Personvern og trafikksikkerhets-teknologi

Dag Wiese Schartum,
Senter for rettsinformatikk, Avdeling for forvaltningsinformatikk,
Universitetet i Oslo

Om innholdet av rapporten

Rapporten inneholder en personvernrettslig analyse av trafikksikkerhetsteknologi (ts-teknologi). Spesielt blir streknings-ATK,[1] automatisk fartstilpasning,[2] og atferdsregistrering[3] behandlet.

Vilkårene for at ts-teknologi skal komme inn under personopplysningsloven drøftes spesielt. Av særlig interesse er forholdet til unntaket i personopplysningsforskriften § 1-3 om saker som behandles eller avgjøres i medhold av rettspleielovene. Konklusjonen er at loven i stor grad kommer til anvendelse. Rapporten går deretter gjennom de viktigste kravene personopplysningsloven stiller. Særlig blir spørsmålet om plassering av behandlingsansvar viet oppmerksomhet.

Rapporten drøfter også hver av de tre typene ts-teknologi i forhold til personvernidealet. Konklusjonen er at streknings-ATK kan sies å være mest inngripende dersom en legger dagens teknologier til grunn. Imidlertid har automatisk fartstilpasning og (særlig) atferdsregistrering potensiale som kan være meget problematiske for personvernet. For disse to teknologiene er det imidlertid også mulig å velge løsninger som gir ubetydelig negative effekter.

I rapporten foretas det også en sammenligning mellom effektene for personvernet ved "verste-tilfelle scenario" for de tre ts-teknologiene, og teknologi som benyttes av politiet i forbindelse med etterforskning av alvorlige forbrytelser. Konklusjonen er at den negative effekten for personvernet av slik ts-teknologi, kan sammenlignes med etterforskningsteknologi som bare kan brukes i tilfelle forbrytelser med fem år som nedre strafferamme.

Avslutningsvis gis en forholdsvis detaljert gjennomgang av rettsspørsmål som bør løses for å foreta en forsvarlig rettslig regulering og avveining mellom trafikksikkerhet og personvern. Det pekes blant annet på at teknologi kan anvendes på måter som helt gjør det unødvendig å behandle personopplysninger for å begrense kjøretøyers hastighet. Det er med andre ord neppe en nødvendig konflikt mellom hensynet til personvern og teknologiske tiltak for å øke trafikksikkerheten.

[1] Automatisk trafikkontroll med måling av kjøretøyets fart over en lengre strekning.
[2] Registrering av kjøretøyets fart med varsel eller inngripen ved for høy hastighet.
[3] Registrering av kjøretøyets bevegelser, kjøreatferd og instrumentbetjening.

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn mv

Denne rapporten er skrevet som del av et større forskningsarbeid i prosjektet "Personvern og trafikk". Prosjektet har vært ledet av Transportøkonomisk institutt (TØI) og gjennomført i samarbeid med Statens väg- och transportforskningsinstitut (VTI, Sverige) og Avdeling for forvaltningsinformatikk (AFIN) ved Universitetet i Oslo. Oppdragsgiver har vært Statens vegvesen.

Prosjektets tema er spørsmål om personvern knyttet til visse IKT-baserte trafikksikkerhetstiltak som i stor grad innebærer registrering og videre behandling av opplysninger som er eller kan knyttes til bestemte personer. Tiltakene kan derfor sies å gjelde personvern eller mer presist; person*opplysnings*vern.

Arbeidet har primært vært knyttet til tre grupper teknologier:

- Streknings-ATK, dvs automatisk trafikkontroll (ATK) med måling av kjøretøyets fart over en lengre strekning (i stedet for som i dag bare på et bestemt punkt);
- automatisk fartstilpasning (ISA),[4] som registrerer om bilførers fart er over fartsgrensen, og gir varsel eller effektuerer fartssperre eller motstand i gasspedalen e.l. som hindrer for høy hastighet; samt
- atferdsregistrator ("Event Data Recorder" - EDR eller "black box") som kan registrere kjøretøyets bevegelser, kjøreatferd og instrumentbetjening.

I rapporten bruker jeg "trafikksikkerhetsteknologi" (ts-teknologi) som en felles betegnelse på IKT-baserte trafikksikkerhetstiltak, som de tre nevnte teknologiene er eksempler på.[5]

De to problemstillingene i Statens vegvesens etatsprogram ”Personvern og trafikk” som er undersøkt i prosjektet er:

1) Hvilke forhold påvirker trafikanters aksept av trafikksikkerhetstiltak med personvernimplikasjoner?
2) Hvilke institusjonelle og prosessuelle forhold fremmer og hemmer innføringen av trafikksikkerhetstiltak med personvernimplikasjoner?

Denne rapporten gir noen svar til den andre problemstillingen vedrørende institusjonelle og prosessuelle forhold som fremmer og hemmer nevnte trafikksikkerhetstiltak. Slike forhold gjelder i stor grad juridiske spørsmål. Denne rapporten inneholder en juridisk gjennomgang og analyse av aktuelle implikasjoner for personvernet, med vekt på personvern knyttet til behandling av personopplysninger.

Temaet personvern og informasjonssikkerhet innen intelligente transportsystemer (ITS) er tidligere behandlet i forskningsrapporten Meland m.fl. 2007. Slik ts-teknologi som er omhandlet i dette prosjektet, kan sies å høre til kategorien ITS. Den nevnte rapporten gir imidlertid kun en summarisk oversikt over enkelte lovbestemmelser, institusjoner mv, og inneholder ingen rettslige drøftelser av verdi for problemstillingen i dette arbeidet.

For uten denne rapporten vil arbeidet med det juridiske delprosjektet av Personvern og trafikk, omfatte en artikkel som spesielt gjelder den norske forsøksvirksomheten med streknings-ATK. Artikkelen vil trolig bli ferdigstilt sommeren 2010.

[4] ISA refererer til "intelligent speed adapter".

[5] Ts-teknologi kan også ses som en undergruppe av intelligente trafikksystemer (ITS), se Tveit m.fl. 2007 som for eksempel behandler ISA og streknings-ATK under denne betegnelsen.

1.2 Problemstillinger og oversikt over fremstillingen

Personvern er et vidt og til dels dynamisk begrep.[6] I denne delrapporten er utfordringen først å undersøke hvorledes personvern kan/bør forstås når ts-teknologi skal vurderes rettslig. Også annet enn personvern kan bidra til å fremme og hemme de aktuelle trafikksikkerhetstiltakene. Det blir da avgjørende å angi hva som kan sies å kjennetegne personvern. Likevel er det lite hensiktsmessig å forsøke å foreta en skarp avgrensing mellom personvern og andre typer hensyn. Det vil særlig være vanskelig å skille skarpt mellom hensynene til personvern og rettssikkerhet. Også enkelte problemstillinger vedrørende rettssikkerhet som samtidig kan sies å angå personvernet vil derfor bli behandlet, se særlig avsnitt 2.1.

Med et klargjort personvernbegrep, blir neste oppgave å finne svar på hva som er gjeldende rett på området. Oppgaven er med andre ord å kartlegge hvilke rettsregler om personvern som gjelder for slike trafikksikkerhetstiltak som forskningsprosjektet spesielt diskuterer (streknings-ATK, ISA og atferdsregistrator). Siden ts-teknologiene i begrenset grad er innført og i bruk i Norge, er det i dag ingen særskilt regulering av de aktuelle teknologiene. Kartleggingen vil derfor primært gi oversikt over *generelle* bestemmelser i lov og forskrift mv som kan komme til anvendelse på ts-teknologi.

Personopplysningsloven er hovedloven for beskyttelse av personopplysninger, og gjelder i utgangspunktet alle sektorer av samfunnet og alle teknologier som kan sies å behandle personopplysninger.[7] Loven er derfor det åpenbare utgangspunktet for en rettslig drøftelse. Det første og sentrale rettslige spørsmålet jeg behandler er vilkårene for at personopplysningsloven skal komme til anvendelse på den aktuelle ts-teknologien (kapittel 3). Dernest gjør jeg rede for de viktigste rettslige effektene når denne loven gjelder (kapittel 4). Kapitlene 3 og 4 bidrar med andre ord til en konkretisering av de rettslige krav som må etterleves dersom ts-teknologi skal tas i bruk.

I rapporten vil det også bli gjennomført to personvernrettslige analyser som ikke tar sikte på å kartlegge gjeldende rett. Den ene analysen tar sikte på å bringe større klarhet i på hvilken måte og med hvilken grad av nødvendighet streknings-ATK, ISA og atferdsregistrator kan sies å krenke personvernet (kapittel 5). De såkalte personverninteressene vil ligge til grunn for drøftelsen.[8] Den andre analysen gjelder sammenligning mellom de aktuelle ts-teknologiene og bruk av teknologisk baserte, inngripende etterforskningsmetoder i alvorlige straffesaker (kapittel 6). Valget av denne sammenligningen er trolig kontroversiell i seg selv. Spørsmålet er hvor krenkende streknings-ATK, ISA og adferdsregistrator kan sies å være sett i forhold til annen teknologi som i meget stor grad griper inn i personvernet, men som lovgiver likevel har tillatt. Hvilken vekt og argumentasjonskraft en slik sammenligning vil ha, avhenger bl.a av hvor likt det som sammenlignes er. Selv om det er klare forskjeller mellom inngripende etterforskningsmetoder på den ene side og de utvalgte ts-teknologiene på den andre, er det etter min mening tilstrekkelig mange likheter til at en sammenligning gir mening.

Personvernet representerer en grunnleggende menneskerettighet, jf artikkel 8 i Den europeiske menneskerettighetskonvensjonen (EMK). Bestemmelsen må derfor legges til

[6] Se gjennomgangen av begrepet i NOU 2009: 1, avsnitt 4.1.
[7] Se særlig lovens §3.
[8] Kataloger over personverninteresser har vært lagt til grunn i alt norsk lovarbeid vedrørende vern av personopplysninger, og spiller derfor en forholdsvis stor rolle ved fortolkningen av denne lovgivningen. En oversikt over personverninteressene finnes bl.a. i Schartum og Bygrave 2004, s 35 - 73.

grunn for norsk lovgivning og samfunnsliv ellers. Derfor kan den rettspolitiske drøftelsen ikke bli verdinøytral. Konvensjonen slår fast at "1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse." Samtidig er det klart at hensynet til personvern ikke alltid vil gå foran andre hensyn. Artikkel 8 nr 2 gir vilkårene for å kunne krenke rettighetene i første avsnitt: "2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, *for å beskytte helse* eller moral, eller for å beskytte andres rettigheter og friheter." (min kursiv) Unntakene inneholder dels noen prosessuelle krav (samsvar med loven) og dels et krav til innhold ("nødvendig i et demokratisk samfunn"). Videre inneholder den en oppregning av noen tillatte formål som vurderingen av nødvendighet er knyttet til. Blant disse formålene er beskyttelse av helse. Ts-teknologi som er nødvendig i et demokratisk samfunn for å redusere tap av menneskeliv og trafikkskader på mennesker, kan med andre ord begrunne inngrep i retten til personvern etter nr 1.

Kartlegging av gjeldende generell lovgivning om personvern inviterer til en nærmere rettspolitisk diskusjon, dvs en diskusjon av hvorledes avveiningen mellom trafikksikkerhet og personvern *bør* være, og hvordan ts-teknologi *bør* reguleres i framtiden (kapittel 7). Dette er ingen enkel vurdering å gjøre innenfor rammene av et forskningsprosjekt. Jeg har i stor grad begrenset meg til å angi hva som etter min mening er de beste lovgivningstekniske løsningene. I tillegg angir jeg retningslinjer og identifiserer mulige veivalg.

En rettspolitisk diskusjon er uansett beheftet med stor grad av usikkerhet mht det framtidige innholdet av ts-teknologier. Drøftelser som kun baserer seg på dagens teknologi har meget kortvarig verdi. Jeg forsøker å takle dette problemet ved å forutsette ulike teknologiske og bruksmessige egenskaper som på kort og mellomlang sikt kan anses å være mulige. Dermed er det ikke sagt at realiseringen av alle mulighetene er sannsynlige.

2 Personvern sett i sammenheng med andre rettslige idealer

2.1 Om personvern generelt og om forholdet til rettssikkerhet og rettsbeskyttelse

Innledningsvis er det av betydning å avklare hva begrepet personvern i generell mening kan sies å gjelde. Jeg vil her legge stor vekt på fremstillingen i Personvernkommisjonens innstilling (NOU 2009: 1). Kommisjonen gir en oversikt over og oppsummerer viktige deler av den terminologiske og teoretiske debatten rundt "personvern", "personopplysningsvern", "privatlivets fred" mv. De konkluderer med å definere personvern til å gjelde:

> " ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse."

Kommisjonen legger til grunn at person*opplysnings*vern dreier seg om

> "[…] regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv."

Kommisjonen understreker videre at det er viktige sammenhenger mellom personvern og personopplysningsvern, ved at det ene ofte er en forutsetning for det andre. Manglende respekt for personers selvbestemmelse vil for eksempel lett medføre at det samles inn personopplysninger om dem. Behandling av personopplysninger vil kunne gi forstyrrelser i personenes privatliv og begrense deres selvutfoldelse. Selv om det er nær sammenheng mellom personvern og personopplysningsvern, understreker Kommisjonen at de to begrepene ofte står godt på egne ben. Personopplysningsvern trenger for eksempel ikke alltid noen begrunnelse i det alminnelige personvernet - og vise versa. Her vil jeg ikke gå nærmere inn på de mange diskusjonene som Personvernkommisjonens begrepsdefinisjoner kan reise. Jeg legger i stedet definisjonene til grunn som generelt utgangspunkt for dette arbeidet.[9]

Et sentralt begrep som ofte brukes i personvernsammenheng er "overvåkning". Ofte brukes overvåkning om systematisk og rutinemessig innsamling og behandling av personopplysninger. Derfor er fjernsynsovervåking i personopplysningsloven § 36 bl.a. definert som "vedvarende eller regelmessig gjentatt personovervåking". I tillegg til systematisk og/eller rutinemessig tilnærming til informasjonsinnsamlingen, er også formålet tatt med som del av definisjonen (jf "personovervåking"). Overvåkning vil derfor typisk ha som formål å styre, kontrollere eller på annen måte øve innflytelse over personer, sosiale prosesser mv.[10]

Overvåkingsbegrepet blir ofte gitt et negativt innhold eller det blir knyttet negative assosiasjoner til ordet, jf "overvåkningssamfunn" mv. Slike negative konnotasjoner er imidlertid primært knyttet til situasjoner og samfunn der overvåking har tatt overhånd og derfor ikke kan forsvares innenfor et demokratisk samfunnssystem bygget på rettsstatens prinsipper. Det betyr imidlertid ikke at overvåkning som sådan er uforenelig med slike

[9] Som et detaljert supplement til denne fremstillingen kan min fremstilling i Schartum 2007 s 15 - 84 der jeg utvikler og forklarer personvern spesielt i lys av transportsikkerhet (security).
[10] Se NOU 2009: 1 med henvisninger.

styringsprinsipper. Overvåkning kan tvert i mot ha demokratiske begrunnelser; for eksempel slik at overvåkingstiltak skal bidra til at demokratisk fattede vedtak faktisk blir etterlevet. Overvåkningstiltak for å sikre gjennomføring av bestemmelser om fartsgrenser for kjøretøy, kan for eksempel sies å ha en slik demokratisk begrunnelse. Diskusjonen om overvåkingen i et demokrati der personvern og rettsstatens prinsipper legges til grunn, gjelder derfor hva som er *for mye* overvåking. Dette kan igjen forstås som et spørsmål om hva som er den riktige avveiningen mellom personvern, rettssikkerhet, rettsbeskyttelse (herunder for eksempel trafikksikkerhet), jf nedenfor.

I denne rapporten legger jeg til grunn at overvåkning er en legitim aktivitet i en demokratisk rettsstat, men at overvåking likevel kan legges slik opp og skje i et slikt omfang at det blir uforenlig med slike styringsidealer. Slik jeg forstår den aktuelle ts-teknologien som står til diskusjon i denne rapporten, vil mye av den mulige bruken nettopp ha preg av å være overvåkning. Teknologien bruker nemlig teknikker for systematisk og rutinemessig informasjonsinnsamling og bearbeiding. Formålet er å kontrollere og øve innflytelse på etterlevelsen av regler i vegtrafikkloven og annen lovgivning som skal sikre liv og helse i trafikken.

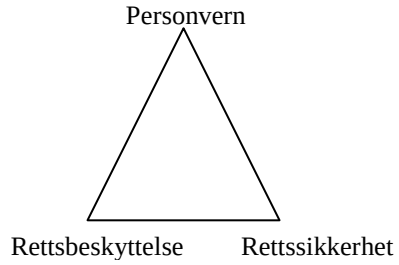
Personvern er sammen med rettssikkerhet to grunnleggende komponenter i en rettsstat. Også begrepet "rettssikkerhet" er på samme måte som "personvern" gjenstand for en rekke definisjoner. Også her er det mulig å ta utgangspunkt i personlig integritet og autonomi. Rettssikkerhet kan da knyttes til individenes beskyttelse mot overgrep og vilkårlighet fra myndighetenes side. Et viktig element er dessuten individenes mulighet til å forutberegne sin rettsstilling og forsvare sine rettslige interesser overfor offentlige myndigheter. I tillegg inkluderes gjerne hensynet til likhet og rettferdighet i rettssikkerhetsbegrepet. [11]

Det er enkelte distinksjoner og sammenligninger mellom personvern og rettssikkerhet som det kan være grunn til å oppta seg med i denne sammenhengen. For det første gjelder rettssikkerhet tradisjonelt relasjonen borgere - offentlige myndigheter, mens personvernet gjelder generelt uansett sektor/relasjon. Personvern kan imidlertid sies å være spesielt viktig når det kombineres med og direkte gjelder myndighetsutøvelse, dvs i situasjoner der både personvern- og rettssikkerhetsidealene aktualiseres.

For det andre er det åpenbart at overgrep, vilkårlighet, manglende forutberegnelighet, forskjellsbehandling mv kan skje på måter som får følger for privatliv og behandling av personopplysninger. Når rammen er myndighetsutøvelse kan det derfor være vanskelig å stille opp noen klare skiller mellom personvern og rettssikkerhet. Jeg velger likevel ikke å bruke de to begrepene uavhengig av hverandre. Selv om begrepene peker inn i mange av de samme problemstillingene når vi bruker dem i situasjoner som gjelder myndighetsutøvelse, har de ulikt idémessig opphav og ulike kvaliteter. Systematikk og begreper vedrørende personopplysningsvern er for eksempel bedre egnet til analyse av informasjonssystemer enn systematikk og begreper vedrørende rettssikkerhet. Rettssikker er på den annen side best egnet til bredt å angi krav til myndigheters bruk av sine inngripende fullmakter til å kontrollere, ilegge straff og bruke andre offentligrettslige sanksjoner. Riktignok kan straffeprosessuelle krav om kontradiksjon, objektivitet, uavhengighet mv langt på vei også utledes med utgangspunkt i personvern, men rettssikkerhetsteori og rettspleielovgivning gir en bedre og mer direkte tilgang til disse sidene ved rettsstaten.

[11] Se NOU 2009: 15 med henvisninger til bl.a. Doublet; Rett, vitenskap og fornuft s 503-504 og Eckhoff/Smith; Forvaltningsrett 8. utgave s 50.

Noen bruker også begrepet rettssikkerhet om politiets beskyttelse av borgere mot angrep og krenkelser fra andre borgere. I denne rapporten bruker jeg begrepet "rettsbeskyttelse" om denne dimensjonen, og innen strafferetten kan vi generelt tale om "kriminalitetsbekjempelse" eller "kriminalitetsbeskyttelse". Bruk av ts-teknologi kan settes i sammenheng med denne terminologien, fordi streknings-ATK mv kan sies å være en del av samfunnets beskyttelse mot kriminell atferd (overskridelser av fartsgrenser) for derved å beskytte folks liv og helse. Det kan med andre ord sies å foreligge minst tre typer krav til styring/myndighetsbruk som må ses i sammenheng med hverandre. Spørsmålet er derfor langt på vei hvorledes hensynet til rettsbeskyttelse (beskyttelse av liv og helse mv i trafikken) kan kombineres med hensynet til personvern og rettssikkerhet.



Figur 1. Forholdet mellom grunnleggende rettigheter med særlig relevans for denne rapporten

Disse ulike aspektene er alle knyttet til universelle menneskerettigheter, og det er derfor ikke grunnlag for generelt å påstå at ett hensyn er viktigere enn de andre. I den grad det oppstår konflikt må hensynene derfor balanseres mot hverandre, jf særlig artikkel 5 (right to liberty and security), artiklene 6 og 7 (right to fair trial and no punishment without law) og artikkel 8 (right to respect for private and family life). Utgangspunktet for slike avveininger må imidlertid antas å være nødvendig motstrid, jf kravet i art. 8 om at inngrep i personvernet etter annet ledd må være "necessary in a democratic society". Dette betyr at personvernet for eksempel ikke kan settes til side for å beskytte liv og helse, med mindre dette er nødvendig i et demokratisk samfunn. Vurderingen av "nødvendig" kan videre ikke ta utgangspunkt i én bestemt teknologi eller fremgangsmåte. Dersom noen slike metoder innebærer mindre inngrep i personvernet enn andre, følger det av et slikt resonnement at denne minst inngripende metoden skal velges.

2.2 Hovedpunkter om personvern og trafikk i Personvernkommisjonens innstilling

Personvernkommisjonen (NOU 2009: 1) drøftet samferdselssektoren som ett av flere utvalgte områder som kommisjonen analyserte spesielt, se kapittel 17. Perspektivet i kapittelet er meget bredt, og omfatter både telekommunikasjon, kollektivtransport og biltrafikk. Kommisjonen tar dessuten både opp spørsmål om sikkerhet mot terrorhendelser mv ("security") og trafikksikkerhet ("safety"). Trafikksikkerhet kan ikke sies å være undergitt noen grundig beskrivelse og analyse i rapporten. I det følgende vil jeg derfor primært trekke frem overordnede og mer prinsipielle synspunker som kommisjonen formulerer i nevnte kapittel.

Kommisjonen kritiserer for det første relevant regelverk for at det er for uoversiktlig, komplekst og for at det åpner for mange tolkningsmuligheter. Det understrekes at kritikken både rammer regelverk som skal fremme personvernet og regelverk som kan sies å undergrave/begrense slikt vern. Kommisjonen ser denne regelverkssituasjonen som et problem for ivaretakelse av rettssikkerhet og muligheter for demokratisk styring og kontroll.

Personvernkommisjonens inntrykk er at personvernhensyn i forholdsvis begrenset grad har vært vurdert før innføring av nye tiltak innen samferdselssektoren. De trekker i denne

sammenheng frem at personvern vies lite plass i Samferdselsdepartementets IKT-strategi "Fra A til B... Bedre, tryggere og mer effektiv transport – med IKT".

Kommisjonen understreker også at dagens teknologi nærmest gir uavgrensede muligheter for registrering og overvåking, og stiller spørsmål om det finnes noen grense for øking av sikkerhet og effektivitet på bekostning av personvernet. Kommisjonen antydet ikke hvorledes en slik grense kan trekkes, men understreker at det ikke er akseptabelt med en sektor-tilnærming som tillater at én sektor skaper effekter på sitt område, uten å se dette i sammenheng med utvikling på andre områder.

Personvernkommisjonens tilrådinger på området er ikke særlig konkrete men har mer preg av retningslinjer. Med henvisning til EMK artikkel 8 ble det foreslått å legge økt vekt på proporsjonalitet i samband med planer om personverninngripende tiltak innen transportsektoren. Forslaget innebærer gjennomføring av systematiske kost-nyttevurderinger og konsekvensutredninger forut for gjennomføring av slike tiltak. I dette ligger trolig også krav om å dokumentere beslutningsgrunnlag og virkninger, samt å klargjøre forutsetninger for at tiltakene kan anses å være akseptable.

Personvernkommisjonen tilrår at det så langt som mulig legges til rette for sporfrie og anonyme løsninger ved betaling og bruk av transporttjenester. Billige sporfrie løsninger bør i alle fall tilbys som alternativ til de som gir elektroniske spor. Informasjon om sporfrie alternativer bør dessuten gjøres lett tilgjengelig.

Jeg går ikke nærmere inn i en diskusjon av Personvernkommisjonens uttalelser her. Flere av de forhold kommisjonen peker på inngår imidlertid i drøftelser og vurderinger i denne rapporten, jf særlig kapittel 7.

3 Om anvendelse av personopplysningsloven på trafikksikkerhets-teknologi

3.1 Innledning

Selv om vi rent allment kan fastslå at ts-teknologi har virkninger som kan sies å gjelde personvern, er det ikke dermed sagt at virkningene er slike som lovgiver til nå har regulert. Det er derfor behov for en nærmere analyse av i) om de aktuelle typene ts-teknologi faller inn under eksisterende rettslig regulering, og ii) hva denne reguleringen i så fall går ut på, herunder hva slags konsekvenser reguleringen har for bruken av ts-teknologi. Denne kartleggingen er en viktig basis for den rettspolitiske diskusjonen om behov for å endre dagens lovregulering. Det kan for eksempel være aktuelt å vedta særlige regler om ts-teknologi for å balansere hensynene mellom trafikksikkerhet og personvern bedre enn i dag.

Kapittel 3 inneholder en analyse av om og i hvilken grad ts-teknologi kommer inn under personopplysningsloven mv. I kapittel 4 vil det så bli foretatt en nærmere analyse av det nærmere innholdet av denne rettslig reguleringen.

3.2 Vilkår for anvendelse av personopplysningsloven på ts-teknologi

3.2.1 Oversikt

I avsnitt 3.2 går jeg gjennom vilkår for at personopplysningsloven kommer til anvendelse på ts-teknologi. Spørsmålene jeg gjennomgår er i grove trekk:

i) Om/ i hvilken grad ts-teknologi kan sies å behandle "personopplysninger".
ii) Om personopplysninger i ts-teknologier er gjenstand for elektronisk behandling eller ikke.
iii) I hvilken grad norsk eller andre EØS-lands lovgivning kommer til anvendelse.
iv) I hvilken grad ts-teknologi gjelder saksområder som er unntatt fra personopplysningslovens bestemmelser, og hva som i så fall kommer til anvendelse i stedet.

De tre første spørsmålene representerer kumulative vilkår som må være oppfylt for at personopplysningsloven skal komme til anvendelse. Dersom personopplysningsloven ikke kommer til anvendelse, kan annen lovgivning ha betydning, jf avsnitt 3.2.5.

3.2.2 I hvilken grad behandler ts-teknologi "personopplysninger"?

Felles for streknings-ATK, ISA og atferdsregistrator er at teknologiene registrerer kjøreatferd, dvs fart, nedbremsing, instrumentbetjening osv. I tillegg vil blant annet bilens posisjon og kjørevei kunne registreres. Slike registrerte data vil være direkte knyttet til kjøretøyet. Så lenge opplysningene bare kan knyttes til kjøretøyet er de ikke "personopplysninger" som kommer inn under personopplysningsloven. For å komme inn under loven må opplysningene kunne knyttes til en bestemt, identifiserbar fysisk person. Derfor blir selve identifiseringsprosessen viktig, eventuelt med tilhørende autentisering.

For streknings-ATK vil det skje identifisering ved hjelp av personfoto *en face* i kombinasjon med fotografering av kjøretøyets kjennetegn. Dette vil i de fleste tilfelle gjøre det mulig å foreta sikker identifisering av føreren. I noen tilfelle vil det imidlertid være tvil om førerens

identitet, for eksempel fordi det er teknisk feil på kameraet, kameraet tar bilde med for dårlig kvalitet, fordi føreren skjuler seg, registreringsnummer mangler, er tilsølt eller lignende. Kan det ikke fastslås hvem føreren er, eller er det stor usikkerhet med hensyn til identiteten, vil det i disse konkrete tilfellene ikke foreligge personopplysninger fordi opplysningene ikke kan knyttes til en bestemt enkeltperson, jf pol § 2 nr 1.

Når det gjelder atferdsregistrator og automatisk fartstilpasning, brukes ikke personbilde, og identifisering av føreren skjer på annen måte. Utgangspunktet vil trolig være at det er eieren eller annen person med disposisjonsrett over kjøretøyet (leier, leaser mv) som er fører. Likevel kan det åpenbart også være en rekke andre personer som fører bilen. I slike tilfelle kan førerens identitet være usikker. Identiteten kan da bare fastslås ved å granske eierforhold, hvem som faktisk har hatt adgang til bilen, andres observasjoner mv. Er usikkerheten stor nok, for eksempel slik at 4 - 5 personer eller flere kan ha ført bilen, kan konklusjonen bli at det ikke foreligger personopplysninger i lovens forstand. Foreligger det ikke personopplysninger vil ikke personopplysningsloven komme til anvendelse.

Dersom formålet med adferdsregistratoren er å avdekke straffbare overtredelser av veitrafikkloven mv, er forventningen at det vil skje etterforskning for å bringe den skyldiges identitet på det rene. I så fall kan dette tale for at opplysningene må ses som person-opplysninger. Konklusjonen vil med andre ord avhenge av en konkret vurdering av selve informasjonsbehandlingen og de typiske situasjonsbestemte forholdene knyttet til bruken av systemet for registrering og etterforskning.

Dersom atferdsregistrator og ISA er knyttet til en autentiseringsmetode, for eksempel personlig kode, fingeravtrykkleser eller lignende, vil identiteten av føreren kunne fastslås med stor grad av sikkerhet. Når opplysningene i registratoren sikkert og entydig kan knyttes til bestemte enkeltpersoner, vil det utvilsomt foreligge personopplysninger.

Selv om det forekommer enkelttilfelle der føreren ikke kan identifiseres (jf streknings-ATK), spiller dette neppe noen rolle for spørsmålet om det foreligger personopplysninger eller ikke så lenge tilstrekkelig sikker identifisering er mulig i andre tilfelle. Avgjørende for om personopplysningsloven kommer til anvendelse er hvorvidt trafikksikkerhets*systemet* kan sies å behandle personopplysninger eller ikke. Selv om kun et lite antall førere lar seg identifisere i systemet, vil systemet behandle noen personopplysninger, jf pol § 2 nr 2. I så fall vil det eneste praktiske være at hele systemet må innrettes etter disse tilfellene, dvs. følge personopplysningsloven.

Konklusjonen er at streknings-ATK åpenbart behandler personopplysninger, og at atferdsregistrator og ISA utvilsomt behandler personopplysninger dersom føreren kan identifiseres og knyttes til opplysningene som teknologien behandler. Dersom identifisering er meget vanskelig og usikker, kan det være mer tvilsomt om koplingen mellom opplysningene og føreren(e) er entydig og sikker nok til at det kan sies å foreligge "personopplysning". Det spiller i utgangspunktet ingen rolle om identifiseringen av personer skjer gjennom flere ledd. Dersom ISA for eksempel styres ved hjelp av mobiltelefon i hvert kjøretøy, vil meldinger til denne mobilen om for høy fart generere personopplysninger om føreren. Forutsetningen er at det kan klargjøres hvilken bil med hvilken fører mobiltelefonen befant seg i.

Det er etter dette generelt grunn til å anta at atferdsregistratorer og ISA vil bli brukt på måter som innebærer behandling av personopplysninger. Dette er et nødvendig men ikke tilstrekkelig vilkår for at slike ts-teknologier kommer inn under personopplysningsloven.

