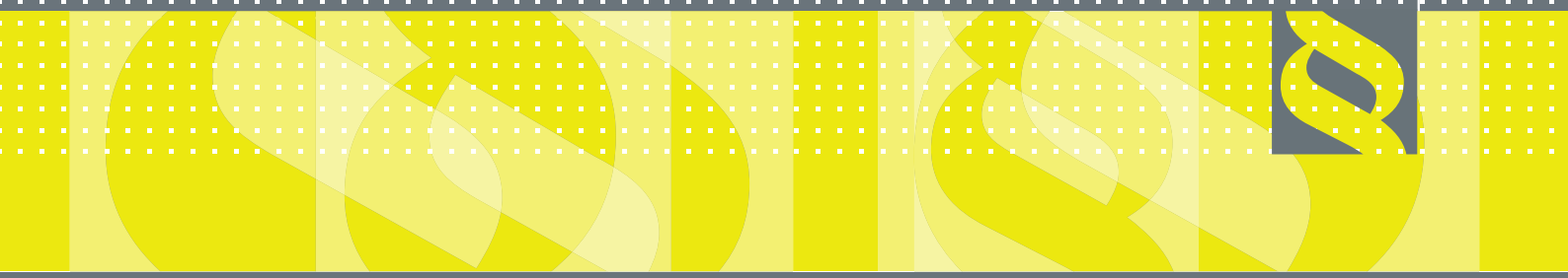
Rapport 2008

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

Professor dr. juris Dag Wiese Schartum i samarbeid med førsteamanuensis dr. juris Lee A. Bygrave



JUSTIS- OG POLITIDEPARTEMENTET

Rapport 2008

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

Professor dr. juris Dag Wiese Schartum i samarbeid med førsteamanuensis dr. juris Lee A. Bygrave

JUSTIS- OG POLITIDEPARTEMENTET

Sammendrag

Rapporten inneholder en drøftelse av den rettslige reguleringen i personopplysningsloven av spørsmål vedrørende bruk av fødselsnummer og biometriske teknikker for identifisering og autentisering av enkeltpersoner. Utgangspunktet for drøftelsen er personopplysningsloven § 12.

Redegjørelser og drøftelser munner ut i konkrete forslag til endringer av person-opplysningsloven. Et utgangspunkt er at fødselsnummer og biometri må reguleres i et samspill mellom personopplysningsloven og særlovgivning.

Forslaget til ny regulering i personopplysningsloven av fødselsnummer bygger på dagens § 12, men slik at:

- Den behandlingsansvarlige må ha gjennomført en risikovurdering som klart viser at fødselsnummer er nødvendig for å oppnå sikker identifisering.
- Det innføres et forbud mot bare å benytte fødselsnummer for å autentisere personers identitet.

Forslaget til ny regulering i personopplysningsloven av biometri bygger på et skille mellom formålene identifisering og autentisering, slik at:

- Bruk av fingeravtrykk og andre biometriske metoder for å avdekke en persons identitet (identifisering), ikke er tillatt uten lovhjemmel.
- Bruk av fingeravtrykk og andre biometriske metoder for å autentisere personers identitet er tillatt dersom det foreligger lovhjemmel eller samtykke. Visse krav til gyldig samtykke foreslås presisert, bl.a. at det må tilbys alternative fremgangsmåter for personer som ikke ønsker å bli autentisert ved hjelp av biometri.

I tillegg foreslås det mindre, supplerende endringer i andre deler av personopplysningsloven, bl.a. når det gjelder plikt til å vurdere nødvendigheten av å behandle personidentifiserbare opplysninger, sletting, straff og erstatning.

1 Bakgrunn for utredningen

Lov om behandling av personopplysninger (personopplysningsloven) 31. mars 2000 nr. 31 trådte i kraft 1. januar 2001 sammen med forskrifter til loven. Formålet med loven er å beskytte den enkeltes personvern ved behandling av personopplysninger. Loven gjennomfører Europa-parlamentets og rådets direktiv 95/46/EF om beskyttelse av personopplysninger (EU-direktivet) i norsk rett. I Ot. prp. nr. 92 (1998-1999) side 100 ble det understreket at reglene skal anvendes på en teknologi som er i stadig utvikling. I forbindelse med vedtakelsen av loven bestemte Stortinget at det skulle finne sted en etterkontroll som skulle påbegynnes fire år etter at loven trådte i kraft (se Innst. O. Nr. 51 (1999-2000) side 26).

Justisdepartementet har ansvaret for personopplysningsloven og Fornyings- og administrasjonsdepartementet har ansvaret for forskriftene til loven. En del av spørsmålene i etterkontrollen var av en slik art at disse departementene ba ekstern ekspertise på fagfeltet utrede enkelte spørsmål før et forslag om lov- og forskriftsendringer sendes på høring. På denne bakgrunn avga professor dr. juris Dag Wiese Schartum og førsteamanuensis dr. juris Lee A. Bygrave etter oppdrag fra JD 8. juli 2005, rapporten "Utredning av behov for endringer i personopplysningsloven" (31. mars 2006). I ettertid viste det seg at det også var ønskelig å få vurdert behovet for endringer i personopplysningsloven § 12 om bruk av fødselsnummer mv. Departementet ba Schartum og Bygrave om også å utrede andre spørsmål knyttet til denne bestemmelsen. På grunn av intenst arbeid i Personvernkommisjonen har Bygrave likevel ikke hatt mulighet for å arbeide aktivt med denne tilleggsutredningen. Utredningen er derfor skrevet av Schartum og gjennomgått og diskutert med Bygrave i aller siste fase av arbeidet.[1]

Mandatet for utredningen følger som vedlegg 1 til denne rapporten. Utredningen skulle særlig dekke følgende punkter:

Anbefale sentrale begreper.

- Vurdere behovet for lovendringer som tydeliggjør hva som er akseptabel bruk av fødselsnummer og biometriske kjennetegn/data og som tydeliggjør forskjellen mellom disse.
- Vurdere spørsmål om valg av lovstruktur og -teknikk herunder bl.a. om det bør være separate paragrafer for henholdsvis fødselsnummer og biometri i stedet for en felles bestemmelse som i dag.
- Beskrive de teknologiske løsningene og forsøke å angi på hvilke bruksområder denne teknologien er aktuell.
- Kort redegjøre for hvordan biometri og biometriske metoder ligner på og skiller seg fra andre identifikatorer og autentiseringsmidler, særlig med hensyn til koblingsfare, eksponering av overskuddsinformasjon og vern mot feilautentisering.
- Klargjøre personvernmessige konsekvenser av at biometriske løsninger tas i bruk, herunder redegjøre for hvilke hensyn og vurderingstema som bør være avgjørende for om bruk av biometriske kjennetegn/data skal aksepteres i det enkelte tilfelle.

I rapporten har spørsmål vedrørende biometri fått forholdsvis større oppmerksomhet enn de som gjelder fødselsnummer. Utrederen mener biometrisk teknologi vil komme til å spille en stadig større rolle, og antar teknologien vil bli sikrere, langt billigere og mer tilgjengelig enn i dag. Fordi dette er en teknologi som leser kjennetegn ved det enkelte menneskes kropp og adferd, har den langt større potensiale for negative konsekvenser for personvernet enn tildeling og bruk av

[1] Hjertelig takk til universitetslektor Gisle Hannemyr for nyttig samtale om biometrisk teknologi.

fødselsnummer. Av hensyn til omfanget av arbeidet, har jeg i gjennomgangen av ulike andre metoder for identifisering og autentisering kun tatt opp enkelte spørsmål knyttet til bruk av RFID-teknologi.[2] Dette fordi denne teknologien kan tilføres kroppen og således kan sies å være en mellomstasjon mellom biometrisk teknologi og teknikker der en gjør bruk av gjenstander i samband med identifisering og autentisering. Bruk av tradisjonelle legitimasjonskort mv uten biometriske data og elektroniske signaturer mv er primært behandlet for å synliggjøre den sammenheng biometriske identifikasjonsteknikker står i, men uten at jeg har redegjort for detaljer i fremstilling og bruk av disse.

Utredningen konkluderer med at det er behov for lovendring, og i kapittel 7 fremsetter jeg forslag til konkret lovtekst. Mandatet synes å forutsette at lovendring kun er aktuelt i personopplysningsloven. Forslagene forutsetter imidlertid også enkelte andre lovendringer, men konkrete forslag til lovtekster omfatter bare personopplysningsloven.

[2] Dvs radiofrekvensidentifikasjon som innebærer at data kan lagres og innhentes ved hjelp av små enheter kalt RFid-brikker. Brikkene kan festes til eller plasseres inn i et produkt, et dyr eller en person.

2 Om identifisering og autentisering

2.1 Identitetshåndtering

Denne utredningen handler om teknikker og fremgangsmåter som med stor grad av sikkerhet kan vise hvem personer er. Helt generelt spenner dette emnet over alt fra selvfølgelige, mellommenneskelige prosesser (jeg kjenner igjen personen P når jeg treffer henne), til teknikker og fremgangsmåter som i stor grad involverer avansert teknologi (en person viser seg å være P fordi en DNA[3]-analyse har dette som resultat). Mellom disse ytterpunktene ligger det en rekke muligheter for å ta stilling til personers identitet. I dette avsnittet, før jeg har gjennomgått aktuelle begrepsbruk nærmere, velger jeg å bruke betegnelsen "identitetshåndtering" eller "id-håndtering" om de forskjellige aktiviteter/vurderinger som gjelder personers identitet. Senere i utredningen bruker jeg samme uttrykk som overbegrep og fellesbetegnelse.

En vanlig systematikk er å ta stilling til spørsmål om personers identitet med utgangspunkt i hva personen

- er (utseende, og andre fysiske karakteristika);
- har (adgangskort);
- vet (passord, for eksempel en tallkode eller annen sammensetning av tegn); eller
- eller kombinasjoner av nevnte teknikker (har id-kort med pin-kode og bilde av den personen som innehar kortet).

Jeg kan ikke her gjennomgå de mange sinnrike måter mennesker har brukt for å håndtere spørsmålet om identitet, men kun kort skissere det jeg mener er noen viktige karakteristika når id-håndtering skal beskrives. Eksemplene vil i stor grad være knyttet til kulepunktene ovenfor. Ikke alle systematiske og begrepsmessige distinksjoner i denne utredningen vil bli aktivt brukt i begrunnelser og utforming av forslag til fremtidig lovgivning, jf kapittel 7. Jeg tror imidlertid det også er ønskelig å ha et forholdsvis bredt fundament for videre refleksjon.

Manuell og automatisert id-håndtering

Et hovedskille går mellom id-håndtering som kun skjer ved hjelp av menneskelig sansing og analyse, og id-håndtering som helt eller delvis skjer ved automatiserte rutiner. Bruk av tradisjonelle "legitimasjonsbevis" der identiteten for eksempel vurderes ved at et menneske sammenligner personbilde, fødselsdato og underskrift med personens fysiske fremtoning, er eksempel på manuell id-håndtering. Bruk av elektronisk signatur,[4] kort med pin-kode eller biometriske data i en kortleser der programsystemet sammenligner inntastet tall eller avlest fingeravtrykk med tilsvarende informasjon som er lagret i kortet, er eksempler på automatisert id-håndtering. Manuelle og automatiserte elementer kan dessuten selvsagt kombineres, for eksempel slik at kortet med pin-kode har personbilde og signatur som også kan benyttes ved behov.

