende, og det er følgelig heller ingen diskusjon av personvern knyttet til security-tiltak. Det er riktignok stort fokus på personvernspørsmål hos veimyndighetene, men dette dreier seg om personvernimplikasjoner av trafikkstyringstiltak som AutoPASS og safety-tiltak som streknings-ATK.

Fokus på personvern i forhold til security henger nært sammen med hvor høyt på agendaen terrortrusselen oppleves. I luftfart har terror vært en aktuell trussel helt siden slutten av 1960-tallet da flykapringer begynte å gjøre seg gjeldende. Før den tid var det ingen security-tiltak i luftfarten. Parallelt med innføringen av security-tiltak i luftfarten har personvernspørsmål blitt stadig mer aktualisert, ikke minst fordi utviklingen av overvåkningsteknologi og elektronisk registrering har gitt stadig større muligheter for å samle og lagre personopplysninger. Forholdet mellom sikring og personvern har dermed vært en problemstilling som nesten kontinuerlig har vært under avveining i luftfarten; det er bare noen måneder siden Datatilsynet ga grønt lys for et system for å matche bagasje og passasjerer ved hjelp av fingeravtrykk.

Avinor, som eier og drifter norske flyplasser, har som nevnt ønsket å prøve ut nye former for sikkerhetskontroll av passasjerer ved hjelp av passasjerskanning, men tiltaket er foreløpig skrinlagt pga personvernimplikasjoner og motstand fra publikum (Aftenposten 2007b). Dette er symptomatisk for fokuset på sikring og

personvern i luftfart, og det står i markant kontrast til for eksempel jernbanen. Som nevnt i kapittel 4 opplever Jernbaneverket at det i rollen som infrastrukturforvalter i svært liten grad er involvert i spørsmål knyttet til security og personvern. Avinor må derimot forholde seg til dette daglig.

Det er mange mulige forklaringer på hvorfor det er slike enorme sprik i trusselbildet og i tiltakene som vurderes. Det er ikke mulig å komme med noen fullstendig analyse av dette her, men det er mulig å antyde noen mulige forklaringer som forhåpentligvis videre forskning kan undersøke nærmere.

5.2 To hovedstrategier for sikring

Sikring mot terrorangrep kan i prinsippet skje på to forskjellige måter. Man kan forsøke å sikre potensielle *objekter* mot angrep gjennom ulike fysiske barrierer (sikkerhetssjekk, inngjerding, identitetskontroll osv), eller man kan forsøke å sikre seg mot terrorangrep gjennom å *forebygge* terrorhandlinger ved å overvåke og eventuelt pågripe potensielle terrorister før de får gjennomført terrorhandlinger.

Prinsipielt sett vil den ene strategien kunne gjøre den andre overflødig: Dersom alle potensielle terrormål er tilstrekkelig fysisk sikret, er det ikke nødvendig å vite hvem som er potensielle terrorister. Og dersom man overvåker alle potensielle terrorister, og kan slå til og pågripe dem før noe angrep blir iverksatt, er det unødvendig å sikre objektene. Selv om det prinsipielt sett er slik, er det i praksis ikke slik at den ene strategien utelukker den andre. Myndighetene benytter da også begge strategier for å sikre samfunnet mot terrorangrep.

Dette gjenspeiler seg blant annet når det gjelder security i transport. Her er det et vesentlig skille mellom transportgrenene knyttet til i hvilken grad fysisk sikring er mulig. I luftfarten er objektsikring av fly og lufthavner som kjent gjennomført i stor utstrekning gjennom sikkerhetssjekk av passasjerer, bagasje osv. Så lenge alle personer, all bagasje samt alt annet utstyr som bringes inn på flysiden på lufthavner kontrolleres, antar man at sikkerheten er ivaretatt. Som nevnt spiller det i prinsippet ingen rolle hvem personene er så lenge man er sikret at de ikke bringer om bord våpen eller gjenstander som kan benyttes til terrorhandlinger. Behovet for personopplysninger er dermed også svært begrenset. Et system med objektsikring truer derfor i liten grad person*opplysnings*vernet, men sikkerhetssjekken kan oppleves som et inngrep i person*integritets*vernet.

Motsatt vil behovet for personopplysninger være desto større når man ikke har muligheter for fysisk objektsikring. Som nevnt er det nærmest utenkelig å sikre T-bane, trikk og buss, samt en rekke andre potensielle terrorobjekter i sentrale byområder ved hjelp av fysiske virkemidler. Sikring må her baseres på registrering og overvåkning av personer. Fordi potensielle terrorister er ukjente, og fordi truende planer/intensjoner kan gi seg så mange utslag, blir behovet for tilgang til personopplysninger vidt og ubestemt. Det innebærer at det er vanskelig på forhånd å ta stilling til hvilke opplysninger og hvilke personer som vil kunne være interessante. Selv om bare et meget lite utvalg av innsamlet personinformasjon faktisk vil komme til nytte, er det problematisk dersom en på forhånd må binde seg til å bruke visse opplysningstyper på bestemte måter. Informasjonsbehovet kan derfor grunnleggende sett sies å være åpent og dermed uavgrenset.

For å ivareta personvernet kan et system med fysisk sikring og sikkerhetssjekk av personer framstå som prinsipielt sett mindre truende enn et omfattende system for registrering av personopplysninger, ikke minst fordi personregistre lett kan koples og fordi slike opplysninger lagres. For den enkelte borger kan det imidlertid framstå som mindre truende med slike personregistre enn det er å gå gjennom nitide personsjekker jf. diskusjonen om innføringen av kroppskanner på norske flyplasser (Aftenposten 2007b). I Teknologirådets spørreundersøkelse fra 2007 var det for eksempel et klart flertall som ønsket et sentralt register over biometriske data (DNA eller fingeravtrykk).

5.2.1 Kostnader

I tillegg til de prinsipielle forskjellene mellom de to sikringsstrategiene og forskjeller i strukturelle betingelser for å implementere en objektsikringsstrategi, er det viktige økonomiske aspekter ved valget av sikringsstrategi. Det er åpenbart at for den enkelte transportvirksomhet vil en strategi basert på fysisk sikring innebære store utgifter og utgifter som den enkelte transportvirksomhet må bære selv. Forebygging av terrorangrep gjennom å styrke politi og sikkerhetstjenestene er derimot en kostnad som bæres av hele samfunnet.