3.2.3 Skjer det "elektronisk behandling" av personopplysninger i ts-teknologi?

"Behandling av personopplysninger" er i pol § 2 nr 2 definert som "enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter". "Enhver bruk" og den etterfølgende eksemplifiseringen, innebærer at det uansett skjer "behandling" av opplysninger i ts-teknologi. Jeg har tidligere konkludert med at disse opplysningene stort sett må anses å være "personopplysninger". Denne behandlingen er imidlertid spesiell fordi den er knyttet til fotoapparat og ulike måleapparater, sensorer mv som registrerer/dokumenterer resultater av førerens handlinger. Slike særegenheter har imidlertid ingen betydning for vurderingen av om det foreligger behandling i lovens forstand eller ikke.

Personopplysningsloven kommer for det første til anvendelse på elektronisk behandling av personopplysninger, og det er nok at behandlingen bare *delvis* er elektronisk. All ts-teknologi har vesentlige innslag av komponenter som er "elektroniske". Siden også delvis elektronisk behandling kommer inn under loven, er det neppe grunn til å foreta en videre vurdering av hvor meget av utstyret som må være elektronisk.[12]

For at personopplysningsloven skal komme til anvendelse, kan opplysningene alternativt være i et "personregister" eller de skal føres inn i et slikt register.[13] "Personregister" er definert som "registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen". Definisjonen dekker bl.a tilfelle der det tas utskrift av registrerte persondata fra ts-teknologi og disse utskriftene har et innhold som er ordnet systematisk for å lette gjenfinning av personer, for eksempel etter bilens kjennemerke.[14]

Jeg legger til grunn at det primært skjer elektronisk behandling av opplysninger i ts-teknologi. Uansett om det delvis skulle skje manuell etterbehandling i tilknytning til den elektroniske behandlingen eller manuell behandling i personregister, vil loven kunne komme til anvendelse. Om behandlingen skjer elektronisk eller i manuelt register har primært betydning for kravene til informasjonssikkerhet i personopplysningsforskriftens kapittel 2. Denne delen av forskriften får kun anvendelse på elektronisk behandling av personopplysninger.

3.2.4 Når kommer norsk personopplysningslov til anvendelse?

Når det skjer behandling av personopplysninger i ts-teknologi i Norge, vil norsk eller annen europeisk personopplysningslovgivning helt eller delvis regulere bruken av systemene. Om norsk lov gjelder avhenger av om den behandlingsansvarlige er "etablert i Norge" eller ikke, se pol § 4 første ledd. Den behandlingsansvarlige er i loven definert som "den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som kan brukes." Det er primært den behandlingsansvarlige som har plikter etter loven. For ts-teknologi er Politidirektoratet og Vegdirektoratet de mest aktuelle kandidatene til denne rollen, se

[12] Se pol § 3 første ledd bokstav a.
[13] Se pol § 3 første ledd bokstav b.
[14] Personregister kan også oppstå dersom andre lagringsmedium enn papir som inneholder personopplysninger, ordnes for å lette gjenfinning av opplysninger om enkeltpersoner.

drøftelsen i avsnitt 4.2.2 nedenfor. For å være etablert må det utøves en aktivitet gjennom fast organisatorisk infrastruktur over et ubestemt tidsrom.[15] Disse direktoratene er åpenbart etablert i Norge.

Er den behandlingsansvarlige etablert i et annet EØS-land, kommer vedkommende lands personopplysningslov til anvendelse. Er behandlingsansvarlige etablert utenfor EØS men gjør bruk av utstyr på norsk territorium, gjelder norsk lov, men denne muligheten velger jeg ikke å gå nærmere inn på, jf pol § 4 annet ledd.

Ofte er det aktuelt å benytte en "databehandler", dvs. en oppdragstaker som utfører behandlingen av personopplysninger på den behandlingsansvarliges vegne. Valg av databehandler[16] som ikke er etablert i Norge, får ingen direkte konsekvenser for hvilken lov som gjelder. Dersom behandlingsansvarlige må følge norsk lov, vil også databehandlers del av arbeidet reguleres av samme lov.[17]

Spørsmålet om norsk lov kommer til anvendelse eller ikke, får neppe noen stor praktisk rolle for myndigheters bruk av ts-teknologi, med mindre en går radikalt til verks og outsourcer kontrollvirksomheten til en utenlandsk tjenesteleverandør. Langt mer praktisk blir spørsmålet dersom en tenker seg slik teknologi brukt av bilfabrikanter, forsikringsselskaper og andre med formål å bedre sikkerhetsutstyr, kartlegge skadeårsaker mv. Dette kan for eksempel tenkes i kombinasjon med myndigheters bruk av slik teknologi, eventuelt etter at myndigheters bruk har banet vei for teknologien.

3.2.5 Er ts-teknologien brukt på måter som gjør at den kommer inn under unntak fra personopplysningsloven?

I forskriften til personopplysningsloven (pof) § 1-3 er det gjort unntak fra personopplysningsloven for behandling av "*saker* som behandles eller avgjøres i medhold av rettspleielovene" (min kursiv). Rettspleielover er betegnelse på lover som regulerer politiets, påtalemyndighetens og domstolenes virksomhet. I pof § 1-3 er dette eksemplifisert som domstolloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven. Også forskrifter på området må regnes inn under denne kategorien bestemmelser, herunder forskrift om ordningen av påtalemyndigheten ("påtaleinstruksen").[18] Saker som for eksempel skal behandles etter straffeprosesslovens bestemmelser, kommer med andre ord inn under unntaket i pof § 1-3.

Pof § 1-3 unntar ikke det generelle opplegget (systemet) for behandling av personopplysninger. Unntaket gjelder for behandling av *den enkelte sak*. Det betyr for eksempel at alle bestemmelser i personopplysningsloven som fastsetter rettigheter for registrerte personer eller plikter for den behandlingsansvarlige overfor slike personer, ikke gjelder (innsynsrettigheter, plikter til å informere, rette, slette mv.). Denne forståelsen av unntaket i forskriften følger ikke med nødvendighet av ordlyden, men er basert på direkte uttalelser i forarbeidene til personopplysningsforskriften.[19] Unntaket begrunnes med den potensielt ødeleggende effekten for etterforskning mv av registrerte personers rett til innsyn

[15] Se Schartum og Bygrave 2006 s 49 – 53.
[16] Det vil si en virksomhet eller person som behandler personopplysninger på vegne av den behandlingsansvarlige, jf pol § 2 nr 5.
[17] Dette følger av behandlingsansvarliges styringsrett (og -plikt) overfor databehandlere, jf pol § 15.
[18] Forskrift av 8. august 2008 nr 883.
[19] Se kongelig resolusjon av 15. desember 2000 nr. 1265, kommentarer til § 1-3.

og rett til å få opplysninger om seg rettet og slettet mv. Det blir også fremhevet at plikten til å varsle registrerte ved innhenting av personopplysninger i samsvar med pol § 20 ville ha skadelige effekter for politiet.

I tillegg til unntaket i pof § 1-3 følger det av lex specialis-prinsippet[20] og pol § 5 at straffeprosessloven og andre rettspleielover går foran personopplysningsloven dersom det er motstrid mellom bestemmelser. Om det oppstår motstrid eller ikke må imidlertid avgjøres konkret, og jeg vil ikke her vurdere hvilke bestemmelser i personopplysningsloven som det kan være aktuelt helt eller delvis å sette til side på dette grunnlaget. Utgangspunktet er imidlertid at de systemmessige kravene i personopplysningsloven (dvs de som ikke spesielt gjelder krav til behandling av enkelte saker) også gjelder for politi, påtalemyndigheter og domstoler, så lenge det ikke kan påvises motstrid med bestemmelser i rettspleielovene.

Forklaringen av pof § 1-3 i kgl. res. av 15.desember 2000 nr 1265 inneholder også en presisering av Datatilsynets rolle i forhold til behandling av personopplysninger der rettspleielovene gjelder: "Men Datatilsynet har alminnelig tilsynskompetanse i medhold av personopplysningsloven." Dette innebærer at Datatilsynet har kompetanse til å føre tilsyn med etterlevelse av systemmessige krav i personopplysningsloven med forskrifter.

Det generelle bildet er etter dette at hele personopplysningsloven med forskrifter vil gjelde for den systemmessige utformingen og driften av ts-teknologi. For hver sak der det er registrert en overtredelse av veitrafikkloven og saken blir behandlet med tanke på straffeforfølging, vil straffeprosessloven og andre rettspleielover komme i forgrunnen og regulere behandlingen av den enkelte sak, for eksempel bildene med tilhørende data fra streknings-ATK. Med mindre rettspleielovene gir holdepunkter for en annen løsning, vil imidlertid *systemkravene* i personopplysningsloven gjelde. For eksempel vil kravene i pol § 15 til avtale mellom behandlingsansvarlige (ofte Politidirektoratet) og databehandler (ofte Vegdirektoratet) gjelde i tilknytning til gjennomføring av automatisk trafikkontroll.[21]

Som nevnt gjelder unntaket *saker* der rettspleielover får anvendelse. Det er imidlertid ikke alltid trivielt å fastslå hva som er en "sak". Spørsmålet er derfor hva som markerer at det oppstår en "sak" som gjør at rettspleielovene får anvendelse. Utgangspunktet er at personopplysninger knyttet til de aktuelle ts-teknologiene oppstår *utenfor* (tidligere enn) de situasjoner der rettspleielovene gjelder. Årsaken er at alle aktuelle teknologier registrerer og lagrer noe opplysninger uavhengig av om det har skjedd et brudd på trafikkreglene eller ikke.[22] Neste spørsmål blir derfor hva som er skjæringspunktet mellom tilfelle der personopplysningsloven gjelder fullt ut, og de tilfelle der bare deler av loven får anvendelse fordi også rettspleielover gjelder?

Straffeprosessloven (strpl) vil gjelde fra og med tidspunktet da ts-teknologi registrerer en hendelse eller tilstand som gir "rimelig grunn til å undersøke om det foreligger et straffbart forhold …", se politiinstruksen § 7-4 første ledd, jf strpl § 224 første ledd. Det faktum at ts-teknologi registrerer hendelser/tilstander som er ment å være indikasjon på overtredelser av veitrafikkloven mv, må trolig regnes som en slik hendelse. For slike opplysninger gjelder derfor unntakene fra personopplysningsloven trolig fra og med automatisk registrering av et mulig straffbart forhold, for eksempel ved annen gangs fotografering og beregning av fart

[20] Det vil si at spesiell lov går foran generell lov.
[21] Se nærmere om databehandleravtaler i avsnitt 5.4 (nedenfor).
[22] Jeg ser her bort i fra muligheten for å opplysningene til etterforskning av andre lovbrudd enn de som er omfattet av primærformålet, jf avsnitt 4.3.2.

med streknings-ATK. Forutsetningen er imidlertid trolig at en annen enn fører har behandlingsansvaret for opplysningene. Dersom en privatperson har bestemmelsesrett over atferdsregistrator i egen bil, vil en registrering i denne av et straffbart forhold neppe gjøre at unntaket i pof § 1-3 kommer til anvendelse.[23]

Dersom en registrering *ikke* indikerer noe straffbart brudd på vegtrafikkloven, må det tvert i mot antas at personopplysningsloven gjelder fullt ut. Blir slike opplysninger lagret[24] og senere koplet sammen med annen etterforskning, vil unntaket fra personopplysningsloven imidlertid trolig gjelde fra og med tidspunktet for sammenkoplingen med denne etterforskningen.[25]

Når det gjelder tidspunktet for overgangen mellom personopplysningsloven og rettspleielovene, kommer streknings-ATK trolig i en noe annen stilling enn ISA og atferdsregistrator. Årsaken er at streknings-ATK gjelder teknologi som i sin helhet er plassert utenfor det enkelte kjøretøyet. Teknologien kan derfor ikke ordinært rettes mot en bestemt bil eller bilfører. En atferdsregistrator og system for ISA med logging av aktivitet, kan tenkes brukt i etterforskning mot konkrete mistenkte personer, også i saker som ikke gjelder trafikkreglene. Dersom GPS inngår i system for automatisk fartsjustering, kan utstyret for eksempel brukes til teknisk sporing, jf strpl § 202b. I så fall vil det være tale om å anvende et straffeprosessuelt tvangsmiddel som ledd i etterforskning. Unntaket fra personopplysnings-loven vil i så fall trolig gjelde allerede fra aktiviseringen av systemet, dvs før det er registrert noen opplysninger i saken.

3.2.6 Spesielt om privat behandling av personopplysninger

Personopplysningsloven gjelder ikke for "behandling av personopplysninger som den enkelte foretar for rent personlige eller andre private formål", se pol § 3 annet ledd. Elektronisk kjørebok[26] med funksjoner for måling av gjennomsnittsfart (jf. streknings-ATK), vil for eksempel ikke komme inn under loven så lenge bruken er rent personlig eller privat. Dersom formålet både er personlig/privat og *i tillegg* å drive kontroll, veiledning, opplæring mv i regi av en myndighet, bilprodusent, forsikringsselskap eller lignende, vil loven likevel gjelde.

Det er uansett formålet som er avgjørende for om behandlingen kan anses å være privat, og ikke for eksempel om bruken er frivillig eller ei. Vurderingen av formål må skje ut i fra hva som er planlagt og intendert.[27] Andre sporadisk forekommende formål og bruk er neppe avgjørende. For eksempel vil det kunne skje at politiet innhenter data fra private kjørebøker som ledd i etterforskning av kriminalsaker, dvs. når vilkårene for ransaking og beslag er oppfylt.[28] Loven må trolig forstås slik at ransaking og beslag mv av slikt privat utstyr kan skje flere ganger, uten at behandlingen av den grunn mister karakteren av å være "for rent private eller andre personlige formål". Forutsetningen er trolig at tilgangen til opplysninger

[23] Jf. også neste avsnitt.
[24] For streknings-ATK vil lagring være ulovlig dersom det ikke registreres fartsovertredelse. I andre ts-teknologier vil imidlertid lagring ikke nødvendigvis være avhengig av lovovertredelser.
[25] Jf avgjørelsen i Rt. 1990 s 1008, Fotobokskjennelsen.
[26] Dvs systemer i kjøretøy som ved hjelp av GPS, mobilsamband e.l. holder rede på hvor biler oppholder seg, beregner kjørelengde og kjøregodtgjørelse mv. Formålet kan både være effektiv utnyttelse av bilparken i et firma og å skaffe pålitelig dokumentasjon overfor ligningsmyndigheter mv. ABAX og NELFO er eksempler på slike produkter.
[27] Jf pol § 11 første ledd bokstavene b og c.
[28] Se straffeprosessloven kapitlene 15 og 16.

fra den rent personlige/private behandlingen kun er basert på domstolenes prøving i enkeltsaker i samsvar med straffeprosesslovens regler.

Konklusjonen blir trolig motsatt dersom det for eksempel gis hjemmel i vegtrafikkloven e.l. til at politiet har rett til å aksessere slikt privat utstyr som ledd i løpende trafikkontroll, uten rettens kjennelse. Behandlingen av personopplysninger i det private utstyret vil da neppe regnes å skje for *rent* private eller personlige formål, og unntaket fra loven gjelder ikke.[29]

Kommer privat teknologi (kjørebøker, atferdsregistratorer mv), som ikke kan regnes som rent privat/personlig, inn under personopplysningsloven, innebærer det i utgangspunktet at hver privatperson (eiere) *selv* blir behandlingsansvarlig med en rekke plikter etter loven. En slik effekt fremstår som ganske paradoksal fordi de fleste opplysninger kun vil gjelde personen selv, og vil uansett kun omfatte et lite antall andre personer (dvs andre som eventuelt bruker bilen).

Dersom formålet med bruk av privat ts-teknologi helt eller delvis blir lovregulert og det herunder stilles krav til det teknologiske utstyret, må vedkommende myndighet trolig anses å ha behandlingsansvaret for det private utstyret. Årsaken er at lovgiver i så fall har bestemt *formål* for behandlingen av personopplysninger og hvilke *hjelpemidler* som skal nyttes (se nærmere om behandlingsansvaret under avsnitt 4.2).

Generelt innebærer gjennomgangen i dette delavsnittet at ts-teknologi i den enkelte bil som kun brukes for private eller personlige formål, faller utenfor personopplysningslovens virkeområde. Slike hjelpemidler kan imidlertid likevel komme inn under denne lovens virkeområde dersom offentlige myndigheter definerer nye formål for bruken av slikt (eksisterende) utstyr og/eller stiller andre krav til hvorledes utstyret skal virke mv. Slik regulering vil altså kunne innebære at vedkommende myndighet får behandlingsansvaret for personopplysninger som samles inn ved hjelp av privat utstyr i bilene, jf avsnitt 4.2 (nedenfor). Dersom en slik effekt skal unngås, må spørsmålet lovreguleres.

***

I de to neste kapitlene forutsetter jeg at rettspleielovgivning får anvendelse slik jeg har konkludert i avsnitt 3.2.5. I så fall vil følgende bestemmelser i personopplysningsloven i utgangspunktet[30] gjelder for saker som (for øvrig) skal behandles etter rettspleielovene:

- Kapittel II. Alminnelige regler for behandling av personopplysninger
- Kapittel V. Overføring av personopplysninger til utlandet
- Kapittel VI. Melde- og konsesjonsplikt
- Kapittel VII. Fjernsynsovervåking
- Kapittel VIII. Tilsyn og sanksjoner

I tillegg er kapittel I om lovens formål og virkemåte nødvendig for å forstå kapitlene på listen.[31] I det følgende vil jeg drøfte sentrale utvalgte bestemmelser i de nevnte kapitlene.

Bestemmelser i personopplysningsloven som gir individuelle rettigheter mv kommer som nevnt ikke til anvendelse. I stedet vil det kunne gjelde lignende bestemmelser i

[29] Jf dog konklusjonen i avsnitt 3.2.5
[30] Med reservasjon for det som i det enkelte tilfellet måtte følge av pol § 5 og prinsippet om lex specialis.
[31] Kapittel XI og ikrafttreden mv er lite aktuell mer enn åtte år etter lovens ikrafttredelse.

straffeprosessloven mv. Av kapasitetsmessige grunner kommer jeg imidlertid ikke nærmere inn på disse bestemmelsene.

4 Nærmere om den rettslige reguleringen av ts-teknologi

4.1 Oversikt

I dette kapittelet vil jeg gjennomgå hovedtrekkene i hvorledes dagens rettslige regulering av personvern vil virke på streknings-ATK, ISA og atferdsregistrator. Drøftelsene er basert på bestemte antakelser om teknologiutforming, organisering mv som jeg vil presentere under veis. I noen grad vil jeg også drøfte alternative forutsetninger.

Drøftelsen vil skje ut i fra den generelle fortolkningen av personopplysningsforskriften § 1-3 som jeg har redegjort for i avsnitt 3.2.5. Dette innebærer at deler av personopplysningsloven ikke kommer til anvendelse når brudd på vegtrafikkloven er registrert, og ellers når behandlingen av personopplysninger kommer inn under straffeprosesslovens bestemmelser. Til grunn for fremstillingen ligger et sjablonmessig skille mellom bestemmelser i personopplysningsloven som normalt kommer til anvendelse uansett om straffeprosessloven og andre rettspleielover kommer til anvendelse eller ikke, og slike bestemmelser som normalt ikke kommer til anvendelse når rettspleielover gjelder. Bare først nevnte kategori bestemmelser vil bli drøftet på inngående måte i forhold til de tre ts-teknologiene (avsnittene 4.2 - 4.6). Jeg drøfter ikke hvordan *rettspleielovene* kan komme til anvendelse i tilknytning til etterforskning og iretteføring av saker når data fra de aktuelle ts-teknologiene inngår.

4.2 Ansvar for behandling av personopplysninger ved hjelp av ts-teknologi

4.2.1 Innledning

Personopplysningsloven stiller bestemte krav til organisering av aktiviteter som innebærer behandling av personopplysninger, herunder personopplysninger knyttet til ts-teknologi. Det viktigste spørsmålet er å klargjøre hvem som har det overordnede ansvaret etter loven, dvs hvem som har *behandlingsansvaret* for personopplysningene.[32] Det er denne aktøren som har plikter etter loven og som registrerte personer og andre[33] i stor grad må henvende seg til for å få brukt rettigheter loven gir dem.

Ikke sjelden vil behandling av personopplysninger involvere arbeid eller utstyr mv som den behandlingsansvarlige ikke selv rår over, og som kan skape behov for å gi oppdrag til aktører utenfor egen organisasjon. Slike eksterne aktører med oppdrag for den behandlingsansvarlige er "databehandlere". Også databehandlere har selvstendige plikter etter loven, men er primært underlagt vilkår i avtale med den behandlingsansvarlige som oppdragsgiver. Identifiseringen av slike databehandlere er viktig for behandlingsansvarliges styring over behandling av personopplysninger som er satt bort til andre.

Personopplysningsloven med forskrifter inneholder både eksplisitte og implisitte organisatoriske krav som jeg ikke kommer nærmere inn på her. Dette gjelder særlig organisering av arbeidet med informasjonssikkerhet etter personopplysningsforskriftens (pof) kapittel 2. Slike krav må være med dersom en skal gjøre konkrete vurderinger av hvorledes bruk av ts-teknologi bør organiseres.

---

[32] Jf pol § 2 nr 4.

[33] Loven gir både rettigheter for alle registrerte, for registrerte i visse partslignende situasjoner og for enhver, se personopplysningsloven § 18 første ledd (innsyn for enhver) og § 21 (varsling om personprofiler).

4.2.2 Behandlingsansvarlig

4.2.2.1 Den grunnleggende vurderingen av hvor ansvaret skal plasseres

"Behandlingsansvarlig" betegner den aktøren som primært har plikter etter personopplysningsloven, og er definert som "den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes". Ts-teknologi kan i utgangspunktet tenkes anvendt av flere aktører; særlig veimyndigheter, politi, bilprodusenter og forsikringsselskaper. Bilprodusenter ønsker for eksempel å innhente personopplysninger fra atferdsregistratorer. Hensikten kan for eksempel være å bruke opplysningene til produktutvikling. På lignende måte kan en tenke seg at forsikringsselskaper innhenter opplysninger på grunnlag av forsikringsavtalen.

For å gi sikre svar på spørsmålet om plasseringen av behandlingsansvar, må en minst drøfte fire spørsmål. De to første spørsmålene fremgår direkte av lovens definisjon av behandlingsansvarlig (jf ovenfor). De to neste spørsmålene er kriterier som er oppstilt i juridisk litteratur, og er i stor grad basert på den underliggende hierarkiske tenkningen i personopplysningslovgivningen:[34]

- Hvem bestemmer *formålet* med behandlingen av personopplysninger?
- Hvem bestemmer hvilke *hjelpemidler* en skal gjøre bruk av når personopplysningene behandles?
- Hvem har øverste *instruksjons og organisasjonsmyndighet* i spørsmål vedrørende behandlingen av personopplysninger?
- Hvem har *søksmålskompetanse* etter tvisteloven?
- Andre momenter

De fire spørsmålene glir langt på vei over i hverandre. De to første spørsmålene tar tak i *hva* det skal bestemmes over (formål, hjelpemidler), mens de to neste spørsmålene gjelder formelle posisjoner i hierarkiske organisasjoner (f.eks. i offentlig forvaltning). I dette og neste avsnitt vil jeg primært behandle de to spørsmålene/kriteriene som følger direkte av loven. De to siste kriteriene vil i første rekke bli brukt for å plassere behandlingsansvaret på riktig *nivå* i et organisasjons-/forvaltningshierarki (se avsnitt 4.2.2.3).

Når det spørres etter *hvem* den behandlingsansvarlige er, er utgangspunktet at dette både kan være fysiske personer (i seg selv), og en virksomhet/organisasjon (representert ved en fysisk person). Innen offentlig sektor vil det i denne sammenhengen bare være spørsmål om hvilken virksomhet (departement, direktorat mv) som er behandlingsansvarlig. Fysiske personer vil derfor være uaktuelle som behandlingsansvarlige i slike forvaltningsorganisasjoner. Den behandlingsansvarlige organisasjonen vil imidlertid være representert ved en person som er øverste leder i virksomheten. Dersom virksomheten har et kollegialt organ som øverste ledelse (for eksempel et styre), vil behandlingsansvaret plasseres i styret ved styreleder. Uten et styre eller lignende vil det være direktøren som representerer den behandlingsansvarlige.

<u>Formål</u>

Plasseringen av behandlingsansvar er som nevnt bl.a. avhengig av hvem som kan bestemme over formålet med innsamling og videre bruk av personopplysningene. Bestemmelsesretten over formålet gjelder retten til å bestemme hva personopplysningene kan brukes til. I

[34] Se Coll og Lenth 2000 s 33 flg. og Schartum og Bygrave 2006 s 28 flg.

offentlig sektor kan slike formål delvis være politisk bestemt i lovgivning, budsjettvedtak eller på annen måte. Dette innebærer imidlertid neppe at den politiske ledelsen eller lovgiver av den grunn blir behandlingsansvarlig. Når politiske vedtak skal gjennomføres, vil vedkommende offentlige myndighet måtte gjøre en selvstendig vurdering og presiseringer av spørsmålet om formålet med behandlingen. Det kan for eksempel være aktuelt å definere flere formål for samme behandling,[35] og formålene må uansett være gjenstand for videre vurdering mht de rettsforholdene formålet har direkte betydning for. Dette gjelder særlig saklighetsvurderingen mv etter pol § 11 første ledd bokstav b,[36] spørsmål om eventuelt endret formål (bokstav c i samme bestemmelse), vurderingen av opplysningskvalitet relatert til formålet (pol § 11 første ledd bokstavene d og e), og bestemmelse av krav til sletting fordi formålet ikke lenger tilsier lagring (pol § 28). Selv om formålet i utgangspunktet er politisk bestemt, vil bestemmelsesretten over formål etter personopplysningsloven altså ligge til den forvaltningsorganisasjon som skal sette vedtaket ut i livet.[37] Ofte vil dette være "departementet", som samtidig gis myndighet til å fastsette forskrifter/nærmere regler.

Hjelpemidler

Også bestemmelsesrett over hjelpemidler er avgjørende for plasseringen av behandlingsansvaret. Med hjelpemidler må en trolig forstå omtrent det samme som "virkemiddel", dvs innsatsfaktorer som anvendes for å realisere formålet med behandlingen. En må trolig også inkludere hjelpemidler som anvendes for å sikre at behandlingen er lovlig, jf pol § 14 om internkontroll. Hjelpemidler er med andre ord ikke bare fysiske gjenstander og programvare, men kan også være kursvirksomhet, utferdigelse av interne regelverk, tilsetting av personer med særlig personvernkompetanse mv. Også når det gjelder bestemmelsesretten over hjelpemidler kan det oppstå spørsmål om hvem det egentlig siktes til. Riktignok vil det være sjelden at politiske myndigheter fastsetter hjelpemidler på annen måte enn at det blir bevilget penger til nødvendig systemutvikling mv. Særlig når det gjelder maskin- og programvare mv vil imidlertid eksterne leverandører og konsulentfirmaer mv spille en sentral rolle mht valg og nærmere utforming av hjelpemidlene. Selv om andre enn forvaltningen har stor innflytelse på valg av hjelpemidler, vil det avgjørende være hvem som formelt har beslutningskompetanse på området, og denne vil normalt ligge hos forvaltningsmyndigheten som kjøper/oppdragsgiver.

Det fremgår av det som er nevnt ovenfor at det avgjørende ved plasseringen av behandlingsansvaret i utgangspunktet er hvem som *formelt sett* har kompetanse til å bestemme. At andre faktisk utøver bestemmelsesretten fordi den med formell kompetanse ikke er klar over den, eller av andre grunner ikke bruker den, spiller neppe noen avgjørende rolle. En annen løsning ville jo innebære at en kunne komme unna de rettsplikter behandlingsansvaret innebærer ved å forholde seg passiv til lovens krav.

Andre momenter

I tillegg til de kriterier som følger direkte av loven (formål, hjelpemidler) eller som følger av den systematikk som loven er bygget på (instruksjonsmyndighet, søksmålskompetanse), kan det selvsagt være konkrete forhold knyttet til utøvelsen av behandlingsansvaret som kan tenkes å bli tillagt en viss vekt dersom det er sterk tvil om hvor behandlingsansvaret skal plasseres. Dersom for eksempel Politidirektoratet og Vegdirektoratet samarbeider om

[35] For eksempel å bruke opplysningene til å generere ulike former for statistikk og styringsinformasjon.
[36] Kravet om at formålet må være saklig begrunnet i den behandlingsansvarliges (for eksempel forvaltningsorganets) virksomhet.
[37] En annen ting er at det kan gjøres gjeldende politisk ansvar dersom forvaltningen gjør grove feil når de utøver behandlingsansvaret, med dette kommer jeg ikke nærmere inn på her.

etablering av ts-teknologi og det er uklart hvem av dem som skal regnes som behandlingsansvarlig, kan det for eksempel være relevant å spørre hvem som tok initiativ til at behandlingen av personopplysninger startet. Et annet mulig relevant spørsmål vil være hvilke av direktoratene som har best faglige, økonomiske mv forutsetninger for å ivareta behandlingsansvaret. Dette siste momentet kan særlig ha relevans og vekt fordi svaret kan ha stor betydning for hvor godt formålet med personopplysningsloven kan bli realisert, jf pol § 1.

4.2.2.2 Delt behandlingsansvar

Til nå har jeg basert fremstillingen av behandlingsansvar på forutsetningen om at kun én aktør er behandlingsansvarlig. Personopplysningsloven regulerer bare slike tilfelle direkte, men er likevel ikke til hinder for at behandlingsansvaret er delt mellom to eller flere aktører, for eksempel mellom Vegdirektoratet og Politidirektoratet. Deling av ansvaret kan både tenkes "horisontalt" og "vertikalt".

Med vertikal deling sikter jeg til tilfelle der ansvaret er delt slik at to eller flere behandlingsansvarlige har alt ansvar for hver sine *deler* av en behandling. Dersom det for eksempel skjer streknings-ATK, kan det tenkes at en behandlingsansvarlig har ansvar for registrering av fartsdata, mens en annen har behandlingsansvar for den videre behandlingen av registrerte fartsovertredelser. Forutsetningen for en slik deling må være at hver aktør har en reell bestemmelsesrett over formål, hjelpemidler mv vedrørende hver sin del, uten at den ene kan instruere den andre.

Med horisontal deling, sikter jeg til tilfelle der hver av to eller flere behandlingsansvarlige har ansvar for hver sine *gjennomgående aspekter* ved behandlingen av personopplysninger. Dette kan tenkes gjort på ulike måter; for eksempel slik at en aktør har behandlingsansvaret for all telekommunikasjon mens en annen aktør har ansvar for den resterende behandlingen. På tilsvarende måte kan det tenkes en deling av ansvaret slik at bildebehandling, spesielle typer analyser av data mv var underlagt en egen behandlingsansvarlig. Horisontal deling av ansvar vil imidlertid neppe kunne skje på en hvilken som helst måte. Derfor må det kreves at delingen skjer på måter som er tjenlige ut i fra formålet med loven (jf pol § 1). Noen typer horisontal deling av ansvaret kan motvirke effektiv etterlevelse av personopplysningsloven, og vil derfor neppe kunne godtas. Det kan for eksempel neppe aksepteres at en aktør har behandlingsansvaret informasjonskvalitet, mens en annen har ansvar for sletting og retting mv. Årsaken er at slike ansvarsområder er så sentrale og integrerte at en oppsplitting ikke vil være formålstjenlig.