Umiddelbar og middelbar id-håndtering

Et annet skille går mellom id-håndtering som skjer umiddelbart, og håndtering som skjer via mellomledd (middelbart). Her er det delvis sammenfall med henholdsvis manuell og automatisert id-håndtering. Således skjer bruk av tradisjonelle legitimasjonskort normalt i umiddelbare situasjoner, menneske til menneske. Også legitimasjonskort kan imidlertid brukes

[3] Deoksyribonukleinsyre (engelsk: Deoxyribonucleic acid) som våre gener er bygget opp av.
[4] Se lov av 15. juni 2001 nr 81 om elektronisk signatur (e-signaturloven) og MOD 2005.

middelbart, for eksempel ved at en annen person gjør bruk av kortet (eller en kopi av kortet) sammen med en fullmakt fra personen som er innehaver av kortet. Automatisert id-håndtering kan sies å være umiddelbar når id-håndteringen skjer direkte i brukssituasjonen, men er middelbar dersom id-håndteringen for eksempel krever en nærmere analyse av DNA eller lignende.

Obligatorisk og pragmatisk id-håndtering

Det tredje skillet jeg vil trekke frem gjelder hvor konsekvent og omfattende id-håndteringen er. I mange tilfelle vil en bestemt id-håndtering være obligatorisk og gjelde for alle personer på like måter. Alle norske borgere må for eksempel legitimere seg med pass før de stiger om bord på et fly. I andre tilfelle kan det foreligge en valgfrihet, enten hos den id-håndteringen direkte gjelder eller hos den som håndterer identiteten. I sist nevnte tilfelle er id-håndteringen pragmatisk, dvs den kommer an på konkrete subjektive forhold. Således kan håndteringen sies å være pragmatisk dersom en vakt kan slippe personer han kjenner igjennom sperrer med adgangskontroll, uten at personene bruker adgangskort. Det kan også skje en pragmatisk id-håndtering dersom personen kan velge håndteringsmåte, for eksempel om hun vil gå til skranken for manuell kontroll eller bruke fingeravtrykkleser for automatisk kontroll. Jeg bruker bevisst "pragmatisk" i stedet for "frivillig", fordi valgfriheten kun gjelder måten identiteten skal håndteres på, ikke om identifisering mv skal skje eller ikke.

2.2 Begreper og systematikk

Jeg har ikke funnet noe etablert og helt dekkende begrepsapparat innen området for identitetshåndtering som imøtekommer behovene i denne utredningen. Det er imidlertid lagt vekt på å unngå begrepsbruk som avviker fra det som er anvendt i sentrale dokumenter på området,[5] men jeg har for øvrig gjort de presiseringer og tilføyelser som jeg antar er nødvendige og fruktbare ut i fra oppdraget. I dette avsnittet gjennomgår jeg grunnleggende begreper og systematikker vedrørende identifisering mv generelt, mens jeg i avsnitt 2.4 gjennomgår de begrepene som spesielt er knyttet til biometri. En del andre begrepsavklaringer gjøres underveis i fremstillingen.

Identitet og identifisering

I denne utredningen anvender jeg menneskers "identitet" for å betegne individer adskilt fra andre individer. Identiteter er derfor per definisjon unike. "Identifisering"[6] er som oftest betegnelse på prosessen *å fastslå en persons identitet*, dvs gjenkjenning av personer blant flere mulige personer (et en-til-mange forhold). Begrepet kan imidlertid også betegne det å *etablere en entydig binding* mellom et individ og et identifikasjonsmerke/-middel (jf nedenfor), for eksempel tildele fødselsnummer til en person (navnefunksjonen). Jeg har valgt å avstå fra å foreslå ulike begreper for hver av de to mulige forståelsene av identifisering. Det er neppe mulig å få gjennomslag for nye begreper som forutsetter helt stringent begrepsbruk. Spørsmål om identifisering må derfor kunne håndteres med et noe flertydig begrepsapparat. I denne utredningen vil jeg som regel legge den først nevnte betydningen til grunn, og det er trolig også denne betydningen som er dominerende i dagligtale.

Autentisering (verifikasjon av identitet)

Identifisering innebærer som nevnt å fastslå en persons identitet blant mange identiteter, dvs. i et en-til-mange forhold. Dette må prinsipielt sett holdes adskilt fra spørsmålet om å *autentisere*,

[5] Se særlig JD 2007 s 6 (definisjoner) og FAD 2008, avsnitt 2.1.
[6] Jf også "identifikasjon".

dvs. verifisere identiteter. Ved autentisering går jeg ut i fra situasjoner der personen selv har fremsatt en påstand om en bestemt identitet (en person presenterer seg som Ola Nordmann), og verifiseringen går ut på å kontrollere at denne påstanden er korrekt, dvs at det virkelig er Ola Nordmann jeg har med å gjøre.[7] Mens jeg i identifiseringstilfellene står overfor et en-til-mange forhold, gjelder autentisering med andre ord et en-til-en forhold. Situasjonen ved slik verifisering av identitet er for eksempel at en person som krever bagasje B fra flyselskapet, bekreftes å være den samme som leverte denne bagasjen. For å vise dette brukes en bagasjelapp (noe personen har, og der nummeret på lappen tilsvarer nummeret på bagasjen) eller et fingeravtrykk (noe personen er, og der avtrykket ved avhenting av bagasjen tilsvarer det som ble avgitt ved innlevering). Vi trenger i så fall - strengt tatt - ikke vite hvem denne personen er, noe som gjør slike tilfelle klart forskjellig fra tilfelle med identifisering.[8] I praksis vil det imidlertid også kunne være knyttet opplysninger til autentiseringen som gjør at det også skjer identifisering.

Utenfor autentiseringstilfellene faller situasjoner der *andre* fremsetter påstand om en persons identitet. Jeg forutsetter at autentisering krever en tydelig påstand om identitet fra personen i form av tale eller annen handling (fremsi navn, dra kortet i kortleseren). Faktisk opphold på sted der kun person P har adgang, faller utenfor det jeg betegner autentisering fordi personen ikke aktivt har fremsatt påstand om en bestemt identitet.

I fortsettelsen bruker jeg verifisering av identitet og autentisering som synonyme uttrykk. I relevante fagmiljøer innen informasjonssikkerhet og -teknologi mv, vil autentisering (engelsk: authentification) være godt innarbeidet. Men jeg antar dette ordet ikke uten videre vil være godt forståelig for lekfolk. Verifikasjon av identitet angir mer eksplisitt et meningsinnhold, og er trolig noe lettere å forstå for uinnvidde personer (men ikke språklig elegant!). Et annet spørsmål er hvilke begreper som bør benyttes i en eventuell lovtekst. Jeg kommer nærmere tilbake til spørsmålet i avsnitt 7.1.2.

For å verifisere identiteter har det vært vanlig å bruke "identitetsbevis". Situasjonen er gjerne at det foreligger et behov for å sikre at personen som det er aktuelt å tildele et gode, gi rett til å motta informasjon mv, faktisk er den hun eller han utgir seg for å være.[9] I så fall blir disposisjonen legitim, dvs lovlig/rettferdig/moralsk. Derfor er det ikke uvanlig å kalle slike identitetsbevis for å sikre legitime disposisjoner for "legitimasjonsbevis" eller bare "legitimasjon". Identitets- og legitimasjonsbevis er med andre ord betegnelse på et dokument som inneholder en kombinasjon av opplysninger (typisk; personnavn, personbilde og fødselsnummer), og som godtas som tilstrekkelig bevis for en persons identitet i samband med visse disposisjoner som en ønsker å sikre legitimiteten av (for eksempel disponering av bankkonto, tilgang til et fly, adgang til et offentlig festlokale mv).

Legitimasjonsbevis er primært knyttet til bruk av visse fysiske dokumenter. Biometriske teknikker kan brukes for å verifisere en identitet uten bruk av noe fysisk dokument som identitetsbevis. Det kan derfor være hensiktsmessig å bruke andre ord som er uavhengig av

[7] Til autentisering vil det ikke sjelden være knyttet funksjoner vedrørende "uavviselighet"/"ikke-benekting" (eng.: non-repudiation), dvs " å bekrefte at en handling eller et informasjonselement er uendret (informasjonsintegritet) og at det kan knyttes til en bestemt identitet", se FAD 2008 avsnitt 2.1. Slike funksjoner kommer jeg ikke nærmere inn på i den videre begrepsavklaringen, men spørsmålet har relevans for diskusjonene om personvernmessige konsekvenser av biometriske metoder, se særlig avsnitt 5.3.3.

[8] I så fall kan vi tale om autentisering av *roller* (snarere enn identiteter), jf Olsen 2008 med videre henvisninger. Se nærmere om dette straks nedenfor.

[9] Hvor stor sikkerhet som kreves, avhenger tradisjonelt av hvor alvorlige virkningene vil være av at det skjer feil identifisering.

metode om det å verifisere en identitet, og jeg er i tvil om legitimasjon(sbevis) er egnet i en slik utvidet betydning av ordet. I utredningen vil jeg derfor ikke bruke uttrykk knyttet til "legitimasjon".

Identifikatorer, identitetsmidler og identitetsmerker

Identifisering og autentisering skjer dels ved hjelp av *naturlig*e identitetsmerker (noe du er; irismønster, oppførsel; ganglag) og dels ved hjelp av *tildelte* identitetsmidler (noe du har eller vet; fødselsnummer, pin-kode, kundenummer mv). Identifisering og autentisering innebærer med andre ord å kjenne igjen et bestemt individ ved hjelp av identitetsmerker og/eller - midler.[10] Som fellesbetegnelse på identitetsmerker og identitetsmidler bruker jeg *identifikatorer*.

Identifikatorer kan gi større eller mindre fare for feil i id-håndteringen pga. forveksling, forfalskning, feil og unøyaktigheter ved teknologien som anvendes mv. Både identifisering[11] og autentisering betegner derfor hele spennet fra litt usikre til veldig sikre resultater. Autentisering alene ved hjelp av numre, passord mv er åpenbart usikkert, fordi det lett kan skje at andre enn vedkommende person kan ha fått tilgang til identitetsmiddelet. Bruk av åpne personalia (navn, adresse og telefonnummer) som passord gir derfor meget liten sikkerhet. Fødselsnummer alene er også uegnet som autentisering fordi nummeret er forholdsvis lett å skaffe kunnskap om.[12] Hemmelige tallkoder som er generert for å verifisere en persons identitet (f.eks. pin-kode[13]), gir større grad av sikkerhet, men er også sårbare i tilfelle uforsiktighet mv.[14] Blant sikre metoder for id-håndtering er bruk av identifikasjonsmidler som fingeravtrykk og irisgjenkjenning, men heller ikke disse gir 100% sikre resultater. I avsnitt 2.4.3 kommer jeg tilbake til spørsmålet om hvor sikre biometriske id-metoder kan sies å være.