Et interessant aspekt ved de store forskjellene mellom transportgrenene når det gjelder å implementere nye tiltak for økt security er nettopp de økonomiske mulighetene de har for å iverksette tiltak. I den grad transportgrenene er underlagt internasjonale avtaler og reguleringer, er man forpliktet til å følge opp eventuelle nye tiltak som besluttes sentralt. Dette har vært tilfellet for både luftfart og sjøfart (særlig havnevesenet), og kostnadene til nye sikringstiltak har ikke vært noe tema. Det er åpenbart store kostnader involvert, men om tiltakene kan forsvares rent kostnadsmessig har i liten grad vært tema i debatten om tiltakene.

I 2006 uttalte Avinors direktør Sverre Quale at kostnadene til securityformål var ti ganger høyere enn før 11. september 2001. Mye av inndekningen av disse kostnadene har skjedd gjennom utvidet salg på flyplassene. Kostnadsøkningen for flyselskapene har vært i form av økt passasjeravgift, men flyselskapene har ikke hatt tilsvarende inntjeningsmuligheter som eierne av lufthavnene. Samtidig har konkurransen presset prisene dramatisk. Dette må bety at mange flyselskaper har hatt et økonomisk innsparingspotensial som man ikke finner i andre transportgrener. T-banen i Oslo har for eksempel i mange år hatt etterslep når det gjelder vedlikehold.

Det kan derfor synes som om luftfarten både har opplevd behovet for økt sikring langt mer påtrengende enn andre transportgrener samtidig som de økonomiske mulighetene for å investere i security har vært bedre. Som nevnt ville det bare ut fra kostnader alene være umulig å tenke seg ”flyplasslignende tilstander” på T-banen.

Mange av security-tiltakene som er blitt iverksatt i luftfarten har blitt innført som en direkte respons på en ny terrortrussel – som f. eks. væskeforbudet fra høsten 2006 – uten grundige konsekvensutredninger i forkant. Det betyr at tiltakene ikke har vært gjenstand for vanlige nytte-kostnadsvurderinger (Akthar 2004). Dette reiser en rekke interessante spørsmål, som for eksempel hva slags kostnader som eventuelt burde inngå i beregningene (tidskostnader ved security-køen osv.?),

hvordan estimere nytten av tiltakene, og hvordan estimere risiko for angrep, konsekvenser ved eventuelle angrep osv.

I følge Mueller (2006) står ikke ressursene som benyttes på security i luftfart i forhold til risikoen; det er for eksempel ingen som har omkommet i terroraksjoner på amerikansk jord etter 9/11; risikoen for å bli drept av lynnedslag er større enn risikoen for å bli drept i en terroraksjon osv.

5.2.2 Kombinerte systemer

En absurd side ved sikkerhetskontrollene slik de praktiseres på norske flyplasser i dag er at pilotene sjekkes på samme måter som vanlige passasjerer. Pilotene oppfatter naturlig nok seg selv som en viktig ivaretaker av flysikkerheten, og en pilot kan naturligvis selv styrte et fly om han/hun skulle ønske det. Tollpersonell og politi er til sammenligning ikke gjenstand for tilsvarende sikkerhetssjekk. Grunnen er at de har avgitt personopplysninger som sikrer at de ”er til å stole på” gjennom vandelsattester, sikkerhetsklareringer osv. Pilotene ønsker det samme (Dieset 2007).

For mange grupper kan personopplysningsvernet framstå som mindre viktig enn personintegritetsvernet; VIP-sjekk på enkelte flyplasser der man får forenklet sikkerhetssjekk gjennom å registrere bestemte opplysninger på forhånd, er et eksempel på en slik ”trade-off”. Svært mange er villige til å la myndigheter og andre sitte på opplysninger om dem selv dersom de oppnår enklere tilgang til sikkerhetskontrollerte områder eller andre fordeler. Som nevnt har man i Storbritannia innført muligheter for rimeligere bilforsikring om man aksepterer å installere en atferdsregistrator i bilen.

Faktisk kan man tenke seg å gjøre sikkerhetssjekken så omfattende og brysom at mange vil være villige til å gi fra seg omfattende opplysninger om egen person. Denne avveiningen er interessant, og foreløpig i liten grad vært gjenstand for mye diskusjon. At folk frivillig aksepterer overvåkning og registrering som i mange tilfeller går langt utover hva som tillates etter loven, oppleves trolig som et problem for personvernmyndighetene. Og det reiser et viktig spørsmål om den enkelte er tilstrekkelig i stand til fullt ut å ivareta sine egne interesser når det gjelder personvern.

En mulig strategi for å redusere kostnadene ved omfattende security-kontroll er å innføre differensierte systemer. Et system der alle er gjenstand for nitid sjekk er meget kostbart og kan på mange måter framstå som lite rasjonelt. Dersom man ved hjelp av registre og overvåkningssystemer kunne etablere valide registre over potensielt truende personer og velge ut disse for sjekk, ville man sluppet å sjekke en rekke personer som ikke utgjør noen sikkerhetsrisiko. Slike systemer er utviklet, som f. eks. CAPPS i USA, og digitalisert signatur i Israel (Aftenposten 2007c). Norske luftfartsmyndigheter ser for seg økt bruk av biometriske identifikasjonssystemer for å forenkle sikkerhetssjekken på flyplassene (Quale 2007).

Slike kombinerte systemer der man differensierer sikkerhetssjekken basert på personopplysninger, kan forenkle og rasjonalisere kontrollen på flyplasser og lignende. Systemer som baserer seg på ulike registre for personopplysninger har imidlertid også de samme implikasjonene for personopplysningsvernet som andre

personregistre; risikoen for ulovlig lagring og spredning av opplysninger, risiko for feilregistreringer osv. Personer som ved en feil blir innlemmet i slike registre vil sannsynligvis møte en vanskelig og tidkrevende prosess for å rette feilen.[81]

5.3 Safety og security må vurderes forskjellig

Intervjuene som er gjengitt i kapittel 4 viste at implementeringen av security-tiltak varierer enormt mellom transportgrenene, og representanten fra NSM var inne på at det trolig ikke var samfunnsmessig rasjonelt med så store forskjeller i security-tiltak mellom transportgrener.

Det framstår på mange måter som et paradoks at stadig større ressurser går med til sikringstiltak i luftfart og til dels sjøfart, mens det omtrent ikke finnes slike tiltak på bane og på vei. En viktig grunn til at det er slik, er at sikring og sikkerhet tradisjonelt har vært fokusert innenfor hver enkelt transportgren. Når det gjelder tradisjonell sikkerhet (safety) er det som regel ikke noen spesiell grunn til å samordne tiltak på tvers av transportgrener fordi sikkerheten i luftfart ikke påvirker for eksempel sikkerheten i veisystemet og omvendt.[82]

Når det gjelder security er det derimot absolutt gode grunner til å samordne innsatsen. Jo bedre luftfarten er sikret, desto større er sannsynligheten for at neste angrep kommer mot andre deler av transportsystemet (Bier 2007). En viktig grunn til at T-bane og jernbane ble angrepet i London og Madrid var trolig at sikring av luftfart var blitt betydelig skjerpet etter 11. september 2001.