Den tredje muligheten for deling som trolig kan være av praktisk betydning, er tilfelle der flere aktører behandler hver sine personopplysninger ved hjelp av samme utstyr ("diagonal deling"). Et tankeeksperiment kan for eksempel være at atferdsregistratorer både leverer data til Vegmyndighetene og forsikringsselskaper. Datasettene/personopplysningene kunne med andre ord tenkes å være separate/ulike, samtidig som begge sett opplysninger blir behandlet ved hjelp av samme utstyr (atferdsregistratoren). I så fall vil det være to eller flere behandlingsansvarlige som sammen må bestemme over hjelpemidlene, samtidig som de har hver sine formål med å behandle personopplysninger.[38]

Uansett hvorledes deling skjer, er en forutsetning for delingen at denne ikke etterlater særlig tvil om hvorledes ansvaret er plassert. Det må dessuten forutsettes at delingen er

[38] Jf kriteriene hjelpemidler og formål i pol § 2 nr 4. som definerer behandlingsansvar. Felles *formål* kan alene neppe begrunne noe felles behandlingsansvar.

formålstjenlig sammenholdt med pol § 1. I tillegg må det trolig kreves at det tydelig fremgår hvorledes ansvaret er delt, jf flere bestemmelser i personopplysningsloven som forutsettes at denne opplysningen skal fremkomme.[39] Det er flere mulige måter å skape slik klarhet på. Mest nærliggende er imidlertid å avtaleregulere forholdet, jf pol § 15 og kravet til avtaleregulering mellom behandlingsansvarlig og databehandlere.

En annen forutsetning er trolig at behandlingsansvaret deles i samsvar med hver forvaltningsaktørs kompetanse til å utøve offentlig myndighet. Politiet har for eksempel kompetanse til å avdekke og straffeforfølge brudd på vegtrafikkloven. Da bør de fortrinnsvis ha behandlingsansvar for de personopplysninger de trenger i den sammenhengen. Ansvaret bør for eksempel ikke deles slik at vegmyndighetene har behandlingsansvar for fartsmålinger som politiet bruker for å etterforske overtredelser.

Ved planlegging av ny ts-teknologi der slike spørsmål kan bli aktualisert, er det viktig å avklare disse ansvarsspørsmålene så tidlig som mulig. Dette kan åpenbart skje på flere måter, og her vil jeg peke på tre fremgangsmåter som er særlig aktuelle:

1. Det kan innhentes råd og uttalelse fra eksperthold; enten fra uavhengig hold (advokater mv) eller fra Datatilsynet. Datatilsynets råd vil i slike situasjoner være basert på den rettsforståelse de legger til grunn som ledd i sin myndighetsutøvelse, og slike synspunkt kan derfor gi merverdi fordi det skaper forutberegnelighet. På den annen side er personopplysningslovens bestemmelser til dels svært vurderingspregede, noe som innebærer mulighet for at ulike kompetente organer kan trekke ulike konklusjoner. I løpet av de første ti årene av Personvernnemndas virke, har derfor nesten 50 % av Datatilsynets vedtak som er klaget inn for nemnda helt eller delvis blitt omgjort.[40] Slik faglig uenighet vil være særlig aktuelt i vanskelige spørsmål, som for eksempel i spørsmål om behandlingsansvar.

2. I samband med introduksjon av ny ts-teknologi kan det være aktuelt å lov- eller forskriftsregulere spørsmålet om behandlingsansvar. Dette kan for eksempel skje for å avklare tvil som oppstår etter at lovens generelle kriterier mv har vært anvendt på tilfellet. En lov- eller forskriftsregulering kan imidlertid også tenkes å plassere behandlingsansvar et annet sted enn det som kunne ha fulgt av lovens definisjon av behandlingsansvarlig. En kan for eksempel tenke seg at ansvaret i særlovgivning ble lagt til et direktorat direkte, og ikke til vedkommende departement.

3. Som en mellomløsning kan det være hensiktsmessig å gi uttalelser i forarbeidene til lov- og/eller forskriftsbestemmelser som aktualiserer spørsmålet om behandlingsansvar. Forutsetningen er da at uttalelsen tar utgangspunkt i hva som må anses å være en rimelig fortolkning av personopplysningslovens alminnelige regler om behandlingsansvar. En slik fremgangsmåte vil kunne innebære at spørsmålet også ble gjort til gjenstand for offentlig høring, noe som kan gi forarbeidene relativt stor vekt ved senere fortolkning av spørsmålet.

I drøftelsene foran har jeg forutsatt at behandlingsansvaret deles mellom to eller flere myndigheter eller private organisasjoner. Det er imidlertid også mulig å tenke seg delt behandlingsansvar mellom en myndighet og hver enkelt *eier* av kjøretøy med utstyr som behandler personopplysninger for trafikksikkerhetsformål. Behandlingsansvaret forutsetter stor grad av bestemmelsesrett. For å ha behandlingsansvar må den enkelte bileier derfor kunne bestemme formålet med å behandle opplysningene fra atferdsregistrator i kjøretøyet, og

[39] Se for eksempel pol §§ 18 første ledd bokstav a, 19 første ledd bokstav a og 32 første ledd bokstav a.
[40] Omgjøringsprosenten har visstnok gått ned de siste årene.

hva slags hjelpemidler som skal benyttes. Vedkommende må med andre ord både kunne velge teknologi og medhjelpere (verksted mv). Dersom eiers rett til å bestemme begrenses gjennom påbud i lov mv, kan det være at behandlingsansvaret helt eller delvis må anses å ha gått over på vedkommende myndighet.

Etter min mening vil det være en klar fordel dersom spørsmålet om behandlingsansvar vedrørende ts-teknologi ble avklaret direkte i lov- eller forskriftsbestemmelse. Eventuelt kan problemet løses ved hjelp av klare uttalelser i forarbeider til slike regelverk. Det finnes uansett neppe noen fornuftig grunn til at det skal eksistere tvil om spørsmålet.

4.2.2.3 Behandlingsansvar og forholdet mellom de ulike nivåene i et forvaltningshierarki

Er det en organisasjon som har behandlingsansvaret, blir neste spørsmål på hvilket *organisasjonsnivå* ansvaret skal plasseres. I organisasjoner som står i et hierarkisk forhold til hverandre, vil spørsmål vedrørende instruksjonsmyndighet ofte være avgjørende. Den organisasjonen med øverste instruksjonsmyndighet i spørsmålet om behandling av personopplysninger vil normalt være behandlingsansvarlig. Kan et departement instruere et direktorat om hvorledes behandlingen av personopplysninger kan skje, er det departementet som har behandlingsansvaret.

De fleste organisatoriske enheter innen statlig forvaltning er hierarkisk plassert under et departement[41]. Under departementer er det bl.a. lagt direktorater, eventuelt med tilhørende statlig lokalforvaltning. Spørsmålet oppstår om det er departementet som normalt er behandlingsansvarlig for behandling av personopplysninger i staten, eller om ansvaret må plasseres lengre ned i hierarkiet? I det følgende bruker jeg Statens vegvesen som eksempel.

Statens vegvesen er underlagt Samferdselsdepartementet, og er i hvert fall i utgangspunktet fullt ut underlagt departementets instruksjonsmyndighet. Etaten består av Vegdirektoratet, fem regionvegkontor og 30 distriktsvegkontor. Det er gitt Instruks for Statens vegvesen,[42] som gir organisasjonsmessige og politiske rammer for etatens virksomhet.[43] Vegdirektoratet under ledelse av vegdirektøren er øverste myndighet for etaten. Direktøren har vide organisatoriske fullmakter til å styre etaten (§ 2-1), og er tildelt vidt ansvar, bl.a. for at etaten etterlever gjeldende rammebetingelser (lov, forskrift, avtaleverk m.m.).[44] Vegdirektoratet ved vegdirektøren er derfor bl.a. ved instruks tildelt ansvar for at etaten etterlever personopplysningsloven. Dette betyr imidlertid ikke uten videre at direktoratet dermed er behandlingsansvarlig etter personopplysningsloven.

Selv om Vegdirektøren kan delegere og instruere underliggende etat (jf instruksen § 2-3 annet ledd), er han samtidig underlagt departementet, og skal "følge opp beslutninger og styringssignaler fra overordnet myndighet", jf § 2-3 første ledd. Dette kan konkret trekke i retning av at det er departementet, og ikke direktoratet, som må regnes som behandlingsansvarlig, selv om det er direktoratet som utfører de tilknyttede oppgavene.

---

[41] Enkelte statlige organer, for eksempel tilsyn, er ikke underlagt noe departement i saker som gjelder myndighetsutøvelse.

[42] Fastsatt ved kongelig resolusjon av 27. mai 2005, og tilgjengelig fra http://www.regjeringen.no/nb/dep/sd/dep/underliggende-etater/Statens-vegvesen.html?id=443412

[43] Samferdselsdepartementet har i kongelig resolusjon av 27. mai 2005 § 4 fått delegert myndighet til å fastsette ny instruks. Ny eller endret instruks behøver således ikke vedtas av Kongen i statsråd.

[44] Se instruksens 2-2 første ledd, bokstav b.

Bruk av den øverste instruksjons- og delegasjonsmyndigheten som kriterium gjør at en i statlig forvaltning finner det rette nivået ved å begynne på toppen av hierarkiet og spørre om dette nivået har instruksjonsmyndighet vedrørende den konkrete behandlingen av personopplysninger. Dersom vedkommende departement har instruksjons-/organisasjonsmyndighet i saken, er det departementet som normalt er behandlingsansvarlig. Mangler departementet slik myndighet, vil det være et underliggende direktorat som er behandlingsansvarlig.

Formelt blir behandlingsansvaret knyttet til vedkommende organisasjons øverste leder. Behandlingsansvaret i en forvaltningsorganisasjon vil med andre ord kunne knyttes til departementsråden, direktøren eller en styreleder.

Et siste spørsmål som kan kaste lys over spørsmålet om den hierarkiske plasseringen av behandlingsansvaret gjelder sivilprosessuell partsevne. Behandlingsansvaret må normalt plasseres slik at personer som krenkes på grunn av eventuelle lovbrudd kan saksøke den behandlingsansvarlige. Særlovgivning kan plassere partsevnen hos en annen del av forvaltningen enn det som følger av tvisteloven.[45] Ansvaret etter personopplysningsloven bør imidlertid fortrinnsvis plasseres i den organisasjonen som må saksøkes dersom det skjer feil.

4.2.2.4 Forholdet innen det forvaltningsorgan som skal utøve behandlingsansvaret

Det kan tenkes at et behandlingsansvarlig departement eller direktorat har delegasjonsadgang, dvs. kan delegere ansvar til en underliggende organisasjon. Slik delegasjon innebærer imidlertid ikke at det grunnleggende behandlingsansvaret for det delegerende departementet blir redusert. Departementet må fremdeles sikre forsvarlig utøvelse av ansvaret sitt ved å følge med og eventuelt instruere den tildelegerte myndigheten. I ytterste fall må delegasjonen trekkes tilbake slik at behandlingsansvaret blir utøvet direkte av departementet.

Den forvaltningsmyndigheten som har det primære behandlingsansvaret eller som har fått tildelegert ansvaret fra overordnet myndighet, har i utgangspunktet organisasjonsmyndighet. De kan derfor selv ta stilling til hvorledes det daglige arbeidet med behandlingsansvarliges oppgaver skal organiseres. Samtidig har de en plikt til å organisere arbeidet slik at behandlingsansvaret blir utøvet på effektiv måte. Med dette utgangspunktet er det imidlertid to viktige presiseringer som må gjøres: For det første kan det være gitt organisatoriske og andre føringer da behandlingsansvaret ble delegert. Departementet har for eksempel delegert til et direktorat og samtidig bestemt noe om hvorledes direktoratet skal organisere arbeidet sitt. I så fall innskrenkes direktoratets organisasjonsmyndighet tilsvarende. For det andre er det gitt flere organisatoriske bestemmelser i personopplysningsloven med forskrifter. Slike bestemmelser innebærer selvsagt en tilsvarende innskrenking av organisasjonsmyndigheten. Her skal jeg gi en oversikt over sist nevnte bestemmelser.

De rettslige kravene til organiseringen av behandlingsansvaret bygger på forutsetningen om at det for hver behandling av personopplysninger alltid skal være utpekt én eller flere *daglig ansvarlige* personer. Ingen bestemmelse i personopplysningsloven gir direkte bestemmelse om plikt til å utnevne slik person, men rollen fremkommer klart i flere bestemmelser. For det første er "Hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter" blant de opplysninger enhver har innsynsrett i forhold til, jf § 18 første ledd bokstav b. Nøyaktig samme opplysning skal meldes til Datatilsynet i henhold til § 32 første ledd

[45] Jf § 2-1 (1) bokstav f.

bokstav c. Meldinger skal sendes Datatilsynet minst 30 dager før behandlingen begynner (jf § 31 annet ledd). Lovgivers forutsetning er derfor at denne delen av organiseringen skal være klar før personopplysningene tas i bruk. Så lenge den øverste lederen i den behandlingsansvarliges organisasjon ikke selv makter å følge med på hvordan behandling av opplysninger skjer, eksisterer det derfor en plikt til å delegere dette ansvaret. Sagt med andre ord, må det alltid være en person med reell mulighet til å følge med på den daglige behandlingen av personopplysninger.

I offentlig forvaltning vil størrelsen på organisasjonen ofte være slik at rollen som daglig ansvarlig må plasseres på mellomledernivå eller lavere for å komme nær nok de faktiske forholdene. Loven stiller imidlertid ingen detaljerte krav til organisatorisk plassering. Loven sier heller ingen ting om hvor mange daglig ansvarlige det kan være i en organisasjon. Utgangspunktet er at valgfriheten er stor. Den behandlingsansvarlige kan oppnevne flere daglig ansvarlige i egen organisasjon, for eksempel en ansvarlig for hver type behandling (en for streknings-ATK, en for ISA, en for atferdsregistrering mv). En og samme person kan også være daglig ansvarlig for flere behandlinger, og det er heller ingen formelle hindringer mot at det er flere daglig ansvarlige personer for hver behandling, så lenge ansvarsforholdet mellom dem er klart definert.

Et annet krav til organisering av behandlingsansvaret gjelder arbeidet med informasjonssikkerhet i tilknytning til elektronisk behandling[46] av personopplysninger. Ansvaret for sikkerheten er knyttet til "daglig ledelse",[47] noe som i praksis må innebære at daglig leder (departementsråd, direktør for direktorat mv) har ansvaret.[48] I tillegg er det antydet enkelte andre organisatoriske krav, bl.a. vedrørende sikkerhetsrevisjon, jf pof § 2-5. Det er også i samband med unntak for meldeplikt etter pol § 31 gitt muligheter for å få godkjent et personvernombud, jf pof § 7-12. Jeg kommer imidlertid ikke her inn på forholdet mellom slike ombud, personer med daglig ansvar og andre organisatoriske roller.[49]

4.2.3 Om bruk av databehandlere

Under utvikling og drift av ts-teknologi kan det være behov å sette bort arbeid til aktører utenfor den behandlingsansvarliges organisasjon. For eksempel kan Politidirektoratet inngå avtale med en annen offentlig virksomhet eller et privat firma om teknisk drift av streknings-ATK. Skal behandlingen helt eller delvis skje ved hjelp av en slik databehandler, gjelder det spesielle regler.

Databehandler er alltid utenfor den behandlingsansvarliges egen organisasjon. Derfor kan ikke databehandlere instrueres men må styres gjennom avtale, jf pol § 2 nr 5. Databehandler kan være en enkeltperson, men vil ofte være en organisasjon. Behandlingsansvarlig er med andre ord oppdragsgiver og databehandler oppdragstaker i et avtaleforhold som går ut på å behandle personopplysninger. Dersom all behandling av personopplysninger skjer i regi av behandlingsansvarliges organisasjon, er det med andre ord ingen som får rollen som "databehandler" etter personopplysningsloven. Dette gjelder selv om den interne organiseringen er basert på internfakturering og kontraktslignende styringsmekanismer. Så lenge ledelsen har en mulighet til å styre behandling av personopplysninger gjennom

[46] Jf personopplysningsforskriften § 2-7.
[47] Jf personopplysningsforskriften § 2-3.
[48] Også dette ansvaret kan delegeres, jf ovenfor.
[49] Organisatoriske krav til sikring av personopplysninger er behandlet i Schartum 2005.

instruksjon mv, er den som instrueres trolig ikke databehandler, men en del av den behandlingsansvarliges egen organisasjon.

Dersom oppdrag gis til en databehandler, skal det etter pol § 15 inngås skriftlig avtale med denne. Det er databehandleravtalen som er det rettslige grunnlaget for databehandlers tilgang til og behandling av personopplysningene. Uten slik avtale er derfor databehandlers befatning med personopplysninger ulovlig.

Databehandleravtalen skal særlig inneholde to elementer. For det første skal det være uttømmende avtalt hva databehandler kan gjøre med personopplysningene. Databehandler kan med andre ord bare foreta slike bearbeidelser og analyser mv av personopplysninger fra ts-teknologi når dette fremgår av avtalen med behandlingsansvarlige. Avtalen bør beskrive omfanget av databehandlers tilgang til personopplysninger og de nærmere fremgangsmåter som skal følges.

Avtalen skal for det andre inneholde bestemmelse om databehandlers selvstendige ansvar for informasjonssikkerhet. Dette ansvaret fremgår direkte av pol § 13 første ledd. Avtalen understreker derved lovens ansvarsregel. Herunder skal avtalen angi hvorledes forholdet mellom behandlingsansvarliges og databehandlers arbeid med informasjonssikkerhet skal være. Loven må forstås slik at behandlingsansvarlige har primæransvar for sikkerheten, i den betydning at vedkommende har den øverste sikkerhetsledelsen. Behandlingsansvarlige bør derfor vurdere om det skal gis nærmere bestemmelser om informasjonssikkerhet i avtalen med databehandler, dvs. slike rammer og minstekrav som behandlingsansvarlig antar er påkrevet for at informasjonssikkerheten skal bli tilfredsstillende. Databehandlers selvstendige ansvar for informasjonssikkerhet kommer til syne ved at han plikter å sørge for tilfredsstillende sikkerhet uavhengig av om behandlingsansvarlig har etablert særlige sikkerhetskrav i avtalen.

Loven forutsetter bare databehandleravtaler direkte mellom behandlingsansvarlige og en eller flere databehandlere. Den er trolig til hinder for at databehandler gjør avtaler med underleverandører om at de (også) skal være databehandler. Loven synes med andre ord å forutsette at behandlingsansvarlig skal være direkte avtalepart i alle avtaler med databehandlere. I motsatt fall ville behandlingsansvarlig lett miste kontroll med hva som faktisk skjer med de personopplysninger han har overført til en databehandler. Er det behov for flere samarbeidende databehandlere, kan en praktisk løsning være å inngå en felles avtale mellom behandlingsansvarlig og databehandlere.

Databehandleroppgaver kan selvsagt deles, dvs. den behandlingsansvarlige kan inngå avtale med flere databehandlere innen ulike deler av oppgaveløsningen. I nære samarbeidsforhold mellom to etater kan det også oppstå situasjoner der hver etat både blir delvis behandlingsansvarlig og delvis databehandler. En kan for eksempel tenke seg at forvaltningsorganene A og B har behandlingsansvar for hver sin del av behandlingen, samtidig som de fyller rollen som databehandler for hverandre på områder der de ikke har behandlingsansvar.

4.3 Grunnkrav til behandling av opplysninger

4.3.1 Krav til rettslig grunnlag for behandling av personopplysninger

Grunnkrav til behandling av personopplysninger er slike krav som enhver behandlingsansvarlig må tilfredsstille før behandlingen igangsettes. I motsatt fall vil behandlingen være ulovlig. Grunnkravene gjelder krav til rettslig grunnlag (§§ 8 og 9), krav til fastsettelse av formål (§ 11 første ledd bokstavene b og c) og krav til opplysningskvalitet (§ 11 første ledd bokstavene d og e, jf § 27).

Kravet om rettslig grunnlag innebærer at det skal eksistere et samtykke, en lovhjemmel eller en nødvendig grunn som angitt i personopplysningsloven. De alminnelige bestemmelsene om rettslig grunnlag finnes i pol § 8, mens § 9 inneholder særlige regler om rettslig grunnlag for sensitive personopplysninger, jf avsnitt 4.5.2. Jeg forutsetter at de aktuelle ts-teknologiene har kontrollformål og derfor har betydning for mulige reaksjoner i form av straff, erstatningsplikt mv, dvs. bruken av teknologien kan gi negative konsekvenser for førere og/eller eiere av kjøretøyene. Det er da upraktisk å tenke seg at behandling av personopplysninger knyttet til slik teknologi kan være basert på samtykke fra de aktuelle personene. Behandlingen av personopplysningene må derfor være basert på lovhjemmel eller en av de "nødvendige grunner" som er angitt i pol §§ 8 og 9. Det er flere nødvendige grunner som kan tenkes brukt som begrunnelse for behandling av personopplysninger for trafikksikringsformål, og § 8 bokstav e ("nødvendig for å utøve offentlig myndighet") er mest aktuell.

Behandlingen må forutsettes å innebære en (i perioder) konstant overvåking av trafikk og registrering av overtredelser med tilhørende etterforskning og iretteføring Det er derfor grunn til å legge stor vekt på legalitetsprinsippet og behovet for en klar og sterk rettslig basis for tiltaket. Ut i fra et hensynet til personvern- og rettssikkerhet vil egen lovhjemmel for behandling av personopplysninger i tilknytning til ts-teknologi være klart å foretrekke.[50] Et så alvorlig inngrep i personvernet som vid og massiv innsamling av personopplysninger er, gjør at et demokratisk fattet vedtak bør velges som grunnlag for krenkelsen. Vedtakelse av lovhjemmel for bruk av ts-teknologi legger dessuten til rette for en videre lovregulering av tiltaket (krav til framgangsmåter mv), noe både personvern- og rettssikkerhetshensyn kan begrunne.

4.3.2 Krav til fastsettelse av formål for behandling av personopplysninger

Det skal alltid fastsettes ett eller flere bestemte formål for behandlingen av personopplysninger, og dette/disse skal være saklig begrunnet ut i fra den behandlingsansvarliges virksomhet.[51] Fastsettelse av formål har særlig betydning i tre sammenhenger. For det første utgjør formålet en begrensning for hva opplysningene kan brukes til. Det er ikke angitt hvordan formålet skal angis, for eksempel hvor generelt det kan være. For det andre er det derfor viktig å være klar over betydning for kravene til opplysningskvalitet av hvilke(t) formål som er angitt.[52] Slike krav (til oppdatering, korrekthet, fullstendighet mv) skal alltid vurderes ut i fra formålet/formålene med behandlingen. Et vidt formulert formål vil derfor kunne gi strengere og dyrere krav til ivaretakelse av kvalitet enn snevre formålsangivelser gjør. For det tredje har formålet

[50] Se nærmere om dette i avsnitt 7.3.
[51] Se pol § 11 første ledd bokstav b.
[52] Jf. pol § 11 første ledd bokstav e.

betydning for hvor lenge personopplysningene kan beholdes før de må slettes etter pol § 28. Dette kan begrunne vidt angitte formål på områder der eldre opplysninger kan få ny og aktuell betydning for eksempel i tilknytning til etterforskning.

Fastsettelse av formål i tilknytning til ts-teknologi, vil trolig variere avhengig av hvem som er behandlingsansvarlig. Dersom Politidirektoratet er behandlingsansvarlig kan formålet for eksempel være knyttet til forebyggelse, avverging eller etterforskning av straffbare handlinger. Det kan vanskelig tenkes andre formål med innsamling av personopplysninger ved hjelp av ts-teknologi som er saklig begrunnet ut i fra Politidirektoratets virksomhet. Dersom Vegdirektoratet er behandlingsansvarlig kan det tenkes flere formål vedrørende trafikksikkerhet, trafikkavvikling mv. Vegdirektoratet har imidlertid neppe saklig grunnlag i sin virksomhet til å definere straffeforfølging blant sine formål for å behandle personopplysninger i tilknytning til ts-teknologi. Dersom Vegdirektoratet er behandlingsansvarlig og bruken av opplysningene er knyttet til deres formål, vil det i utgangspunktet være ulovlig å benytte opplysningene for andre formål enn de Vegdirektoratet har definert. I forhold til politiet vil likevel opplysningene kunne innhentes som ledd i etterforskning i konkrete saker i samsvar med reglene i straffeprosessloven. For eksempel kan politiet på nærmere bestemte vilkår ta beslag i medhold av bestemmelsene i straffeprosessloven kapittel 16.

Formålet med innsamling av personopplysninger ved hjelp av ts-teknologi, vil primært være å forebygge og avdekke brudd på regler i veitrafikkloven. Som nevnt kan en videre politimessig bruk imidlertid alltid være aktuell. ISA basert på GPS, vil for eksempel kunne gi vid kartlegging av bevegelser, tidspunkt for passeringer mv, og kan derfor tenkes å bli et praktisk hjelpemiddel i mye annen etterforskning enn den som direkte gjelder vegtrafikkloven. Lovgiver bør derfor ta eksplisitt stilling til spørsmålet om det skal gjelde begrensninger i forhold til bruk i etterforskning. Uten lovbestemte formålsbegrensninger, vil domstolene uansett kunne legge vekt på bevismateriale som er innhentet fra ts-teknologi (jf. Fotobokskjennelsen, Rt. 1990 s 1008).

Hensynet til personvern og konfidensialitet er i utgangspunktet argument for å begrense formålet, for eksempel til å gjelde bestemte overtredelser av vegtrafikkloven. Velger en et videre formål er personvernet en begrunnelse for å stille strenge krav til opplysningskvalitet, og generelt til at det skal skje kontroll med at kravene til behandling av personopplysninger blir etterlevet. Blir etterforskning av alvorlige lovbrudd utenfor trafikklovgivningen et formål, innebærer dette at kravene til opplysningskvalitet mv må innrettes etter de kvalitetskrav som er akseptable i saker om alvorlig kriminalitet.

4.3.3 Krav til opplysningskvalitet

Krav til opplysningskvalitet er sentralt og må ses i sammenheng med formålsangivelsen, jf pol § 11 første ledd bokstavene d og e. Personopplysningsloven § 14 om internkontroll understreker hvorledes den behandlingsansvarlige må arbeide med kvalitetsspørsmålene.[53] I § 27 fastsettes det noe om den behandlingsansvarliges plikt til å rette, slette og blokkere mv opplysninger som er uriktige eller ufullstendige eller som mangler rettslig grunnlag.

Når det gjelder opplysningskvalitet er det ikke eksplisitt fastsatt noen plikt til å gjennomføre vurdering av risiko for feil og ufullstendigheter mv, tilsvarende det som gjelder i for

[53] Krav om planlegging, systematisk tilnærming og dokumentasjon.

risikovurdering og informasjonssikkerhet (jf neste avsnitt). Reguleringen av kvalitet i personopplysningsloven er langt på vei basert på en forestilling om at det vil være mulig å vurdere og objektivt bedømme kvaliteten av hver enkelt personopplysning. Ved bruk av ts-teknologi vil det i tillegg trolig være et behov for å gjennomføre kvalitetsvurderinger på systemnivå, dvs. *generelt* kartlegge muligheter og farer for feil på teknisk utstyr, uriktige måleresultater mv. Slik utprøving av utstyr kan begrunne fastsettelse av bindende regler om sikkerhetsmarginer knyttet til registreringer/målinger som ts-teknologien foretar. Dette er gjort i instruks form for de fleste typer etablerte metoder for fartsmålinger, men bør vurderes som et mulig obligatorisk element knyttet til alt utstyr som har avgjørende innvirkning på slike måleresultater som kan være grunnlag for straff mv. Det bør trolig også vurderes å vedta regler som gir plikt for behandlingsansvarlig til å foreta risikovurderinger vedrørende målemetoder mv og treffe nødvendige tiltak for å sikre kvaliteten.[54]

Kvalitetskrav kan også være argument for teknisk standardisering av måleutstyr med eventuell sertifiseringsordning. Regulering med direkte betydning for informasjonskvalitet mv, kan for eksempel skje i lovs eller forskrifts form, eventuelt slik at en der viser til etablerte tekniske standarder.[55]

4.4 Krav til informasjonssikkerhet og internkontroll

Bestemmelsene i pol § 13 (informasjonssikkerhet) og § 14 (internkontroll) er bygget opp over samme lest. Begge bestemmelser kan sies å være uttrykk for samme reguleringsstrategi med vekt på rettslige krav til egenaktivitet som den behandlingsansvarlige (og eventuelle databehandlere) skal utvise. Bestemmelsen i § 14 om internkontroll gjelder etterlevelse av hele loven, forskrifter og eventuelle enkeltvedtak vedrørende behandlingen av personopplysninger, herunder det som gjelder informasjonssikkerhet. Bestemmelsen i § 13 gjelder kun sikring av slike opplysninger.[56] Det kan derfor hevdes at § 13 langt på vei er et særtilfelle av bestemmelsene i § 14, og at det er betydelig overlapp mellom de to bestemmelsene. Dokumentasjonskravene i medhold av § 13 om informasjonssikkerhet er imidlertid langt mer omfattende enn det som følger av bestemmelsene om internkontroll i og i medhold av § 14.

Felles for de to bestemmelsene er at etterlevelsen av dem skal skje ved hjelp av planlagte og systematiske tiltak. Sammenholdt med bestemmelsene i personopplysningsforskriften kapitlene 2 (informasjonssikkerhet) og 3 (internkontroll), fremgår det imidlertid at også det arbeidet som leder frem til tiltakene - langt på vei - må være planlagte og systematiske.[57]

Internkontrollbestemmelsen i (pol § 14) pålegger den behandlingsansvarlige å "etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet." Rutinene for internkontroll skal med andre ord også omfatte kontroll med at forskrifter og eventuelle enkeltvedtak blir etterlevet. Dersom behandlingen av personopplysninger kommer inn under

[54] Deler av kvalitetskravene blir også ivaretatt i pol § 13 om informasjonssikkerhet og § 14 om internkontroll. I forhold til kvalitet tar § 13 imidlertid bare for seg spørsmålet om integritet. § 14 gjelder internkontroll generelt, men kvalitetsaspektet nevnes spesielt i første ledd, jf neste avsnitt.

[55] Jf Meland m.fl. 2007 som omhandler spørsmålet om standardisering mv av intelligente trafikksystemer, se avsnitt 3.4.

[56] Informasjonssikkerhet er i første ledd definert som spørsmål om konfidensialitet, integritet og tilgjengelighet (for/av personopplysninger).