Identifisering og autentisering av roller

Det at denne utredningen gjelder identifisering og autentisering av enkeltindividers identitet, forutsetter at det blir behandlet personopplysninger, jf pol § 2 nr 2, jf nr 1. Thomas Olsen fremhever muligheten for å identifisere og autentisere *roller* i stedet for hele personens identitet.[15] Særlig kan det være nyttig å *autentisere* roller/aspekter ved personer snarere enn personen selv. Dersom det primære for eksempel er å forsikre seg om at det kun er autoriserte personer som kan få tilgang til en bygning, er det verifikasjonen av rollen som autorisert person som er vesentlig, og ikke nødvendigvis autentisering av individenes identiteter. Tilsvarende dersom et flyselskap ønsker å forsikre seg om at det er samme person som sjekker inn bagasje og går om bord i flyet. Her er det rollen som passasjer med bagasje som er det vesentlige, ikke hvem denne personen er.

Jo mer begrenset en gjør slik identifisering og autentisering ved å knytte an til roller mv, jo mindre blir behovet for personopplysninger. I noen tilfelle vil en også kunne klare seg uten at det blir behandlet personopplysninger eller kun behandler personopplysninger på veldig begrensede og beskyttede måter. Dersom en på denne måten legger minimalitetsprinsippet[16] i den internasjonale personopplysningsretten til grunn ved utforming av enhver identifiserings- og

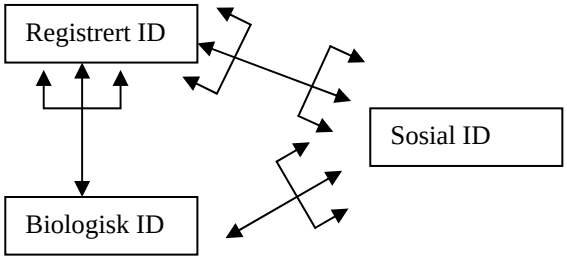
[10] Eventuelt også å *tildele* et identifikasjonsmiddel, jf ovenfor.
[11] Dvs å gjenkjenne personen ved hjelp av en eller flere identifikatorer.
[12] Se nærmere drøftelse i avsnitt 6.2 (nedenfor).
[13] Eller Personlig IdentifikasjonsNummer. Det er vanlig å benytte PIN-kode for å få tilgang til minibanker, nettbanker, porter/bygninger/rom/heiser og mobiltelefoner.
[14] De klassiske eksempelene er PIN-koder som skrives opp på huskelapper og PIN-koder som røpes fordi bruker ikke skjermer tallene under inntasting.
[15] Se Olsen 2008 med videre henvisninger.
[16] Om de europeiske personvernprinsippene, se Bygrave 2002 kap. 3 og 18.

autentiseringsrutine, kan behovet for biometri begrenses. Skillet mellom håndtering av identiteter og roller samt valg av løsninger som minimaliserer behovet for personopplysninger, er helt vesentlig fra et personvernsynspunkt som jeg kommer tilbake til i avsnittene 5.7 og 7.1.3 og 7.4. I fortsettelsen forutsetter jeg imidlertid at det blir behandlet biometriske opplysninger om enkeltindivider og dermed personopplysninger.

2.3 Identiteter og identitetslag

Ovenfor har jeg gått ut i fra at identitet betegner én ting. Jeg tror imidlertid det er mulig og fruktbart å skjelne mellom ulike typer identitet. I denne sammenhengen mener jeg særlig det kan være fruktbart å skjelne mellom:

- Biologisk (naturlig) identitet: Den du er ved å være barn av dine biologiske foreldre med bestemte fysiske og biologiske kjennetegn som biometrisk teknologi gjør bruk av;
- Sosial identitet: Den du presenterer deg som eller blir presentert/oppfattes som, av deg selv og/eller andre samfunnsmedlemmer. Personer er for eksempel barn av sine sosiale (ikke biologiske) foreldre;
- Registrert (formell) identitet: Den du er registrert som i samsvar med en disposisjon/bestemmelse hos en registreringsenhet. Dette kan være offentlige myndigheter (jf føring av Folkeregisteret), eller andre som ønsker å innføre personer i sine informasjonssystemer med formell beskrivelse av identitet (for eksempel i form av kunde- og medlemsnummer).



Figur 1: Ulike typer identiteter.

Ofte har vi forventning om at det skal være fullt samsvar mellom disse tre aspektene ved identitet, for eksempel slik at personer fremstår i sosiale sammenhenger som den de biologisk sett er, og som igjen samsvarer med det som er registrert i Folkeregisteret og andre steder. Ikke sjelden er det imidlertid uoverensstemmelse mellom de ulike identitetslagene. Personen opererer for eksempel med en annen *sosial* identitet enn den biologiske og/eller registrerte identiteten, eller nekter å oppgi identiteten. Dette kan være del av et akseptert sosialt spill, som når aktører på Internett gir seg ut for å ha en annen biologisk identitet enn de har og fremstår med uriktig alder, kjønn eller lignende. Men det kan også være ulovlig og sosialt uakseptabelt, som for eksempel når en person begår *identitetstyveri* ved å tilegne seg en annen persons identifikator for derved å oppnå en uberettiget fordel.[17] Det er grunn til å minne om at det i mange situasjoner er og bør være sosialt spillerom for avvik mellom disse tre identitetslagene. Enkelte deler av lovgivningen legger også opp til at registrert og sosial identitet ikke alltid skal være i overensstemmelse med den biologiske identiteten.[18]

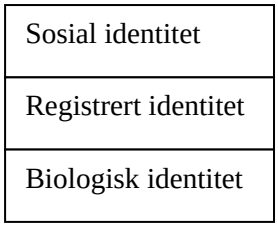
[17] Jf f.eks. strl §§ 182, 183 og 185 vedrørende dokumentfalsk og falske legitimasjonsbevis mv. En mer fullstendig definisjon av identitetstyveri er "Uautorisert innsamling, besittelse, overføring, reproduksjon eller annen manipulering av annen persons personlige informasjon med den hensikt å begå svindel eller annen kriminell handling som involverer bruk av falsk identitet." Definisjonen er oversettelse av definisjonen som er anvendt av CIPPIC 2008.

[18] Se politiloven kap. IIa om tildeling av fiktiv identitet.

I figur 1 (ovenfor) har jeg gått ut i fra at det for hvert individ finnes én biologisk identitet.[19] Til hver biologiske identitet kan det være flere/mange registrerte og sosiale identiteter.[20] Til hver registrerte identitet kan det være mange sosiale identiteter - og omvendt.[21] En og samme person vil med andre ord ofte ha flere registrerte identiteter. Personer er for eksempel registrert som norsk borger, bilfører, bankkunde mv. Hver registrering kan gjøre bruk av noe ulike identifikatorer, både med hensyn til type (alle personnavn, fødselsnummer eller ikke mv) og innhold (feilskrift av navn, kundenummer mv).

Den *biologiske* identiteten vises ved naturlige identitetsmerker, dvs. særlig visuelle og/eller auditive aspekter som personen uansett eksponerer overfor omverdenen. Alle har et bestemt utseende, noen har arr mv., et stemmeleie mv som kan brukes til å skjelne dem fra andre individer mv. Slike identifikasjonsmerker kan noen ganger gjemmes bort, ødelegges osv. Personen kan for eksempel gjennomgå kirurgisk operasjon, ta på parykk og endre stemmeleiet. Andre biologiske/fysiske identitetsmerker kan ikke effektivt endres eller skjules. Selv om fingeravtrykket slipes bort, vil det være utvokst etter ca 14 dager, mønsteret i iris er der så lenge du har øyne, osv. Noen biologiske kjennetegn er tilgjengelige uten utstyr (utseende, lyden av stemmen), andre kreves det utstyr for å avdekke (fingeravtrykk, irismønstre, målt stemmefrekvens, kjennetegn ved skjelettet osv.). Enkelte av disse identitetsmerkene er lett tilgjengelige og kan i tillegg leses ved hjelp av automatisert utstyr, og det kan derfor være relativt sikkert og billig å bruke for å gjennomføre identifisering og verifikasjon av identitet i ulike sosiale sammenhenger.

Når det gjelder den *registrerte* (formelle) identiteten vil jeg her kort belyse den ut i fra et myndighetsperspektiv. I mange tilfelle registrerer offentlige myndigheter navn på og beskrivelse av personer, dvs. etablerer en forbindelse mellom den fysiske personen og navn med nærmere beskrivelser av personen. Slik sikker etablering av forholdet mellom en persons biologiske og registrerte identitet er selvsagt helt avgjørende for at senere bruk av identifikatorer skal gi sikre resultater: Folkeregisteret må passe på at det virkelig er Marte Kirkeruds nyfødte barn som registreres som hennes og tildeles fødselsnummer i Folkeregisteret. I slike tilfelle kan det derfor være aktuelt å kvalitetssikre identiteten ved at Skattedirektoratet krever at jordmor, lege eller barnets mor legger frem nærmere opplysninger som kan dokumentere fødselen.[22] Passmyndigheten må på lignende måte sikre at passøker er den han utgir seg for å være, noe som f.eks. kan være et stort problem for personer som er født i land der det ikke finnes autoritative dokumenter som fastslår slektskap, fødested, fødselsdato mv.[23] Også den som utsteder sertifikater i tilknytning til elektroniske signaturer, må forvisse seg om hvilke fysiske personer de har med å gjøre, for eksempel ved hjelp av personlig fremmøte.[24]



Figur 2: Identitetslagene

Dersom jeg illustrerer biologisk, registrert og sosial identitet som horisontale lag, blir det tydeligere hvorledes vi kan sies å stå overfor identitetslag. I små samfunn der alle kjenner alle og når identitetsspørsmålet ikke har stor betydning for myndighetsutøvelse og næringsdrift mv, kan vi i stor grad basere oss på sosiale identiteter. Myndighetsutøvelse og økonomisk virksomhet av betydning er

[19] Her må det imidlertid tas forbehold om at det i sjeldne tilfelle kan skje skifte av kjønn.
[20] Mao. et én til mange forhold, her markert med antallet pilender.
[21] Mao. et mange til mange forhold, her markert med antallet pilender.
[22] Se forskrift av 25. oktober1982 nr 1524 om melding av fødsler, erkjennelse av farskap og melding om valg av navn, § 4.
[23] Jf folkeregistreringsforskriften av 9. november 2007 nr 1268, § 3-3.
[24] Se forskrift av 15. juni 2001 nr 611 om krav til utsteder av kvalifiserte sertifikater mv, § 7.

eksempler på disposisjoner som ikke (bare) kan basere seg på den enkeltes frie presentasjon av seg selv, men der en har behov for å formalisere og registrere ut i fra bestemte krav til sikker id-håndtering. Enten kan dette skje ved at personen får tildelt visse identitetsmidler av den som har behov for sikker identitetshåndtering. Alternativt kan det bestemmes at det er kjennetegn ved personen selv som skal nyttes direkte ved id-håndteringen.