Et utbredt holdning blant representantene fra jernbane og T-bane var som nevnt at det ikke er praktisk mulig å sikre de fleste kollektive transporter mot terror slik man gjør i luftfart, og dermed at tiltak mot terror må skje gjennom etterretning og politimetoder. En slik holdning er ikke bare noe transportørene mener ut fra ”bekvemmelighetshensyn”; det er et synspunkt som også er fremmet av flere eksperter jf. Trajtenberg (2006).

Fra et samfunnsmessig synspunkt virker det likevel nokså åpenbart at det ikke er en rasjonell balanse mellom tiltakene som settes i verk i luftfarten og mangelen på tiltak i andre transportgrener. Det fremstår i dag som litt av et tankekors at man ikke kan ta med seg en vannflaske om bord i fly, mens det ikke foregår noen som helst kontroll av passasjerer eller bagasje på tog og T-bane (Bjørnskau 2007).

---

[81] I Daily Mail 20.8.2007 kunne man for eksempel lese om en 7 år gammel muslimsk gutt som ble stoppet gjentatte ganger på flyplasser i USA fordi han hadde samme navn som en person man mistenkte for å ha tilknytning til terroristorganisasjoner. http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=476369&in_page_id=1770

[82] Dette er riktignok en sannhet med modifikasjoner. I følge Anders Hovdum i Samferdselsdepartementet er det for eksempel et problem at merking og sikring av farlig gods på ferjer er så ressurskrevende at mange transportører velger å frakte dette lange omveier med godsbiler i stedet, med høyre risiko for trafikkuhell som konsekvens (Hovdum 2007).

5.3.1 Tradisjon for lokalt ansvar for sikkerhet

Det er trolig flere grunner til dette misforholdet. En viktig grunn er at ansvaret for sikkerhet tradisjonelt har vært plassert hos de enkelte virksomhetene og at sikring mot terror har fulgt denne tradisjonen. Det er for eksempel samme avdelinger og personer som har ansvar for trafikksikkerhet og for terrorsikring i NSB og i T-banen. Det har følgelig ikke vært noen tradisjon for å se sikkerhetstrusler i ulike transportgrener i sammenheng.

En annen grunn, som er beslektet, er at man ikke har sett på terrorsikring som noe prinsipielt annerledes enn ordinær sikkerhet, og følgelig har man heller ikke sett behovet for helhetlig samordning og for å forutse trusler. Sikring mot terror skiller seg helt avgjørende fra ordinær trafikksikkerhet; det vil til enhver tid være de objektene som er dårligst sikret som er mest utsatte for angrep, og man kan i svært begrenset grad lære av tidligere hendelser for å forebygge nye. Det ligger i sakens natur at terrorister vil forsøke å ramme på tider og steder der man ikke venter det.

Vanetenkningen gir seg også utslag i at folk aksepterer lettere kontrolltiltak på flyplasser enn for eksempel på jernbanestasjoner. Teknologirådets undersøkelse av folks aksept for overvåkning og registrering viste at 82 % aksepterte bruk av fingeravtrykk på flyplasser, mot bare 35 % på hovedbanestasjonen (Teknologirådet 2007b).

5.3.2 Hendelsesbaserte tiltak

I tradisjonelt sikkerhetsarbeid tar man ofte utgangspunkt i og lærer av tidligere hendelser. Man kartlegger hva som ikke fungerte forrige gang – da uhellet eller hendelsen skjedde – og utbedrer de antatte feilene, enten det var prosedyrefeil, komponentfeil eller organisasjonsfeil. Det betyr imidlertid samtidig at tiltakene man iverksetter er mot "gårsdagens" trussel. Når omgivelsene endres fort, vil tiltak mot gårsdagens trussel lett bomme. Innenfor sikkerhetsforskningen diskuterer man derfor i økende grad betydningen av "resilience" (robusthet) i betydningen å forutse og iverksette tiltak ut fra vurderinger av mulige framtidige trusler snarere enn ut fra tidligere hendelser (Hollnagel m.fl. 2006).

Står man overfor en intelligent motpart (terrorist) som ønsker å ramme et objekt, er man i en ekstrem situasjon av usikre omgivelser. Terrorangrep er nærmest per definisjon overraskende, og suksess avhenger av at angrep er utforutsigbart. Bortimot det eneste man kan være sikker på er at samme aksjon ikke vil gjentas. Det betyr også at tradisjonell sikkerhetstenkning basert på læring av hendelser og feil er særlig dårlig egnet til å møte truslene fra mulige terrorangrep.

Et ytterligere problem her er at dersom systemene man skal sikre er kompliserte med tette koplinger og avhengigheter, vil det alltid være en viss risiko for hendelser og ulykker (Perrow 1999). Slike hendelser og uhell vil opptre fordi komponenter (eller mennesker) som interagerer av og til vil oppføre seg i ytterkanten av hva som er normalt. Dersom dette skjer samtidig med flere komponenter/operatører, kan det oppstå brister i systemet (Hollnagel m.fl. 2006). Man kan for eksempel lett forestille seg at all aktiviteten som skal samordnes på

store internasjonale flyplasser innebærer at dette blir komplekse systemer med risiko for hendelser og uhell.[83]

At slike kompliserte systemer kan være særlig sårbare overfor hendelser og uhell er velkjent. En annen og mindre påaktet side ved det dette er at de nettopp av den grunn også vil kunne være sårbare for angrep. Det er ikke vanskelig å forestille seg at utenforstående kan manipulere med enkeltelementer og framprovosere "kollisjoner" eller unormale tilstander som får systemet til å bryte sammen. M.a.o. dersom slike kompliserte systemer er sårbare for utilsiktede hendelser, vil de også være det for tilsiktede hendelser.