[57] Se særlig §§ 2-3 - 2-6 og § 3-1 tredje ledd.

rettspleielovene og derfor delvis skal unntas fra personopplysningsloven i samsvar med pof § 1-3, må kravene til internkontroll fortolkes innskrenkende. Det vil derfor trolig ikke gjelde noen plikt til internkontroll for de deler av personopplysningsloven mv som gjelder registrertes rettigheter mv.[58]

Bestemmelsene vedrørende internkontroll fremhever spørsmål om opplysningskvalitet. I forarbeidene er det presisert at "kvalitet er fremhevet særskilt, bl a for å understreke at den behandlingsansvarlige er forpliktet til å tenke gjennom oppdateringsrutiner og sikre prosedyrer for å rette opp feilregistreringer".[59] Spesifikke kvalitetskrav fremgår av pol § 11 første ledd bokstavene d og e, og kravene til retting av feil mv fremgår av § 27. Bestemmelsen om internkontroll kan derfor sies å understreke og forsterke disse forpliktelsene. Sett i forhold til ts-teknologi, er det viktig å bemerke at § 14 ikke er avgrenset til å gjelde de deler av datasystemer som behandler personopplysninger og som behandlingsansvarlig har lett kontroll over. Dersom behandlingsansvaret også omfatter teknologiske enheter som er plassert i hvert enkelt kjøretøy (jf atferdsregistrator), vil forpliktelsene til å ivareta kvalitet mv også omfatte disse. Mer konkret må behandlingsansvarlige for eksempel forsikre seg om at registrerte data i slike enheter er korrekte og fullstendige. De teknologiske løsningene blir derfor betydningsfulle for hvor tyngende behandlingsansvaret blir: Behandlingsansvar for streknings-ATK med utstyr i veikanten som ikke skal samfungere med enheter i hvert kjøretøy, blir vesentlig mindre tyngende å leve opp til enn systemer som er basert på enheter i hver bil. Jo mer spredt og mobilt utstyret er plassert, desto større er trolig denne utfordringen (jf særlig utstyr som er plassert i veikanten, i kjøretøy, i satellitter mv).[60] Myndigheter må ha lovhjemmel dersom de skal kunne gi bindende pålegg til eiere om tilgang til kjøretøyet for å ivareta informasjonssikkerheten.

Personopplysningsloven innebærer med andre ord at ansvaret for tilstrekkelig informasjonssikkerhet ved bruk av ts-teknologi i kjøretøy trolig ligger hos den behandlingsansvarlige. Dette ansvaret vil etter lovens system ofte være en offentlig myndighet, for eksempel et departement, jf avsnitt 4.2.2. For å unngå et slikt resultat må spørsmålet reguleres direkte i særlov. For eksempel kan det i lov eller forskrift etableres en rettsplikt for (visse) eiere og/eller brukere av kjøretøy til å forvisse seg om at enheter av ts-teknologi i deres kjøretøy er i forskriftsmessig stand.[61] I så fall vil bestemmelser i og i medhold av vegtrafikkloven overstyre og modifisere personopplysningslovens bestemmelser om behandlingsansvarliges plikt til å sikre personopplysningene.

Pol § 13 annet ledd stiller opp vidtrekkende dokumentasjonskrav. Både informasjonssystemet og sikkerhetstiltakene skal dokumenteres. Formålet er "å oppnå tilfredsstillende informasjonssikkerhet" og kravet til dokumentasjon av informasjonssystemet må derfor tilpasses til det som har betydning for informasjonssikkerhet. Dokumentasjonskravet gjelder "informasjonssystem", noe som må forstås som et krav om å sikre all informasjon, også den som ikke er formalisert.[62] Også manuell behandling av personopplysninger knyttet til den elektroniske behandlingen skal med andre ord omfattes av dokumentasjonen, jf pol § 3 første ledd bokstav a.

---

[58] Jf ovenfor, avsnitt 3.2.5.

[59] Se ot.prp. nr. 92 (1998-99), kapittel 16, merknader til § 14.

[60] For at et slikt ansvar ikke skal oppstå må en formodentlig forutsette at hver enkelt bileier har bestemmelsesrett over de enheter av ts-teknologi som er plassert i deres kjøretøy, slik at bileier også er behandlingsansvarlig for opplysninger knyttet til bilen.

[61] Jf for eksempel vegtrafikkloven § 23 om ansvar for kjøretøyets stand mv og § 23a om personlig verneutstyr med tilhørende forskrifter.

[62] Jf "datasystem" som ofte betegner system for behandling av formalisert informasjon.

Kravet i § 13 innebærer at det i tilknytning til hver systemløsning for ts-teknologi skal dokumenteres hvilke typer personopplysninger som vil bli behandlet av systemet. Det skal dessuten fremgå hvilke tiltak som er iverksatt for å sikre konfidensialitet, integritet og tilgjengelighet. Det er ikke i loven krav til dokumentasjon av de sikkerhets-/risikovurderingene som danner grunnlag for avgjørelse av hvilke sikkerhetstiltak som skal iverksettes. Etter forskriften § 2-4 siste ledd skal *resultatet* av sikkerhetsvurderingen imidlertid dokumenteres. Forskriften stiller i § 2-7 også krav om å klargjøre og dokumentere ansvars- og myndighetsforhold, jf krav til organisering av sikkerhetsarbeidet i pol § 13 første ledd og pof § 2-3. Pof § 2-7 krever videre dokumentasjon av hvorledes informasjonssystemet er konfigurert, dvs. bl.a. hvorledes programvare, maskinvare mv er ordnet og satt opp i forhold til hverandre. I pof § 2-16 kreves det at også "Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres". Videre skal autorisert bruk og forsøk på uautorisert bruk av informasjonssystemet, samt andre hendelser med betydning for informasjonssikkerheten registreres og lagres minst 3 måneder. De nevnte dokumentasjonskravene må fortolkes i lys av det overordnede kravet om tilfredsstillende informasjonssikkerhet.

Etter pol § 13 er det bare plikt til å treffe sikkerhetstiltak når de er nødvendige for å oppnå "tilfredsstillende" informasjonssikkerhet. Nevnte forskriftsbestemmelser kan leses som påbud om å dokumentere selv om dette ikke er påkrevet for å oppnå tilfredsstillende sikkerhet. I så fall får bestemmelsene et innhold som går videre enn det § 13 i loven hjemler. De aktuelle forskriftsbestemmelsene må derfor tolkes innskrenkende.

Sikkerhetskravene etter forskriften gjelder bare de elektroniske delene av informasjons-systemet, jf pof § 2-1 første ledd. En nærmere systematisering av hovedkravene til dokumentasjon med informasjonssikkerhet som begrunnelse, viser at følgende elementer skal dokumenteres *før* systemet tas i bruk:

- Typer personopplysninger og behandlingsreglene for disse som har betydning for informasjonssikkerheten;
- resultatet av risikovurderingen;
- tiltak for å ivareta informasjonssikkerhet (herunder mot uautorisert bruk av systemet), jf risikovurderingen;
- ansvars- og myndighetsforhold;
- konfigurering av systemet og
- rutiner for bruk av informasjonssystemet

I tillegg er det en rekke dokumentasjonskrav knyttet til *løpende drift* av systemet. Dette gjelder:

- Gjennomgang i tilknytning til vurdering av sikkerhetsstrategi og -mål (§ 2-3);
- sikkerhetsrevisjon (§ 2-5) og
- avvikshåndtering (§ 2-6);

Dokumentasjonskravene angir samtidig hvilke typer vurderinger som skal gjennomføres for å ivareta slik informasjonssikkerhet som er begrunnet i hensynet til personvern. Alle vurderings-/ og dokumentasjonstyper får i utgangspunktet anvendelse på elektronisk behandling av personopplysninger ved hjelp av de aktuelle ts-teknologiene.

4.5 Konsesjonsplikt

4.5.1 Vilkår for at en personopplysning kan anses å være sensitiv

Fram til personopplysningsloven trådte i kraft 1. januar 2000 var konsesjonsplikt hovedregelen etter norsk personvernlovgivning, dvs det var i mange tilfelle krav til forhåndstillatelse fra Datatilsynet før personregistre kunne etableres.[63] Etter dagens lovgivning er den generelle konsesjonsplikten innskrenket til å gjelde behandling av sensitive personopplysninger.[64] Det er kun opplysninger som etter lovens definisjon i § 2 nr 8 som regnes som sensitive:

> "8) sensitive personopplysninger: opplysninger om
> a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
> b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
> c) helseforhold,
> d) seksuelle forhold,
> e) medlemskap i fagforeninger."

I forhold til ts-teknologi blir spørsmålet om slik teknologi vil kunne gjelde person-opplysninger som er å anse som sensitive i henhold til personopplysningsloven? Dersom svaret er ja, er følgen at det i) gjelder skjerpede krav til rettslig grunnlag for behandlingen (jf avsnitt 4.3.1), og ii) er konsesjonsplikt for behandlingen.

Spørsmålet om hva som kan regnes som sensitivt i tilknytning til teknologier som streknings-ATK, atferdsregistratorer og automatisk fartstilpasning, er vanskelig og det er ikke mulig å gi et klart svar uavhengig av hvorledes teknologien konkret er utformet. I det følgende vil jeg kort gjennomgå de viktigste vurderingene som må gjøres.

Det er for det første klart at ts-teknologi i utgangspunktet kan gi informasjon om slike forhold som er nevnt i den siterte bestemmelsen. All bildeteknologi som rettes mot personer i et kjøretøy kan for eksempel vise noe om etnisitet. I tillegg kan bilder vise ytre kjennetegn som sier noe om religion (for eksempel hodeplagg) og helseforhold (jf kjøretøy utstyrt for bevegelseshemmede). Bilde kan også - mer teoretisk - vise seksuelle forhold dersom det er avbildet seksuelle handlinger. Viktigst er det imidlertid at streknings-ATK, atferdsregistratorer og ISA vil kunne vise noe om "en person har vært mistenkt […] for en straffbar handling". For streknings-ATK vil det alltid være et formål nettopp å avdekke straffbare forhold, mens dette formålet er mulig men ikke nødvendig for de to andre teknologiene.

Når en skal ta stilling til hva som er en sensitiv personopplysning, kan det reises spørsmål om ”personopplysning” betegner en opplysnings*type* eller en *–verdi* (forekomst). Opplysnings-typen "kjøretøyets hastighet" er for eksempel åpenbart ikke sensitivt i seg selv, men forekomsten 60 km/t i en femtisone kan ses som sensitiv fordi det gir mistanke om et straffbart forhold. Loven må trolig fortolkes slik at det i utgangspunktet er avgjørende hvorvidt opplysnings*typen* er sensitiv eller ikke.

Tradisjonelle ATK-bilder (på ett punkt) vil være sensitive fordi bildene kun tas av personer som fører kjøretøy med hastighet over tillatt grense. Opplysningstypen kan med andre ord beskrives som "person som fører kjøretøy i ulovlig hastighet". Dette utgangspunktet finner støtte i personverndirektivet der sensitive opplysningstyper er benevnt ”special *categories* of

[63] Jf personregisterloven § 9 (opphevet).
[64] Se pol § 33 første ledd.

data" (min kursiv), dvs. det er understreket at det siktes til *kategorier* av opplysninger. Også ISA kan generere sensitive personopplysninger dersom systemet lagrer opplysninger om hastigheter som overskrider fartsgrensen på stedet.[65]

Personverndirektivet[66] beskriver også en del av disse opplysningskategoriene som "personal data *revealing* racial or ethnic origin" osv. (min kursiv), jf. også Europarådskonvensjon artikkel 6. Det er derfor grunnlag for å åpne for at også *forekomster* av ikke sensitive opplysningstyper kan innebære at det likevel må anses å foreligge sensitive personopplysninger med krav til konsesjon mv. Etter min mening kan sensitive forekomster av personopplysninger regnes som sensitive etter pol § 2 nr 8 selv om opplysnings*typen* ikke er sensitiv. Det er særlig formålsbetraktninger og forholdet til bestemmelsen om rettslig grunnlag (§ 9) og konsesjon (§ 33) som kan begrunne dette.

Dersom det er mest i overensstemmelse med realiseringen av formålet med personopplysningsloven (jf § 1), er dette et moment som kan gi grunn til å se sensitive forekomster som "sensitive personopplysninger". Formålet med loven er å "bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger". Desto større truslene med personvernet er knyttet til slike sensitive forekomster, desto større er grunnen til å betrakte dem som "sensitive personopplysninger".

Videre kan det være grunn til å vurdere formålet med hver enkelt behandling av personopplysningen, jf. avsnitt 4.3.2. Dersom formålet med registrering av akselerasjon i en atferdsregistrator er å bringe klarhet i årsaksforhold ved ulykker, herunder avklare om det har skjedd noe straffbart, trekker dette i retning av å se på opplysningen som "sensitiv" etter personopplysningsloven. Motsatt dersom teknologien for eksempel kun brukes til å samle data som brukes av bilprodusenten til å forbedre teknologien.

4.5.2 Nærmere om konsesjonsplikt mv

Dersom personopplysninger som behandles i ts-teknologi anses å være sensitive (jf pol § 2 nr 8), foreligger det som nevnt konsesjonsplikt. Det kan være gitt unntak fra konsesjonsplikten i lov eller forskrift, jf personopplysningsforskriften kapittel 7, men ingen av disse er relevante for ts-teknologi.[67] Dersom det foreligger positivt lovvedtak om at opplysningene skal samles inn, faller konsesjonsplikten bort, jf pol § 33 fjerde ledd.

Datatilsynet har myndighet til å pålegge konsesjonsplikt selv om personopplysningene som det planlegges behandling av ikke er sensitive. Dette gjelder "dersom behandlingen ellers åpenbart vil krenke tungtveiende personverninteresser", jf pol § 33 annet ledd. I juridisk språkbruk innebærer dette en meget høy terskel, og myndigheten vil derfor kun unntaksvis bli brukt. Slik konsesjonsplikt kan bare fastsettes som enkeltvedtak for et konkret tiltak/prosjekt. Datatilsynet kan med andre ord ikke generelt fastsette at det skal være konsesjonsplikt for ts-

[65] Lagring av opplysninger er imidlertid ikke nødvendig i et ISA-system.

[66] Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Direktivet er bindende for Norge i samsvar med EØS-avtalen. Norsk lov forutsettes derfor å være i samsvar med direktivet, og forståelsen av direktivet er derfor relevant ved fortolkningen av norsk lov på området.

[67] Unntak for aktivitetslogg i edb-system eller datanett kan muligens være aktuell i særlige tilfelle. Forutsetningen for at unntaket gjelder er imidlertid at formålet med loggen er å administrere systemet eller å avdekke/oppklare brudd på informasjonssikkerheten.

teknologi generelt eller for en viss type ts-teknologi. Innen trafikksektoren er bestemmelsen tidligere brukt i sak om rett til anonym ferdsel og helautomatiske bomstasjoner. Saken ble klaget inn for Personvernnemnda.[68] Personvernnemnda konkluderte blant annet med at "det [er] lite tvilsomt at Datatilsynet har hjemmel til ved enkeltvedtak etter personopplysningsloven § 33, 2.ledd å kvalifisere systemet som konsesjonspliktig."

Konsesjonsplikt innebærer krav til forhåndstillatelse. Dersom Datatilsynet gir tillatelse til igangsetting av den konsesjonspliktige behandlingen av personopplysninger, kan de stille vilkår for tillatelsen. Vilkårene kan bare stilles når dette er nødvendig for å "begrense ulempene behandlingen ellers ville medføre for den registrerte", jf pol § 35. Datatilsynets konsesjonsvedtak kan klages inn for Personvernnemnda, jf § 42 siste ledd. Avgjørelsen om å etablere konsesjonsplikt med hjemmel i pol § 33 annet ledd kan være gjenstand for selvstendig klage.

4.6 Tilsyn og myndighet

Datatilsynet har tilsynsmyndighet og vid kompetanse til å gripe inn dersom de oppdager feil og mangler ved behandling av personopplysninger, jf pol kap. VIII om tilsyn og sanksjoner.[69] Personvernnemnda er klageorgan for enkeltvedtak og enkelte andre enkeltavgjørelser som Datatilsynet treffer, se pol § 42 siste ledd. Det faktum at behandling av personopplysninger inngår som integrerte deler av et meget stort antall virksomheter, innebærer at det også kan være andre myndigheter med kompetanse på samme virksomhetsområde. Slik sett vil Datatilsynet arbeide med spørsmål som er nært knyttet til arbeidsområdene til for eksempel Helsetilsynet, Arbeidstilsynet, Forbrukerombudet mv.

Det er i dag ikke separat tilsynsmyndighet for veisektoren, og derfor ikke noe spesielt behov for å gjøre grenseoppgang mellom Datatilsynet og tilsynsmyndigheter innen veisektoren. Flertallet i utvalget som la frem NOU 2009:3 *På sikker veg* gikk imidlertid inn for å opprette et vegtilsyn for infrastruktur. Med veginfrastrukturen siktet utvalget til "vegar, inkludert bruer, tunnelar og tekniske innretningar som er ein integrert del av infrastrukturen, som til dømes skilt, vegmerking, signalanlegg, ferjekaier og vegbelysning".[70] Ts-teknologi som direkte er knyttet til offentlig vei mv (f.eks. streknings-ATK), kan trolig anses å være tekniske innretninger som inngår i veginfrastrukturen. Andre slike teknologier som i hovedsak er basert i hvert enkelt kjøretøy, vil trolig falle utenfor det som kan ses som del av infrastruktur. Ulike teknologiske løsninger for ts-teknologi kan med andre ord føre til at et eventuelt vegtilsyn bare har noen av de aktuelle ts-teknologiene under sitt arbeidsområde. Mye taler for å se behovet for tilsyn med teknologien i sammenheng, uavhengig av definisjonen av begrepet veginfrastruktur.

4.8 Noen samlede vurderinger

Gjennomgangen i kapittel 4 illustrerer for det første at ts-teknologi med personopplysninger som brukes av politiet delvis reguleres av personopplysningsloven og delvis av

[68] Se Personvernnemndas sak PVN-2005-11 om klage på vedtak om pålegg om konsesjonsplikt for helautomatiske bomstasjoner.
[69] Datatilsynet har også lignende kompetanse i forhold til flere andre lover.
[70] Se avsnitt 6.2.2 i utredningen.

straffeprosessloven og andre rettspleielover. Unntaksbestemmelsen i personopplysnings-forskriftens § 1-3 gir ikke en klar og enkel grenseoppgang mellom de to regimene.

Personopplysningslovens bestemmelser er ikke lett å anvende på den aktuelle ts-teknologien. Dette er for så vidt ikke spesielt for dette livsområdet, men er langt på vei uttrykk for en generell observasjon. Grunnen er i stor grad at loven bygger på generelle og teknologiuavhengige begreper og systematikk, noe som kan gjøre det vanskelig å forstå betydningen av bestemmelsene på de forskjellige konkrete områdene der loven gjelder.

I gjennomgangen har jeg særlig vært opptatt av å klargjøre spørsmål om behandlingsansvar, eventuelt bruk av databehandler og andre organisatoriske krav i loven. De organisatoriske kravene er viktige fordi det er grunn til å tro at streknings-ATK og annen ts-teknologi vil kunne trenge en organisering der flere offentlige myndigheter (politi og vegmyndigheter) og eventuelt private aktører må samarbeide tett. Arbeidsdeling som bryter med den standard forventningen om én behandlingsansvarlig med ansvar for alt, gir lett tolkingsproblemer ved anvendelse av personopplysningsloven.

Rettsspørsmålene knyttet til personopplysningsloven er selvsagt et problem for involverte myndigheter. Viktigere er det imidlertid at regelverket er enda vanskeligere å forstå for den jevne sjåfør. Uten en greit forståelig rettslig regulering av ts-teknologi vil både personvern og rettssikkerhet kunne bli satt i fare. Dette peker i retning av særregulering på området, for eksempel i eller i medhold av vegtrafikkloven og/eller politiloven. Særregulering vil både kunne gjøre den rettslige reguleringen mer forståelig, og gi anledning til å justere på enkelte av de løsninger som i dag følger av personopplysningslovens generelle bestemmelser. Også særlovgivning må imidlertid holde seg innenfor rammene av EUs personverndirektiv.[71]

[71] Jf særlig personverndirektivets fortale, punktene 22 og 23.

5 Diskusjon av personvernidealet i sammenheng med ts-teknologi

5.1 Innledning

I dette kapittelet vil jeg drøfte personvernidealet i lys av streknings-ATK, ISA og atferdsregistrator. Dette er en forholdsvis krevende analyse, bl.a. fordi verken teknologiene eller personvernidealet er helt faste størrelser. Personvern kan ikke avgrenses til klassisk personopplysningsvern, jf redegjørelsen for deler av dagens generelle rettslige regulering av personopplysninger. De spørsmål som personopplysningsloven regulerer gjelder derfor kun en del av det samlede personvernet. På det allmenne planet er begrepet personvern et omfattende begrep som ingen har noen direkte definisjonsmakt over, jf avsnitt 2.1 (ovenfor). Til grunn for drøftelsen legger jeg en vid forståelse, i det jeg går ut i fra at personvern grunnleggende sett handler om beskyttelse av det enkelte menneskes integritet og rett til selvbestemmelse (autonomi). Jeg legger videre til grunn at denne integriteten og autonomien er knyttet til noen sfærer som kan sies å være private. Oppgaven blir da å drøfte hvilke spørsmål som kan sies å være knyttet til integritet og autonomi innen disse sfærene.

Heller ikke de nevnte ts-teknologiene kan sies å representere helt faste størrelser, men er gjenstand for fortsatt utvikling. Dette gjelder både utvikling av de grunnleggende teknologiske løsningene og utvikling av det enkelte produkt som er tilgjengelig på markedet. Erfaringen tilsier at den teknologi som vil eksistere om noen år, når det eventuelt er gjort vedtak om bruk, ikke vil være den samme som i dag. Hvordan teknologien konkret vil komme til å bli er det umulig å si noe sikkert om. Drøftelser som baserer seg på framskrivinger av dagens teknologi behøver ikke nødvendigvis representerer en mindre realistisk tilnærming enn om dagens teknologi er diskusjonsgrunnlag. Jeg har valgt å beskrive generell status for de tre utvalgte typene ts-teknologi, og samtidig ta med mulige utviklingspotensialer for de samme teknologiene.

Både atferdsregistratorer og ISA kan tenkes slik utformet at behandling av personopplysninger ikke skjer. Jeg har imidlertid likevel valgt å legge til grunn teknologiske løsninger som innebærer behandling av personopplysninger. Dette valget innebærer ingen forutsigelse, men er forutsetningen for drøftelser som kan tydeliggjøre mulige personvernspørsmål. Uansett er det så mange muligheter for myndigheter og kommersielle aktører knyttet til innsamling og behandling av personopplysninger, at ts-systemer som gjør bruk av slike opplysninger framstår som sannsynlige.

Teknologien forandrer seg og menneskene forandrer seg (med den). Heller ikke personvernidealet representerer noen fast størrelse som er uforandret over tid. Det er i alle fall en kjensgjerning at den rettslige beskyttelsen av personvern er vesentlig endret fra 1978 da personregisterloven ble vedtatt og frem til i dag. Selv om det er vanskelig å finne holdbart empirisk grunnlag for sammenligning, vil mange også være enige i at folks holdninger til personvern er endret i løpet av de siste tretti årene. Om og eventuelt i hvilken grad også personvern*idealet* er endret, er enda vanskeligere å ta sikkert stilling til. Jeg legger likevel til grunn at idealet er endret i den forstand at det er mer sammensatt enn tidligere, og dessuten at enkelte elementer kan være tillagt annen vekt enn før. Jeg mener for eksempel det er

grunnlag for å hevde at kravet til opplysningskvalitet er viktigere i dag enn da personregisterloven ble vedtatt.[72]

I drøftelsene vil idealet primært bli utfordret gjennom beskrivelsene av mulig teknologisk utvikling. Nye teknologier med nye egenskaper og effekter vil kunne aktualisere spørsmål vedrørende enkeltmenneskes integritet og autonomi som ikke tidligere har fått oppmerksomhet. Slik kan teknologisk utvikling avdekke nye sider ved idealet. Det blir da nærmest et filosofisk spørsmål å avgjøre om teknologien kun synliggjør noe som allerede var del av idealet, eller om de integritets- og autonomispørsmålene som teknologiutviklingen genererer er genuint nye.

De følgende enkle teknologibeskrivelsene tar utgangspunkt i to typer kilder. For det første baserer jeg meg på en litteraturstudie som er felles for hele prosjektet "Personvern og trafikk".[73] For å aktualisere og undersøke bredden i hver type ts-teknologi, har jeg dessuten brukt materiale som har fremkommet som resultat av brede Internett-søk på de engelskspråklige teknologibetegnelsene.

I det følgende vil jeg først identifisere egenskaper ved hver av de tre ts-teknologiene som kan knyttes til personvernidealet. Deretter drøfter jeg implikasjoner for personvernet som disse egenskapene kan ha. Jeg gjennomgår personvernspørsmål som fremstår som særlig aktuelle, men gir ingen fullstendig drøftelse. Supplerende spørsmål om forholdet mellom ts-teknologiene og personvern vil fremkomme som resultat av sammenlikningen i kapittel 6.

De neste avsnittene tar utgangspunkt i følgende elementer i beskrivelsen av ts-teknologienes funksjonsmåte:

a) Identifisering av kjøretøyet og eventuelt føreren og andre i bilen.
b) I hvilken grad eier har bestemmelsesrett over systemet.
c) Hvor omfattende og intens målinger/registreringer er.
d) I hvilken grad måleresultater er pålitelige og ikke kan manipuleres.
e) Lagring, tilgjengelighet og eventuell sletting av opplysninger.
f) Sikring av opplysningene, særlig av opplysningenes konfidensialitet og integritet.

Listen er basert på fremstillingen av personvernidealet i kapittel 2, og jeg skal her gi en kort begrunnelse for hver av de fem elementene:

Ad a): Identifisering av person er en forutsetning for krenkelse av personopplysningsvern. Jo mer beskyttet identitetene er, desto mindre problematisk vil teknologien være for personvernet.

Ad b): Et bærende element i personvernet er den enkeltes rett til selvbestemmelse over egen person og privatliv, herunder over opplysninger om egen person. Jo større rett til selv å bestemme over privatlivet, desto mindre problematisk vil teknologien være for personvernet.

[72] Seip-utvalget foreslo ingen egen bestemmelse om plikt til å rette og slette personopplysninger mv, jf NOU 1975: 10 Offentlig persondatasystem og personvern. Departementet satt imidlertid inn en slik bestemmelse i personregisterloven § 8. Ved vedtakelse av personopplysningsloven i 2000, ble kvalitetsspørsmålene en integrert del av formålsbestemmelsen (§ 1), bestemmelser om konkrete kvalitetskrav (§ 11 bokstavene d og e), internkontrollbestemmelsen (§ 14) og en plikt til å rette, slette og blokkere personopplysninger mv i § 27 (som var utvidet i forhold til § 8 i personregisterloven).

[73] Se Grunnan 2008 og Hrelja 2008.

Ad c): Jo mer omfattende og intens innsamlingen av opplysninger er, desto mer utsatt er personvernet . Omfanget gjelder hvor mange opplysningstyper som samles inn, mens intensiteten gjelder hvor mange registreringer av hver opplysningstype som skjer.
Ad d): Krav til opplysningskvalitet står sentralt ved bedømmelsen av de personopplysninger som blir samlet inn, og senere når de anvendes.
Ad e): Hvor lenge opplysninger blir lagret er sentralt for vurderingen av personopplysnings-vernet. Kort lagring vil normalt være å foretrekke fremfor lagring over lang tid. Så lenge opplysningene er lagret, vil spørsmålet om tilgang til opplysningene være sentralt, bl.a. fordi det er en forutsetning for å kunne påpeke feil.
Ad f): At opplysninger er godt skjermet for utenforstående er mer akseptabelt for person-vernet enn at opplysninger er åpent tilgjengelige.

5.2 Streknings-ATK

Streknings-ATK betegner en metode for automatisk trafikkontroll med måling av kjøretøyets fart over en lengre strekning, i stedet for bare på et bestemt punkt som i dag Identifisering av kjøretøyene ved hvert målepunkt skjer på basis av gjenkjennelse av registreringsskilt. Nøyaktig tidspunkt for første og andre passering blir registrert og dokumentert ved hjelp av et kamera, og gjennomsnittsfarten blir beregnet. Dersom den gjennomsnittlige hastigheten er høyere enn tillatt hastighet på strekningen, lagres opplysningene og anvendes som grunnlag for videre straffeforfølging. Dersom gjennomsnittshastigheten ikke overskrider fartsgrensen, slettes opplysningene.

I samsvar med avsnitt 5.1 skjer vurderingen forhold til:

a) Identifisering av kjøretøyet og eventuelt føreren og andre i bilen.
b) I hvilken grad eier har bestemmelsesrett over systemet.
c) Hvor omfattende og intense målinger/registreringer er.
d) I hvilken grad måleresultatet har tilstrekkelig informasjonskvalitet.
e) Lagring, tilgjengelighet og eventuell sletting av opplysninger.
f) Sikring av opplysningene, særlig av opplysningenes konfidensialitet og integritet.

Ad a). Identifisering ved hjelp av foto gjør at personopplysninger oppstår, og registrering av identiteter skaper spørsmål om personopplysningsvern. Alle andre spørsmål om personopplysningsvern vil være avledet av denne registreringen. Personvernet i en bredere forstand kan imidlertid være krenket selv om det ikke skjer identifisering. Derfor kan det ses som en krenkelse dersom personer uriktig tror at myndigheter kjenner deres identitet og kartlegger bevegelsesmønstre mv ved hjelp av streknings-ATK. Slike falske forestillinger kan tenkes å styre atferd eller på annen måte ha negativ innvirkning på den enkeltes opplevelse av privatliv og fred.

Også eventuell usikkerhet med hensyn til hvilken person det er registrert opplysninger om er et problem for personvernet. En rekke kjøretøy vil være kjørt av andre enn personen som er ført opp som eier. Mange kjøretøy vil for eksempel være eiet av virksomheter, slik at eierforholdet ikke gir noen indikasjon på hvem som har vært føreren. En slik usikkerhet er i seg selv problematisk for personvernet fordi det innebærer grunnleggende usikkerhet og mistanke mot uskyldige personer. For å avskaffe usikkerheten vil det dessuten kunne være nødvendig å gjøre nærmere undersøkelser, noe som innebærer ytterligere behandling av personopplysninger for å bekrefte eller avkrefte at bestemte personer kjørte bilen.

Usikkerhet om hvilken person som kjørte bilen vil dessuten selvsagt representere et rettssikkerhetsproblem i tilfelle etterfølgende straffereaksjon. Uten annet enn bilde av registreringsnummeret må det på annen måte kunne bevises at en bestemt person førte bilen.

I en dom fra Eidsivating lagmannsrett[74] ble en mann frifunnet etter først å ha blitt domfelt for to fartsovertredelser. Bevisgrunnlaget var ATK-fotografier, og mannen hadde hele tiden hevdet sin uskyld. Etter domfellelsen innrømmet siktedes bror ansvaret for kjøringen, noe som til slutt ledet fram til frifinnelse. I dom avsagt i Agder lagmannsrett[75] ble en mann frikjent for å ha kjørt i 130 km/t i en 70-sone. To personer som kunne ligne hverandre var mulige sjåfører, og politiet hadde ikke foretatt undersøkelser vedrørende den andre personen.

Identifisering med utgangspunkt i foto er med andre ord problematisk når rettssikkerhet og personvern skal vurderes. Dersom lovgiver har bestemt at personer skal identifiseres, vil sikrere identifisering av personer imidlertid kunne ses som en forbedring av personvernet. Dette kan kanskje virke paradoksalt. Usikker identifisering innebærer imidlertid at to eller flere personers personvern krenkes; eieren, familiemedlemmer og andre kan alle bli trukket inn som mulige førere. Med sikker identifisering gjelder krenkelsen kun én person.