2.4 Biometri mv.

2.4.1 Generelt

Id-håndtering kan som nevnt bl.a. skje ved hjelp av noe en person er, har eller vet. Biometri handler om identifisering og autentisering ved hjelp av personers naturlige egenskaper, dvs noe personer er, jf straks nedenfor. Før jeg går nærmere inn på biometri, kan det være grunn til å peke på en fjerde mulighet for id-håndtering, nemlig identifisering ved hjelp av noe et menneskes kropp *har blitt tilført*, dvs en mellomting mellom "er" og "har". Slike metoder avviker fra metoder som gjør bruk av noe personen "har", fordi det ikke er trivielt eller mulig å kvitte seg med identifikatoren. Samtidig er identifikatoren integrert i kroppen men ikke del av kroppen. Eksempelet er tilfelle der en identifikator festes til kroppen, eller integreres i kroppen som implantat e.l. For eksempel kan radiofrekvensidentifikasjon (RFID) tenkes anvendt på mennesker ved at en brikke med unik identitet festes til mennesket. Denne teknologien har til nå primært vært brukt i varehandelen og på husdyr mv, men har anvendelsesmuligheter som også kan omfatte mennesker. Det er også utviklet spiselige RFid-brikker, noe som innebærer at unik elektronisk merking av individer ikke forutsetter operative inngrep.[25]

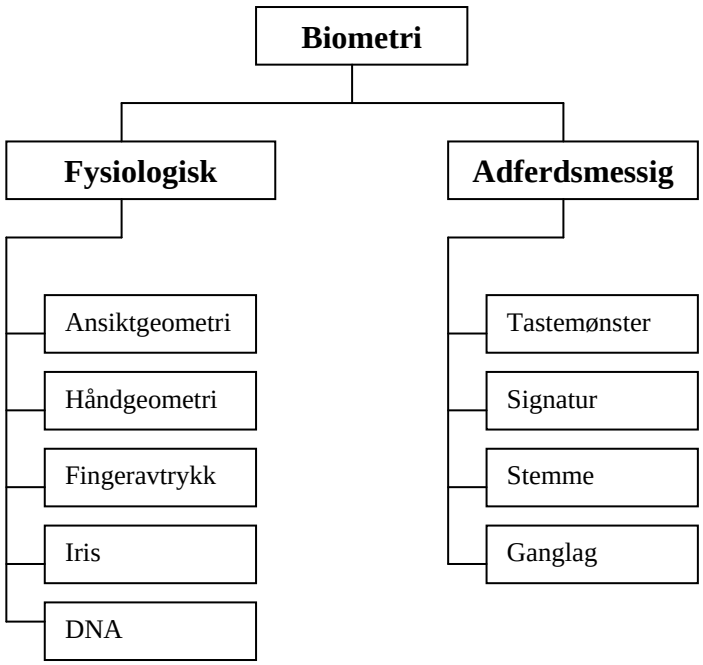
Jeg vil ikke her gå nærmere inn på denne teknologien, bare minne om at det foreligger muligheter for å tilføre enkeltindivider (barn, demente, straffedømte mv) unike identifikatorer som sender ut radiosignaler, og som både gjør det mulig å identifisere personer og verifisere identitet. RFid-brikker kan selvsagt gjerne inneholde og kommunisere biometrisk informasjon og således være et alternativ til lagringsmedier som personer *har* (id-kort mv). I motsetning til bruk av håndholdte id-kort og biometriske leseutstyr, vil ikke slik teknologi kreve noen aktiv handling fra angjeldende person, noe som kan legge til rette for bruk av biometriske opplysninger mv som personen ikke er seg bevisst.

2.4.2 Biometri

Rent språklig betyr "biometri" å "måle liv" (*bios* ="liv", *metron* ="måle"). Betegnelsen har vært brukt på visse kvantitative metoder innen biologi. I biologisk og plantefysiologisk leksikon[26] er biometri således definert som "Vitenskapen som omhandler bruk av statistiske og matematiske metoder anvendt på biologiske systemer. Statistisk undersøkelse og studium av likheter og forskjeller mellom grupper av arter." I den norske versjonen av Wikipedia er biometri definert som "måling av biologiske mønstre. Biologiske mønstre kan være fysiologiske karaktertrekk (for eksempel fingeravtrykk) eller adferdsmønstre (for eksempel ganglag)." I sist refererte definisjon har en med andre ord valgt en generell beskrivelse, kombinert med en forklaring som peker i retning av identifisering av mennesker og verifisering av menneskers identiteter.[27] I de senere årene har biometri i stadig større grad blitt brukt for å betegne entydig gjenkjennelse av enkeltpersoner ved hjelp av fysiske trekk ved deres fysikk/kropp eller oppførsel. I tilknytning til

[25] Se http://www.idg.no/bransje/bransjenyheter/article43936.ece.
[26] Se http://www.bio.uio.no/plfys/haa/leks/index.htm.
[27] Se også http://en.wikipedia.org/wiki/Biometrics.

høring av forslag til endring av passloven i mars 2005, ble "biometri" således definert som "biometriske kontrollelementer (eng; biometric identifier), (unike) fysiske karakteristika knyttet til en person (ansiktstrekk, fingeravtrykk, irismønster, DNA-profil) eller som beskriver en persons opptreden eller handlemåte (stemme, signatur), og som kan benyttes til å identifisere person eller verifisere at innehaveren av et identitetskort er samme person som kortet opprinnelig ble utstedt til."[28] Europarådet har anvendt en definisjon som også legger vekt på identifiserings- og autentiseringsformål: "Biometrics' refers to systems that use measurable, physical or physiological characteristics or personal behaviour traits to recognise the identity, or verify the claimed identity of an individual", jf. Europarådet 2005, s. 8.[29]



Figur 3: Noen typer biometriske mønstre
Kilde: Fritt etter Wikipedia 2008

Språklig og prinsipielt sett er ikke biometri spesielt knyttet til mennesker, men kan tenkes anvendt på alle biologiske mønstre, uansett biologisk art. I ordets grunnleggende betydning trenger biometri heller ikke være knyttet til funksjonen/formålet å identifisere enkeltindivider og/eller verifisere identitet. Biometri kan for eksempel tenkes anvendt innen medisinsk forskning og behandling som betegnelse på måling av ulike sider ved kroppens kjennetegn og tilstander mv. Selv om jeg avgrenser biometri til det som gjelder mennesker, kan begrepet - prinsipielt sett - derfor vanskelig avgrenses til spørsmål vedrørende identifisering og verifisering. Til tross for at disse formålene i dag er dominerende i diskusjonene om biometri, vil det etter min mening derfor være lite hensiktsmessig å benytte begrepet i lovgivning mv uten samtidig å presisere *formålet*, dvs. om det dreier seg om identifisering og/eller verifisering av identitet.

[28] Se http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2005/Horing-forsalg-til-endringer-av-passloven-mm/3.html?id=98152.
[29] Lignende definisjon legges til grunn i forretningskretser: se f.eks. International Biometrics Group (US-basert firma) som definerer "biometrics" som "[t]he automated use of physiological or behavioural characteristics to determine or verify identity", jf. http://www.biometricgroup.com/reports/public/reports/biometric_definition.html.

Heller ikke om jeg avgrenser biometri til formål som gjelder identifisering og verifisering av identitet, kan begrepet sies å ha et helt klart og avgrenset innhold. Dette skyldes for det første at det kan være usikkerhet mht hvilke biologiske mønstre som anses å falle innenfor biometri.[30] Det ser ut til å være enighet om at biometriske mønstre kan deles inn i i) de som gjelder fysiologiske karakteristika og ii) adferdsmessige karakteristika ved individer. Innen hver av disse gruppene er det imidlertid ulike mønstre som kan benyttes. I fremstillinger om biometri er det noen grad av variasjon mht hvilke mønstre og teknikker som trekkes frem. Figur 3 (ovenfor) illustrerer den nevnte todelingen av biometri og gir noen eksempler innen hver gruppe. Dessuten er det sannsynlig at forskning vil påvise at nye, til nå ukjente biologiske mønstre kan benyttes for identifiseringsformål mv. En forholdsvis nylig introdusert teknikk er således bruk av mønstre i blodårer på fingre, som i 2007 ble introdusert som integrert del av betalingssystem uten bruk av bankkort.[31]

2.4.3 Biometriske systemer

Figur 4 (nedenfor) angir grunnrisset av biometriske systemer, dvs av teknologiske hjelpemidler som utnytter biologiske kjennetegn og teknikker for å identifisere personer og verifisere personers identitet. Biometriske systemer kan sies å utføre mønstergjenkjenning som både forutsetter at det er registrert mønstre som skal være sammenligningsgrunnlag, og at det ved bruk registreres mønstre som skal sammenholdes med dette grunnlaget for å avgjøre om mønstrene er tilstrekkelig like til at det kan sies å foreligge likhet. Den først nevnte bruken av systemet kan jeg kalle *innrullering* av biologiske mønstre (eng.: "templates"), mens den siste delen gjelder *bruk* i form av identifisering og/eller verifisering.

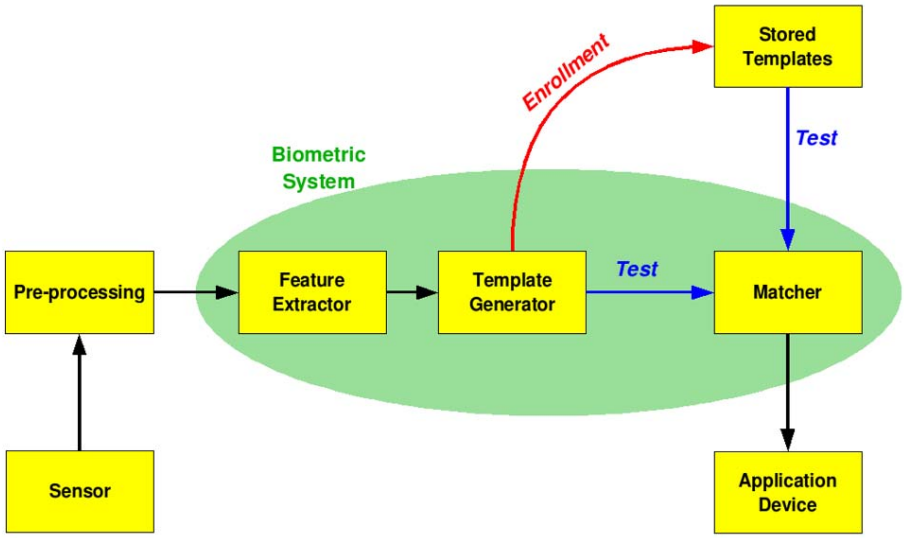
Mønsteret er en representasjon av det fingeravtrykket mv som det skal sammenlignes i forhold til. Innrulleringen av slike mønstre kan beskrives i fire steg. Første steg er bruk av en sensor som gjør datafangst og registrerer det/de biologiske kjennetegnene en ønsker å gjøre bruk av (fingeravtrykk, iris mv). Denne første registreringen gjelder fingeravtrykket mv slik det i virkeligheten fremstår. En sensor vil også registrere enkelte data som det ikke er formålstjenlig å behandle videre, dvs "støy" som ikke gjelder det ønskede mønstret. Slik støy fjernes gjennom andre steg som kan kalles "forbehandling". I tredje steg velges de egenskaper ved de registrerte dataene som (i fjerde steg) skal danne grunnlag for registrering av det biologiske mønstret. For eksempel velges det ut et visst antall punkter som karakteriserer fingeravtrykket. Det biologiske mønsteret utgjør i så fall en slags forenklet modell av det virkelige avtrykket. Ved innførsel av mønstre (dvs. registrering av personer) i systemet, lagres mønsteret i en database, på et kort eller et annet lagringsmedium. Det er også mulig å bruke avbildning av hele det virkelige avtrykket, dvs slik at det i tredje steg ikke skjer noe utvalg. I begge tilfelle velger jeg å snakke om biologiske mønstre. Når mønstrene kan knyttes til fysiske enkeltpersoner kan de betegnes "biometriske personopplysninger" (eller i kortform: biometriske opplysninger).