5.3.3 Væskeforbudet – et eksempel

Det mest dramatiske antiterrortiltaket som er gjennomført den senere tid er forbudet om å bringe om bord i fly flasker med mer enn 1 dl væske som ble innført i internasjonal luftfart høsten 2006. Bakgrunnen var at man gjennom spaning mot en terrorcelle i London avdekket planer om å innføre eksplosive væsker om bord i fly kamuflert i drikkeflasker. Dette førte til umiddelbare tiltak og kort tid etter ble det væskeforbudet innført. Det er naturlig at man reagerer med å forby væskebeholdere etter dette, men det illustrerer samtidig meget klart hvordan slike tiltak er tilbakeskuende; dette er tiltak for å møte gårsdagens trusler. Mange har reist tvil om de terrormistenkte faktisk var i stand til å gjennomføre en terroraksjon ved hjelp av å blande eksplosive væsker om bord på fly. [84]

Det er også blitt hevdet at tiltaket uansett ikke er effektivt. Det er for eksempel blitt påstått at det fint er mulig å lage sprengstoff av mindre væskekonsentrasjoner enn 1 dl, og det vil jo ikke være noe problem å alliere seg med flere som alle har med små væskekonsentrasjoner om bord. Det er jo også et tankekors at alle slike potensielt farlige flasker blir kastet i store søppelsekker ved securitysjekken der tusenvis av mennesker passerer daglig.

Høsten 2007 gikk Samferdselsminister Navarsete sammen med flere samferdselsministre i EU inn for å avvikle forbudet mot å ha med vannflasker og lignende om bord i fly med den begrunnelse at dette inngrepet i folks integritet ikke står i forhold til den risikoen som væskebeholdere representerer:

"Jeg styrer en sektor hvor flere hundre liv går tapt på veiene hvert år, og mens vi mangler penger å sette inn, bruker vi masse ressurser på kontroll av ærlige og skikkelige folk", sier Navarsete, som synes forbudet mot å ha med væske gjennom sikkerhetskontrollen bare er tull.

Aftenposten (2007d)

---

[83] I følge Hudson (2007) skjer det mange kollisjoner på flyplasser og mange uhell ved bagasjehåndtering.

[84] Tidligere sjef for terrorbekjempelse i New York-politiet, Michael Sheehan uttalte for eksempel følgende om arrestasjonene i Storbritannia og det påfølgende væskeforbudet: "In retrospect, there may have been too much hyperventilating going on". (New York Times, 28. august 2006)

5.4 Policyimplikasjoner

Som nevnt ser det ut til at de ulike transportgrenene (bortsett fra vei) i utstrakt grad har innført og ønsker å innføre security-tiltak som har implikasjoner for personvern, men at de i begrenset grad selv vurderer om hensynet til personvernet er ivaretatt. Hensynet til personvern kan på mange måter sammenlignes med hvordan hensynet til HMS ble ivaretatt på 1970-tallet; offentlige myndigheter (Arbeidstilsynet) måtte sørge for tilsyn for å sikre at HMS-hensyn ble ivaretatt. Dette endret seg som kjent radikalt med prinsippet om internkontroll, som først ble innført på sokkelen, men som senere er blitt hovedprinsippet i arbeidslivet. En lignende modell kan tenkes også når det gjelder personvern. I stedet for at Datatilsynet mer eller mindre alene må sørge for at personverninteressene er tilstrekkelig ivaretatt kunne ansvaret for dette også i større grad bli overført til den enkelte virksomhet.

Som nevnt innføres security-tiltakene i transport i stor utstrekning innenfor samme tradisjon som ordinære sikkerhetstiltak (safety-tiltak). Mulighetene for å heve blikket og se flere transportgrener (og andre objekter) i sammenheng er dermed også begrenset fra den enkelte virksomhets ståsted. Trolig kan derfor en samordnet sikringsstrategi av objekter bare utvikles gjennom internasjonalt forpliktende samordning mellom stater, slik som gjennom EU, NATO og lignende. Det vil bare være gjennom slike institusjoner at det vil være mulig å utvikle en balansert sikringsstrategi som tar hensyn til hele spekteret av sårbare objekter.

Et neste spørsmål er om dette overhodet er en farbar vei, selv om det i teorien er mulig å tenke seg en balansert strategi. Enkelte transportgrener og objekter vil være bortimot umulig å sikre. En tankbil som kapres og som kjøres ut på et jernbanespor rett foran et passasjertog ville være en katastrofe, og det er vanskelig å tenke seg muligheten for å sikre seg fullt ut mot slike trusler. Det finnes også en rekke andre eksempler. Det er omtrent bare fantasien som setter grenser, og fantasien er trolig minst like godt utviklet hos potensielle terrorister som hos sikringsmyndighetene.

Det betyr imidlertid at det sannsynligvis er langt mer rasjonelt og langt mer kostnadseffektivt å forsøke å forebygge terrorangrep gjennom preventiv politietterforskning. Det finnes få om noen eksempler på at sikkerhetssjekk på flyplasser har stanset potensielle terrorister (det finnes derimot eksempler på at terrorister har bestukket security-personell), men det er etter hvert mange eksempler på terrorceller som er oppdaget og angrep som er forhindret ved hjelp av tips, spaning, avlytting av spesielle grupper som kan mistenkes for å være en sikkerhetstrussel. Nylig informerte PST-sjef Jørn Holme om at Politiets sikkerhetstjeneste har mellom 200 og 300 personer under oppsikt fordi de anses som potensielle sikkerhetstrusler.

Det innebærer også at den eneste effektive strategien mot terrorangrep også er den som kanskje i størst grad utfordrer personvernet; overvåkning av personer i form av avlytting, kameraovervåkning, spaning, registrering av e-post og internettilknytning osv. Security-sjekken på flyplasser er generell, alle sjekkes, også pilotene og inngrepet i personvernet er forholdsvis lite. Overvåkning av potensielle terrorister er derimot selektiv og med store inngrep i personvern. Det betyr at den virkelig store diskusjonen knyttet til personvern er den vanskelige

diskusjonen knyttet til selektiv overvåkning av enkeltpersoner. Hvem bestemmer hvem som er mistenkelige? Hvem får informasjon?

5.5 Terrorsikring og rettsstatshensyn

Det følger logisk av diskusjonen foran at effektiv terrorsikring ikke kan baseres på å sikre utsatte objekter. Det er gjennom overvåkning og registrering av potensielle terrorister man har lyktes i antiterrorarbeidet. Effektig terrorsikring innbærer dermed at politi og etterretning må få store ressurser og vide fullmakter for å ivareta oppgavene knyttet til å forebygge terrorhandlinger.