Resonnementet ovenfor har to konsekvenser. For det første bør kun personer som kjører bilen bli identifisert. For det andre bør identifiseringen skje så sikkert at muligheten for personforveksling minimaliseres. Dersom en gjør bruk av kamera og personfoto, innebærer dette bl.a. at fotokvaliteten bør være så høy som mulig. Fotografi vil kun være et utgangspunkt for identifisering. Hensynet til personvern tilsier at den videre identifiseringen innebærer så lite innsamling av tilleggsopplysninger som mulig.

Det er neppe helt usannsynlig at identifisering av fører i fremtiden vil kunne skje ved hjelp av biometri. For eksempel kan fingeravtrykk eller irisskanning brukes for å registrere førers identitet når bilen startes. Slik teknologi brukes i tilknytning til adgangskontroll og pålogging på PCer mv, og vil i en bil også kunne tjene som tyverisikring. Det kan med andre ord tenkes systemer der førerens identitet med 99 % sikkerhet er registrert idet fartsmålingen utføres, og at det kun blir nødvendig å registrere kjøretøyet. *Isolert sett* vil et slikt mulig opplegg trolig måtte anses som mer gunstig for personvernet enn et system som baserer seg på fotografi av personer i forsetene mv. Årsaken er at opplysninger om medpassasjerer blir unødvendig og at identifisering av fører blir sikker, uten behov for ytterligere opplysninger om vedkommende.[76]

Ad b). Når det først har skjedd registrering av personopplysninger som gjør det mulig å identifisere en bestemt person, blir spørsmålet om råderetten de aktuelle personopplysningene avgjørende for bedømmelsen av personvernet. Med autonomi som utgangspunkt vil spørsmålet være om registrerte personer kan bestemme over utstyret og opplysningene, og eventuelt hvem andre som har bestemmelsesrett, samt hvor sterk andres rett til å bestemme er. Dersom registrerte personer ikke har bestemmelsesrett eller denne retten er meget begrenset, samtidig som andre har stor grad av rett til å bestemme over personopplysningene, er dette problematisk i forhold til personvernidealet. Med streknings-ATK er situasjonen at opplysningene helt behandles utenfor de registrertes kontroll, og registrerte personer har ingen selvbestemmelsesrett.

[74] Se Eidsivating lagmannsretts dom LE-2007-155972.
[75] Se Agder lagmannsretts dom LA-2004-30029.
[76] Utbredt bruk av biometri i samfunnet, vil imidlertid kunne være problematisk for personvernet, se Schartum og Bygrave 2008.

Ad c). Det neste spørsmålet gjelder hvor omfattende og intense målinger/registreringer av personopplysninger skal være. Desto kortere avstand mellom første og siste målepunkt som er grunnlag for streknings-ATK er, desto gunstigere for personvernet. Årsaken er at måling over lengre distanser normalt vil gi mer personopplysninger enn når distansen er kort. Jo lenger avstanden mellom målepunktene er, desto større er sannsynligheten for at registrering nr 2 ikke skjer. Manglende registrering nr 2 er i realiteten opplysning om at føreren har stanset, kjørt av veien eller snudd. To registreringer gir informasjon om personens reiserute mv. Lang avstand vil derfor ofte gi mer informasjon enn kort avstand. Desto mindre avstand mellom målepunktene, desto bedre kan det ofte sies å være for personopplysningsvernet.

I slekt med spørsmålet om avstanden mellom målepunkter er spørsmålet om *antall* målepunkter. Dersom en for eksempel har fartsovervåking ved hjelp av flere enn to målepunkter (parvis eller i serie), vil dette være mer problematisk for personvernet enn ved enkeltstående målinger. Generelt vil altså frekvensen/hyppigheten av fartsmålingene være av stor betydning for personvernet, fordi hvert målepunkt genererer nye personopplysninger.

I et rettssikkerhetsperspektiv kan det også spørres om streknings-ATK måler én eller flere straffbare handlinger. Med tradisjonell ATK og ett målepunkt, er det klart at målingen gjelder én overtredelse av fartsbestemmelsene. Med streknings-ATK vil sjåføren ha for høy gjennomsnittshastighet. Det kan bety at personen har gjort seg skyldig i moderat fartsovertredelse over hele strekningen, eller en vesentlig grovere fartsovertredelse i en kort periode, eventuelt flere overtredelser. Straffverdigheten av den først nevnte overtredelsen er langt mindre enn den sist nevnte. Likevel gjør måleteknikken det umulig å skjelne mellom tilfellene. Desto større avstand det er mellom målepunktene, desto mer alvorlig blir dette problemet. Også hensynet til rettssikkerhet og en rettferdig rettshåndhevelse kan derfor tilsi kort avstand mellom målepunktene.

Målemetoden ved streknings-ATK kan også gjøre det mulig å kjøre vesentlig fortere enn fartsgrensen uten å få ulovlig høy gjennomsnittshastighet. Dersom en vet at kontroll er påbegynt ved første målepunkt, er det lite som kan hindre sjåfører å sakne farten tilstrekkelig før andre målepunkt til at gjennomsnittshastigheten blir lovlig. Fartsglade ungdommer vil for eksempel fortsatt kunne prøve akselerasjon mv mellom målepunktene.

Spørsmålet om én eller flere handlinger kommer også på spissen dersom streknings-ATK blir systematisk brukt langs en lengre veistrekning, enten ved at det skjer gjennomsnittsmåling ved hjelp av flere enn to målepunkter, eller ved at det skjer gjentatte målinger med to målepunkter langs en lengre veistrekning. I begge tilfelle er forutsetningen at farten til sammen måles over en lang strekning. Dersom gjennomsnittshastigheten er for høy på fem målepunkter (f.eks. plassert med mellomrom på 1 km), skal dette regnes som én overtredelse eller som fire selvstendige overtredelser? Slike spørsmål om identifisering og avgrensing av den straffbare handlingen og grunnlaget for straffereaksjonen, bør primært avklares i lovgivningen før streknings-ATK igangsettes. Problemet er først og fremst relevant for vurdering av rettssikkerhet, men har også en side mot personvernet fordi straffereaksjonen er basert på innsamling av personopplysninger.

Ad d). I en kjennelse fra Høyesterett fra 2008[77] kom retten fram til at en fartsmåling som var kansellert av fotobokssystemet Datarec410[78] ikke kunne legges til grunn for domfellelse. Domstolen avviste også å gjøre et skjønnsmessig fradrag fra målingen. En viktig del av

[77] Rt. 2008 s 44.
[78] Systemet hadde kansellert målingen fordi det var for stort avvik i målingen av kjøretøyets akselavstand.

informasjonskvaliteten ved streknings-ATK vil være knyttet til funksjonsegenskapene og påliteligheten til det utstyret som er plassert på målepunktene. Lysforhold, fuktighet, nedbør, temperatur(svingninger) og fysiske omgivelser ellers er aktuelle faktorer som hver for seg og i kombinasjon muligens kan virke inn på måleresultater. Jeg har ikke her grunnlag for å vurdere slike risikofaktorer. Et generelt poeng er imidlertid at både hensynet til personvern og rettssikkerhet tilsier at informasjon om mulig feilfunksjon og feilkilder må være åpent tilgjengelige for personer som ønsker å motsi at målte opplysninger er korrekte. Det er dessuten et poeng at behandlingsansvarlige selv må teste og vurdere risiko for at uriktige målinger kan forekomme.

Ad e). Vurderingen av personvern vil også være avhengig av hvor lenge identifiserbare personopplysninger i form av måleresultater mv lagres, for eksempel i samband med videre bruk pga straffeforfølging mv. Hensynet til personvernet tilsier i utgangspunktet fortløpende sletting dersom hastigheten ikke har vært for høy. I den grad opplysningene skal lagres og eventuelt brukes videre, kommer også hensynet til at føreren skal kunne kontrollere og motsi riktigheten av målingen inn som et viktig personvernargument (jf kvalitet på personopplysninger).[79] Slik kontradiksjon[80] er aktuelt fra og med måling er foretatt og så lenge denne opplysningen er lagret. Kontradiksjon er spesielt viktig i tilknytning til iretteføring av fartsovertredelsen. Retten til å motsi fordrer størst mulig grad av åpenhet rundt de forhold som kan ha betydning for bedømmelsen av måleresultatene. Åpenheten må derfor både gjelde selve måleresultatene (vedrørende identitet, målt hastighet, sted, tid mv), og alle andre forhold som kan kaste lys over grad av pålitelighet og mulige feilkilder (lysforhold ved fotografering, mulige årsaker til feilfunksjon på fartsmåler mv). Den sist nevnte informasjonen vil dels gjelde generelle forhold vedrørende selve teknologien, og dels lokale forhold vedrørende bruken av teknologien på vedkommende sted.

Ad f): Dersom måling av hastighet og identifisering av person skjer på måter som er upålitelige, kan manipuleres mv, er dette i seg selv et personvernproblem. Streknings-ATK kan innebære bruk av flere målepunkter spredt over en lang strekning og bundet sammen ved hjelp av elektronisk kommunikasjon. Som for alt elektronisk utstyr er det derfor en viktig utfordring å sikre opplysningene mot datainnbrudd mv som kan sette opplysningenes konfidensialitet og integritet i fare. Dette gjelder i forhold til innbrudd i det enkelte målepunkt, i det sentrale driftssystemet og kommunikasjonen mellom enhetene.

5.3 ISA

Utgangspunktet for ISA er registrering av kjøretøyets fart i forhold til tillatt hastighet. Systemene kan enten være passive eller aktive.[81] Passive systemer gir kun varsel til føreren om at hastigheten er for høy. Aktive fartstilpasningssystemer utløser en reaksjon på fartsoverskridelsen. Reaksjonen kan for eksempel være fartssperre, motstand i gasspedalen eller ubehagelig lyd, dvs tiltak som enten tvinger eller tydelig påvirker føreren til å sette ned hastigheten. GPS, mobiltelefoni og radiotårn i veikanten (festet til trafikkskilt e.l.) er eksempler på teknologier som kan brukes for at bilene kan motta informasjon om fartsgrense på stedet. Poenget er at teknologien skal kunne gi nøyaktig stedsbestemmelse, og at hvert sted på en vei har en definert høyeste hastighet. Slike løsninger kan bygge på behandling av

[79] Jf. for eksempel Eidsivating lagmannsretts dom LE-2007-155972, referert ovenfor.
[80] Dvs. rett og mulighet til å motsi et måleresultat eller lignende.
[81] Tveit m.fl. 2007 s 30 skiller i stedet mellom systemer som er informative (informere om fartsgrensen), støttende (gir råd om å senke farten) eller inngripende (for eksempel aktivt redusere farten).

personopplysninger. Det kan imidlertid også tenkes løsninger der kjøretøyene og infrastruktur i veikanten kommuniserer anonymt.[82] ISA spenner med andre ord over teknologier som klart behandler personopplysninger, til løsninger der personopplysninger ikke behandles. Hvilken retning den teknologiske utviklingen på området vil ta, er vanskelig å vite. Svensk og Ehrström 2007 antar at "[…] ISA kommer att divergera till olika system som riktar sig mot olika delar av marknaden. På sikt tror vi dock att den gemensamma nämnaren för alla typer av system är att ISA kombinera med andra typer av tjänster. För privatbilisten handlar det om ISA i kombination med navigation, city-guider, POI:ar etc." (s 15). Integrasjon med andre tjenester ofte gjøre det nødvendig å behandle personopplysninger. Slike kombinerte løsninger kan motivere den enkelte til å anskaffe teknologien, og kan derfor ses som en bedre spredningsstrategi enn for eksempel påbud i lov mv.

I samsvar med avsnitt 5.1 skjer vurderingen forhold til:

a) Identifisering av kjøretøyet og eventuelt føreren og andre i bilen.
b) I hvilken grad eier har bestemmelsesrett over systemet.
c) Hvor omfattende og intense målinger/registreringer er.
d) I hvilken grad måleresultatet har tilstrekkelig informasjonskvalitet.
e) Lagring, tilgjengelighet og eventuell sletting av opplysninger.
f) Sikring av opplysningene, særlig av opplysningenes konfidensialitet og integritet.

Ad. a). Ved ISA er det ikke nødvendig at noen utenforstående kjenner kjøretøyets eller sjåførens identitet, men det er også mulig å utforme denne teknologien slik at det genereres personopplysninger. Dersom en imidlertid forutsetter at fartsmålinger logges av systemet, og denne farten knyttes til bestemte personer ved hjelp av identifiseringsmetoder som gjør bruk av pinkode, smartkort, bioteknologi eller lignende, vil dette gi en lignende situasjon som for streknings-ATK.

Ad. b) Dersom det skjer logging av fartsdata, blir vurderingen av personvernet avhengig av hvem som er behandlingsansvarlig for opplysningene i loggen. Slike opplysninger må normalt regnes som personopplysninger (jf avsnitt 3.2) med en behandlingsansvarlig person eller virksomhet (jf avsnitt 3.3.2).

Er eier behandlingsansvarlig vil utfordringene for personvernet bli relativt små. Eieren vil da for eksempel stå fritt med hensyn til sletting. Er det bare eier som bruker bilen, vil personvernhensynene primært gjelde sikring av at opplysningene ikke blir tilgjengelige for uvedkommende. I tillegg kommer personvernspørsmål i de meget sjeldne tilfellene der det er aktuelt for politiet å gjøre beslag i loggopplysningene som ledd i etterforskning av alvorlige forbrytelser.

Desto flere brukere uten bestemmelsesrett over opplysningene, desto viktigere blir personvernspørsmålene. Er bileier/behandlingsansvarlig en arbeidsgiver eller et bilutleiefirma, slik at loggen primært sier noe om andre enn eieren, kan situasjonen ligne den som oppstår når en myndighet har behandlingsansvaret.

Selv om eier er behandlingsansvarlig, kan dette bli begrenset ved lov uten at behandlingsansvaret derfor har gått over på en myndighet e.l. (jf avsnitt 4.2.2.2). Desto

[82] I Opel Insigna finnes det et "øye" som leser trafikkskilt, bl.a. fartsskilt, noe som gjør det mulig i fremtiden å overstyre sjåførens valg av fart uten at det registreres personopplysninger (Dagsavisen 2008). En oversikt over aktuelle ISA-teknologier finnes på Vägverkets nettsider, se http://www.vv.se/Startsida-foretag/Trafiken/Hastighet/ISA/Leverantorer-och-anvandare/.

mindre råderett eieren har over opplysningene, og desto flere andre aktører som kan ha tilgang til personopplysningene, desto alvorligere må de personvernmessige problemene anses å være. Derfor vil installering og bruk av ISA som er pålagt eier gjennom offentligrettslig pålegg og som politi, andre myndigheter og forsikringsselskapet mv har tilgang til, reise meget omfattende spørsmål vedrørende personvern.[83]

Hvem som har bestemmelsesrett over fartstilpasningssystemet har betydning ut over det som med rimelighet kan ses som personvernspørsmål. Tvungen installasjon av automatisk, aktiv fartstilpasning og fravær av bestemmelsesrett over systemet for den som bruker kjøretøyet, berører vedkommendes autonomi i generell forstand. Når systemet griper aktivt inn og regulerer hastigheten vil dette primært begrense den enkeltes *handlefrihet*. Denne begrensningen er av en annen karakter enn begrensninger/inngrep i personvernet gjennom behandling av personopplysninger. "Direkte virkende trafikkregler" virker automatisk på kjøretøyet og presser derfor gjennom lovlydighet uavhengig av om sjåføren ønsker det selv eller ikke.

Ad. c) Ved ISA vil det ikke være målepunkter, men fartsmålingen vil i utgangspunktet skje kontinuerlig i kombinasjon med system som gir kjøretøyet informasjon om fartsgrensen på stedet. Personvernspørsmål vil primært aktualiseres i den grad målingene også blir logget. I så fall vil måling som er avgrenset til bestemte strekninger (forbi skoler, idrettsarenaer mv) eller i bestemte fartssoner (for eksempel med fartsgrense 70 eller lavere), være mindre inngripende enn logging av fartstilpasning som over alt og alltid er i funksjon.

Ad. d) Jeg har ikke grunnlag for å anta noe om hvor pålitelige målinger av hastighet er ved automatisk fartstilpasning. Så lenge opplysninger ikke logges, vil upålitelighet imidlertid kun ha betydning på begrensede måter, for eksempel ved at sjåføren blir forstyrret til tross for at fartsgrensen ikke er overtrådt. Det er imidlertid vanskelig å se dette på annen måte enn om annet teknisk utstyr på kjøretøyet har feilfunksjon. I den grad opplysningene logges og brukes for senere straffeforfølging, forsikringsoppgjør mv, vil utilstrekkelig opplysningskvalitet både fremstå som et personvernproblem og ikke minst som et problem for sjåførens rettssikkerhet.

Ad. e) Dersom det skjer logging av fartsmålinger og eier har liten grad av bestemmelsesrett over opplysningene, blir spørsmålet om lagringstid for opplysninger om fart og (eventuelt) bilførerens identitet viktig. Desto kortere lagringstid, desto bedre for personvernet. Opplysninger om hastighet kan muligens regnes som personopplysning, selv om opplysninger om identiteter er slettet. I private biler vil det kunne være så få mulige brukere at det likevel er relativt enkelt å komme frem til hvem som faktisk har kjørt.

En kan tenke seg ISA der det ikke skjer logging av hendelser i systemet, og derfor ikke registreres personopplysninger. I så fall vil personvernhensyn kun komme inn på helt begrensede måter. Fartssperre og motstand i gasspedal kan vanskelig sies å berøre personvernet slik dette idealet med rimelighet må avgrenses, jf avsnitt 2.1. Skriftlige varsler til fører på førerplassen som kan leses av passasjerer og lydsignal eller lignende som kan oppfattes av alle i kjøretøyet, kan til en viss grad sies å gripe inn i/berøre private relasjoner på lignende måte som med lys-/lydvarsel ved manglende bruk av bilbelte. Varslingsfunksjoner åpenbarer overfor passasjerer at sjåføren trolig kjører ulovlig fort. Slike slutninger vil imidlertid enhver passasjer kunne trekke allerede i dag på grunnlag av speedometerinformasjon, og en slik effekt for personvernet har derfor mest teoretisk interesse.

[83] Gjendiges Karmøy-prosjekt er eksempel på at bruk av ISA gir fordel for forsikringstaker.

Ad f): Når det gjelder sikring av personopplysningenes konfidensialitet og integritet i tilknytning til ISA, vil dette igjen kun være et problem i den grad det skjer logging av opplysningene. Dersom det skjer logging, og opplysningene kun befinner seg lokalt i hvert kjøretøy er skadepotensialet ved sikkerhetsbrudd begrenset til hvert enkelt kjøretøy. Mulighet for å hente ut opplysninger fra hvert kjøretøy til en sentral base, gir selvsagt en langt høyere sikkerhetsrisiko. Informasjonssikkerhetsspørsmålene knyttet til ISA spenner med andre ord over alt fra helt enkle utfordringer med meget begrenset skadepotensiale, til meget store utfordringer med meget stort skadepotensiale.

Generelt kan det konkluderes at ISA *kan* være nesten problemfritt for personvernet, men kan også være meget inngripende. Variasjonsbredden er så stor at det er lite hensiktsmessig å se på fartstilpasningssystemer som ett saksforhold.

5.4 Atferdsregistrator

Atferdsregistratorer kan virke på ulike måter. Et hovedskille går mellom registratorer som utløses av forvarsler til en mulig ulykke (f.eks. kraftig oppbremsing, aktivisering av bilens sikkerhetssystemer mv.), og registratorer som kontinuerlig lagrer data som viser kjørestil/-atferd. Registrering kan være begrenset slik at systemet periodisk skriver over tidligere data med nye data, men kan også tenkes å logge en lang historikk som ikke slettes. I sist nevnte tilfelle kan atferdsregistratoren tenkes å nærme seg en *ferdskriver*, lignende den teknologien som finnes på fly. Teknologien dekker med andre ord et kontinuum fra en serie øyeblikksbilder innen begrensede tidsintervaller, til registrering av nøyaktig kjøreatferd over lange tidsperioder.

Dersom utløsermekanismer er knyttet til hendelser, kan en tenke seg mekanismer som er følsomme og som derfor gir mye data, eller utløsermekanismer som er robuste og bare gir data ved kraftige/ekstreme hendelser. I så fall blir det kun registrert få (om noen) opplysninger i systemet. Dersom systemet virker mer eller mindre kontinuerlig for å fange opp alle hendelser, kan en tenke seg stadig overskriving av gamle data innen helt korte intervaller eller sjelden overskriving av innsamlede data. Eventuelt kan sletting tenkes å skje ut i fra en beslutning/aktiv handling fra en myndighet eller verksted. I alle tilfelle vil fremtidens atferdsregistratorer kunne befinnes seg i begge ender av nevnte kontinuum. Dersom teknologien oppnår sosial aksept og ikke blir uforholdsmessig dyr, kan det være grunn til å tro at det vil bli argumentert for relativt omfattende registrering av kjøreatferd.

I samsvar med avsnitt 5.1 skjer vurderingen forhold til:

a) Identifisering av kjøretøyet og eventuelt føreren og andre i bilen.
b) I hvilken grad eier har bestemmelsesrett over systemet.
c) Hvor omfattende og intense målinger/registreringer er.
d) I hvilken grad informasjonskvaliteten er tilstrekkelig.
e) Lagring, tilgjengelighet og eventuell sletting av opplysninger.
f) Sikring av opplysningene, særlig av opplysningenes konfidensialitet og integritet.

Ad. a): På dette punktet blir situasjonen temmelig lik den som er gjennomgått for automatisk fartstilpasning, se forrige avsnitt punkt a.

Ad. b): På dette punktet blir situasjonen temmelig lik den som er gjennomgått for automatisk fartstilpasning, se forrige avsnitt punkt b.

Ad. c): I innledningen til dette avsnittet har jeg allerede fremholdt muligheten for at atferdsregistratorer i kjøretøy kan tenkes å legge til rette for registrering av en rekke opplysningstyper med intensiv registrering innen hver type. Fordi et stort antall opplysningstyper kan tenkes å ha stor interesse for trafikksikkerhetsarbeidet, er det grunn til å anta at denne teknologien kan bli innført med få opplysningstyper som er kostnadsmessig og sosialt akseptabelt. Deretter vil antallet opplysningstyper mv kunne øke. Også bilprodusenter, forsikringsselskaper og andre har stor interesse i slik teknologi for produktutviklingsformål mv, noe som langt på vei også kan bidra til økt trafikksikkerhet. Samtidig øker antallet interessenter som kan ønske mer omfattende og inngående registrering sjansene for at registreringen gradvis øker.

Biler inneholder i stadig større grad digitale styringsenheter, noe som legger til rette for å måle en lang rekke forhold som kan si noe om hvordan kjøretøyet blir brukt og hendelser kjøretøyet utsettes for, jf den generelle beskrivelsen av atferdsregistratorer ovenfor. Flere slike hendelser vil gi direkte informasjon om sjåførens handlinger som direkte er knyttet til bruken av kjøretøyet (akselerasjon, oppbremsing). I ytterste fall, kan trafikksikkerhet også begrunne registrering av annen sjåfør-/passasjeratferd i tilknytning til en ulykke, for eksempel vedrørende bruk av mobiltelefoner, GPS, underholdningskonsoller osv. Enhver bruk av tilleggsutstyr som kan forårsake distraksjon og dermed fare for ulykker, kan for eksempel foreslås fortløpende logget med tanke på å dokumentere foranledningen til eventuelle ulykker. I tillegg kommer at den digitale teknologien gjør det mulig å diagnostisere kjøretøyets *tekniske tilstand* med tanke på å varsle og lokalisere feil.[84]

Det samlede fremtidsbildet er med andre ord biler der logging av en rekke data kan være ønskelig for å motvirke og oppklare årsaker til trafikkulykker. Dette må antas å gjelde opplysninger om i) ytre begivenheter/krefter som virker på bilen, ii) bilens tekniske stand på ulykkestidspunktet, iii) sjåførens håndtering/bruk av kjøretøyet, og iv) sjåførens og eventuelle passasjerers sporbare handlinger (for øvrig). Alle slike muligheter kan passe inn i trafikksikkerhet som begrunnelse for atferdsregistratorer. Erfaringer med tidligere teknologiutvikling og -anvendelse gjør at det er grunn til å forvente at flere slike muligheter etter hvert vil bli benyttet. Sosial aksept, pris og antatt forebyggende effekt på ulykker vil åpenbart være viktig for hvor langt og raskt en slik utvikling vil gå.

Her er det ikke grunn til å gå for langt i spekulasjoner om hva fremtiden vil bringe. Det avgjørende poenget når personvernet skal vurderes, er å understreke at jo mer omfattende og intens slik logging av forhold vedrørende bruk av kjøretøy blir, desto mer problematisk. Brukes mulighetene fullt ut, vil førere (og delvis passasjerer) være totalt overvåket så lenge de sitter i bilen. Fra et rent personvernperspektiv vil dette være en totalt uakseptabel situasjon.

Dersom en ser ut over det som bare gjelder personvern og også tar hensyn til den enkeltes rettssikkerhet og rettsbeskyttelse, blir bildet noe mer nyansert. Hensynet til rettssikkerhet tilsier bl.a. at det bør kunne være mulig å dokumentere ulykkeshendelser slik at spørsmålet om skyld i strafferettslig og/eller erstatningsrettslig forstand blir riktig avgjort. Likevel er det et problem med uriktige opplysninger og opplysninger som gir grunnlag for feiltolking. Det er derfor neppe noe automatikk i at desto flere opplysninger som kan dokumentere et hendelsesforløp, desto bedre for ivaretakelsen av rettssikkerhet.

[84] Se for eksempel om On-Board Diagnostics i biler; http://en.wikipedia.org/wiki/On-board_diagnostics.

Spørsmålet om rettssikkerhet handler også om borgernes interesse i å unngå maktovergrep og vilkårlighet fra myndigheters side, for eksempel ved at opplysninger som er samlet inn gjennom atferdsregistratorer brukes til andre formål enn å bedre trafikksikkerheten. Hvilken slik tilleggsbruk som vil kunne bli aktuelt er umulig å ta stilling til her. Poenget er at foreliggende opplysninger har en tendens til å bli brukt, og at muligheter for uakseptabel bruk foreligger.

Dersom en tar utgangspunkt i kravet om rettsbeskyttelse for borgerne, blir perspektivet et noe annet enn med rettssikkerhet som utgangspunkt. Her blir det vesentlige at politi, påtalemyndighet og domstoler opptrer slik at personer som har forbrutt seg mot trafikkreglene og derfor forårsaket skade på personer og kjøretøy mv skal holdes ansvarlige for sine handlinger. Dette perspektivet begrunner trolig en mer omfattende og intensiv informasjonsinnsamling enn rettsikkerhetsperspektivet alene.

Ad d): Spørsmålet om informasjonskvalitet blir etter det jeg kan forstå temmelig likt for atferdsregistratorer som for ISA, og jeg viser derfor til foregående avsnitt. En forskjell er imidlertid at opplysningstypene fra atferdsregistratorer kan være langt flere, noe som kan gjøre at sviktende opplysningskvalitet får langt større konsekvenser.

Ad. e): På dette punktet blir situasjonen temmelig lik den som er gjennomgått for ISA, se forrige avsnitt punkt e.

Ad f): Også når det gjelder sikring av opplysningene (konfidensialitet, integritet mv), blir situasjonen temmelig lik den som er gjennomgått for automatisk fartstilpasning, se forrige avsnitt punkt f. En forskjell er imidlertid at opplysningstypene fra atferdsregistratorer kan være langt flere, noe som kan gjøre at sviktende informasjonssikkerhet får langt større konsekvenser.

5.5 Noen samlede vurderinger

Identifisering

Identifisering av personer er avgjørende for at det skal oppstå personopplysninger, og dermed for om ts-teknologien kan sies å reise spørsmål om personopplysningsvern.

Streknings-ATK innebærer (som tradisjonell ATK) fotografering av personer i bilens forsete, herunder også passasjersiden. Streknings-ATK gir med andre ord mulighet for identifisering av personer som ikke har noe med fartsovertredelsen å gjøre.[85] Identifiseringen er med andre ord relativt lite målrettet. Streknings-ATK kan antagelig ikke utformes slik at identifisering blir unødvendig.

En kan tenke seg at identifisering i fremtiden kan skje på annen og mer presis måte. Sjåføren kan for eksempel knyttes til kjøretøyet ved hjelp av pin-kode, smartkort, fingeravtrykkleser eller lignende. I så fall vil det kun samles inn opplysninger om sjåføren. Isolert sett vil dette kunne ses på som en forbedring av personvernet for passasjerer. Slik identifisering vil imidlertid gi mulighet for sikkert å knytte sjåfører til data fra ulike typer ts-teknologi. I så fall kan streknings-ATK med fartsmålere på bakken framstå som lite hensiktsmessig. I stedet kan fartsmåling ved hjelp av GPS eller ISA framstå som mer rasjonelt. Fotoboksene i veikanten

[85] Passasjeren er likevel vitne til lovbruddet og er således en relevant person i tilknytning til eventuell straffeforfølging.

er jo begrunnet i behovet for identifisering ved hjelp av foto. Skjer identifisering på annen måte, vil selve fartsmålingen trolig skje på annen måte.

Atferdsregistratorer krever i utgangspunktet ingen identifisering før det eventuelt har skjedd et ulykkestilfelle. Aktiv ISA kan trolig ha god effekt på trafikksikkerhet uten at det behandles personopplysninger noen gang. Begge teknologier kan imidlertid tenkes utformet slik at det skjer rutinemessig identifisering av fører ved hjelp av biometri mv, jf ovenfor. Den mest moderate bruken av disse teknologiene kan med andre ord gi veldig beskjedne effekter på personvernet - hvis noen. Den mest radikale bruken med omfattende logging av personopplysninger, gir veldig store og negative effekter for personvernet.

Logging knyttet til aktiv ISA med fartssperre atskiller seg fra annen logging. Her vil opplysningene ikke gjelde overtredelser av fartsgrenser, men *forsøk* på overtredelse. Årsaken er at slik teknologi håndhever rettsregelen om fart, i stedet for bare å registrere overtredelser av den, slik atferdsregistrator og streknings-ATK gjør.

Sjåførens bestemmelsesrett

Det kan vanskelig tenkes at sjåfører (dvs personer det registreres opplysninger om) kan få bestemmelsesrett av betydning over streknings-ATK. Uansett er denne kontrollen kun basert på teknologi utenfor kjøretøyet. Ved ISA og atferdsregistrator er teknologien helt eller delvis plassert i kjøretøyet. Dette åpner for å gi sjåfør eller eier en viss grad av bestemmelsesrett. Slik teknologi kan i utgangspunktet tenkes frivillig brukt, for eksempel slik at det installeres som ledd i avtale om redusert forsikrings- og avgiftsbetaling eller lignende.

Dersom sjåførene i liten eller ingen grad kan utøve selvbestemmelsesrett over ts-teknologien, blir neste spørsmål hvem som da skal/bør ha retten til å bestemme over teknologien. Vurderingen av spørsmålet avhenger i stor grad av maktforholdet mellom sjåføren og den som har bestemmelsesrett. Hovedskillet gjelder om bestemmelsesretten er gitt til noen som kan utøve offentlig myndighet eller andre beslutninger med stor betydning for sjåføren. Dersom bestemmelsesretten tilhører myndigheter som kan ilegge straff og/eller forsikringsselskaper som kan avkorte forsikringsoppgjør eller lignende, vil dette være mer alvorlig for ivaretagelsen av den enkeltes rettigheter. Dersom bestemmelsesretten lå hos instanser som for eksempel brukte teknologien til å utføre trafikksikkerhetsforskning mv ville det være mindre alvorlig for de registrerte.