Etter innrullering, ved bruk av systemet, vil det lagrede mønsteret bli anvendt som sammenligningsgrunnlag. Når systemet anvendes vil det bli samlet inn mønstre fra personer som skal identifiseres eller verifiseres identiteten av, og dette innsamlede mønsteret vil bli sammenlignet med de lagrede mønstrene. Ved autentisering er sammenligningen foranlediget av

[30] Problemstillingen forutsetter at vi gjør de biometriske teknikkene til en del av definisjonen av biometri. Alternativt kan vi tenke oss at alle teknikker som gjelder menneskers kropp eller adferd ble ansett som biometriske, selv om disse kan anses som direkte uegnet for identifiseringsformål og for å verifisere identitet. Ordet "biometri" har imidlertid fått så stor autoritet, at jeg velger å gjøre teknikkene til en del av definisjonen.

[31] Se http://www.mobilemag.com/content/100/102/C12960/.

at personen fremsetter en påstand om egen identitet. Ved identifisering er det derimot behandlingsansvarlige som undersøker personers identitet ved hjelp av lagrede biologiske mønstre (leser ansiktsgeometri av folk på gaten for om mulig å gjenkjenne ettersøkte personer en har innrullert ansiktsdata på). Sammenligningen mellom lagret og lest mønster vil være styrt av



Figur 4. Modell av biometriske systemer.
Kilde: Wikipedia 2008

et datamaskinprogram som fastsetter hvor stor grad av likhet det skal være for at sammenligningen skal godtas som påvisning av identiske mønstre.

Mange av de biometriske teknikkene som er nevnt tidligere, inngår i systemløsninger som kan gi umiddelbart/raskt resultat. Enkelte mer tidkrevende metoder passer ikke like godt inn i dette bildet. Således kan DNA anvendes for å identifisere og verifisere identitet, men de aktuelle biometriske systemene som i dag er tilgjengelige gir ikke raske resultater. Likevel kan teknologisk utvikling tenkes å gjøre flere teknikker lettere og raskere å anvende, og det kan derfor være grunn til også å ta slike systemer med i betraktningen når en diskuterer den rettslige reguleringen av biometriske systemer.[32]

2.4.3 Sikkerhet ved bruk av biometri

Biometri angir *typisk* teknikker som gir identifisering og verifikasjon av identitet med meget høy grad av sikkerhet. Imidlertid kan jeg ikke ut i fra selve klassifikasjonen av noe som "biometri" konkludere noe helt bestemt om hvor (u)pålitelige resultatene vil være. Feilfunksjonen for biometrisk id-teknologi kan måles i Failure Acceptance Rate (FAR) og Failure Rejection Rate (FRR), dvs andelen uriktig akseptans og avvisning. For begge mål er det ikke uvanlig å sette en grense på 1%.[33] Det er imidlertid grunn til å tro at den teknologiske utviklingen vil gi økt prosesseringskraft i de biometriske systemene og lavere feilrater.

[32] Se http://www.findbiometrics.com/article/54. En omfattende oversikt over tilgjengelige biometriske systemer finnes på http://www.biometricgroup.com/biometricstore.html.
[33] Dette kan virke lite, men i følge Hornung (2007) vil dette innebære mer enn 1000 uriktige avvisninger ved bruk av biometriske pass på Frankfurt flyplass. En uriktig avvisning vil imidlertid lede til flere forsøk, og hvert forsøk vil ikke nødvendigvis ta lang tid. Hvor mange tilfelle som en til slutt må behandle konkret og manuelt er derfor et annet spørsmål.

Egenskap **Type**	Allment forekommende	Entydighet	Holdbarhet	Tilgjengelig-het	Gjennom-føring	Grad av aksept	Omgåelsesfare
Ansikt	H	L	M	H	L	H	L
Hånd	M	M	M	H	M	M	M
Fingeravtrykk	M	H	H	M	H	M	H
Iris	H	H	H	M	H	L	H
DNA	H	H	H	L	H	L	L
Tastemønster	L	L	L	M	L	M	M
Signatur	L	L	L	H	L	H	L
Stemme	M	L	L	M	L	H	L
Ganglag	M	L	L	H	L	H	M

L = Lav, M = Middels, H = Høy. Legg merke til at under "Omgåelsesfare" er L beste verdi, ellers motsatt

Kilde: Fritt etter Wikipedia 2008.

Tabellen ovenfor gjengir de viktigste vurderingskriteriene for kvaliteten av biometrisk id-håndtering.[34] *Allment forekommende* ("universality") gjelder spørsmålet om de biologiske/fysiologiske trekk som måles, er allment forekommende i befolkningen eller ikke. Noen mennesker vil for eksempel mangle hender og kan således ikke benytte teknologien. *Entydighet* ("uniqueness") gjelder i hvilken grad hvert menneske har de egenskapene som måles på måter de er alene om. Irisgjenkjenning har meget høy entydighet, mens for eksempel stemme kan ligne så mye at den ikke kan brukes til å skjelne enhver person fra andre. *Holdbarhet* ("permanence") sier noe om hvor holdbar over tid biometriske kjennetegn er, herunder hvor sårbare de er for skade, elding mv. Ansiktsgjenkjenning er for eksempel lett påvirket av skade og forandringer som skyldes sykdom og eldring mv, mens fingeravtrykk er klart mer stabile og robuste. *Tilgjengelighet* ("collectability") gjelder hvor enkelt eller vanskelig det er å samle inn de biologiske egenskapene som skal brukes. Ganglag er lett å samle inn informasjon om fordi det gjelder en handling som normalt lett lar seg observere, mens kroppslukt er vanskeligere tilgjengelig fordi det hører til den intime sfæren. Kriteriet *gjennomføring* ("performance") gjelder hvor lett eller vanskelig det er å bruke vedkommende biometriske teknikk. I praksis er det for eksempel vanskelig å gjennomføre ansiktsgjenkjenning, og forholdsvis lett å gjennomføre fingeravtrykkavlesning. *Grad av aksept* ("acceptability") gjelder i hvilken grad folk er villig til å la den biometriske teknikken bli brukt på seg selv, noe som igjen kan være et bilde på hvor integritetskrenkende folk mener bruken av teknikken er. Tabellen viser at ansiktsgjenkjenning er mer akseptabelt enn for eksempel skanning av iris, men slike oppfatninger vil trolig være kulturavhengige og i tillegg variere over tid. Til slutt kan biometriske teknikker vurderes ut i fra hvor stor *omgåelsesfare* ("circumvention") det er. Ansiktsgjenkjenning er i tabellen klassifisert som lite utsatt, mens fingeravtrykk er relativt mye utsatt for omgåelse, for eksempel fordi det kan være mulig å benytte avtrykk av andres fingeravtrykk.

Det skal bemerkes at tabellen ovenfor selvsagt må leses og brukes med skepsis, og gir kun indikasjoner på noen typiske forskjeller. Teknologiutvikling, brukssituasjoner og kulturelle forskjeller kan selvsagt virke inn på vurderingene og endre klassifiseringen og dermed forskjellene mellom teknikkene. Det mest vesentlige å merke seg er imidlertid at det finnes vurderingssystemer for bioteknologi som kan og vil bli videreutviklet, og som kan være til hjelp ved fremtidig vurdering om bestemte teknikker bør tillates brukt.

[34] Tabellen og forklarende tekst er basert på Jain et al 2004, gjengitt i Wikipedia. http://en.wikipedia.org/wiki/Biometrics (10.09.2008) og Wei and Li (2006).

Det at visse biometriske metoder er anerkjent som meget sikre (eks.: fingeravtrykk), kan muligens smitte over på andre teknikker og gi disse ufortjent godt renommé. Når ord som "unik" brukes i definisjoner av biometri om personers karakteristika, synes dette således å forutsette fravær av mulighet for feilidentifisering. Dette kan imidlertid neppe legges til grunn i forståelsen av definisjonen. I en artikkel av Jain et al 2004, blir de forskjellige biometriske mønstrene klassifisert ut i fra bl.a. "uniqueness" og "circumvention", og for hver egenskap delt inn i tre grader; høy, middels og lav. Det fremgår her at fingeravtrykk har høy grad av entydighet, mens ansiktsgjenkjenning skårer lavt på samme egenskap. Jeg har ikke forutsetninger for å gå inn i en nærmere diskusjon av slik tilordning av egenskaper, men mener det er viktig å huske at innenfor begrepet "biometri" er det relativt stor variasjon mht hvor unike og sikre de biologiske kjennetegnene er.

Det er dessuten grunn til å skjelne mellom hvor sikker selve den biometriske teknikken er, og hvor sikker *bruken* av denne teknikken kan sies å være. Selv om et fingeravtrykk er unikt, kan det være mulig å manipulere avtrykket eller på annen måte gjøre bruk av det tekniske utstyret der fingeravtrykkene inngår på måter som gir uriktige resultater. Spørsmålet er for eksempel om det er mulig å kopiere fingeravtrykk og få disse lest av systemet, om det er mulig å bryte seg inn i systemløsningene og endre, røpe eller sperre lagrede fingeravtrykkmønstre osv. Dersom det skjer trådløs kommunikasjon mellom chipen med lagrede biometriske data og innretningen som skal avlese disse dataene, er det dessuten fare for ulovlig kopiering av kort (jf "skimming") og avlytting (jf "eavesdropping") av kommunikasjonen mellom kort og leser. Enhver biometrisk teknikk og bruken av den må derfor vurderes konkret, også ut i fra bruksomgivelsene, og ikke kun ut i fra klassifiseringen som "biometri".

2.4.5 Eksempler på aktuell bruk av biometri

Et viktig anvendelsesområde for biometri er i tilknytning til innreisekontroll. USA vil således kreve ti fingeravtrykk ved innreise til landet.[35] Lignende tiltak kan være aktuelt for reisende inn til EU fra et tredjeland.[36] Også i tilknytning til lufttransport er fingeravtrykk aktuelt for å verifisere at det er samme person som sjekker inn bagasje som går om bord på flyet.[37] Fingeravtrykklesere er ikke minst aktuelle for adgangskontroll til bygninger og/eller tjenester. I Norge har for eksempel treningssentere ønsket å introdusere slik teknologi,[38] teknologien har vært brukt for å regulere tilgang til industriområde, og utenlands har fingeravtrykks-scanning vært brukt for å holde fotballpøbler ute fra stadionområder.[39] Teknologien kan selvsagt også anvendes for å regulere tilgang til utstyr, tjenester mv; for eksempel ved pålogging på PC mv,[40] og ved bruk av banktjenester.[41] Fingeravtrykkleser har også vært anvendt for å registrere gjester på utested som leverer inn klær i garderoben,[42] og har vært foreslått brukt for å hindre at reisende kjøper mer enn lovlig taxfreekvote.[43] Ved Meija College i Kina har fingeravtrykk blitt anvendt

