



Transport- og  
kommunikasjonskomiteén

## Notat om personvern i samferdselssektoren

*Vi ser i dag en rask teknologiutvikling innenfor samferdselssektoren. Utgangspunktet for de teknologiene som tas i bruk er å fremme effektiv trafikkavvikling, trafikk sikkerhet og brukervennlighet, men til sammen gir teknologiene et potensial for økt overvåkning og utvikling av en detaljert profil av folks bevegelser. Det er også fare for at dataene kan bli brukt til andre formål enn de opprinnelig ble samlet inn for.*

*Det bør derfor gjennomføres en konsekvensvurdering for personvern for alle prosjekter som har befatning med persondata. I tillegg bør det med jevne mellomrom gjennomføres vurderinger av totalbildet for personvernet.*

Teknologirådet har flere prosjekter om personvern, blant annet Elektroniske spor og personvern, ICT and Privacy in Europe, og en kartlegging av sikkerhetsteknologier og personvern.

Teknologier vi ser som aktuelle for samferdselssektoren er:

- Radio Frequency Identification (RFID)
- Lokaliseringsteknologi (GSM/GPRS og satellittsystemer)
- Kameraovervåkning
- Automatiske identifiseringssystemer (Kjennemerke/Ansikt)
- Biometri
- Samordning av systemer

### **RFID**

RFID-brikker er brikker som inneholder en liten radiosender. Brikken kan være relativt stor, slik som Autopassbrikken, eller så liten at det ikke er mulig å oppdage den dersom den er støpt inn i et kredittkort eller en vare.

De store brikkene er gjerne det vi kaller aktive brikker. Disse inneholder et batteri, og kan sende ut signaler over relativt lang avstand, slik som Autopass. De små brikkene får energien fra leseren som skal lese informasjonen på dem, og må være ganske nær leseren – som regel mellom 10 cm og 1 meter. Slike brikker kan for eksempel brukes i billettssystemer som det Oslo Sporveier har tenkt å innføre, eller i andre typer billetter og identitetspapirer.

Det som er problematisk med RFID fra et personvernståsted, er at brikken gjerne inneholder informasjon om identitet – som kjennemerke på bilen, eller navn, personnummer, passnummer el.l. Brikkene er ofte ikke krypterte, og den som bærer brikken vil ikke merke det når brikken blir avlest.

Fordi RFID brikker kan brukes til unik identifikasjon, ser vi at det også stadig oftere brukes som sikkerhetstiltak i samferdselssektoren: Containerne merkes for sporing, biler merkes som et ledd i tyverisikring etc. I slike tilfeller er brikken gjerne koblet opp mot en form for lokaliseringssystem

### **Lokaliseringsteknologi**

I dag brukes flere teknologier for å spore kjøretøyer eller personer. Ofte benyttes de signalene som en persons mobiltelefon sender ut for å finne en omtrentlig lokasjon for en person eller et kjøretøy (f. eks i flåtestyringssystemer). I stadig økende grad ser vi at satellittposisjonering tas i bruk. I dag er det amerikanske GPS systemet enerådende, men om noen år kommer det Europeiske Galileo-systemet på banen.

Dette systemet er allerede planlagt brukt i et system som heter eCall. Dette systemet ringer opp nødnummeret automatisk dersom et kjøretøy er innblandet i en ulykke, og rapporterer om kjøretøyets posisjon, kjøreretning, kjennemerke etc. På denne måten regner man med å kunne spare mange liv i trafikken. Norge har signert et såkalt *Memorandum of Understanding* for å være med på eCall. Fra 2009 skal alle nye biler være utstyrt med eCall-systemet.

Også RFID-brikkene kan brukes til sporing, men ikke så detaljert. Gjennom systemer som Oslo sporveiers vil man kunne se hvor en person gikk inn og ut av T-banenettet, på en buss el.l. Lesere for RFID kan også settes opp andre steder, slik at man kan registrere når en brikke passerer.

### **Kameraovervåkning, biometri og automatisk gjenkjenning**

Det er en økende trend for kameraovervåkning i samfunnet, også i trafikken. I Norge i dag brukes det for sikkerhet og god trafikkavvikling i tunneler, for å ta fartssyndere etc. I store byer i utlandet brukes kameraer koblet til nummerplategjenkjenning til å sile ut og kontrollere kriminelle som er på vei in til bykjernen (London) eller for å gjenkjenne stjålne biler (Los Angeles m.fl).