Når bestemmelsesretten gjelder offentlig myndighetsutøvelse, er det vanskelig å skjelne mellom spørsmål som kan klassifiseres som personvern og de som gjelder rettssikkerhet. Også når det er private beslutningstakere (forsikringsselskaper mv), kan rettssikkerhets-perspektivet sies å være relevant, fordi beslutningen kan være bestemmende for enkelt-personers rettigheter. I slike tilfelle vil saksbehandlingsregler som styrer hvorledes opplysningene fra ts-teknologien lovlig kan benyttes, kunne ivareta begge idealer.[86]

Omfang og intensitet av registreringer

Omfanget av registrerte personopplysninger vil variere mye avhengig av det konkrete opplegget for bruken av ts-teknologi. Ved streknings-ATK er det kun fart som måles direkte. I tillegg kan det også avledes forholdsvis sikre opplysninger om hvem som kjørte bilen, hvem som eventuelt var passasjer, hvor bilen beveget seg (vei og retning) og tidspunktet for kjøringen (dato og klokkeslett). Samlet utgjør dette forholdsvis mye informasjon som

[86] Se for eksempel Sivilombudsmannen 1996 der ombudsmannen hadde flere innsigelser mot saksbehandlingen knyttet til forelegg etter ATK.

indirekte kan vise noe om sjåførens og passasjerens personlige forhold. Slike opplysninger gjelder imidlertid ytre omstendigheter. Privatlivet vil først og fremst bli berørt når slike variabler sammenholdes med andre personopplysninger (for eksempel hvorfor en person var på stedet S_1 når han skulle ha vært på S_2).

Atferdsregistratorer kan utformes slik at det gir opplysninger om en lang rekke forhold. De direkte målingene gjelder minimum fart samt positiv og negativ akselerasjon, bruk av bilens sikkerhetssystemer mv. Av slike opplysningstyper kan det avledes opplysninger/antagelser om kjøreatferd og vurderingsevne mv (ABS-systemet koplet inn et høyt antall ganger i løpet av begrenset tidsintervall, sammenholdt med opplysninger om vanskelige kjøreforhold). Dersom atferdsregistratorer lages så omfattende som mulig, vil dette kunne gi meget detaljerte opplysninger om private hendelser i bilen. Dermed har en også et bredt grunnlag for videre antakelser hvis opplysningene kombineres med annen informasjon.

ISA gjelder i utgangspunktet kun måling av fart. Dersom fartstilpasningen er basert på sendere i veikanten som gir opplysninger om fartsgrense mv, kan det imidlertid også tenkes registrering av andre opplysninger (strekning/sted mv).

Når det gjelder registrerings*intensitet*, framstår ISA og atferdsregistrering som mer problematisk enn streknings-ATK. De to først nevnte teknologiene vil typisk virke kontinuerlig. Streknings-ATK vil trolig kun være aktuelt på et relativt lite antall steder, og primært på hovedveier.

***

Streknings-ATK er trolig den teknologien som ut i fra *dagens teknologi* og -bruk klart er mest personvernfiendtlig. ISA og atferdsregistrator kan utformes på måter som gjør at det er få og lite alvorlige personvernproblemer knyttet til dem.

Streknings-ATK har trolig et begrenset utviklingspotensiale. Selv om antallet kontrollpunkter øker, er det ikke realistisk at en oppnår den kontinuerlige registreringen av fart og annen atferd som de to andre ts-teknologiene kan gi. Trolig er atferdsregistratorer den av teknologiene som har klart størst potensiale for inngrep i personvernet.

6 Sammenlignende vurdering av personvern for trafikksikkerhet og kriminalitetsbekjempelse

6.1 Begrunnelse og redegjørelse for det sammenlignende opplegget

Personvernkommisjonen understreker i sin innstilling (NOU 2009: 1) at dagens teknologi nærmest gir uavgrensede muligheter for registrering og overvåking. Kommisjonen antydet ikke hvorledes det eventuelt kan trekkes grensene. Det blir imidlertid understreket at det ikke er akseptabelt dersom en sektor skaper effekter for personvernet på sitt område uten å se dette i sammenheng med utvikling på andre områder. Nettopp behovet for å se personvernspørsmål innen én sektor i sammenheng med tilsvarende spørsmål i andre sektorer, er en hovedmotivasjon for opplegget i dette kapittelet. Jeg har valgt å sammenligne ts-teknologi innenfor veisektoren med bruk av lignende teknologi for etterforskningsformål. Det dreier seg altså om å sammenligne to sektorer som begge gjelder forebygging og etterforskning av kriminelle handlinger, og der politiet i begge tilfeller spiller en sentral rolle. Innen veisektoren gjelder det isolert sett små lovbrudd som i sum er et stort samfunnsproblem. Politiets inngripende tvangsmiddelbruk etter straffeprosessloven gjelder et forholdsvis lite antall langt alvorligere forbrytelser.

De typer ts-teknologi som er gjenstand for analyse i denne rapporten har likhetstrekk med enkelte av de teknologier politiet kan anvende som ledd i etterforskning av alvorlige forbrytelser. Den rettslige reguleringen av hva politiet kan få fullmakt til kan derfor hevdes å være relevant for den personvernmessige vurderingen av ts-teknologi. En underliggende forutsetning er at det bør være rimelig grad av sammenheng mellom ulike deler av lovgivningen som regulerer personvernkrenkende teknologi. En vurdering som kun omfatter trafikksikkerhetsområdet kan derfor hevdes å være utilstrekkelig.

I det følgende tar jeg utgangspunkt i hhv streknings-ATK, ISA og atferdsregistrator. Selv om det ikke foreligger helt faste teknologiske standarder for hver av disse teknologiene, og til tross for at teknologiene fortsatt vil bli utviklet, mener jeg det er mulig å foreta en forholdsvis stabil klassifisering av noen overordnete virkemåter.

ISA og atferdsregistrering har åpenbart et utviklingspotensiale i retning av teknologi som logger personopplysninger. Dersom slik behandling av personopplysninger ikke skjer, blir ikke klassifiseringene og sammenligningene nedenfor relevante. Disse elementene i sammenligningen forutsetter med andre ord *et verste fall scenario* og derfor en teknologiutvikling som kanskje ikke vil skje. Likevel er den etter min mening interessant. Da de første bomringene ble bygget rundt store byer fra slutten av 1980-tallet, var det få personvernimplikasjoner knyttet til ordningene.[87] Senere ble slike veibetalingssystemer kontroversielle storforbrukere av personopplysninger.[88] Det er etter min mening en generell erfaring at teknologi utvikler seg på måter som innebærer økt eller ny bruk av person-opplysninger og økte muligheter for krenkelser av personvernet. Utvikling fra manuell til elektronisk veibetaling, og utvikling fra ATK til streknings-ATK er to relevante eksempler på trafikkområdet. Med dette som bakgrunn mener jeg det er relevant å undersøke på basis av en lignende utvikling for ISA og atferdsregistrering. Dersom drøftelsene blir knyttet til

[87] I 1986 var Bergen den første byen i Europa som krevet betaling for kjøring til sentrumsnære områder.

[88] Jf. Personvernnemndas sak PVN-2005-11 om helautomatiske bomstasjoner, som det ble etablert konsesjonsplikt for etter pol § 32 annet ledd, og som gjelder behandling av personopplysninger som "åpenbart vil krenke tungtveiende personverninteresser".

eksisterende teknologi, vil rettslige vurderinger i unødig grad komme på etterskudd i forhold til teknologiutviklingen.

Den følgende klassifiseringen skjer ved hjelp av en systematikk som jeg opprinnelig har skissert som ledd i vurdering av politiets etterforskningsmetoder.[89] Basis for klassifiseringen er nærmere bestemte systematiske skiller som gjenspeiles i straffeprosesslovens bestemmelser om teknisk sporing (strpl § 202b)[90] og kommunikasjonsavlytting (strpl § 216a).[91] Jeg tar dessuten utgangspunkt i dataavlesing slik dette er foreslått i norsk rett og tillatt etter bl.a. dansk rett.[92] Disse etterforskningsmetodene er valgt for å få et spenn fra en metode som er klart inngripende (teknisk sporing, jf strpl § 202b), til metoder som er veldig inngripende men likevel akseptable (kommunikasjonsavlytting jf strpl § 216a), til metode som er så inngripende at den ikke er tillatt i Norge (dataavlesing). For analyseformål har jeg formulert åtte variabler for å identifisere egenskaper ved etterforskningsmetodene som er problematiske ut i fra hensynet til personvern og rettssikkerhet, jf tabellen nedenfor.

I avsnittene nedenfor vil de tre ts-teknologiene bli sammenlignet med de to inngripende etterforskningsteknologier/-metoder som kan sies å ha størst likhet med hver av ts-teknologiene. Derfor sammenligner jeg streknings-ATK og ISA med teknisk sporing, mens atferdsregistrator blir sammenlignet med dataavlesing.

Følgende systematikk er utgangspunktet for analysen:

Variable	Mulige verdier			
Kjennskap	Hemmelig	Åpent, ikke varslet	Varslet	Aktivt varsel
Datanivå	Begge	Primærdata	Sekundærdata	
Kommunikasjonsparter	Menneske - menneske	Menneske - maskin	Maskin - maskin	
Inngrepspunkt	Fysisk miljø	(Slutt)bruker-utstyr	Infrastruktur	
Uttrykksform	Skrift	Bilde	Lyd	Måleresultater
Varighet av data	Lagring	Monitorering		
Tilleggskrenkelse	Ja			
Ekstern bistand	Ja			

Tabell 1. Variable størrelser og mulige verdier for sammenligning mellom ts-teknologi og etterforskningsteknologi

Tabellen viser mulige variable med relevans for personvern (venstre kolonne), og angir i hver rad mulige verdier. Jeg skal her kort gjennomgå hver av variablene:

[89] Jf upublisert notat i tilknytning til arbeidet med NOU 2009: 15.
[90] Det vil si plassering av teknisk peileutstyr på kjøretøy, gods eller andre gjenstander for å klarlegge hvor den mistenkte eller gjenstandene befinner seg.
[91] Det vil si avlytting av samtaler eller annen kommunikasjon (telefoner, datamaskiner mv) som den mistenkte har eller kan antas å ville bruke. Som kommunikasjonsavlytting regnes også identifisering av kommunikasjonsanlegg ved hjelp av teknisk utstyr.
[92] Dataavlesing setter politiet istand til å avlese ikke offentlig tilgjengelige opplysninger i datamaskiner mv uten å være tilstede der maskinen er. Eksempel på bestemmelse som gir adgang til en form for dataavlesing finnes i den danske retsplejeloven § 791 b.

- Kjennskap beskriver i hvilken grad overvåkingstiltaket fremstår som tydelig for personer som tiltaket retter seg mot, og dermed i hvilken grad personene kan ta hensyn til tiltaket, jf kravet om autonomi. "Aktivt varsel" betyr at beskjed/signal blir gitt til personen som er gjenstand for kontrollen når teknologien anvendes. "Varslet" betyr at teknologibruken er gjort tydelig til kjenne ved hjelp av skilt eller lignende, men uten at det gripes aktivt og direkte inn. Når tiltaket er åpent uten å være varslet, har den aktuelle personen mulighet for å skaffe seg kunnskap om tiltaket, men får ikke hjelp til å huske det og innrette seg. "Hemmelig" innebærer at det verken gis varsel eller er tilgjengelig informasjon om at overvåkingsteknologien er i bruk.

- Datanivå sikter til hvor nær de data som samles inn er de faktiske hendelsene som teknologien er satt til å registrere opplysninger om. Jeg antar det som oftest er mulig å skjelne mellom data som beskriver selve handlingen/hendelsen direkte ("primærdata"), og data som kun beskriver de ytre rammene av handlingen/hendelsen ("sekundærdata"). Dette skillet er lett å anvende på telekommunikasjon der et tilsvarende skille kan betegnes "innholdsdata" og "trafikkdata", og der innholdet (jf "primærdata") er selve meningsinnholdet i kommunikasjonen (ordene som blir sagt/skrevet, bildene som blir vist), mens trafikkdata (jf "sekundærdata") forteller om når kommunikasjonen fant sted, mellom hvilke apparater, varighet, størrelsen på filer som blir sendt mv.

- Kommunikasjonspartnere beskriver hvorvidt det skjer kommunikasjon mellom to eller flere parter og i så fall mellom hvem/hva. Fysiske personer kan kommunisere direkte eller helt eller delvis ved hjelp av datamaskinsystemer.[93]

- Inngrepspunkt beskriver hva teknologien retter seg mot. Infrastruktur er for eksempel linjenett for dataoverføring, og sluttbrukerutstyr er telefoner, PCer og annet utstyr som personene det samles data om disponerer (f.eks. adferdsregistrator som er installert i bilen). Inngrepet kan også skje i det fysiske miljøet der personer befinner seg, for eksempel innen en privat sfære.

- Uttrykksform gjelder om dataene som samles inn og behandles er skrift, bilder, lyd eller annet; f.eks. måleresultater fra en sensor eller lignende. Måleresultater kan også sies å være "skrift", men tallverdier som uttrykker mål har jeg valgt å se som noe eget.

- Varighet av data uttrykker noe om hvor varig dataene eksisterer. Lagring innebærer at dataene eksisterer ut over "sann tid", og monitorering innebærer at dataene kun observeres i sann tid - der og da.

- Tilleggskrenkelse sier noe om installering og/eller bruken av teknologien gjør det nødvendig å foreta handlinger som i seg selv er personvernkrenkende. Dersom det kan være nødvendig å stanse kjøretøy for å kontrollere at enheter med ts-teknologi ikke er sabotert/satt ut av drift, vil slike kontroller kunne ses på som en krenkelse av bilen som privat område.

- Ekstern bistand gjelder om behandlingsansvarlige er alene om installering og bruk av teknologien, eller om det er behov for ekstern bistand fra én eller flere andre aktører. Dersom en vurderer personvernet, vil fravær av eksterne aktører ved installering og drift, i

[93] . En persons bruk av egen maskin (jf "menneske - maskin") regner jeg imidlertid ikke som kommunikasjon fordi maskinen er under personens rådighet.

utgangspunktet være å foretrekke fordi det må antas å gi best oversikt og styring med at regler mv blir overholdt.[94]

I tabellen er variable som typisk antas å gi mest inngripende virkninger for personvernet satt til venstre for antatt mer lempelige alternativer. Dette er basert på en skjønnsmessig generell vurdering som derfor inneholder enkelte diskutable valg. Når jeg i de tre neste avsnittene bruker oppsettet for å sammenligne ts-teknologi med relevante politimetoder, gir klassifiseringen og innplasseringen av den enkelte teknologi på skjemaet kun visse *indikasjoner* på hvor inngripende metodene er i forhold til hverandre. Flere klassifiseringer er dessuten basert på forutsetninger som jeg gjør rede for i teksten, og som gjør at tabellene ikke kan leses uten forbehold.

6.2 Streknings-ATK sammenlignet med teknisk sporing

Politiet kan få tillatelse til å foreta teknisk sporing i samsvar med straffeprosessloven § 202b ved etterforskning av forbrytelser som har strafferamme på 5 år eller mer. Metoden innebærer at teknisk peileutstyr plasseres på kjøretøy, gods eller andre gjenstander for å klarlegge hvor den mistenkte eller gjenstandene befinner seg. Et poeng med teknisk sporing er at flere peilinger gir grunnlag for informasjon om rute, tidspunkter og hastigheter. Streknings-ATK bruker kamerateknologi, mens teknisk sporing for eksempel skjer ved hjelp av GPS eller lignende.[95] Selv om den teknologiske gjennomføringen er forskjellig, kan teknisk sporing uansett sies å ligne streknings-ATK, fordi den delvis gir samme type data når sporingen skjer i forhold til et kjøretøy.[96]

*StrekningsATK = **S**, teknisk sporing = **T***

Variable	Mulige verdier			
Kjennskap	Hemmelig **T**	Åpent, ikke varslet	Varslet **S**	Aktivt varsel
Datanivå	Begge	Primærdata	Sekundærdata **S, T**	
Kommunikasjonsparter	Menneske - menneske	Menneske - maskin	Maskin - maskin **S, T**	
Inngrepspunkt	Fysisk miljø	(Slutt)bruker-utstyr **S, T**	Infrastruktur	
Uttrykksform	Skrift	Bilde **S, T**	Lyd	Måleresultater **S, T**
Varighet av data	Lagring **S, T**	Monitorering		
Tilleggskrenkelse	Ja **S, T**			
Ekstern bistand	Ja **S**			

Tabell 2. Sammenligning mellom streknings-ATK og teknisk sporing

En vesentlig forskjell mellom de to metodene er at teknisk sporing alltid er (forsøkt) hemmeligholdt så lenge sporingen skjer, mens streknings-ATK er varslet ved skilting slik at

[94] Et annet spørsmål er ekstern kontroll ("kontroll med kontrolløren") som selvsagt ikke er "bistand".
[95] Streknings-ATK vil i teorien også kunne baseres på GPS dersom hvert kjøretøy hadde hatt en senderenhet som identifiserte kjøretøyet.
[96] Dvs. opplysninger om posisjoner, bevegelser og dermed hastigheter. Personfoto mangler ved teknisk sporing og opplysninger om personers identitet kan derfor være usikker.

føreren kan bli oppmerksom på at kontrollen skjer. Det er derfor godt mulig å innrette seg etter streknings-ATK, mens personer som er utsatt for teknisk sporing kun kan innrette seg ut i fra antagelse om at sporing skjer. I begge tilfelle gjelder det kun innsamling av data som beskriver et kjøretøys bevegelser, og overvåkingen griper ikke inn i kommunikasjon av ytringer mellom kommunikasjonspartnere. I begge tilfelle fremkommer informasjonen primært som måleresultater som delvis også kan fremkomme som bilde/grafikk på kart, for eksempel ved visualisering av hvordan kjøretøyet kan ha beveget seg på veinettet. Felles for begge metoder er at det som minimum skjer kortvarig lagring, og langvarig lagring dersom innsamlede data kan ha betydning som bevis for straffbar handling. Etter strpl § 202b er det ikke hjemmel for at politiet kan bryte seg inn i kjøretøyet for å plassere peileutstyr. Tilgang til innsiden av kjøretøyet er ikke nødvendig med streknings-ATK som gjør bruk av registreringsnummer. Med streknings-ATK vil det imidlertid være nødvendig med ekstern bistand (politiet bistås av Statens vegvesen),[97] mens ved teknisk sporing er politiet alene om tiltaket.

Vurdert ut i fra hensynet til personvern er teknisk sporing mer inngripende enn streknings-ATK. Det at sporingen er hemmelig er særlig viktig for vurderingen. Andre sider ved streknings-ATK kan imidlertid ses som mer problematisk for personvernet enn teknisk sporing. For eksempel deltar flere aktører ved streknings-ATK enn ved sporing, noe som øker muligheten for at personopplysninger kommer på avveie.[98] Selv om de to typene teknologibruk kan sies å være mest inngripende på hver sine områder, må likevel teknisk sporing *samlet sett* sies å være mest inngripende fordi manglene åpenhet/varsling må tillegges relativt stor vekt.

[97] Eventuelt senere av Statens innkrevingssentral.

[98] Forskjell i alvorlighetsgrad om innholdet av opplysningene har åpenbart også betydning. Med teknisk sporing kan opplysningen for eksempel gjelder mistanke om grovt heleri, mens det med streknings-ATK vil gjelde fartsoverskridelser som normalt anses som mindre alvorlig (med mindre den er særlig grov og/eller er knyttet til annet lovbrudd.

6.3 ISA sammenlignet med teknisk sporing

Jeg forutsetter at ISA opererer på grunnlag av informasjon om bilens posisjon og fartsgrensen på vedkommende sted, og at det skjer logging og lagring av disse opplysningene.[99]

*ISA = **I**, teknisk sporing = **T***

Variable	Mulige verdier			
Kjennskap	Hemmelig **T**	Åpent, ikke varslet	Varslet	Aktivt varsel **I**
Datanivå	Begge	Primærdata	Sekundærdata **I, T**	
Kommunikasjonsparter	Menneske - menneske	Menneske - maskin	Maskin - maskin **I, T**	
Inngrepspunkt	Fysisk miljø	(Slutt)bruker-utstyr **I, T**	Infrastruktur	
Uttrykksform	Skrift	Bilde **T**	Lyd	Måleresultater **I, T**
Varighet av data	Lagring **I, T**	Monitorering		
Tilleggskrenkelse	Ja **I, T**			
Ekstern bistand	Ja **I**			

Tabell 3. Sammenligning mellom ISA og teknisk sporing

Den store forskjellen mellom ISA og teknisk sporing gjelder kjennskapen til at teknologien brukes. Politiets tekniske sporing er hemmelig, mens jeg forutsetter at fartstilpasning er aktivt varslet. For øvrig er de to tiltakene temmelig like, målt etter de kriterier som her er valgt. I begge tilfelle vil det skje en "tilleggskrenkelse" fordi forutsetningen for ordningene trolig er at myndigheter må kunne skaffe seg tilgang til utstyret (og dermed bilen) for å sjekke om det virker slik det skal og ikke er manipulert med eller lignende. Teknologi for fartstilpasning kan imidlertid sies å være mest inngripende på punktene "ekstern bistand" (fordi verksted mv trolig må ha tilgang til enheten der data er lagret).

6.4 Atferdsregistrator sammenlignet med dataavlesing

I denne sammenlignende drøftelsen legger jeg til grunn atferdsregistratorer som samler inn relativt mye data. En slik forutsetning er rimelig å gjøre fordi teknologien vil kunne fylle flere behov som også i fremtiden må antas å bli tillagt stor samfunnsmessig betydning. Dette gjelder selvsagt behov knyttet til arbeidet for trafikksikkerhet. I tillegg kan kjøre-/atferdsdata være grunnlag for bruk av økonomiske virkemidler; dels ved at miljøskadelig atferd utløser avgift, og dels ved at data vedrørende bilbruken gir grunnlag for prising av veibruken - eventuelt i kombinasjon.[100] Data fra atferdsregistratorer kan også være av stor verdi ved etterforskning av straffbare handlinger mv. Slike data vil også være meget kjærkomne i

[99] Jf. for eksempel fartstilpasningssystemet SSV4 som bl.a. fungerer ved at "Detailed data is logged and can be downloaded and viewed directly on a PDA using Bluetooth wireless technology. Data includes impact reports, number of times the speed limit was exceeded, average speed and much more." http://www.speedshield.com/main/products/SSV4.aspx.

[100] Jf. for eksempel Ministry of Transport, Public Works & Water Management (Nederland) 2009 vedrørende vedtaket om å innføre GPS-basert veiprising.

tilknytning til forsikringsoppgjør etter ulykker.[101] I tillegg vil dataene kunne være av stor verdi for bilindustriens videreutvikling av sine produkter og som grunnlag for trafikksikkerhetsforskning mv.[102] Det er lite trolig at alle slike sterke interesser vil kunne få gjennomslag i løpet av kort tid. Mer trolig er det at flere interessegrupper gradvis vil kunne få tilgang etter hvert som den sosiale akseptansen - eventuelt - gjør dette mulig.

Bruk av atferdsregistrator tilsvarer ikke noen inngripende etterforskningsmetode som er tillatt etter norsk straffeprosesslovgivning, men har flere likhetstrekk med dataavlesing. Dataavlesing er som sådan ikke tillatt brukt av politiet i Norge, men metoden er innført og brukt i flere andre land, se for eksempel den danske retsplejeloven § 791 a. Dataavlesing har også blitt drøftet som ledd i norske lovgivningsarbeider.[103] Metoden har ingen helt fast definisjon, men innebærer at politiet kan avlese ikke offentlig tilgjengelige opplysninger i informasjonssystemet uten å være tilstede der informasjonssystemet fysisk befinner seg. Både maskin- og programvare kan benyttes for å lese av.[104] I den sjablonmessige klassifiseringen av dataavlesing nedenfor, har jeg tatt utgangspunkt i en vid definisjon av begrepet, dvs. beskrivelsen er basert på den mest inngripende forståelsen av denne etterforskningsmetoden.

*Atferdsregistrator = **A**, dataavlesing = **D***

Variable	Mulige verdier			
Kjennskap	Hemmelig **D**	Åpent, ikke varslet **A**	Varslet	Aktivt varsel
Datanivå	Begge **D**	Primærdata	Sekundærdata **A,**	
Kommunikasjonsparter	Menneske - Menneske **D**	Menneske - maskin **D**	Maskin - maskin **A, D**	
Inngrepspunkt	Fysisk miljø	(Slutt)bruker-utstyr **A, D**	Infrastruktur	
Uttrykksform*	Skrift **D**	Bilde **D**	Lyd **D**	Måleresultater **A, D**
Varighet av data	Lagring **A, D**	Monitorering **D**		
Tilleggskrenkelse*	Ja **D**			
Ekstern bistand	Ja **A**			

Tabell 4. Sammenligning mellom atferdsregistrator og dataavlesing

Tabellen indikerer forholdsvis store forskjeller mellom de to overvåkningsteknologiene. I to spørsmål merket * kan imidlertid likhetene være større enn klassifiseringen gir inntrykk av, jf straks nedenfor. Den største forskjellen er at atferdsregistrator for trafikksikkerhetsformål forutsettes å skje i full åpenhet mens dataavlesing alltid er hemmelig. Begge fremgangsmåter kan sies å innebære innhenting av sekundærdata, men dataavlesing kan også settes opp for å

[101] På lignende måter som ved bruk av ISA.
[102] I sist nevnte tilfelle vil en ofte kunne ha nytte av data i aggregert form, dvs uten direkte bruk av personopplysninger.
[103] Sist i NOU 2009: 15 s 235 - 250.
[104] Se nærmere om definisjonen i NOU 2004: 6 kapittel 10.7.11 side 207 og NOU 2009: 15, avsnitt 23.1.4.

fange opp innholdsdata. Inngrepspunktet er i begge tilfelle utstyr som personer bruker. De kan derfor ikke unngå tiltaket med mindre de avstår fra bruk.

Jeg har forutsatt at atferdsregistratorer kun gir bestemte måleresultater, noe som gir et langt mindre nært og direkte inntrykk enn det for eksempel opptak av tale og bilde mv gjør. Forutsetningen om at tale og bilde ikke vil være del av fremtidige atferdsregistratorer er imidlertid noe usikker. Taleregistrator i fly og Video Event Data Recorder (VEDR) i kjøretøy er tilgjengelig teknologi som lett kan tenkes kombinert med en fremtidig atferdsregistrator, for eksempel i busser og trailere. I begge tilfelle forutsetter jeg at det skjer lagring slik formålet tilsier.

Hvorvidt det vil foreligge en tilleggskrenkelse eller ikke, avhenger av definisjonen av krenkelse. I tilfelle dataavlesing vil det alltid foreligge krenkelse i form av et datainnbrudd eller ulovlig tilgang til og endring av sluttbrukerutstyr. I tilfelle atferdsregistrator, kan det hevdes å foreligge en krenkelse dersom teknologien ikke er frivillig å installere. I tillegg forutsetter en obligatorisk ordning at myndigheter kan skaffe seg tilgang til utstyret for å sjekke om det virker slik det skal og ikke for eksempel ulovlig er satt ut av drift. Ved atferdsregistrering vil det trolig være behov for ekstern bistand, uavhengig av hvem som er behandlingsansvarlig. Dette gjelder både ved installasjon, vedlikehold og avlesing av data. For dataavlesning er det et poeng at politiet skal kunne bruke slike metoder alene uten å involvere utenforstående, noe som gir bedre ivaretagelse av diskresjonshensyn.

6.5 Samlet vurdering

Som en omtrentlig indikasjon på hvor inngripende de ulike overvåkingsteknologiene kan sies å være, har jeg tilordnet hver av variablene i tabellene tall fra 4 - 1, der 4 tildeles første kolonne, 3 i annen kolonne, 2 i tredje kolonne og 1 i fjerde kolonne. Tildelingen av tallverdier er basert på oppsettet der alternativene på venstre side i tabellen er anslått som mer krenkende for personvernet enn alternativene til høyre. Derfor er alternativene under "Kjennskap" tilordnet verdiene "Hemmelig" = 4, "Åpent, ikke varslet" = 3, "Varslet" = 2 og "Aktivt varslet" = 1. Det er flere mulige innsigelser mot denne bruken av tall, men som grov indikasjon mener jeg fremgangsmåten kan forsvares. Sammenstillingen gir følgende resultater:

Dataavlesing	41
Streknings-ATK	25
Teknisk sporing	23
Automatisk fartstilpasning	21
Atferdsregistrator	19

Tabell 5. Tentativ rangering av teknologier som er sammenlignet i kap. 6

Svakheter ved tildelingen av tallverdier gir grunn til ikke å legge avgjørende vekt på forskjellene mellom de fire nederste kategoriene. Resultatet gir imidlertid grunnlag for å konkludere med at de aktuelle ts-teknologiene er klart mindre inngripende enn det (trolig) mest inngripende etterforskningsmiddelet som enkelte lands politimyndigheter rår over (dataavlesing). Samtidig er alle ts-teknologiene klart inngripende i forhold til personvernet, og tilsvarer omtrent samme inngrepsnivå som etterforskningsmetoden teknisk sporing.

En klar forskjell mellom teknisk sporing og streknings-ATK, ISA og atferdsregistrering, er at sporing kun gjelder når det sikkert er begått en straffbar handling som det er startet etterforskning av. I kontrast til dette iverksettes streknings-ATK og de andre trafikksikkerhetstiltakene permanent *uten* at den er foranlediget av en bestemt utført straffbar handling. Begrunnelsen er snarere en forventning om at mange slike straffbare handlinger vil komme til å skje. Forutsetningen er dessuten at eksistensen av overvåkingen statistisk sett vil redusere antallet brudd på vegtrafikkloven, og at tiltaket derfor har en preventiv effekt.

Teknisk sporing etter strpl § 202b kan tillates som ledd i etterforskning av utførte straffbare handlinger som kan gi fengsel i *fem år eller mer*.[105] Streknings-ATK, ISA og atferdsregistrator kan brukes for å avdekke mulige brudd på veitrafikklovens § 31. Denne bestemmelsen alene har en *øverste strafferamme på ett år*. Streknings-ATK og de andre metodene dekker med andre ord et intervall på fengselsstraff fra 0 til 1 år, mens teknisk sporing dekker et intervall fra 5 års fengsel til forvaring på ubestemt tid. Det er følgelig betydelige forskjeller når det gjelder krav til strafferamme. Imidlertid er det ikke straffverdigheten av hvert brudd på veitrafikkloven som alene begrunner slike tiltak, men like meget den avvergende effekten av trafikksikkerhetstiltakene. Vurdert ut i fra den enkelte som blir gjenstand for overvåkningen, kan det likevel synes som om det ikke er et rimelig forhold mellom personverninngrep og straffverdighet, dersom man sammenligner ts-teknologi og "etterforskningsteknologi". Det kan med andre ord synes som om den bruken av ts-teknologi som er forutsatt i dette kapittelet, vil være ute av proporsjon.