[35] Se http://www.vg.no/reise/artikkel.php?artid=504870.
[36] http://www.dinside.no/reise/nyttig/sikkerhet/eu+vil+ha+fingeravtrykk+av+reisende/art490836.html.
[37] Molde lufthavn, Årø, 21.06 2007 Fingeravtrykk ved innsjekking og ombordstigning - verifikasjon, http://www.rbnett.no/apps/pbcs.dll/article?AID=/20070621/LOKALNYTT/70621009.
[38] Denne ble imidlertid ansett å være i strid med pol § 12, se avsnitt 4.3.3.
[39] Se omtale: http://www.itavisen.no/.nyheter/fingeravtrykk+stopper+hooligans/art366579.html.
[40] Se for eksempel Personvernnemndas sak vedrørende Tysvær kommune, referert under avsnitt 4.3.3.
[41] Se http://www.orapp.no/bank_og_finans/20070504/fingeravtrykk_minibank_i_2010/.
[42] Eksempelet er referert i Aftenposten, se http://www.aftenposten.no/nyheter/iriks/article1209557.ece.
[43] Se http://www.aftenposten.no/reise/nyheter/article2569188.ece.

for å kontrollere oppmøte blant elevene.[44] Blant de mest kontroversielle anvendelsene er regjeringen Berlosconis forslag om å registrere fingeravtrykket til alle landets mer enn 250.000 individer tilhørende rom-folket (sigøynere).[45] Forslaget var bl.a. begrunnet med bekjempelse av kriminalitet. En italiensk konsesjonssak viser at biometri også er aktuelt i arbeidslivet for å kontrollere arbeidstakernes arbeidsinnsats.[46]

Det er neppe grunn til å prøve og regne opp alle anvendelsesmuligheter som foreligger for fingeravtrykklesere og andre biometriske teknikker for identifisering. Til det er mulighetene for mange og vår fantasi for begrenset. Jeg tror den følgende kategorisering av behov for identitetskontroll illustrerer dette poenget:

id-teknologi for å erstatte bruk av manuelle identitetsbevis
Dette er tilfelle der jeg i dag benytter identitetsbevis som kontrolleres manuelt (pass, førerkort, ansattekort, personlig grunnkort innen kollektivtrafikk, kundekort i bank, studentbevis mv). I slike tilfelle er fremstillingen av identitetsbeviset relativt dyrt, bl.a. fordi en må sikre seg mot forfalskning, kompensere for slitasje, tap av kortet, og fordi personbilde mv må oppdateres. Samtidig er bruken av bevisene, dvs den manuelle kontrollen, kostbar. Slik identitetskontroll som i dag er knyttet til forholdsvis store ressursmessige innsatser, er åpenbare kandidater for omlegging til nye id-teknologier.

id-teknologi for å erstatte bruk av usikker identitetskontroll
I en del tilfelle bruker vi medlems-/kundekort uten bilde, herunder kort med PIN-kode til å knytte personer til visse disposisjoner og tjenester mv. Kortene er med andre ord utstedt i bestemte personers navn, og skal bare brukes av disse personene, men det er ikke mekanismer i selve kortet som hindrer at også andre personer bruker det. Kundekort, lånekort på bibliotek og nøkkelkort til bygninger mv, er eksempel på dette. Dersom innehaver av kortet ikke selv har særlig risiko når kortet blir overdratt til andre (for eksempel nøkkelkort), er det fare for at kort og kode kan bli utlånt til andre. Det er ikke usannsynlig at en i slike tilfelle vil se en utvikling der kortutsteder ønsker større sikkerhet og således ønsker å innføre bruk av biometri. Dersom dette blir mulig/tillatt er det ikke usannsynlig at flere tjenester enn i dag vil bli gjort personlige.

I en del tilfelle brukes det ikke noen form for medlemskort eller lignende, og identifikasjonen og/eller verifiseringen er bare begrenset til kunnskap om fødselsnummer, og/eller sentrale personalia. I så fall er fremgangsmåtene så usikre at den alene nærmest er uten verdi dersom en ønsker å unngå svindel mv. Selv om sikkerheten kan øke ved hjelp av supplerende teknikker (ringe eller maile tilbake nummer/adresse som er knyttet til fødselsnummeret som er oppgitt), er det fremdeles klar usikkerhet knyttet til sluttresultatet. I tråd med økende vekt på sikkerhet, er det grunn til å anta at også tilfelle der en i dag følger slike usikre fremgangsmåter, kan det være aktuelt å introdusere biometriske teknikker.

id-teknologi for å erstatte sosial kontroll
Med sosial kontroll med identiteter sikter jeg til situasjoner der det ordinært ikke benyttes noen form for identitetsbevis eller skjer noen formell identitetskontroll, men der individene på annen

[44] Se omtalen i Universitas; http://www.universitas.no/omverden/49209/.
[45] Se http://www.aftenposten.no/nyheter/uriks/article2533582.ece.
[46] Se Prior Checking: Use of Fingerprints for Assiduity Control at the Workplace – Provision of July 21, Garante per la protezione dei dati personali, tilgjengelig fra http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf. Bruken av biometri ble i dette tilfellet kjent ulovlig ut i fra en bred begrunnelse der bl.a. de europeiske personvernprinsippene vedrørende minimalitet og formålsbegrensning ble tillagt vekt.

måte blir observert/gir seg til kjenne. Et trivielt eksempel er situasjoner der personene må passere resepsjoner i hoteller og konferanselokaler mv der de må vise ansikt, men normalt slipper å være gjenstand for nærmere identitetskontroll. I samme kategori kommer opphold i første klasse på tog eller bruk av tjenester for en begrenset gruppe ("kun for middagsgjester"), dvs situasjoner der det kan oppdages at enkelte personer i et åpent sosial miljø mangler de rettigheter, privilegier mv som et oppslag, merking mv forutsetter. *Fraværs*kontroll med elever i undervisningsinstitusjoner, og kontroll med hvem som eventuelt mangler etter en militærøvelse eller reiseselskap, er mulige eksempler på sosial kontroll som kan tenkes erstattet av kontroll ved hjelp av id-teknologier.

Også denne kategorien er vid, og spenner over alt fra situasjoner der den sosiale kontrollen er forholdsvis sterk og viktig, til situasjoner der sosial kontroll er uviktig, og der rene administrative aspekter begrunner ordningen med å gi seg til kjenne. Slik må det for eksempel antas å være på mottak hos primærlegen, tannlegen eller andre personlig tjenesteytere. Her vil presentasjonen i skranken med ansikt og angivelse av navn primært være knyttet til behovet for å vite at en bestemt person har kommet. Fordi tjenesten er personlig og dermed knyttet til den enkeltes kropp, er behovet for identitetskontroll i mottaket begrenset. Likevel kan administrative muligheter knyttet til id-teknologi være betydelige. For eksempel kan pasienter identifisere seg med fingeravtrykk og direkte varsle helsepersonellet om at de har ankommet - uten mellomledd.[47] Identifiseringen kan også tenkes knyttet opp til journalsystemer eller lignende, for eksempel slik at identifiseringen også utløser automatisk fremhenting av pasientens elektroniske journal. Slik sett kan enkelte tilfelle som her er plassert under kategorien vedrørende sosial kontroll like gjerne plasseres under neste kategori der poenget er at id-teknologi kan generere ny informasjon.

id-teknologi og generering av personopplysninger

I den grad det skjer overgang fra manuell kontroll med personers identitet mv til bruk av fingeravtrykklesere eller annen ny id-teknologi, vil det samtidig genereres nye personopplysninger i maskinlesbar form. Utgangspunktet er at mange fremgangsmåter for identifisering skjer manuelt, og at overgang til fingeravtrykkleser eller lignende derfor innebærer ny innsamling av maskinlesbar personinformasjon.

I tilfelle der det i dag benyttes kort med pin-kode e.l., vil overgang til fingeravtrykkleser gi personopplysninger med sikrere tilknytning til identiteter, noe som kan øke verdien og anvendbarheten av opplysningene. Sikre opplysninger om at bestemte personer har vært på et bestemt sted, til en bestemt tid, samt opplysninger om personen som er knyttet til selve fingeravtrykkleseren (for eksempel et kjøp, omfang og innhold av forbrukte tjenester mv) kan innebære en selvstendig merverdi for den som har disposisjonsrett over opplysningene.

Ikke minst vil sammenkopling av personopplysninger med slik sikker identitetsforankring kunne ha stor verdi. Økt informasjonsverdi kan tenkes å være en selvstendig begrunnelse for å introdusere ny id-teknologi, dvs uten at det foreligger noe egentlig behov for identifisering som har sikkerhetsmessig begrunnelse. Dersom en på et treningsstudio for eksempel ønsker å skaffe oversikt over medlemmenes bruk av apparatur, kan id-teknologi tenkes introdusert som "brytere" som gir adgang til utstyret. Slike registreringer kan gi grunnlag for statistikk, flytanalyser mv, men kan også gi grunnlag for nye tjenester til medlemmene, for eksempel i form av IT-støttet gjennomføring av personlige treningsprogram.

[47] Se produktet IdentX som eksempel på dette: http://www.extensor.no/identx.htm.

Tyverisikring
Biometri for rene verifikasjonsformål kan åpenbart ha effekter på faren for tyveri mv. Forutsetningen er at bruk av gjenstander (biler, båter, PCer mv) låses til bestemte personer ved hjelp av biometriske teknikker. Dersom slike biometriske teknikker vanskelig lar seg hacke og manipulere med, kan vedkommende gjenstand bli lite verd for ikke autoriserte personer.

Fremtidig bruk ellers
I dag skjer bruk av fingeravtrykklesere som forholdsvis eksplisitte og tydelige handlinger. Uten å bli for spekulativ er det imidlertid grunn til å anta at slikt utstyr i langt større grad enn i dag vil bli brukt som integrerte elementer i annet utstyr. Fingeravtrykklesere som integrert del av dørvridere/låsesystemer er eksempel på dette. Jo større grad av integrering med annet utstyr, desto større grunn er det til å forvente at teknologien faktisk vil bli anvendt, fordi det da vil være lettere å venne seg til og få aksept for. Slik kan en lang rekke håndbetjent utstyr tenkes å inneholde fingeravtrykklesere. Tilsvarende kan situasjoner som fordrer aktiv bruk av øyne/blikk legge til rette for introduksjon av iris-lesere.

Hvor omfattende spredningen av id-teknologi vil bli er det ingen gitt å si noe sikkert om. Det er imidlertid grunn til å anta at det ikke bare er behovet for sikker identifisering ut i fra sikkerhetsmessige årsaker, som vil drive den videre teknologiske og samfunnsmessige utviklingen på området fremover. Sikkerhetsbegrunnelsene kan riktignok være "døråpneren" for slik teknologi, men behovet for praktiske og kostnadseffektive løsninger kan være vel så utslagsgivende på sikt. Slike praktiske begrunnelser mv. kan heller ikke anses å være generelt ønsket eller uønsket, og kan heller ikke generelt sies å være positivt eller negativt for personvernet. Brukt i låsesystemer kan en for eksempel legge til rette for at demente personer kan bevege seg friere og tryggere enn de i dag kan,[48] og kan gjøre det mulig å beskytte sensitive personopplysninger bedre enn i dag.[49]

Dersom vi forutsetter biometrisk id-teknologi i omfattende bruk, vil det oppstå sporproblematikk som ligner den vi i dag diskuterer som "elektroniske spor" og som mange mener er en stor utfordring for personvernet. Mens det er knyttet en viss grad av usikkerhet til elektroniske spor (noen kan ha tatt betalingskortet, lånt bilen osv.), vil de biometriske sporene være langt vanskeligere å fri seg fra. Også dette er "spor" i overført betydning, og kan også klassifiseres som "elektroniske". Poenget er derfor først og fremst at omfattende bruk av id-teknologi i kombinasjon med andre tjenester, entydig vil knytte personene til sine spor og dermed ytterligere skjerpe sporproblematikken, jf nærmere om dette i avsnitt 5.3.3 (nedenfor).