Etter hvert kan også kameraer benyttes for å gjenkjenne ansikter, men denne teknologien er foreløpig ganske umoden. Vi tror imidlertid at det vil bli større press for å koble identitet til både kjøretøy og reisedokumenter. Her ser vi at biometri som ansikt, fingeravtrykk og iris er i vekst. Det å benytte biometri som identifikasjon kan i fremtiden kobles til billettsystemer, erstatte bilnøkkelen, og det er allerede tatt i bruk på flere flyplasser for å sikre at det er riktig person som går om bord i flyet. På denne måten blir det enda lettere å spore enkeltpersoner i trafikken – ikke bare kjøretøyer.

### **Samordning**

En markant trend er at man ønsker å samordne stadig flere systemer. Autopass med felles bomssystem i hele Norge er et slikt system, og et felles system for hele Europa er på gang (som det henvises til i forslaget fra Sponheim og Tenden). Innenfor flyreiser ser vi at det stadig er ønsker om mer og bedre passasjerinformasjon – noe ikke minst USA har vært en pådriver for.

Også forsikringselskapene er en driver for systemer med detaljert informasjon knyttet til et kjøretøys bevegelser. Et britisk selskap – Norwich Union – har lansert tjenester *Pay as you drive*. Her kan kunden installere en sort boks i bilen som registrerer når og hvor han kjører, hvor fort etc. Tanken er at risikoaverse bilister som kjører på rolige småveier utenom rusket ikke skal behøve betale for de som har en høy risikoprofil. Også eCall-systemet legger opp til at man kan ha en utvidet datamodell som inneholder data forsikringselskapene kan ønske seg. Dersom man ser disse systemene i sammenheng med offentlige systemer, kan man få et svært detaljert bilde av enkeltpersoners bevegelser.

### **Hvorfor innføres man teknologiene?**

I utgangspunktet er det ikke fordi man ønsker å drive utstrakt overvåkning, men fordi man ønsker en effektiv trafikkavvikling, med færrest mulig dødsfall og skader. I tillegg ønsker ikke folk å stå i kø – og derfor er systemer som Autopass velkomne, og bruk av biometri vil sannsynligvis bli akseptert fordi det er mye enklere enn å huske en serie med brukernavn og passord.

Bruk av biometri på flyplasser, og samordning og utveksling av passasjerdata er et resultat av terrorfrykten etter 11/9 2001.

Ulempen er at til sammen utgjør alle disse systemene et stort kompleks som kan gi et svært detaljert bilde av en persons bevegelsesmønster, noe som igjen kan avsløre interesser, nettverk og lignende. Dette er bekymringsverdig av flere årsaker:

- For den enkelte vil det være vanskelig å selv skaffe seg et overblikk over omfanget av data lagret om ham eller henne i ulike systemer.
- Det vil alltid være fristende å bruke slike systemer til andre formål enn det opprinnelige.

### **Konsekvensvurdering for personvern**

En konsekvensvurdering for personvern er en prosess som skal hjelpe virksomheter å vurdere hvorvidt prosjekter som skal igangsettes vil ha konsekvenser for behandling av personopplysninger. En slik konsekvensvurdering skal gjennomføres allerede mens prosjektet er i planleggingsfasen. På den måten kan personvernprinsipper innarbeides når prosjektet designes, eller prosjektet kan i ytterste konsekvens stanses før det har påløpt store kostnader.

Dersom personvern og personvernvennlige teknologier blir innarbeidet i prosjektet allerede i designfasen, kan dette øke tilliten til systemet i befolkningen. Dette kan medføre at man slipper å gjøre dyre endringer i systemet på et senere tidspunkt for å kunne tilfredsstille lovverkets krav og befolkningens forventinger til ivaretagelse av personvern.

Slike analyser er det i dag krav om ved offentlige anskaffelser i blant annet Canada. Norge bør også vurdere krav om gjennomføring av slike konsekvensvurderinger. Dette bør i så fall omfatte alle prosjekter som innebærer anskaffelse eller utvikling av systemer som samler, vedlikeholder eller tilgjengeliggjør personopplysninger.

Med vennlig hilsen

Tore Tennøe  
Sekretariatsleder, Teknologirådet

Christine Hafskjold  
Prosjektleder