En forskjell som også skal nevnes her, er at etterforskningsmetoder som teknisk sporing er gjenstand for streng lovregulering, for eksempel med hensyn til hvem som kan beslutte iverksettelse av tiltaket.[106] Forsøk med streknings-ATK er derimot iverksatt uten særlig regulering.

Det er også verd å legge merke til at streknings-ATK fanger opp alle, uavhengig av hver sjåførs individuelle forhold. Til sammenligning kan teknisk sporing kun brukes overfor mistenkte personer, i samsvar med strenge krav som er fastsatt i lov. Selv om det ikke er mulig å gi individuell behandling med dagens ATK-målinger, er denne forskjellen av interesse. Jeg legger således til grunn at det ville latt seg gjøre å installere teknologi for fartsmåling som retter seg mot personer som på grunn av sine trafikale meritter blir ansett å være særlig farlige i trafikken.[107]

[105] Og dessuten for noen utvalgte straffebud vedrørende statens sikkerhet mv selv om strafferammen er lavere.
[106] Se strpl 202b, jf strpl § 216d annet ledd.
[107] En kan for eksempel tenke seg at en sender ble plassert i kjøretøy som er eiet av sjåfører som har vært tatt for grove fartsovertredelser mv. Slik individuell registrering kan tenkes å være en del av straffereaksjonen mot fartsovertrederen.

7 Avsluttende vurderinger

7.1 Noen kommentarer til hovedproblemstillinger i prosjektet

Hovedproblemstillingen i dette prosjektet gjaldt hvilke institusjonelle og prosessuelle forhold som kan sies å fremme og hemme innføringen av trafikksikkerhetstiltak med personvernimplikasjoner. Fokus i rapporten har vært rettslige forhold, særlig personvernlovgivning og generelle vurderinger av personvernet.

"Fremme" og "hemme" uttrykker en enten - eller tilnærming som ikke alltid er særlig oppklarende. Rettslige reguleringer av IKT har ikke sjelden blitt kategorisert som "hemmende", og i enkelte tilfelle er dette en dekkende beskrivelse. Ofte er imidlertid denne todelingen problematisk å legge til grunn uten videre problematisering. Det at lovgiver stiller krav til ts-teknologi kan for eksempel tenkes å være hemmende i den forstand at det forbyr maksimal bruk av teknologien eller at teknologien blir så kostbar å innføre at anvendelsen blir mindre omfattende enn ønsket.

Rettslige krav kan imidlertid også inneholde normer som kan ses som en forutsetning for effektiv og hensiktsmessig bruk av ts-teknologi *samtidig* som den begrenser bruken. Rettslig regulering kan for det første være forutsetning for sosial og politisk aksept for teknologibruken, og dermed for innføring av teknologien over hodet. Det er et grunnleggende og selvfølgelig premiss i demokratiske samfunn at politiske myndigheter kan avvise innføring av (bl.a.) teknologi med mindre det samtidig innføres rettslige garantier. Den rettslige reguleringen vil da åpenbart "hemme", men er samtidig et tiltak som gjør det politisk mulig å introdusere teknologien, noe som vel kan karakteriseres som å "fremme" teknologien?

Gitt grunnleggende rettsstatlige prinsipper, vil rettslig regulering av innføring og bruk dessuten kunne være en forutsetning for effektiv og hensiktsmessig bruk av ts-teknologi. For eksempel kan det i lov pålegge plikt for bileiere til å installere nødvendig teknologi i sine kjøretøy (jf legalitetsprinsippet i norsk rett). En rettsstatlig tilnærming begrunner dessuten stor grad av forutberegnelighet, noe som ofte vil kreve normer som binder trafikk-myndigheter, politi mv. Bare rettslige normer kan ha slik bindende effekt at det skaper særlig forutberegnelighet for allmennheten.[108] Normer som formuleres som instruks internt hos myndigheten, uttalelser i stortingsmeldinger, i informasjonsmateriale og på annen måte, gir typisk relativt større grad av usikkerhet. Tilstrekkelig forutberegnelighet forutsetter ofte rettslige bindinger, og rettslige bindinger kan derfor sies å "hindre".

Forutberegnelighet må også antas å være et viktig hensyn i samarbeidet mellom myndigheter, for eksempel i samarbeidet mellom politi og vegmyndigheter. Selv om en skulle velge å se bort i fra hensynet til borgernes interesser, ville det derfor trolig være et behov for bindende regulering i avtale eller lignende,[109] for på den måten å sikre en ordnet innføring og bruk av ts-teknologi.

[108] Dette betyr selvsagt ikke at rettslige reguleringer alltid etterleves og får den tiltenkte virkningen. Rettslige reguleringer vil imidlertid *typisk* ha større gjennomslagskraft enn andre normer fordi det er mulig å bruke rettssystemet for å sikre gjennomføringen.

[109] Avtaler og instrukser vil være bindende og gi tilstrekkelig forutberegnelighet *for myndighetene*, derimot ikke for befolkningen generelt, jf forrige tekstavsnitt.

At rettslig regulering i utgangspunktet ofte må ses på som nødvendig, betyr selvsagt ikke at slik regulering alltid er hensiktsmessig eller ønskelig. Derfor er diskusjoner om hva som bør være den samlede virkemiddelbruken vedrørende ts-teknologi viktig. Rettslig sett er det første spørsmålet hva som bør være *det garanterte minstenivået* for personvernet og rettssikkerheten i tilknytning til bruk av slik teknologi. Gitt et slikt nivå med garantert beskyttelse, blir spørsmålet hvilke virkemidler som er hensiktsmessige for, så langt som mulig, å ivareta personvern og andre interesser *ut over* dette minimumet. For å ivareta personvern i tillegg til det som må/bør rettslig garanteres, kan annet enn rettslige virkemidler tenkes å være mest hensiktsmessige. For eksempel kan regjeringen styrke personvernet ved å avklare myndighetsforhold, gi økonomiske incentiver til personvernøkende teknologi, iverksette informasjonskampanjer osv. Bruk av rettslige virkemidler der andre virkemiddeltyper vil være tilstrekkelig virksomme, vil ofte kunne klassifiseres som hemmende og uønsket bruk av rettslig regulering.

Lovregulering mv kan også sies å hemme dersom bestemmelsene ikke er utformet med en klarhet som gjør det mulig å forstå og etterleve bestemmelsene på en konsistent måte. En rekke forhold virker inn på forståelighet og problemer med implementering, men spørsmålet om *reguleringsnivå* er ofte en viktig faktor. Helt generell og "høytflyvende" lovgivning kan for eksempel gi store problemer med å fortolke bestemmelsene på konkrete livsområder. Det er for eksempel langt fra trivielt å fortolke personopplysningsloven (som gjelder helt generelt for behandling av personopplysninger) med tanke på ts-teknologi, jf kapitlene 3 og 4 ovenfor. Motsatt kan alt for partikulær regulering gi problemer med å anvende bestemmelser etter hvert som teknologiske og samfunnsmessige forhold endres uten at loven endres. Bl.a. derfor er det grunn til å være forsiktig med rettslig regulering av konkrete teknologier og i stedet regulere på et mellomnivå; for eksempel slik at grupper av teknologier reguleres ut i fra deres formål, virkning mv. Frykt for teknologispesifikk lovgivning må imidlertid ikke føre oss til den andre ytterligheten, jf. for eksempel personopplysningsloven som regulerer "alt" av fremtidig elektronisk behandling av personopplysninger, uavhengig av lovgivers vurdering av nye teknologier.[110] Avveiningen er med andre ord hva som er "passe" reguleringsnivå, ett sted mellom "evighetslovgiving" som passer det meste, og teknologispesifikke bestemmelser som kan ha helt kort varighet.

En annen grunn til å fremheve betydningen av den totale virkemiddelbruken er at rettslige virkemidler (som alle virkemidler) ikke eksisterer i et vakuum. Om rettslige virkemidler hemmer eller fremmer innføring og bruk av ts-teknologi, avhenger derfor også av hvilke *andre* virkemidler som fungerer sammen med rettsreglene. Lovgivning alene vil derfor åpenbart ha mindre effekt enn i kombinasjon med økonomiske, organisatoriske og pedagogiske virkemidler. Dersom det samtidig iverksettes slike andre virkemidler, kan lovgivning som alene fremstår som hemmende og uhensiktsmessig tenkes å bli fremmende og hensiktsmessig.

På bakgrunn av denne lille drøftelsen av hemmende og fremmende effekter av rettslig regulering vedrørende ts-teknologi, er det nærliggende å omformulere og utvide spørsmålet til å gjelde krav til virkemiddelbruk. De sentrale problemstillingene blir da:

1. Hvilke nærmere krav til bruk av rettslige virkemidler må oppstilles for at disse kan sies å være effektive og formålstjenlige?

[110] Utformingen av personopplysningsloven skjedde for eksempel før Internett, RFID og biometri hadde fått stor utbredelse. Internett ble bare undergitt noen enkle vurderinger i lovforarbeidene, mens biometrisk teknologi kun ble nevnt. Loven virker på disse og fremtidige teknologier til tross for at virkningen av lovgivningen ikke er vurdert og/eller kjent.

2. Hvilke institusjonelle og prosessuelle spørsmål vedrørende ts-teknologi må/bør være gjenstand for rettslig regulering av hensyn til personvern, rettssikkerhet, trafikksikkerhet og andre grunnleggende interesser?
3. Hvordan bør den samlede virkemiddelbruken, innbefattet de rettslige virkemidlene, være for å sikre effektiv ivaretakelse av de grunnleggende interessene?

I fortsettelsen vil jeg gi noen avsluttende vurderinger som i stor grad følger disse tre spørsmålsstillingene. I neste avsnitt drøfter jeg generelle krav til rettslig regulering, jf også deler av dette avsnittet. Dernest vil jeg i avsnittene 7.3 - 7.5 drøfte nærmere krav til slik lovgivning. Den samlede virkemiddelbruken vil bare delvis bli diskutert, og det er primært avsnittene 7.4 - 7.6 som er relevante for denne problemstillingen.

7.2 Krav til rettslig regulering

Kapitlene 3 og 4 i denne rapporten viste hvorledes personopplysningsloven trolig kommer til anvendelse på ts-teknologi. Fremstillingen viser en stor grad av kompleksitet i rettsspørsmålene og (dermed) også en usikkerhet mht innholdet av reguleringen. Spørsmål om kompleksitet og usikkerhet er i stor grad knyttet til det faktum at personopplysningsloven er en generell lov som ikke spesielt gjelder den type informasjonsbehandling som ts-teknologi forestår. Dels blir kompleksiteten større enn nødvendig fordi en generell lov må dekke flere eventualiteter enn det som er aktuelt for saksområdet trafikksikkerhet. Politi og vegmyndigheter må for eksempel sette seg inn i alle de detaljerte spørsmålene om rettslig grunnlag i pol §§ 8 og 9, selv om de fleste av disse ikke er aktuelle, jf avsnitt 4.3.1. I stedet kunne slike spørsmål være uomtvistelig avklart i særregler.

Usikkerhet skyldes også at begreper er formulert på et helt overordnet nivå, noe som samtidig skaper unødvendig kompleksitet og problemer med fortolkningen. Hvem som er "behandlingsansvarlig" byr for eksempel på vanskelige fortolkningsproblem når politi og vegmyndigheter samarbeider om streknings-ATK. Slike spørsmål kunne åpenbart forenkles og usikkerhet i stor grad elimineres dersom en i stedet hadde rettsregler som konkret tok stilling til plassering av behandlingsansvar.

Det kan selvsagt hevdes at usikkerheten etter dagens regulering også kan fjernes gjennom forvaltnings- og rettspraksis mv, særlig ved hjelp av praksis i Personvernnemnda. Slik avklaring vil imidlertid kunne ta lang tid å oppnå, og avklaringene vil bare fremkomme som fragmenter, i den takt og i det omfang klagesaker gir grunn til det. En slik strategi vil derfor innebære mer langvarig og større grad av rettsuvisshet enn en direkte rettslig regulering gir.

Hensynet til personvernet og kravet om innsyn og kunnskap,[111] og kravet til forutsigbarhet generelt, tilsier etter min mening en særlig rettslig regulering av spørsmål vedrørende innføring og bruk av ts-teknologi. I hvilken grad og på hvilken måte området bør reguleres rettslig, er imidlertid et annet spørsmål som jeg kommer tilbake til i avsnitt 7.3.

Plasseringen av særregulering kan tenkes i personopplysningsloven selv; mest realistisk med de fleste bestemmelser i forskriften til denne loven. Særregler kan også tenkes knyttet til eksisterende lovgivning på samferdselsområdet (vegtrafikkloven, vegloven), eller i egen ny lov. Hovedvalget gjelder plassering i eller uten for personopplysningsloven (med forskrift). Valg av systematisk plassering bør særlig være avhengig av i) hvilke rettslige sammenhenger

[111] Se Schartum og Bygrave 2004, s 49 flg.

som anses viktigst å kommunisere og ii) hvor store avvik fra personopplysningsloven en ønsker å vedta.

Dersom det i én lov er behov for å synliggjøre hvorledes personvern er ivaretatt i det norske samfunnet, taler dette for å plassere bestemmelser om ts-teknologi i personopplysningsloven med forskrifter. Personvern er imidlertid et så bredt og mangfoldig saksområde, at det åpenbart ikke er mulig å ha en slik ambisjon for denne ene loven. Helseregisterloven, straffeprosessloven og en rekke registerlover (folkeregister, strafferegister mv) er eksempler på lovgivning av vesentlig betydning for personvernet utenfor personopplysningsloven. En realistisk retningslinje for innholdet i personopplysningsloven bør derfor trolig være at loven fortrinnsvis skal inneholde bestemmelser som gjelder problemstillinger av generell karakter, dvs. som ikke er knyttet til en spesiell sektor eller fagområde. Desto mer generelle problemstillinger som reguleres, desto sterkere er argumentet for å regulere i personopplysningsloven. Gjelder reguleringen en spesiell sektor, vil det ofte også foreligge annen særlovgivning på feltet, og eksistensen av slik lovgivning vil være argument for å plassere bestemmelser innen samme området i samme særlov. Slik plassering vil også kunne gjøre det lettere å finne fram i reguleringen blant de som vil være daglige brukere av særreguleringene. Vegtrafikkloven vil for eksempel være godt kjent for politi og vegmyndigheter, mens samme inngående kjennskap til personopplysningsloven hos disse myndighetene ikke uten videre kan forventes.

Lovtekniske hensyn og hensynet til brukere av loven kan dessuten tilsi at en ved valg av plassering av særregler om ts-teknologi legger stor vekt på å få frem sentrale sammenhenger i lovgivningen. Dersom en for eksempel kun ønsker å gjøre enkelte spredte unntak fra personopplysningsloven, taler det i mot å gjenta mer eller mindre like bestemmelser i særloven.[112] I slike tilfelle bør en primært ta inn unntaksbestemmelsene i særloven, samtidig som en viser til de øvrige bestemmelsene i personopplysningsloven. Dersom en ønsker flere/vesentlige avvik fra bestemmelsene i personopplysningsloven, vil det være mest aktuelt å gi en særlov som dekker alle/de fleste aspekter, uten/med noen få henvisninger til personopplysningsloven.

Et annet forhold som taler for regulering i særlovgivning er hensynet til god saklig sammenheng mellom regulering for å ivareta personvern og regulering av andre typer spørsmål. Regulering av personvernspørsmål vedrørende ts-teknologi kan derfor sies å høre sammen med andre regler om trafikksikkerhet som ikke har med personvern å gjøre. Hensynet til politisk markering mv kan også tale for regulering i egen særlov som spesielt gjelder ts-teknologi.

Jeg vil ikke her trekke noen endelig konklusjon mht plassering av lov- forskriftsregulering, men nøyer meg med å legge til grunn at en viss grad av lov-/forskriftsregulering er påkrevet og/eller ønskelig (jf neste avsnitt). Meget taler dessuten for å velge en type særregulering i tilknytning til eksisterende samferdselslovgivning, men jeg avstår fra å drøfte den nærmere plasseringen av slike bestemmelser.

[112] Helseregisterloven er etter min mening et eksempel på problematisk bruk av personopplysningslovens regler som mal for bred regulering i særlovgivning.

7.3 Hvilke institusjonelle og prosessuelle spørsmål vedrørende ts-teknologi bør være gjenstand for rettslig regulering av hensyn til personvern og rettssikkerhet?

7.3.1 Innledning

Jeg vil i det følgende gi en kortfattet gjennomgang av det som kan anses å være de viktigste elementene i en fremtidig rettslig regulering av trafikksikkerhet. Utgangspunktet er ivaretakelse av personvern og rettssikkerhet, samtidig som hensynet til trafikksikkerhet kan ivaretas. Gjennomgangen er ikke ment å være dekkende, og vil ikke omfatte hensyn som alene kan begrunnes i trafikksikkerhet.

Jeg har av fremstillingsmessige grunner holdt spørsmål vedrørende utredning og evaluering av ts-teknologi utenfor gjennomgangen i dette avsnittet og i stedet valgt å behandle disse spørsmålene i egne avsnitt (7.4 og 7.5). Krav til utredning og evaluering kan imidlertid godt tenkes å være gjenstand for fremtidig rettslig regulering og derfor høre til de spørsmål som behandles i dette avsnittet.

Skillet mellom institusjonelle og prosessuelle spørsmål er stort sett greit å anvende. Samtidig er det sammenhenger mellom de to gruppene av spørsmål som det kan være en smakssak hvor en systematisk og framstillingsmessig vil plassere. Her vil jeg legge vekt på prosessuelle og dynamiske spørsmål, mens institusjonelle spørsmål primært er beskrevet som noen enkle (mer statiske) rammer som særlig er knyttet til spørsmål om personell kompetanse.

7.3.2 Rettslig regulering av institusjonelle spørsmål knyttet til ts-teknologi

I avsnitt 4.2 drøftet jeg spørsmålet om behandlingsansvar for personopplysninger knyttet til ts-teknologi. Selv om det er mulig å konkludere vedrørende dette rettslige spørsmålet, er resonnementet langt fra enkelt og svarene ikke sikre. Konklusjonene vil dessuten forbli usikre inntil tilstrekkelig forvaltnings- og/eller rettspraksis har etablert en fast praksis. Det kan hevdes at det er unødvendig og uakseptabelt at det skal være usikkerhet om hvem som primært har rettslige plikter og ansvar for behandling av personopplysninger i samband med ts-teknologi. Spørsmål om hvem som har behandlingsansvar kan derfor hevdes å være så viktig at det bør reguleres direkte i lov.

Det er flere forhold som trekker i retning av direkte regulering av spørsmålet om hvem som har behandlingsansvar. For det første er det grunn til å tro at både Politidirektoratet og Vegdirektoratet vil være forholdsvis likeverdige aktører i samarbeidet om introduksjon og bruk av ts-teknologi. Trolig vil det være mange oppgaver vedrørende utvikling, installering, drift, vedlikehold, evaluering og forbedring av de tekniske ts-systemene, at politi og vegmyndigheter (og andre) vil måtte inngå i tette samarbeidsforhold, noe som kan skape uklarhet om ansvarsdelingen. Spørsmålet er med andre ord spesielt fordi minst to myndigheter kan forventes å være sterkt involverte med formell og/eller faktisk innvirkning på hvorledes teknologien vil bli anvendt til å behandle personopplysninger.

Uansett konklusjon med hensyn til plassering av behandlingsansvar, vil den myndighetsparten som ikke har eller bare delvis har slikt ansvar, trolig være å anse som databehandler (helt eller delvis), jf avsnitt 4.2.3. Innholdet av samarbeidet mellom behandlingsansvarlige myndighet og myndighet som er databehandler vil være så viktig for ivaretakelsen av personvern, at en nøye bør vurdere å også regulere denne relasjonen spesielt (jf pol § 15). For det første bør det vurderes om det er tilfredsstillende at denne relasjonen reguleres i avtale, eller om innslaget

av myndighetsutøvelse i slike samarbeider er så stort at lov- eller forskriftsformen bør velges. Uansett kan en i lov eller forskrift stille mer spesifikke krav og gi fastere rammer for avtaleregulering mellom myndighetene.

Spørsmålet om behandlingsansvar er dessuten spesielt fordi det kan oppstå uklarhet om kjøretøyets eier kan sies å ha kontroll med ts-utstyr i kjøretøyene på måter som gjør at eier helt eller delvis blir behandlingsansvarlig. Problemstillingen kan med andre ord være om det er private eiere eller myndigheter som skal anses å ha behandlingsansvar for de personopplysninger som teknologien i private kjøretøy genererer. Biler vil eksempelvis kunne være utstyrt med kjøreboksystemer med funksjoner som delvis dekker det samme som atferdsregistratorer, slik at private eiere anskaffer utstyr som er egnet for myndighetenes trafikksikkerhetsarbeid. Myndigheter kan endog i lov stille krav til at kjøretøy skal ha slikt utstyr. Utstyret blir da i utgangspunktet privat, samtidig som det er en glidende overgang der myndigheters tilgang til opplysninger fra slike systemer blir så rutinisert og omfattende at opplysningene bør regnes - helt eller delvis - å høre inn under myndighetens behandlings-ansvar.

Det neste institusjonelle spørsmålet som skal nevnes her, gjelder tilsyn og tilsynsmyndighet. Dagens lovgivning innebærer at Datatilsynet vil ha tilsynsmyndighet i forhold til politiets og vegmyndigheters behandling av personopplysninger fra ts-teknologi. Unntaket er de deler av personopplysningsloven som gjelder individuelle rettigheter og der det i stedet er rettspleielovene som regulerer forholdet, jf avsnitt 3.2.5.[113] Utgangspunktet må være at det er viktig med en sterk tilsynsfunksjon i forhold til ts-teknologi. Årsaken er at det både er sentrale personvern- og rettssikkerhetsinteresser som skal ivaretas. Slik teknologi vil i stor grad være innrettet mot personopplysninger som skal/kan være grunnlag som bevis for straffskyld, erstatningsansvar, redusert forsikringsutbetaling mv. Dette gjør at hensynet til personopplysningsvern og rettssikkerhet langt på vei smelter sammen og samlet begrunner et spesielt sterkt tilsyn. Det kan etter min mening være tvilsomt om Datatilsynet kan ha kapasitet til å prioritere dette bestemte saksområdet tilstrekkelig til at det oppnås et godt nok tilsyn. Samtidig kan det være grunn til å vurdere om tilsyn med ts-teknologi, herunder med personopplysninger fra slik teknologi, bør inngå i diskusjonen om opprettelse av et vegtilsyn, jf avsnitt 4.6.

Et siste spørsmål av institusjonell karakter som skal nevnes her, er spørsmålet om behovet for uavhengig kompetanse innen ts-teknologi. Spørsmålet er særlig aktuelt i den utstrekning opplysninger fra slik teknologi vil komme til å inngå som bevis i straffesaker. Dette gjelder straffesaker ved brudd på vegtrafikkloven, men er spesielt viktig på grunn av teknologiens potensiale for generelt å bli kilde for elektroniske bevis ved etterforskning og iretteføring i saker som gjelder enda alvorligere kriminalitet. Hensynet til rettssikkerhet tilsier at det legges til rette for en reell, selvstendig og kritisk granskning av slike bevis, herunder vedrørende påliteligheten av målinger, muligheter for manipulering av data mv. Det er neppe grunnlag for etablering av et eget fagmiljø som skal bistå domstoler og parter innen dette spesielle teknologiområdet. Behov knyttet til ts-teknologi kan imidlertid inngå i en diskusjon av behovet for fagmiljøer som kan sikre bruk av elektroniske bevis mer generelt, jf den rollen Rettsmedisinsk institutt har i forhold til bedømmelse av bevis vedrørende medisinske forhold.

[113] I disse unntakstilfellene er det primært domstolene som kontrollerer etterlevelsen av rett til innsyn i og krav til sletting av personopplysninger mv.

7.3.3 Rettslig regulering av prosessuelle spørsmål knyttet til ts-teknologi

7.3.3.1 Innledning

Jeg vil i det følgende gjennomgå de viktigste prosessuelle spørsmål som aktualiseres av hensynet til personvern og tilknyttede rettssikkerhetsspørsmål. Gjennomgangen vil i stor grad følge systematikken i personopplysningsloven og annen lovgivning som gjelder personvern.

Jeg behandler prosessuelle spørsmål i vid betydning. På dette området kan en velge å spørre hva som må/bør skje/gjøres (jf. prosessen) eller hva som må/bør være tilfellet/situasjonen (jf resultatet). At jeg her har valgt å bruke en prosessuell tilnærming, betyr ikke at jeg argumenterer for at eventuelle fremtidige rettsregler ikke skal formuleres som mer materielle krav til hvilken situasjon som bør foreligge mv.

7.3.3.2 Eksistens og omfang av personopplysninger

Personvernvern i betydningen personopplysningsvern aktualiseres av at det eksisterer personopplysninger. Desto færre personopplysninger som blir behandlet, og desto kortere tid lagring av opplysningene skjer, desto bedre for ivaretakelsen av personvern. Slik sett er streknings-ATK som innebærer to registreringer av alle kjøretøy som passerer, klart mer inngripende overfor personvernet enn punkt-ATK som kun registrerer kjøretøy (én gang) dersom de har for høy hastighet. Tiltak for å øke trafikksikkerheten som ikke innebærer behandling av personopplysninger, og for øvrig tiltak som i minst mulig grad innebærer behandling av personopplysninger, er derfor klart å foretrekke fra et personvernsynspunkt. På denne bakgrunn kan det være grunn til å kreve at alternativ virkemiddelbruk alltid skal være vurdert. Vurderingen bør resultere i at personverninngripende tiltak kun tillates dersom de klart gir bedre resultater for trafikksikkerheten enn andre tiltak, jf også avsnitt 7.6 (nedenfor).

Eksistensen av personopplysninger som er samlet inn må også begrenses ved å velge så kort lagringstid som mulig. Det er her tale om to hovedstrategier: For det første kan det stilles krav til sletting når opplysningene ikke lengre er nødvendige. Av avgjørende betydning her er i hvilken grad og på hvilken måte det skal lagres historikk, og hvem som skal ha tilgang til denne. Historikk for personopplysninger som ikke gjelder påviste lovbrudd kan neppe forsvares over hode, og slike opplysninger må raskest og sikrest mulig slettes. Dersom opplysningene (hevdes) å bevise lovbrudd, må de i utgangspunktet kun lagres inntil saken er rettskraftig avgjort.

Eksistensen av personopplysninger kan også reduseres ved hjelp av rutiner for anonymisering, dvs. ved fjerning av identifiserende kjennetegn slik at identitetene ikke kan gjenopprettes. Det kan bl.a. være ønskelig å beholde slike anonymiserte data av hensyn til effektiv kontroll med trafikksikkerhetstiltaket, styring og statistikk. Evaluering av og forskning på virkning av ts-teknologi kan også gjøre det ønskelig med pseudonymisering av personopplysningene. Dermed kan individer følges uten at disse kan identifiseres. Det bør i så fall vurderes rettslige krav til sikker pseudonymisering. [114]

[114] Om gjennomføring av sikker pseudonymisering mv, se L'Abée-Lund 2006.

7.3.3.3 Hvor identifiserbare skal personopplysninger være?

Når det først foreligger personopplysninger (jf forrige avsnitt), er vurderingen av personvernet blant annet knyttet til hvor lett det er å koble opplysninger til bestemte fysiske personer. Desto mer direkte og åpenbar sammenhengen mellom en konkret person og opplysninger om denne personen er, desto mer kommer personvernspørsmålet på spissen. Opplysninger som primært er knyttet til et kjøretøy og bare indirekte kan knyttes til en eller flere personer, gjør at personvernspørsmålene blir viktigst dersom koplingen til person skjer.[115] Det kan derfor for det første være grunn til å beskytte identiteten i så stor grad som mulig, for eksempel ved at identifiserbare opplysninger (registreringsnummer, personbilder mv) krypteres eller på annen måte gjøres utilgjengelig uten særlig autorisasjon. Identitetene kan også beskyttes på annen måte, for eksempel ved å bruke pseudonymer i så store deler av behandlingen som mulig.[116] I tilknytning til kryptering og/eller pseudonymisering vil det også være behov for regler om vilkår for dekryptering, tilbakeføring av virkelige identiteter i stedet for pseudonymer osv. Identiteter kan for eksempel tenkes kun å foreligge i kryptert/pseudonym form, med mindre det igangsettes straffeforfølging. Opplysninger som ikke leder fram til påtale mv, bør slettes så tidlig som mulig.

7.3.3.4 Rettslig grunnlag for å samle inn og viderebehandle personopplysninger

Enhver innsamling og videre behandling av personopplysninger skal ha et rettslig grunnlag, jf pol § 8, se avsnitt 4.3.1 (ovenfor). Personverndirektivet binder imidlertid ikke statene til å gjøre bruk av en bestemt type grunnlag, noe som bl.a. innebærer at statene står fritt til å fastsette behandlingsgrunnlag i lov. I stedet for å velge behandling av personopplysninger som nødvendiggjør forholdsvis kompliserte vurderinger av rettslig grunnlag[117] kan man derfor velge å gi en uttømmende hjemmel i lov og/eller forskrift for behandlingen. Velger en å etablere rettslig grunnlag i lov eller i medhold av lov, vil det også legge til rette for lovregulering av andre aspekter ved ivaretakelsen av personvern i tilknytning til ts-teknologi.

7.3.3.5 Regler om formål

Det er avgjørende for muligheten til å kunne forutsi graden av personvern at det for all behandling av personopplysninger knyttet til ts-teknologi fastsettes hva opplysningene skal brukes til. Slike formål bør fastsettes på forhånd og være styrende for all bruk av opplysningene. Jo mer stabile formålene er, desto bedre forutberegnelighet. Mest stabile er formål som fastsettes i lov eller i forskrift i medhold av lov, dvs. på måter som krever grundige og relativt tidkrevende vedtak å endre. Forutberegneligheten øker dessuten med detaljeringsgraden i formålsbestemmelsen. Fastsettelse av detaljerte formål i lov gir imidlertid ikke i seg selv noe sterkt personvern; kun en forholdsvis sikker kunnskap om hvor godt eller dårlig personvernet er ivaretatt.

Fastsettelse av formål i lov eller forskrift kan dessuten hevdes å representere den mest demokratiske reguleringsmåten: For det første er formålet/formålene for bruken av personopplysninger sentralt i vurderingen av hvor godt personvernet ivaretas. For det andre

[115] Selve muligheten for at denne koplingen kan skje må imidlertid ses på som et personvernspørsmål, bl.a. på grunn av den usikkerhet dette kan skape.
[116] Pseudonymer innebærer mulighet for å følge enkeltindivider uten at individenes reelle identitet røpes, se f.eks. L'Abée-Lund 2006.
[117] Jf samtykke, lovhjemmel og nødvendig grunn etter pol § 8, samt § 9 dersom det er sensitive personopplysninger.

representerer lov- og forskriftsvedtak de mest demokratiske vedtaksformene, fordi det i begge tilfeller vil skje en åpen offentlig høring før endelig vedtak skjer i et politisk ansvarlig organ.

Til slutt skal nevnes at formål ofte vil være avgjørende for hvilke krav en stiller til opplysningskvalitet, jf avsnitt 7.3.3.7. Formålet vil dessuten kunne ha stor innvirkning på sikkerhetsnivået, for eksempel slik at formål som kommer inn under taushetsplikt krever strengere konfidensialitets- og integritetsvern enn andre opplysninger.