Selv om det er usikkert hva den teknologiske utviklingen vil bringe, og spesielt hvorledes spredningen og bruken av id-teknologi vil bli, er det neppe holdbart å forutsette annet enn en stor utbredelse. Omfattende innsamling av elektroniske spor ble oppfattet som et futuristisk skremmebilde da kortteknologien ble utviklet i 1970-årene. I dag er dette skremmebildet virkelighet, samtidig som de fleste tilsynelatende har tilpasset seg og akseptert situasjonen. Med den erfaringen kan det være grunn til å anta at vi kan få en lignende eksplosiv spredning av biometriske spor, og at det også kan skje en sosial aksept av denne utviklingen. Det kan imidlertid også være at teknologien og dens samfunnsmessige virkninger vil akkumuleres og overskride terskelverdier, dvs. at "begeret blir fullt" fordi for ekstensiv og intensiv kontroll med personers identitet utløser alvorlig sosial uro og protest.

[48] Forutsetningen er imidlertid at det ikke er mulig med konstant personlig samvær og pleie med demente personer.
[49] For eksempel ved fingeravtrykk- eller iris-pålogging til informasjonssystemer innen helsevesenet.

2.5 Fødselsnummer mv

2.5.1 Generelt

Identiteter i Folkeregisteret er bl.a. knyttet til fødselsnummer,[50] fødselsdato, fødested, opplysninger om mor og far, og tilhørighet til Den norske kirke, registrert personnavn, navn mv på foreldre osv. Så snart barnet er gitt navn, vil også dette bli registrert.[51] Ytterligere opplysninger om den registrerte personen kan føyes til senere i personens liv, for eksempel at personen er gift, blir forelder mv. I Folkeregisteret registreres mer enn 30 opplysningstyper. Alle disse opplysningene kan bidra til å skjelne hvert individ fra alle andre individer,[52] og er således helt sentral for statens registrering av identiteter.

Fødselsnummeret ble innført i 1964. Det består av elleve sifre, der de første seks sifrene er fødselsdato, og de fem neste sifre kalles personnummer. Personnummerets tre første sifre er individsifre. Det brukes ulike intervaller av individsifre for å angi i hvilken tidsperiode en person er født; for eksempel er sifrene 500–999 reservert for personer som er/blir født i perioden 2000 - 2039. Det siste tallet i individsifferet angir kjønn; slik at partall betegner kvinne og oddetall betegner mann. De to siste tallene er kontrollsifre, som beregnes ut i fra de foregående tallene.[53]

Fødselsnummer tildeles alle som er bosatt i Norge og andre som har et begrunnet behov for det, se folkeregistreringsloven[54] § 4. For utlendinger som ikke er bosatt i Norge, kan det tildeles et D-nummer[55] dersom vilkårene i forskrift om folkeregistrering § 2-6 er oppfylt. D-nummeret tilsvarer fødselsnummeret, men slik at fødselsdato er modifisert ved at tallet 4 legges til på det første sifferet.[56] Forskriften lister opp i alt åtte alternativer for tilknytning til landet som begrunner utferdigelse av D-nummer. Vilkårene gjelder skatte- og avgiftsplikt, trygderettigheter og visse former for økonomisk virksomhet.

Fødselsnumre kan endres i enkelte særlige tilfelle. Dette gjelder for det første tilfelle der det skjer endring av fødselsdato. Det gjelder egne regler om fastsettelse av fødselsdato i folkeregistreringsforskriftens § 2-3. Bestemmelsen gjelder særlig tilfelle der utlending mangler dokumentasjon eller når dokumentasjonen åpenbart er fingert, og der det derfor kan fastsettes en annen dato enn den virkelige (ukjente) fødselsdatoen. Endring av fødselsdato kan bare skje ved åpenbare skrivefeil og dersom det legges fram original og verifisert fødselsattest og fødselen er registrert senest et år etter fødselen. I spesielle tilfelle kan også annen troverdig dokumentasjon legges til grunn for endring. Fødselsnummeret kan også endres dersom kjønnsstatus endres, se folkeregisterforskriften § 2-2.

---

[50] Fødselsnummer gis på basis av fødselsmelding fra lege eller jordmor til Skattedirektoratet, jf forskrift av 25. oktober 1982 nr. 1524 om melding av fødsler, erkjennelse av farskap og melding om valg av navn, kapittel I.

[51] Forskriftene inneholder nærmere regler for tildeling av navn mv i tilfelle navnevalget ikke er brakt på det rene innen fristen, se forskrift av 25. oktober 1982 nr. 1524, kap. IV.

[52] Selv om de også har mange andre funksjoner.

[53] Oppbygging av fødselsnummeret er fastsatt i forskrift av 9. november 2007 nr 1268 om folkeregistrering, § 2-2.

[54] Lov om folkeregistrering av 16 januar 1970 nr 1.

[55] D'en i "D-nummer" er knyttet til Direktoratet for sjømenn. Nummeret ble visstnok innført på grunn av behov i tilknytning til utenlandsk mannskap på norske skip.

[56] Se folkeregistreringsforskriften § 2-5. En person som har fødselsdato 11.06.56 får for eksempel 510656. Det finnes også et hjelpenummer (H-nummer) som visstnok brukes innen helsevesenet. Dette brukes når det ikke eksisterer fødselsnummer eller D-nummer, og i tilfelle der disse numrene ikke er kjent. H-nummeret er bygget på tilsvarende måte som D-nummeret, men slik at tallet 4 legges til det tredje sifferet i fødselsdatoen.

2.5.2 Bruk av fødselsnummer mv. i hht folkeregistreringsloven[57]

Viktige opplysninger i folkeregisteret registreres på grunnlag av meldinger fra annen myndighet eller fra den folkeregistrerte selv.[58] Til det enkelte fødselsnummer og D-nummer kan det være knyttet en rekke opplysninger om vedkommende person. Folkeregisterforskriften § 2-1 angir i alt 37 opplysningstyper som er aktuelle og som både gjelder personen selv, fødselsnummer for personens foreldre, ektefelle/registrert partner og barn. Jeg skal ikke her komme nærmere inn på hvilke andre opplysningstyper som registreres, men nevner som eksempel opplysninger om fødested, aktuell adresse, sivil status, yrke, tilhørighet til Den norske kirke og opplysninger vedrørende oppholdstillatelse.

De fleste opplysninger i folkeregisteret er underlagt taushetsplikt i henhold til folkeregisterloven § 13. Opplysninger om fulle navn, fødested, fødselsdato og personnummer, adresse og eventuell dødsdato er normalt ikke underlagt taushetsplikt og kan utleveres til personer og private institusjoner på visse nærmere vilkår. Unntak gjelder når slike opplysninger kan røpe klientforhold eller andre forhold som må anses å være personlige. Fødselsnummer (fødselsdato + personnummer) er med andre ord i utgangspunktet ikke underlagt taushetsplikt og kan derfor ofte utleveres.

Vilkåret for å utlevere visse opplysninger om personalia fra folkeregisteret til private om noen *få* personer er at opplysningene er nødvendige for å ivareta lovmessige rettigheter eller plikter.[59] Gjelder utleveringen mange personer må det foreligge en lovmessig rettighet eller plikt til selve utleveringen.[60] Utlevering av noen få opplysninger om visse personalia til offentlige myndigheter er betinget av at det foreligger et begrunnet behov.[61] Gjelder det flere opplysninger må den offentlige myndigheten ha hjemmel for innhentingen.

Det kan bestemmes at andre lands offentlige myndigheter skal få tilgang til slike opplysninger. Når det finnes rimelig, og det ikke medfører skade for aktuelle personers interesser, kan Skattedirektoratet dessuten bestemme at opplysninger uten hinder av taushetsplikten i § 13 skal gis til forskning.

Skattekontorene avgjør begjæringer om utlevering. Krav om utlevering av opplysninger som omfatter mer enn noen få personer eller når det skjer regelmessige forespørsler om utlevering, avgjøres av Skattedirektoratet.[62] Før utlevering i maskinlesbar form kan skje, skal det være mottatt dokumentasjon som viser at den som ønsker opplysningene utlevert, har sendt melding til Datatilsynet i samsvar med personopplysningsloven § 31, eventuelt har konsesjon til å behandle sensitive personopplysninger, jf pol §33.[63] Ved krav om utlevering av fødselsnummer skal det med andre ord utøves i) kontroll ift personopplysningsloven, ii) skjønn mht mulighetene for å røpe klientforhold mv, og iii) begrunnelsen for å fremsette kravet om utlevering skal vurderes. Jeg har ikke undersøkt i hvor stor grad det er en realitet i disse vurderingene og om skattekontorene gjør konkrete undersøkelser av hver henvendelse, til tross for arbeidspress mv.

---

[57] Den følgende fremstillingen er klart forenklet.
[58] Dette gjelder meldinger om fødsler, død, vigsler, adopsjon mv, se folkeregisterforskriften kap. 3. I tillegg kommer plikt til å sende flyttemeldinger, se folkeregisterloven §§ 7 og 8 (bosattes meldeplikt), § 10 (utleiers meldeplikt) og folkeregisterforskriften § 7-14 (offentlige myndigheters meldeplikt i tilknytning til opphold i institusjon og ved privat pleie).
[59] Se folkeregisterforskriften § 9-4 første ledd.
[60] Se folkeregisterforskriften § 9-4 tredje ledd.
[61] Se folkeregisterforskriften § 9-3 første ledd.
[62] Se folkeregisterforskriften § 9-4 annet ledd.
[63] Se folkeregisterforskriften § 9-2 første ledd.

Fødselsdato og personnummer, som til sammen utgjør fødselsnummer, kan med andre ord ofte utleveres fra folkeregisteret til personer, private institusjoner og offentlige myndigheter. Et stort antall forvaltningsorganer og private organisasjoner innhenter fødselsnummer. Fødselsnummeret er normalt heller ikke underlagt taushetsplikt i slike situasjoner. Nummeret kan således være gjenstand for innsyn i samsvar med regler om innsynsrett i forvaltningsloven § 18, offentleglova § 3 og personopplysningsloven § 18. Regler om taushetsplikt for opplysninger som kan røpe klientforhold kan imidlertid begrense innsynsretten.