Dette reiser imidlertid en rekke vanskelige spørsmål. Mueller (2006) hevder at den voldsomme satsingen på security-tiltak i luftfarten er uttrykk for bestemte interesser og der en rekke forskjellige interesser; man har en egeninteresse i å opprettholde en følelse av fare og utrygghet. Mueller (2006) hevder også at det lett vil utvikle seg egeninteresser knyttet til trusselnivået som vil være spesielt problematiske fordi det i stor grad er de samme enhetene som til enhver tid bestemmer trusselnivået, som også får tilført ekstra ressurser når trusselnivået øker. Det er godt mulig at dette til nå ikke har vært noe problem, men uansett er konstellasjonen uheldig; det er lett å mistenke at f.eks. sikkerhetstjenesten kan se seg tjent med å gi uttrykk for at terrortrusselen er høyere enn den faktisk er.[85]

5.5.1 Kontroll med kontrollørene

Hvordan man skal kontrollere kontrollørene er en aktuell problemstilling uansett hvilken strategi for sikring man benytter; objektsikring gjennom fysisk sikkerhetskontroll eller samfunnssikring gjennom overvåning og registrering. Selv om det kan være et demokratisk og rettstatlig problem knyttet til kontrollen av de som kontrollerer oss på flyplassen, er det likevel småtterier i forhold til det potensielle demokratiske og rettstatlige problemet knyttet til hvem som skal avgjøre om noen skal overvåkes, hvilken informasjon som skal være offentlig tilgjengelig osv. Dette er ikke bare utfordringer for personvernet, dette er store utfordringer for hele vår demokratiske rettstradisjon. Hemmelig politi med utvidete fullmakter og monopol på informasjon om trusler er noe vi ikke assosierer med rettsstaten. Spørsmålet som må stilles er om truslene vi står overfor kan forsvare slike brudd på demokratiske rettsstatsprinsipper. Det er klart at slike tiltak kan ses som helt grunnleggende vern av samfunnets borgere, og slik sett som det ultimate personvern. Samtidig er det klart at slike tiltak bare kan aksepteres om trusselen er stor. Det er viktig å huske at ingen i Norge har noen gang blitt drept i terroraksjoner, og ingen i hele Europa ble drept i slike aksjoner i 2006.

---

[85] Det er mange andre interesser også. Flyselskapene og luftfartsindustrien må, for i det hele tatt få og bevare passasjerer, vise at sikkerhet – både safety og security – verdsettes og prioriteres meget høyt. Etter 11. september 2001 mistet amerikanske flyselskaper en mengde passasjerer – noe som førte til en voldsom trafikkøkning og dermed også ulykkesøkning på amerikanske veier. Det er anslått at over 2000 personer mistet livet i trafikkulykker som følge av økt biltrafikk etter 9/11 (Blalock, Kadiyali & Simon 2007).

Det er de samme hemmelige tjenester som informerer om trusselnivået. Når grunnlaget for trusselvurderingene er hemmelig, samtidig som trusselnivået i seg selv både påvirker hvilke ressurser som skal tilflyte de hemmelige tjenester og hvilke metoder som skal tillates, er det åpenbart at vi står oppe i et betydelig habilitetsproblem. Det er imidlertid ikke lett å angi noen gode løsninger på dette problemet. Kanskje er det slik at demokratiet og rettsstaten bare kan fungere godt om ingen fiende anvender ikke-demokratiske midler. Når terror anvendes, må også rettsstaten la en del demokratiske hensyn vike for å møte truslene. Men dermed er vi også i ferd med å fjerne oss fra demokratiet og rettsstaten.

Det fremstår som et tankekors at behovet for å verne om etablerte demokratiske samfunn mot terrortrusselen fører til at en rekke beskyttelsestiltak iverksettes uten at disse tiltakene er gjenstand for demokratisk kontroll. Og ikke bare er mange av tiltakene og trusselvurderingene som ligger til grunn unndratt vanlig demokratisk innsyn; det har også vært hevdet at tiltakene i seg er grobunn for nye terrorhandlinger.

Den tidligere leder for politiets etterretningstjeneste i Danmark, Hans Jørgen Bonnichsen har sterkt advart mot denne utviklingen:

"Vi risikerer at bringe retsstaten i fare og opgive de vestlige frihedsrettigheder, som vi har kæmpet for i 200 år. Dermed vinder terroristerne i sidste ende, påpeger han. I kampen mod terror skal Danmark passe på ikke at skrue så højt op for overvågningen og beføjelserne til efterretningstjenesten, at det blot gøder jorden for flere terrorister og koster de danske frihedsrettigheder."

Jyllandsposten 5.9.07

6 Referanser

Abeyratne, R. I. R. (2004): *Aviation in crisis.* Aldershot: Ashgate.

Adey, P. (2004): Secured and Sorted Mobilities: Examples from the Airport. *Surveillance & Society* 1(4): 500-519. www.surveillance-and-society.org

Aftenposten (2007a): ”Når frykten vinner”. Kommentar av Morten Fyhn, 9. august 2007.

Aftenposten (2007b): ”Vil ikke kles av på flyplassen” 11. november 2007.

Aftenposten (2007c): ”Bekjemper terror med teknologi”. 10. november 2007.

Aftenposten (2007d): ”Mener det er greit med vannflasker”. 14. september 2007.

Akhtar, J. (2004): *A risk analysis and assessment of the ISPS code in cruise shipping*. Trondheim; Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management: Master Thesis.

American Civil Liberties Union (2002): Airport Security: Increased Safety Need Not Come at the Expense of Civil Liberties. *Facts On Airport Security* (6/12/2002), http://www.aclu.org/safefree/resources/16748res20020612.html

Aven, T. (2003): *Foundations of Risk Analysis*. John Wiley & Sons.

Avinor (2005): *Årsrapport 2004.* Avinor

Bergens Tidende (2005): ”De fleste sier ja til overvåkning”, 18. januar 2005 http://www.bt.no/lokalt/bergen/article7128.ece

Bier, V. M. (2007): Choosing What to Protect. *Risk Analysis* vol. 27: 607-620.

Bing, J. (1982): *Rettslige kommunikasjonsprosesser*. Oslo, Universitetsforlaget.

Bjørnskau, T. (2007): Security checks – et nødvendig onde for økt sikkerhet? Foredrag, Sola-konferansen, Sola 19. september 2007.

Blalock G., Kadiyali V. & Simon D.H. (2007): The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel. *Journal of Law and Economics*, Forthcoming.

Bygrave L.A. (1996): *Ensuring Right Information on the Right Person(s): Legal Controls of the Quality of Personal Information.* Universitetet i Oslo, Forvaltningsinformatisk notatserie, nr.4, 1996.