7.3.3.6 Regler om innsyn og åpenhet

Bruk av ts-teknologi som behandler personopplysninger vil trolig ofte være begrunnet i at teknologien har preventiv effekt og/eller at den gjør det lettere å kunne dokumentere lovbrudd og/eller forklare ulykkestilfeller. Det er trolig intet ved slike målsettinger som i utgangspunktet tilsier begrenset innsyn i og informasjon om hvilke personopplysninger teknologien registrerer og behandler. Tvert i mot tilsier mulige forebyggende effekter at sjåfører er bevisst eksistensen av og funksjonsmåten for ts-teknologi som finnes i kjøretøyet eller som kjøretøyet ellers vil kunne bli eksponert for. Unntak er informasjon som kan gjøre det mulig for sjåføren å unngå de ønskede effektene av teknologien, jf avsnitt 7.3.3.9 om informasjonssikkerhet.

Det er i utgangspunktet trolig ikke grunn til å forutsette andre regler om innsyn mv for personopplysninger knyttet til ts-teknologi enn for innsyn etter de generelle bestemmelsene i pol § 18, jf § 23. Uansett er det grunn til spesielt å legge vekt på åpenhet rundt ts-teknologi for derved å motvirke unødvendig skepsis og mytedannelser. Her er trolig generell informasjon av sentral betydning.

En grunnforutsetning for tilstrekkelig ivaretakelse av personvern er at det er fastsatt hvem som er ansvarlig for de personopplysninger som blir behandlet (jf avsnitt 7.3.2 om behandlingsansvar), og særlig hvem som konkret kan kontaktes dersom en ønsker å rette spørsmål og/eller krav om behandlingen av personopplysninger (jf. "daglig ansvar"). Det er videre viktig at det er lett tilgang til åpen informasjon om eksistensen av teknologien og hvorledes den fungerer. Den generelle informasjonen bør også dekke opplysninger om hvorledes behandlingen av personopplysninger er regulert. Informasjonen må endatil omfatte individuelle rettigheter til innsyn i opplysninger om egen person, adgangen til å kreve opplysninger supplert, slettet e.l. Sist men ikke minst bør informasjonen omfatte opplysninger om hvem som kan svare på spørsmål og veilede om relevant teknologi og rettslig regulering. Særlig gjelder dette hvis det (også) er andre som medvirker enn den med daglig ansvar for behandlingen.

7.3.3.7 Krav til opplysningskvalitet

Krav til kvaliteten på personopplysninger gjelder selvsagt ikke bare identifiserende opplysninger (personalia mv), men også alle andre opplysninger som kan knyttes til personen. Derfor vil mange opplysninger som kan være grunnlag for strafferettslig reaksjon eller lignende være personopplysninger som det må stilles kvalitetskrav til. Dette kan for eksempel gjelde opplysningens om kjøretøyets posisjon og fart og alle opplysninger som er resultatet av behandlingen, dvs. opplysninger i en påtaleavgjørelse, dom eller lignende. Krav til opplysningskvalitet kan for eksempel gjelde apparatur og fremgangsmåter ved bruk av utstyret på lignende måte som det er fastsatt regler for utstyr, fremgangsmåter mv for ulike

typer fartsmålinger.[118] For å utgjøre en tilstrekkelig garanti for personvern og rettssikkerhet, bør regler om opplysningskvalitet mv fastsettes på generelt bindende måte, dvs som lov eller forskrift (ikke som instruks slik det i dag er gjort for ATK).

7.3.3.8 Regler om sammenstilling av opplysninger

I de generelle reglene i personopplysningsloven er det ikke noe direkte regulering av adgangen til å sammenstille personopplysninger fra flere kilder eller stilt krav til gjennomføringen av slik sammenstilling. Reguleringen er i stedet indirekte ved at det er restriksjoner på bruk av de mest kraftige identifikatorene som legger til rette for sammenstilling,[119] og ved at det er fastsatt egne regler om bruk av personprofiler.[120] For øvrig må sammenstillingen være i tråd med alle lovens øvrige krav, for eksempel vedrørende rettslig grunnlag, formål, opplysningskvalitet mv. I enkeltvedtak om konsesjon etter pol § 33 vil spørsmål om sammenstilling ofte være særlig regulert.

Sammenstilling av personopplysninger er særlig personvernsensitivt når det gjennomføres ved hjelp av personopplysninger som er samlet inn med forskjellige formål, til ulik tid, og med ulike krav til opplysningskvalitet mv. Slike forskjeller kan lett også gi problemer for kvaliteten av de opplysninger som sammenstillingen resulterer i.

Fra et personvernsynspunkt er det avgjørende at sammenstilling skjer på måter som gir tilfredsstillende opplysningskvalitet. Det er generelt grunn til å anta at sammenstilling av opplysninger fra bestemte, faste kilder vil gi bedre og sikrere resultater enn sammenstilling som bestemmes ut i fra situasjoner som oppstår og skjer ad hoc. Hensynet til personvern tilsier derfor en nærmere regulering av adgangen til å sammenstille personopplysninger fra flere kilder. Dersom det skal gis slik adgang, bør det videre positivt gis anvisning på hvilke kilder som kan benyttes og i tillegg stilles krav til bestemte fremgangsmåter som skal følges. En slik avgrensing og anvisning på prosedyrer og metoder vil med stor sannsynlighet gi langt bedre opplysningskvalitet enn uten. I samband med saker der opplysningene brukes som grunnlag for straffreaksjoner mv vil høy opplysningskvalitet også være av avgjørende betydning for den enkeltes rettssikkerhet.

Når det gjelder valg av reguleringsnivå for sammenstilling av personopplysninger, er det nærliggende å velge lov eller forskrift. Regulering av fremgangsmåter/metoder bør muligens reguleres på smidigere måter, for eksempel ved at det i lov eller forskrift henvises til etablerte standarder eller lignende. En slik tilnærming vil trolig gjøre det enklere å oppnå forbedringer av målemetoder mv.

7.3.3.9 Regler om informasjonssikkerhet

Behovet for sikring av personopplysninger knyttet til ts-teknologi vil jevnt over være høyt. Dette skyldes primært at opplysningene for en (liten) del av personene vil danne grunnlag for ileggelse av straff, erstatningsansvar, regresskrav fra forsikringsselskap og andre negative reaksjoner. Særlig vil det være behov for sikring av opplysningenes integritet og konfidensialitet, dvs. opplysningene må ikke kunne endres og må kun være tilgjengelig for en

[118] Se for eksempel instruks GP-4027 fra Politidirektoratet (2008) avsnittene 01.2 (generelt) og 02.1 - 02.5 (manuelle fartsmålinger).
[119] Jf. pol § 12 første ledd vedrørende entydige identifikatorer.
[120] Jf. pol § 21. Sammenstilling av personopplysninger skjer ofte ut i fra personprofiler, dvs. en antar at visse kombinasjoner av opplysninger kan si noe om personers egenskaper, behov, preferanser mv.

liten gruppe autoriserte personer. Samtidig er det viktig at opplysningene er tilgjengelige for de personer som skal ha slik tilgang, noe som bl.a. er en forutsetning for virkeliggjøring av registrerte personers rett til innsyn mv.

Reglene om informasjonssikkerhet i personopplysningsloven § 13 og detaljreglene i personopplysningsforskriften kapittel 2 er av helt generell karakter fordi reguleringen gjelder behandling av personopplysninger innen "alle" sektorer og saksfelt. Dagens generelle sikkerhetsbestemmelser angir for eksempel at sikkerheten skal være "tilfredsstillende"[121] og "at [det] skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig".[122] Slik generell og åpen regulering gir usikkerhet ved fortolkningen som er lite ønskelig. Sikkerhetsregler som konkret gjelder ts-teknologi kan gi klart mindre tolkningstvil og usikkerhet. Dette gjelder for eksempel institusjonelle spørsmål om hvem som har daglig ansvar for sikkerheten og hvem som skal gjennomføre sikkerhetsrevisjoner. Det gjelder også spørsmål om hvorledes risikovurdering skal skje, samt minstekrav til sikkerhetstiltak. Rettslige krav til sikring av ts-teknologi som er formulert på et "mellomnivå" vil både kunne kombinere ønsker om klarhet/forutberegnelighet og fleksibilitet.

7.3.3.10 Avsluttende bemerkninger

Gjennomgangen i avsnitt 7.3.3 dekker det jeg mener er de viktigste momentene i en vurdering av personvernet. Den er imidlertid resultatet av en bestemt tankegang som i dag er rådende ved rettslig regulering av personvernspørsmål i Europa, og sterkt preget av personverndirektivet og andre internasjonale rettslige instrumenter på området. Personverndirektivet gjelder ikke innen det strafferettslige området.[123] Personvernfeltet er dessuten dynamisk og det kan skje at det over tid utvikles andre tilnærminger. Endrede oppfatninger i befolkningen er selvsagt blant de bevegelser som kan gi grunn til å endre oppfatninger av hva som er viktig for realiseringen av personvern. Stemningen kan trolig slå begge veier: Vi kan tenke oss en stadig større tilnærming til at personopplysninger blir behandlet, og dermed en gradvis avsliping og modifisering av vernet. Motsatt kan det tenkes at en eller flere saker/hendelser får begeret til å renne over,[124] med skjerpede krav til personvern som resultat.

7.4 Krav til utredning

Utredningsinstruksen[125] stiller en rekke krav til statlige utredningsarbeider. Et sentralt element i instruksen er kravet om konsekvensutredninger i instruksens kapittel 2. Kravet gjelder *forhåndsvurderinger* av konsekvenser, og det er derfor ikke i tråd med instruksen "å vente å se". Konsekvensutredningen skal gjelde tre aspekter: økonomiske konsekvenser, administrative konsekvenser og andre vesentlige konsekvenser. Her skal jeg nøye meg med å kommentere den sist nevnte gruppen.

Andre vesentlige konsekvenser er en forholdsvis åpen kategori, og i instruksen er det nevnt sju eksempler på hva slags konsekvenser det her siktes til. En av disse er konsekvenser for befolkningens helse og en annen gjelder forholdet til menneskerettighetene. I veiledningen til

[121] Se pol § 13.
[122] Se personopplysningsforskriften § 2-11
[123] Jf personverndirektivets artikkel 3 nr 2, se avsnitt 3.2.5 i denne rapporten.
[124] FRA-lagen, Datalagringsdirektivet og Iam.no er blant saker i det siste som tilsynelatende har skapt massive og negative reaksjoner.
[125] Se Utredningsinstruksen 2000.

Utredningsinstruksen punkt 11.3 fremgår det dessuten at personvern er et område hvor det kan være aktuelt med konsekvensvurderinger. Dersom saken kan forventes å ha klare konsekvenser for personvernet, skal disse altså utredes som et ledd i den ordinære utrednings-prosessen. Fornyings- og administrasjonsdepartementet har utarbeidet en egen veileder for vurdering av personvernkonsekvenser.[126]

I tilknytning til utredninger om innføring av ts-teknologi vil det etter dette foreligge klare føringer for innholdet i arbeidet. Økt trafikksikkerhet vil være det primære formålet med teknologien, og vil derfor være et hovedtema i utredningen. Utredning av helsemessige konsekvenser mv vil med andre ord bli utredet uavhengig av Utredningsinstruksens krav. Instruksen har primært betydning for utredning av avledede effekter, for eksempel vesentlige virkninger for personvern og rettssikkerhet. Virkninger for personvern og rettssikkerhet vil lett bli sett på som "andre vesentlige konsekvenser" med den virkning at det oppstår utredningsplikt.

Vurderingen av vesentlighet vil trolig måtte skje i to trinn: For det første må det vurderes hvor vesentlig vedkommende interesse er. Personvern og rettssikkerhet må generelt ses på som vesentlige samfunnsinteresser. Det er likevel ingen automatikk i at alle personvernspørsmål blir ansett å være vesentlige i henhold til utredningsinstruksen. I tillegg må det vurderes om slike interesser blir berørt på vesentlige måter. I veilederen er det listet opp momenter ved vurdering av om konsekvensene er vesentlige nok til å utløse særlig utredning (kapittel IV). Blant de momentene som nevnes er klart inngripende virkning, stort omfang og lav grad av selvbestemmelse for den enkelte. Bompengepasseringer som innebærer kartlegging av folks bevegelsesmønster er nevnt blant eksempeler på tiltak med vesentlige personvernkonsekvenser, og det er neppe tvil om at de fleste typer ts-teknologi som innebærer registrering av personopplysninger vil måtte vurderes på samme måte.

Utredningsinstruksen med veiledere bygger på en forutsetning om at utredninger skal avgrenses til det problemfeltet som diskuteres. I veilederen vedrørende personvern-konsekvenser framheves det imidlertid at det i offentlige utredninger kan være aktuelt å gi rom for overordnede vurderinger og forsøke å sette personvernaspektet i den konkrete saken i en større sammenheng.[127] Sammenligninger av typen som finnes i kapittel 6 i denne rapporten (jf ovenfor) kan derfor være aktuelt også i en offentlig utredning, og kan være ønskelig for å unngå for snevre sektortilnærminger til spørsmål om personvern. Slike tverrgående sammenligninger er også i tråd med Personvernkommisjonens etterlysning av nærmere vurderinger av proporsjonalitet når personvern skal vurderes på transportområdet, se avsnitt 2.2 (ovenfor).

Jeg vil ikke her komme nærmere inn på hvilke elementer en forhåndsutredning av personvernkonsekvenser bør inneholde eller hvilke metoder som bør følges. Utredningen forutsetter imidlertid en operasjonalisering av personvernet for på den måten å gjøre det mulig med konkrete analyser. Den samme operasjonaliseringen vil være nødvendig i samband med senere evaluering, se neste avsnitt. Generelt må det derfor forventes å være stor grad av samsvar mellom de forventede konsekvensene for personvernet (og målene for dette), og de målte effektene for personvernet som ledd i den etterfølgende evalueringen.

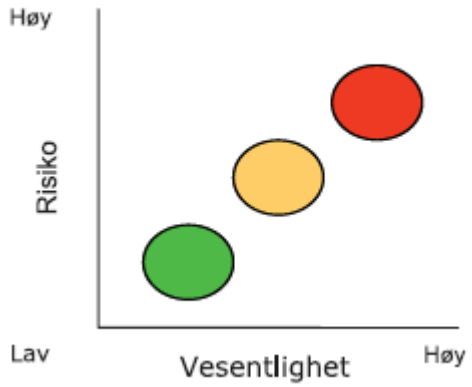
[126] Se Fornyings- og administrasjonsdepartementet 2008.
[127] Se Fornyings- og administrasjonsdepartementet 2008, kap. IV.

7.5 Krav til evaluering

Begrunnelsen for ts-teknologi vil være at det direkte eller indirekte bidrar til å senke antall skader i trafikken. Et sentralt spørsmål blir derfor om teknologien virkelig har slike effekter, og om effektene er slik at de kan sies å forsvare eventuelle negative effekter; for eksempel for personvernet. På lignende måte kan det være forutsatt at ts-teknologi vil få negative virkninger på personvernet, og også slike antatte effekter er det grunn til å få bekreftet eller avkreftet.

I reglement for økonomistyring i staten[128] er det i § 16 etablert plikt for statlige virksomheter til å gjennomføre evaluering av effektivitet, måloppnåelse og resultater innen virksomhetens ansvarsområde. Finansdepartementet har utdypet kravene til evalueringer i en veileder,[129] og for lover har Senter for statlig økonomistyring utviklet en egen veileder for evaluering av lover og forskrifter.[130] Plikten til å evaluere gjelder generelt og er uavhengig av hva slags virkemidler som er brukt. For den grunnleggende plikten til å evaluere spiller det med andre ord ingen rolle om en velger lov- og forskriftsstyring[131] eller ikke.

Tidspunkt og omfang av evalueringer kan være fastsatt i vedtaket som ligger til grunn for et tiltak, for eksempel vedtak om innføring av ts-teknologi. I mangel av slik konkret bestemmelse, avhenger spørsmålet om gjennomføringen av evalueringer av egenart, risiko og vesentlighet av det som skal evalueres. Finansdepartementet 2009 understreker særlig sammenhengen mellom risiko og vesentlighet, og ser egenart som et element som både kan påvirke risiko og vesentlighet, samt være en del av disse vurderingene.



Figur 2. Betydningen av risiko og vesentlighet for frekvens og omfang av evalueringer (hentet fra Finansdepartementet 2005)

Økonomiske risikoer er selvsagt et viktig element i mange evalueringer, men vil ikke bli nærmere kommentert her. Spesielle risikofaktorer knyttet til ts-teknologi (jf figuren) kan for eksempel være manglende erfaring med teknologien og dermed fare for utilsiktede negative virkninger. For eksempel kan sjåfører reagere annerledes enn forventet og dermed gjøre tiltaket mindre virkningsfullt. Også framvekst av bred motstand i befolkningen mot trafikksikkerhetstiltaket kan være en mulig risiko. Jeg har ikke grunnlag for å bedømme samlet risiko vedrørende ts-teknologi, men antar at det kan sies å eksistere risikoer som er knyttet til/begrunnet i personvern. Jeg antar videre at slik risiko ikke er lav (men nødvendigvis heller ikke høy).

Spørsmålet om vesentlighet (jf figuren) gjelder for eksempel om det som skal evalueres berører særlig viktige samfunnsmessige verdier eller ikke. Trafikksikkerhetsspørsmål gjelder åpenbart vesentlige verdier, fordi det gjelder beskyttelse av liv, helse og materielle skader. Ts-teknologi berører i tillegg vesentlige verdier som personvern og rettssikkerhet, jf innholdet av denne rapporten. Når kravene til evaluering skal bedømmes er det derfor klart at området må sies å gjelde meget vesentlige forhold ("høy" i figuren).

[128] Se Finansdepartementet 2006.
[129] Se Finansdepartementet 2005.
[130] Se Justisdepartementet 2009.
[131] Som forutsatt i avsnittene 7.2 og 7.3.

Dersom vi forutsetter at mine løse anslag av middels risiko og høy vesentlighet er riktig, vil det foreligge plikt til å evaluere bruk av ts-teknologi. Evalueringen må i så fall skje relativt hyppig og ha relativt stort omfang. Personvern og rettssikkerhet er faktorer som bidrar sterkt til denne konklusjonen, fordi det er risiko knyttet til begge faktorer, og fordi personvern og rettssikkerhet uansett er blant de vesentligste verdiene som vil bli berørt.[132]

Jeg kommer ikke nærmere inn på en konkretisering av de nærmere krav til slike evalueringer, men vil trekke frem noen sentrale elementer. Evaluering med relativt stort omfang innebærer for eksempel at både effekter for trafikksikkerhet og for personvern og rettssikkerhet må omfattes av evalueringen. Kravet til omfang innebærer dessuten at en ikke kan nøye seg med noen enkle indikatorer, men må gå inn i flere delaspekter. Dette har særlig betydning for relativt komplekse områder som personvern og rettssikkerhet. På dette området er det også store metodiske utfordringer fordi det er vanskelig å fastsette konkrete mål.

Plikten til å evaluere med relativt høy frekvens innebærer at en ikke kan vente lenge med å evaluere første gang. Evalueringen må dessuten skje flere ganger, og det må ikke gå for lang tid mellom hver gang.

Evaluering innebærer analyse og vurderinger i forhold til noen fastsatte mål; for eksempel "positive mål" som kvantifiserer reduksjon av trafikkskader mv, og/eller "negative mål" som fastsetter/kvantifiserer følger for personvernet. For at det skal være realistisk å kunne evaluere hyppig og omfattende, er det en forutsetning at en innretter innsamling av primærdata fra dag én. For eksempel kan ts-teknologien settes opp for å generere data som ledd i den løpende driften, på en måte som er nyttig for evalueringen.

7.6 Konklusjon

I denne rapporten har jeg analysert forholdet mellom personvern og ts-teknologi. Det primære resultatet er en nærmere klargjøring av hvorledes dagens personvernlovgivning vil virke på ts-teknologi (kap. 3 og 4), hvorledes aktuell ts-teknologi kan bedømmes sett fra et personvernsynspunkt (kap. 5), hvor inngripende slik teknologi kan anses å være i relasjon til annen særlig inngripende teknologi (kap. 6), og hvilke personvernspørsmål som det er særlig grunn til å rette oppmerksomheten mot (kap. 7). Flere av problemstillingene er spesielt vanskelige å behandle fordi i) den teknologiske utviklingen gjør det uklart hvilke egenskaper ts-teknologi vil få, og ii) fordi personvernbegrepet er omfattende, vanskelig avgrensbart og dessuten dynamisk.

Arbeidet har kun gitt svar som kan være til nytte i en fortsatt analyse, og inneholder ingen bastante konklusjoner om hvorledes avveiningen mellom trafikksikkerhet og personvern bør være. Fordi ts-teknologi og personvern er fellesbetegnelser som kan dekke over en rekke variasjoner, er det helt nødvendig også å gjøre konkrete vurderinger. Og det er først når vi gjennomfører konsekvensutredninger og løpende evalueringer av konkrete teknologier at det er mulig å gi forholdsvis sikre svar.

Det er grunn til å advare mot en videre diskusjon som kjører seg fast i en avveining mellom trafikksikkerhet og personvern, jf behovet for å minimalisere innslaget av personopplysninger

[132] Spørsmålet er i tillegg egenartet ved at det gjelder mange mennesker, noe som øker betydningen av risiko og vesentlighet.

(avsnitt 7.3.3.2). Riktignok er det trolig sant at enkelte trafikksikkerhetstiltak som innebærer en viss grad av personvernkrenkelse er "uunngåelige".[133] For øvrig er det imidlertid avgjørende at vi leter etter trafikksikkerhetstiltak som *ikke* involverer behandling av personopplysninger, og som *også* kan føre til vesentlige reduksjoner av antallet skader i trafikken. Krav til sikkerhetsutstyr i kjøretøy, veistandard og annen infrastruktur kan også ha sikkerhetsmessige effekter. Den store diskusjonen om trafikksikkerhetstiltak kan derfor sies å handle om i hvilken grad vi skal velge tiltak som er knyttet opp mot personer/sjåfører og i hvilken grad vi skal velge tiltak som er knyttet opp mot kjøretøy og infrastruktur. På alle områder kan det være tale om bruk av IKT, men kun når teknologibruken er knyttet opp mot konkrete personer genereres det med nødvendighet personvernspørsmål.

IKT kan alternativt være i *infrastrukturen*, samtidig som kjøretøy trekkes inn i og gjøres til del av denne.[134] Et "intelligent" skilt med angivelse av fartsgrense som kommuniserer direkte med kjøretøyet,[135] vil for eksempel ikke krenke sjåførens personvern fordi det ikke vil bli lagret personopplysninger, eksponert privatliv eller lignende. Et underliggende viktig spørsmål bak en slik tilnærming, er hva som kjennetegner trafikkregler som kan håndheves uavhengig av om sjåføren har identifisert og akseptert normen. Spørsmålet er med andre ord i hvilken grad håndhevelse av trafikkregler kan automatiseres. Teknologien kan for eksempel tenkes å la trafikkreglene få direkte anvendelse og virkning uten at sjåføren (nødvendigvis) selv ønsker å etterleve reglene.

Dersom trafikkregler kan realiseres som en teknologistyrt funksjon som ikke kan omgås, vil dette riktignok begrense den enkelte sjåførs handlefrihet, men kan neppe sies å berøre vedkommendes personvern. ATK ved skoler reduserer bare risikoen for ulykker i den grad sjåfører minnes på eller "skremmes" til å etterleve fartsgrensen pga. høy oppdagelsesrisiko. Trafikkbegrensninger som virker *direkte* på kjøretøyet gir 100% etterlevelse av normen.[136] I det første tilfellet skjer det personvernkrenkelse, mens sist nevnte tilfellet ikke gir slike effekter fordi hastighetsbegrensningen virker direkte på kjøretøyet uten at personopplysninger blir samlet inn.

Det skal helt avslutningsvis medgis at også den sist nevnte tilnærmingen byr på en rekke utfordringer. Manglende teknologiutvikling og -spredning samt kostnader er åpenbare utfordringer. På den rettspolitiske siden er det nærliggende å tro at en i stedet for diskusjoner om personvern får diskusjoner om grensene for den alminnelige handlefrihet. Vi er imidlertid vant til at vår handlefrihet er begrenset av en rekke fysiske forhold knyttet til topografi, kjøretøy, veistandard mv. Jeg antar derfor at en slik diskusjon vil være mindre kontroversiell enn en diskusjon om teknologi som innebærer registrering av personopplysninger.

[133] Det uunngåelige gjenspeiler ingen teknologideterminisme, men uttrykker kun hva jeg anser som en sikker prognose ut i fra min kjennskap til norsk politikk og samfunnsforhold.
[134] En slik fremgangsmåte kan gjøre det unødvendig med personvernkrenkelser, jf diskusjonen til slutt i avsnitt 2.1 (ovenfor).
[135] Eller en sensor på kjøretøy som leser tradisjonelle veiskilt, jf eksempelet i Dagsavisen 2008.
[136] En kan imidlertid tenke seg systemer med "blålysfunksjoner", dvs som tillater en å overskride normen dersom det oppstår en tilstrekkelig alvorlig nødsituasjon. I så fall vil handlingen alltid måtte logges og personen alltid stå til ansvar og begrunne at det forelå nødrett.

Litteratur og kilder:

- Agder lagmannsretts dom LA-2004-30029
- Coll og Lenth 2000: Line M Coll og Claude A Lenth.: *Personopplysningsloven – en håndbok*, Kommuneforlaget AS, 2000 Oslo.
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.I.1981.
- Dagsavisen 2008: Dagsavisen, *I farta mot full brems*, torsdag 23. oktober 2008 s 34.
- Eidsivating lagmannsretts dom LE-2007-155972
- Engstrøm 2004: Bjørn Engstrøm; *Vegtrafikkloven*, kommentarutgave, 4. utgave, Universitetsforlaget 2004
- Finansdepartementet 2005: *Veileder til gjennomføring av evalueringer*, Finans-departementet 2005.
- Finansdepartementet 2006: *Reglement for økonomistyring i staten*, fastsatt 12. desember 2003 med endringer, senest 14. november 2006
- Fornyings- og administrasjonsdepartementet 2008: *Vurdering av personvernkonsekvenser. Veileder til Utredningsinstruksen*, Fornyings- og administrasjonsdepartementet 2008.
- Forskrift om ordningen av påtalemyndigheten (Påtaleinstruksen) av 28. juni 1985 nr 1679.
- Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr 1265.
- Gjensidige: Karmøy-prosjektet (tilgjengelig fra: http://www.gjensidige.com/web/Forsiden/Samfunnsansvar/Samfunnsbidrag/Karm%C3%B8yprosjektet
- Grunnan 2008: Tonje Grunnan. *Litteraturgjennomgang av strekningsbasert-ATK*, TØI arbeidsdokument, Oslo 27. august 2008.
- Hrelja 2008: Robert Hrelja. *Litteraturgenomgång ISA och EDR*, VTI opublicerad forskningspromemoria, Linköping 2008.
- Innst. O. nr. 51 (1999–2000), om lov om behandling av personopplysninger (person-opplysningsloven).
- Justisdepartementet 2009: Justis- og politidepartementet. *Evaluering av lover. Med tilsvarende anvendelse på forskrifter og andre rettsregler*, januar 2009.
- Kongelig resolusjon av 15. desember 2000 nr. 1265 (om forskrift til personopplysningsloven)
- Kongelig resolusjon av 27. mai 2005 (Instruks for Statens vegvesen).
- L'Abée-Lund 2006: Åsa L'Abée-Lund, *Pseudonymisering av personopplysninger i sentrale helseregistre*, hovedoppgave, Avdeling for forvaltningsinformatikk, UiO 2006.
- Lov om rettergangsmåten i straffesaker (Straffeprosessloven) av 22. mai 1981 nr 25.
- Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr 31.
- Meland m.fl 2007: Solveig Meland, Hanne Samstad, Ragnhild Wahl og Marit Killi; *Utfordringer innen personvern, ansvar og roller ved ITS-anvendelser i transportsektoren*, rapport STF50 A4135, SINTEF, TØI, 2007.
- Ministry of Transport, Public Works & Water Management (Nederland) 2009: "Road pricing: Different Payment for Mobility" (tilgjengelig fra http://www.verkeerenwaterstaat.nl/english/topics/mobility_and_accessibility/road_pricing/index.aspx)
- NOU 1975: 10 Offentlig persondatasystem og personvern
- NOU 2004: 6 Mellom effektivitet og personvern
- NOU 2009: 1 Individ og integritet

- NOU 2009: 3 På sikker veg
- NOU 2009: 15 Skjult informasjon - åpen kontroll (Metodekontrollutvalget)
- Ot.prp nr 22 (1994-95) Om lov om politiet (politiloven)
- Ot prp nr 92 (1998-99), Om lov om behandling av personopplysninger (personopplysningsloven).
- Personverndirektivet: Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger
- Personvernnemndas avgjørelse PVN-2005-11 om klage på vedtak om pålegg om konsesjonsplikt for helautomatiske bomstasjoner.
- Rt. 1990 s 1008, Fotobokskjennelsen (Høyesterettsavgjørelse)
- Rt. 2008 s 44, kjennelse om fartsovertredelse (Høyesterettsavgjørelse)
- Schartum og Bygrave 2004: Dag Wiese Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger*, Fagbokforlaget, Bergen 2004.
- Schartum 2005: Dag Wiese Schartum, *Krav til sikring av personopplysninger*, I: Arild Jansen og Dag Wiese Schartum (red.), Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT, Fagbokforlaget, Bergen 2005, s 98 - 148.
- Schartum og Bygrave 2006: Dag Wiese Schartum og Lee A Bygrave, *Utredning av behov for endring av personopplysningsloven*, Justisdepartementet, rapport 2006.
- Schartum 2007: Dag Wiese Schartum, *Personvern og transportsikkerhet. Personvernmessige spørsmål knyttet til tiltak for å sikre transportmidler mot fiendtlige anslag*, Complex 3/07, Senter for rettsinformatikk, Oslo 2007.
- Schartum og Bygrave 2008: Dag Wiese Schartum og Lee A Bygrave, *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12* Skrevet etter oppdrag fra Justis- og politidepartementet, Justisdepartementet, rapport 2008.
- Sivilombudsmannen 1996: Somb-1996-53, sak om saksbehandlingen knyttet til forelegg etter ATK.
- SpeedPilot: Informasjon om kjørebok mv med gjennomsnitts fartsmåling http://www.speedpilot.no/detaljer.htm
- Svensk og Ehrström 2007: Per-Olof Svensk og Natalie Ehrstrøm, Slutrapport Mobile ISA, Triona, Appello, 14. august 2007.
- Tveit m.fl. 2007: Ørjan Tveit, Ragnhild Wahl, Hanne Samstad, Mattias Gripsrud, Marit Killi og Børge Bang; *Trafikale virkninger og nytte av ITS*, rapport STF50 A3817, SINTEF, TØI 2007.
- Utredningsinstruksen 2000: *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 og revidert ved kongelig resolusjon 24. juni 2005.
- Vegtrafikklov av 18. juni 1965 nr 4.
- Wiik Johansen m.fl. 2001: M. Wiik Johansen, K-B. Kaspersen og Å.M. Bergseng Skullerud, *Personopplysningsloven. Kommentarutgave* (Oslo: Universitetsforlaget, 2001).