Dagbladet (2005): ”Terrormål i Norge”, 15. januar 2005 http://www.dagbladet.no/magasinet/2005/01/15/420278.html

Dagbladet (2007): 25.7.2007

Datatilsynet (2004a): *Spor i samferdselssektoren. Rett til anonym ferdsel*. Oslo, Datatilsynet, prosjektrapport.

Datatilsynet (2007): Alle blir fotografert i bomstasjonene. http://www.datatilsynet.no/templates/Page____1914.aspx

derStandard.at: "London will bei der Bahn Kontrollen wie am Flughafen", derStandard.at

Dieset J. (2007): "Security Checks fra en daglig brukers synspunkt". Foredrag, Solakonferansen, 19. september 2007.

DSB (2004): *Erfaringer etter terrorangrepet i Madrid. Krisehåndtering og ressurstilgjengelighet i forbindelse med en tenkt tilsvarende hendelse i Oslo*, Rapport fra Direktoratet for samfunnssikkerhet og beredskap, Tønsberg.

Dwyer, A. (2003): "'Prudent pessimism'. The management of Terrorist Threats against the Railways in England, Scotland and Wales", in: ECMT: *Vandalism, Terrorism and Security in Urban Public Passenger Transport. Round Table 123*, ECMT/OECD: Economic Research Centre

ECAC (2006) Policy Statement in the Field of Civil Aviation 10th Edition/December 2006. ECAC-CEAC Doc No. 30, Part I. http://www.ecac-ceac.org/index.php?content=docstype&idtype=38

ECMT (2005): *Container Transport security across modes*, OECD/ECMT

Elliot, P. (1990): *Through transport security a practical guide*, London: Witherbys.

EUPolitix (2004): *Special Report: Combating terror in the EU.* http://www.theparliament.com/EN/News/200403/a746daaf-9ddd-4948-b542-4a2630ad0f6b.htm

EurActiv (2005): "New anti-terror technology to be trialled in London", euractiv.com (EU News, Policy Position & EU Actors online)

Europäische Kommission (2001): *Weissbuch. Die Europäische Verkehrspolitik bis 2010. Weichenstellung für die Zukunft*, Brussel: Amt für amliche Veröffentlichungen der Europäischen Gemeinschaft

European Council (2004): *Declaration on combating Terrorism*, Brussel 25th March 2004.

European Commission (2003): *Consultation Paper. Freight Transport Security.* Brussels, 23rd December 2003, DG TREN, Directorate G – Maritime Transport and Intermodality.

European Commission (2005): Framework Decision on data protection in police and judicial cooperation: COM (2005) 475 final, 4th October 2005.

European Parliament (2005): *Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored (…),* Committee on Civil Liberties, Justice and Home Affairs (A6-0174/2005 Final), Brussel

Forsvarsdepartementet (2002): *Forebyggende sikring av objekter mot terror- og sabotasjehandlinger. Rapport fra arbeidsgruppe om objektsikkerhet avgitt til forsvarsdepartmentet*, Forsvarsdepartemenet, FO/S

Graven, A.S. (2005) "Ser overvåkerne fra innsiden" i: www.forskning.no 19. desember 2005

Gripsrud M. og Grunnan T. (2007) *Avveining mellom security i transport og personvernsinteresser*. Oslo, Transportøkonomisk institutt, Arbeidsdokument SM/1917/2007.

Hagen, J.M., Rodal, G.H., Hoff, E., Lia, B., Torp, J.E. og Gullichsen, S. (2003): *Beskyttelse av samfunnet med fokus på transportsektoren*. Kjeller: Forsvarets forskningsinstitutt, FFI/Rapport-2003/00929

Hempel, L. & Töpfer E. (2002): *Inception Report*. Working Paper no. 1. UrbanEye, Berlin: Technical University Berlin

Hollnagel E., Woods D. D. & Leveson N. (eds.) (2006): *Resilience Engineering – concepts and precepts*. Aldershot: Ashgate.

Hudson P. (2007): Achieving a Safety Culture in Aviation. Fordrag, Solakonferansen, 18. September 2007.

Hovdum A. (2007): Om risiko for terrorhandlinger i transportsektoren. Foredrag AFIN-seminaret: Terrobekjempelse og personvern i transportsektoren – hva bør vi tåle? Oslo, 10. oktober 2007.

ICAO (2000): *Convention on International Civil Aviation*, 8th Edition (7300/8), ICAO

Jernbaneverket (2005): Handlingsprogram for Jernbaneverket – oppfølging av St.meld. nr. 24 (2003-2004) Nasjonal transportplan 2006 – 2015 (Jernbaneverkets høringsutkast februar 2005), Jernbaneverket

Justis- og politidepartementet (2000): Lovteknikk og lovforberedelse. Veiledning om lov- og forskriftsarbeid, Justisdepartementets lovavdeling 2000.

Jyllandsposten (2007): Tidl. PET-chef: Pas på retsstaten. 5. september 2006.

Karanja, S.K. (2006): *Schengen Information and Border Control Co-operation: A Transparancy and Proportionality Evaluation*, Doctoral Thesis, Faculty of Law, University of Oslo, January 2006.

Leite T. 2006: *Sikring mot ulovlige handlinger i transportsektoren, Deloppgave 1 av RISIT-prosjekt "Security i transport. Personvernets grenser"*. Oslo, Transportøkonomisk institutt, Arbeidsdokument TR/1340/2006.

Lia, B. (2003): *Terror mot transport: En revurdering av terrortrusselen mot transportrelaterte mål i lys av 11. september*. Kjeller, Forsvarets forskningsinstitutt FFI/rapport-2003/00731.

Lindkvist, A., Kronborg P., Forward S. & Obrenovic S. (2002): *Vem vet var Du är och vad Du gör? Transportinformatik och personlig integritet*, TFK-rapport 2002: 5, TFK- institutet för transportforskning, Stockholm

Mueller J. (2006): *Overblown. How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. New York, London, Toronto, Sydney: Free Press.

Nettavisen (2007): ”Ungdommer overvåkes i bilen”. 18. september 2007.

NOU 2000: 24: *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Justis- og politidepartementet.

NOU 2004: 6: *Mellom effektivitet og personvern. Politimetoder i forebyggende øyemed*. Justis- og politidepartementet.

NOU 2006: 6: *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Justis- og politidepartementet.

NSM (2005a): *NSMs risikovurdering 2005*. Ugradert versjon. Oslo, Nasjonal sikkerhetsmyndighet.

NSM (2005b): Ugradert sikkerhetsvurdering. Sikkerhetsvurdering gis ut grunnet en koordinert terroraksjon mot buss- og undergrunnsnettverket i London 7.7.05. Oslo, Nasjonal sikkerhetsmyndighet.

NSM (2006): *NSMs Risikovurdering 2006*. Oslo, Nasjonal sikkerhetsmyndighet.

Oslo Sporveier (2005): *Årsrapport 2004*. Oslo. http://www.sporveien.no

Perrow, C. (1999): *Normal Accidents. Living with High-Risk Technologies*. Princeton, New Jersey: Princeton University Press.

Quale, S. (2007): Safety vs security. Foredrag, Sikkerhetsdagene 2007, Trondheim 30.10.2007.

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

Ravlum, I-A. (2005): *Setter vår lit til storebror …og alle småbrødre med? Befolkningens holdninger til og kunnskap om personvernet*, Oslo, Transportøkonomisk institutt, TØI rapport 789/2005

Schartum, D.W. og Bygrave L.A. (2004): *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger.* Oslo: Fagbokforlaget

Schartum, D.W. (2007): *Personvern og transportsikkerhet. Personvernmessige spørsmål knyttet til tiltak for å sikre transportmidler mot fiendtlige anslag.* Complex 3/07, Senter for rettsinformatikk, Avdeling for forvaltnings-informatikk, Universitetet i Oslo

Schneier B. (2004): *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York: Springer.

SL (2002): Årsberetning 2002. Stor-Oslo Lokaltrafikk AS, http://www.slnett.no

Statens vegvesen (2006): *Automatiske bomstasjoner. Evaluering av automatiske bomstasjoner i Bergen, Tønsberg og Gjesdal* (foreløpig upuplisert utkast)

Statens vegvesen (2002): *ITS på veg. Programbeskrivelse for etatsprosjekt*. Oslo, Vegdirektoratet.

Statewatch 2004: “Scoreboard” on post-Madrid counter-terrorism plans

St.meld. nr. 5 (2007-2008): *Datatilsynets og Peronsvernnemdas årsmeldingar for 2006.* Fornyings- og administrasjonsdepartementet.

St.meld. nr. 10 (2004-2005): *Om ILO-konvensjon nr. 185 om sjøfolks identitetsbevis*. Nærings- og handelsdepartementet

St.meld. nr. 31 (2003-2004): *Vilje til vekst – for norsk skipsfart og de maritime næringer,* Nærings- og handelsdepartementet http://odin.dep.no/filarkiv/207626/STM0304031-TS.pdf

St.meld. nr. 39 (2003-2004): *Samfunnssikkerhet og sivilt-militært samarbeid*. Tilråding fra Justis- og politidepartementet av 14. mai 2004

Ström P. (2006a): *Med storebror i uppfinnarverkstan. Ny digital övervakning, från automatiska öron till internetdammsugare*. Stockholm, Den Nya Välfärden.

Ström P. (2006a): *Med storebror i baksätet. Digital övervakning av dina bilfärder.* Stockholm, Den Nya Välfärden.

Sætnan, A.R., Lomell H.M. og Wiecek C. (2004): Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations. *Surveillance & Society* CCTV Special 2(2/3): 396-414.

Sætnan, A.R., Dahl J.Y. og Lomell H.M. (2004): *Views from under surveillance. Public opinion in a closely watched areal in Oslo* (Urbaneye, Working Paper no. 12), Trondheim: NTNU

Teknologirådet (2005): *Elektroniske spor og personvern*, Rapport 1, 2005. Oslo.

Teknologirådet (2007a): *Sikkerhet og personvern. Oversikt over sikkerhetsteknologier*. Oslo, PRISE-prosjektet, EU: Preparatory Action on the enhancement of the European industrial potential in the field of Security research (PASR).

Teknologirådet (2007b): Nordmenn positive til å bli overvåket. http://www.teknologiradet.no/FullStory.aspx?m=28&amid=3673

Trajtenberg M. (2006): Defence R&D in the anti-terrorist era. *Defence and Peace Economics*, 17 (3), 177-199.

UK ICO (2005):"Advanced Scanning Technologies (Scanning Summary 03/05 JMK)". UK Information Commissioner's Office

Wahlgren, P. (ed) (2006): *A Proactive approach, Scandinavian studies in law*. University of Stockholm. vol 49, 2006.

Wiecek C. og Sætnan A.R. (2002) *Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark*. UrbanEye, Working Paper No. 4. 5th Framework Programme of the European Commission.

Vedlegg 1: Intervjuguide

Intervjuspørsmål

1. Innledning

- Kan du fortelle litt om din egen stilling?
- Hva er din rolle i forhold til arbeidet med sikkerhet og security i virksomheten?
- Hvordan er securityarbeidet organisert i din virksomhet? Hvordan har dere tenkt rundt dette i din virksomhet?
- Er det samme personer/avdelinger som steller med sikkerhet som også steller med security?

2. Risiko og sårbarhet

- Hva er det virksomheten skal sikres mot, hva er mest aktuelt her? Har virksomheten en trusseloppfatning?
- Har virksomheten gjennomført en ROS-analyse?
- Hva legger dere i en slik analyse – både safety og security?
  Hvilke nye typer trusler er med i securityarbeidet?
- Hvem utarbeidet ROS-analysen? Eksterne eller interne?
- Oppdateres dette arbeidet på noen måte?
  Fra hvilke kilder?

3. Securitytiltak

- Hvordan vil du beskrive securitytiltakene generelt i din bransje?
- Brukes ROS-analysen aktivt i det daglige arbeid (eller mer som bakteppe)?
- Hvilke securitytiltak har dere gjennomført i virksomheten? Nevn tre (om mulig)
- Hvilke personvernimplikasjoner tror du disse tiltakene har?
- Hvor effektive tror du tiltakene er for å motvirke vold/krim/hærverk?
- Hvordan vurderer du virkningen av tiltaket mht effektivitet og kostnader?
- Er det andre tiltak som er viktige, men som er for kostnadskrevende eller på andre måter for vanskelige å gjennomføre? I så fall, hvilke?

Hvis de ikke var for kostnadskrevende, hva var problemet med å gjennomføre dem)

- Kjenner du til tilsvarende securitytiltak i andre virksomheter i din bransje?
- Er securitytiltakene dere gjennomfører noe dere må gjøre ut fra påbud fra overordnete myndigheter? Gjelder det noen av tiltakene du har nevnt?
- I hvor stor grad har virksomhetene kontakt med nasjonalt og internasjonalt fagmiljø på securityområdet?
- Synes du at det er behov for en samlet koordinering av securitytiltakene på tvers av transportgrener/bransjer?
- Har du noen tanker om securityarbeidet i beslektede transportgrener?
- Hvor ser du mulighetene for forbedring av arbeidet med security i din virksomhet. Myndigheter? Teknologi? Organisatorisk?
- Hvordan vil du beskrive utviklingen inne securitytiltak i din bransje? Hvor er dere om 10 år?

4. Personvernimplikasjoner

- Hvordan er personvern integrert i arbeidet med transportsikring?
- Er det noen som har ansvar for personvernspørsmål i virksomheten? De samme som har ansvar for sikring?
- Hvilket lovgrunnlag når det gjelder personvern har dere forholdt dere til?
- Hvilke personvernimplikasjoner tror du tiltakene dere har gjennomført har?
- Har du opplevd at hensyn til personvern har kommet i konflikt med tiltak for økt security? Eventuelt ved hvilke tiltak?
- Kjenner du til tiltak som ville ha økt sikkerheten i din sektor, men som ikke er implementert fordi de strider mot personvernhensyn?
- Har terrorhendelsene i NY, Madrid og London ført til konkrete endringer i organisasjonen med hensyn til sikringstiltak? I så fall, hva ble gjort konkret? Står det nedfelt i dokumenter? Er det gjort vurderinger mht personverninteresser ved implementering av disse tiltakene?

Vedlegg 2: Regelverk

Direktiver (EU)

DIREKTIV 94/55/EF om innbyrdes harmonisering av medlemsstatenes lovgivning om transport av farlig gods på vei

DIREKTIV 95/46/EF om personvern, Europaparlamentet og Rådet for den Europeiske Union

DIREKTIV 2002/58/EF om beskyttelse av personopplysninger og elektronisk kommunikasjon, Europaparlamentet og Rådet for den Europeiske Union

DIREKTIV 2004/52/EF om interoperasjonalitet mellom elektroniske bompengesystemer i det Europeiske fellesskapet, Europaparlamentet og Rådet for den Europeiske Union

DIREKTIV 2006/24/EF om lagring av data generert eller behandlet i forbindelse med tilveiebringelse av offentlig tilgjengelige elektroniske kommunikasjonstjenester eller elektroniske kommunikasjonsnett og om endring av direktiv 2002/58/EF

Forskrifter og instrukser

FOR-1995-05-30 nr. 4295: Instruks om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS).

FOR 2000-12-15 nr. 1265: Forskrift om behandling av personopplysninger (personopplysningsforskriften).

FOR 2001-07-01 nr. 744: Forskrift om informasjonssikkerhet, Forsvarsdepartementet

FOR 2003-02-05 nr. 136: Forskrift om tillatelse til å drive jernbane, herunder sporvei, tunnelbane og forstadsbane m.m., samt tilgang til å trafikkere det nasjonale jernbanenettet (tillatelsesforskriften), Samferdselsdepartementet

FOR 2003-03-26 nr. 401: Forskrift om yrkestransport innenlands med motorvogn og fartøy (yrkestransportforskriften), Samferdselsdepartementet

FOR 2004-06-22 nr. 972: Forskrift om sikkerhet og terrorberedskap om bord på skip og flyttbare boreinnretninger, Nærings- og handelsdepartementet

FOR 2004-04-30 nr. 715: Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten (BSL A 2-1). Samferdselsdepartementet

FOR 2005-03-01 nr. 235: Forskrift om skipsførerens og rederiets plikter i tilfelle straffbare handlinger av alvorlig art begås om bord og melding om savnede personer, Nærings- og handelsdepartementet

FOR-2005-06-24 nr. 692: Vedtak om endring i instruks om utredning av konsekvenser, foreleggelse og høring ved arbeidet med offentlige utredninger, forskrifter, proposisjoner og meldinger til Stortinget.

FOR 2007-07-03 nr 825: Forskrift om sikring av havner og havneterminaler mot terrorhandlinger mv.

Kgl. Res. 2005-08-19: Instruks for politiets sikkerhetstjeneste, PST

Forordninger

FORORDNING 2320/2002/EF om sikkerhet i luftfarten, Europaparlamentet og Rådet for den Europeiske Union, Europaparlamentet og Rådet for den Europeiske Union

FORORDNING 725/2004/EF om bedre sikring av skip og havnefasiliteter, Europaparlamentet og Rådet for den Europeiske Union

FORORDNING 648/2005 om endring av Rådets forordning (EØF) nr. 2913/92, om innføring av en EF-tollkodeks.

Kommisjonsforordning (EF) nr. 622/2003 om fastsettelse av tiltak for gjennomføring av felles grunnleggende standarder for luftfartssikkerhet (NOR/302R0622.00T)

Lover

LOV-1902-05-22 nr. 10: Almindelig borgerlig Straffelov (Straffeloven).

LOV 1965-06-18 nr. 4: Vegtrafikkloven, Samferdselsdepartementet

LOV-1970-01-16 nr. 1: Lov om folkeregistrering. Finansdepartementet

LOV-1985-06-14 nr. 77: Plan- og bygningsloven, Miljøverndepartementet, Kommunal og regionaldepartementet

LOV 1992-11-27 nr 109: Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven).

LOV 1993-06-11 nr. 100: Lov om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (jernbaneloven), Samferdselsdepartementet

LOV 1993-06-11 nr. 101: Lov om luftfart (luftfartsloven). Samferdselsdepartementet

LOV 1995-08-04 nr. 53: Lov om politiet (politiloven). Justis- og politidepartementet

LOV 1998-03-20 nr. 10: Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), Forsvarsdepartementet

LOV 2000-04-14 nr. 31: Lov om behandling av personsopplysninger (personopplysningsloven), Justis- og politidepartementet

LOV 2002-06-21 nr. 45: Lov om yrkestransport med motorvogn og fartøy (yrkestransportloven), Samferdselsdepartementet

LOV 2007-02-16 nr 09: Lov om skipssikkerhet (skipssikkerhetsloven). Nærings- og handelsepartmentet.

Besøks- og postadresse:
Transportøkonomisk institutt
Gaustadalléen 21
NO 0349 Oslo

Telefon: 22 57 38 00
Telefaks: 22 60 92 00
E-post: toi@toi.no

www.toi.no

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 samfunnsinstitusjoner, forsknings- og undervisningssteder i Norge og i utlandet
- gjennomfører forsknings- og utredningsoppdrag 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
- deltar i CIENS, Forskningssenter for miljø og samfunn, i Forskningsparken nær Universitetet i Oslo