2.5.3 Bruk av fødselsnummer mv i henhold til undersøkt praksis

Innsamling av fødselsnummer er selvsagt ikke bare avhengig av hva som er tillatt etter folkeregistreringsloven. Størst betydning har trolig hva som faktisk etterspørres av offentlig forvaltning, forretningsdrivende, frivillige organisasjoner osv. I Ravlum 2005b, ble representanter for norske virksomheter innen henholdsvis privat og offentlig næringsvirksomhet, og offentlig tjenesteyting og forvaltning, spurt om hva slags personopplysninger de behandlet. Nesten alle (94%) behandlet fødselsnummer om egne ansatte, og det var ikke nevneverdig forskjell mellom respondenter i de to kategoriene.[64] Når det gjaldt registrering av fødselsnummer for eksterne (kunder, klienter, brukere osv.), var andelen som behandlet fødselsnumre i næringsvirksomhet, klart lavere (43%) enn innen offentlig tjenesteyting og forvaltning (85%).[65]

Undersøkelsen viser at registrering av fødselsnummer har betydelig omfang på mange samfunnsområder. Den nesten helt konsekvente bruken av fødselsnumrene i forhold til egne ansatte mv, skyldes imidlertid primært krav i ligningslovgivningen i tilknytning til innsending av lønns- og trekkopplysninger mv til skattemyndighetene.[66] Også behandling av fødselsnummer om eksterne (kunder mv) er resultat av lignende plikt til å sende ligningsoppgaver, for eksempel om bank- og forsikringskunder.[67] Det undersøkelsen fra 2005 imidlertid ikke sier noe om er i hvilken grad offentlige og private virksomheter anvender fødselsnummer mer generelt, og ut over de tilfelle der det følger av lovbestemte plikter. Spørsmålet om adgangen til å bruke fødselsnumre skal innskrenkes eller ikke, gjelder primært ikke lovpålagt bruk, se avsnitt 7.2.1 (nedenfor) og påfølgende forslag til ny bestemmelse om fødselsnumre i personopplysningsloven.

[64] Se Ravlum 2005b, tabell 2.1.
[65] I kategorien "andre virksomheter" (interesseorganisasjoner mv) var andelen 77%, men antallet respondenter var lavt.
[66] Se f.eks. § 3 nr 4 i forskrift av 23. desember 1988 nr 1083 om levering av lønnsoppgave, og en rekke andre forskrifter med hjemmel i ligningslovens kapittel 6 om kontrollopplysninger og ligningsoppgaver fra tredjemann.
[67] Se f.eks. forskrift av 22. desember 1992 nr 1190 om levering av ligningsoppgaver over innskudd og lån i banker, forsikringsselskaper m.v.

3 Oversikt over rettslig regulering og regjeringsinitiativ vedr. identifisering og biometri

3.1 Innledning

I dette kapittelet vil jeg kort gi oversikt over det jeg antar er status for norske sentrale myndigheters behandling av spørsmål om identifisering, fødselsnummer og biometri. Nærmere bestemt vil jeg gi oversikt over lovgivning, budsjettforslag og meldinger til Stortinget mv. som gjelder dette temaet. Jeg understreker at det følgende materialet ikke pretenderer å være resultater av forskning, men er basert på bearbeiding av enkle søk i Lovdata.no og Regjeringen.no med målsettingen å skaffe en oversikt snarere enn å gi en nøyaktig status. Jeg mener slik oversikt er ønskelig som basis for diskusjonen om rettslig regulering av fødselsnummer og biometri. Årsaken er primært behovet for å ha en rimelig sammenheng i lovgivningen, dvs. at eventuell regulering i personopplysningsloven av disse spørsmålene må ses i sammenheng med eksisterende reguleringer i annen lovgivning samt eventuelle planlagt lovgivning og andre initiativ. Blant annet er det viktig å finne ut om det eksisterer systematikker og begreper som kan/bør danne grunnlag for en tverrgående og sammenhengende tilnærming til spørsmål om identifisering og biometri. Oversikten er også viktig for spørsmålet om arbeidsdelingen mellom generell lovgivning i personopplysningsloven mv og ulike typer særlovgivning.

3.2 Oversikt over lov- og forskriftsregulering av identitet, identifisering og biometri

3.2.1 Aktuelle legaldefinisjoner mv

Det finnes en rekke spredte bestemmelser i lovgivningen som angår spørsmål om identifisering, fødselsnummer og biometri. Som ledd i denne utredningen har jeg søkt i Lovdatas fulltekstbaser med lover og sentrale forskrifter etter forekomster av de grunnbegreper som inngår i denne utredningen.[68] Jeg har kun funnet ett tilfelle av regulær legaldefinisjon av relevante begreper. Det gjelder helseregisterlovens (hrl) definisjon av "avidentifiserte helseopplysninger", "anonyme opplysninger" og "pseudonyme helseopplysninger", se hrl § 2 nr 2, 3 og 4.[69] Disse begrepene ligger imidlertid i periferien av behovene knyttet til denne utredningen. Passloven omhandler bl.a. "verifisering eller kontroll av passinnehaverens identitet" (§ 6). Selv om denne loven i utstrakt grad benytter slike sentrale begreper, er de ikke definert i loven.[70] De ordinære forarbeidene til passloven[71] går etter det jeg kan se heller ikke inn på spørsmålet om definisjon av sentrale begreper. I stedet er definisjoner gitt i innledningen til høringsnotatet fra Justis- og politidepartementet fra mars 2005.[72]

---

[68] Dvs med søkeord som "fødselsnummer", "identitet", "legitimasjon", "autent" og "verifisere". Alle søk har vært trunkerte, dvs. alle endelser av nevnte ordstammer er med i søket. Søk på "autent" vil for eksempel også omfatte "autentisering", "autentisk" osv.

[69] "Helseopplysning" er definert som en type personopplysning (se hrl § 2 nr 1, jf pol § 2 nr 1).

[70] I tillegg er det i passloven én forekomst av ordet "personalisering" (av passet). Begrepet er ikke forklart i loven, men er definert i høringsnotatet til endringen av passloven i mars 2005. Personalisering betegner en del av passutstedelsen der personinformasjonen blir lagt inn i passet, som visuell informasjon, navn, foto mv., dels som maskinlesbar tekst og dels med biometrisk informasjon lagret elektronisk i en databrikke.

[71] NOU 1994: 13 Passlov og Ot.prp. nr. 61 (1996-97) Om lov om pass (passloven).

[72] Se http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2005/Horing-forsalg-til-endringer-av-passloven-mm/3.html?id=98152.

I tillegg til definisjon av biometri (som tidligere er referert i avsnitt 2.4.2), inneholder høringsnotatet to andre definisjoner som er spesielt relevante for denne utredningen:

- "Identifisering, prosessen i forbindelse med at identiteten til en person blir fastsatt, f. eks. ved utstedelse av et identifikasjonsdokument. For senere identifisering eller verifisering kan det sammen med personinformasjon som navn og fødselsnummer opptas og lagres biometri (eng. enrolment). Senere identifisering kan skje mot biometri, for eksempel ved et fingeravtrykk som er tatt opp i forbindelse med tidligere identifisering."
- "Verifisering, betegner den prosessen som skjer når f eks et pass blir sammenlignet med passinnehaveren for å bekrefte at vedkommende er den passet er utstedt til. Ved tilpasset utstyr på passkontrollsted (grenseovergangssted), kan det foretas en automatisert sammenligning av den elektronisk lagrede personinformasjonen (ansiktsfoto, fingeravtrykk) i passet , mot tilsvarende informasjon som tas opp av personen ved kamera eller fingeravtrykklese."

Disse definisjonene inkorporerer i stor grad forhold vedrørende pass, og fremstår derfor ikke som generelle, og de er dessuten ikke særlig stringent formulerte men har et forklarende innhold. Derfor er de trolig ikke direkte egnet som utgangspunkt for legaldefinisjoner i personopplysningsloven og annen særlovgivning. Fordi identifisering og verifisering av identitet vedrørende pass er noe de fleste mennesker i Norge vil bli gjort kjent med, er det likevel grunn til å legge vekt på stor grad av samsvar mellom definisjonene i passloven og i person-opplysningsloven.

Autentisering av avsender mv er benyttet flere steder i lov- og forskriftsverket, særlig i forbindelse med elektronisk kommunikasjon. Kilden for denne språkbruken er i stor grad lov om elektroniske signaturer (e-signaturloven av 15. juni 2001 nr. 81). Denne lovens legaldefinisjoner inneholder imidlertid ingen nærmere avklaring av begreper som er sentrale for denne utredningen.

Flere sentrale definisjoner vedrørende identitet og biometri inngår i rapporten vedrørende eventuelt tilbud om nasjonalt id-kort for norske statsborgere og andre med fast opphold i Norge.[73] Dette er med andre ord ikke legaldefinisjoner, men forslaget fra arbeidsgruppen som skrev rapporten er at spørsmålet om id-kort bør lovreguleres i fremtiden, noe som vil kunne skape behov for fremtidige legaldefinisjoner. Jeg har ikke valgt å kopiere definisjonene i rapporten, men begrepsforståelsene i denne utredningen er stort sett i overensstemmelse med definisjonene i rapporten.

3.2.2 Lovgivning vedrørende identitet og identifisering mv

Dersom en grovt skal dele inn gjeldende lovgivning som regulerer spørsmål vedrørende identitet mv, er det særlig tre kategorier som er fremtredende:

1. Regulering av hjemmel for og kompetanse til å registrere opplysninger om identitet.
2. Regulering av bruk av id-kort mv og plikt til å identifisere seg.
3. Regler som gjelder beskyttelse av identitet og rett til å opptre anonymt.

Hjemmel for/kompetanse til å registrere opplysninger om identitet

I denne kategorien finner vi bestemmelser innen kriminalområdet, for eksempel i strpl § 160a om registrering i identitetsregisteret som er del av DNA-registeret,[74] flere bestemmelser i

[73] Se JD 2007 s. 6.

[74] Identitetsregisteret inneholder DNA-profiler fra personer med kjent identitet, deres personalia og henvisning til grunnlaget for registreringen. I tillegg er det et sporregister med informasjon om DNA-profiler fra åsteder med ukjent gjerningsmann, med opplysninger om funnsted og tid, samt eventuelt fornærmedes identitet.

straffegjennomføringsloven og bestemmelse om rett til å registrere opplysninger om identitetsbevis i lov om Schengen informasjonssystem (§ 6). Hvitvaskingsloven § 6 inneholder krav for rapporteringspliktige til å registrere "entydig identitetskode". Bestemmelser om registrering av identitet for personer med tilgang til innsideinformasjon finnes i verdipapirhandelloven § 3-5, og i partilovens § 20 stilles det krav til identifisering av bidragsytere.

I tillegg til kriminalområdet er det trolig helseområdet der rettslige krav vedrørende identitet fremstår som viktigst. Bioteknologiloven § 2-8 inneholder for eksempel hjemmel for å registrere sædgivers identitet i donorregisteret. Det er imidlertid ikke gitt nærmere regulering av kravene til sikker identifisering. Også i regulering av elektroniske signaturer (e-signaturloven)[75] står spørsmål om identifisering sentralt i tilknytning til utferdigelse av kvalifiserte elektroniske sertifikater, se lovens § 13. I tilhørende forskrift om krav til utsteder av kvalifiserte sertifikater mv § 7, er hovedregelen for identitetskontroll imidlertid bare personlig oppmøte.[76]

Regulering av bruk av id-kort mv og plikt til å identifisere seg

En rekke krav i lovgivningen gjelder bruk av id-kort og krav til å identifisere seg. Blant de mest sentrale bestemmelsene er krav i tilknytning til sikkerhet på arbeidsplassen,[77] id-kort som sikringstiltak i transportsektoren,[78] krav til å identifisere seg i økonomiske forhold,[79] spørsmål vedrørende pass[80] og søknad om statsborgerskap,[81] valg,[82] identifisering overfor politi- og fengselsmyndigheter,[83] og i forbindelse med utlendingers adgang til riket mv.[84] I lov om anerkjennelse og fullbyrding av utenlandske avgjørelser om foreldreansvar mv og om tilbakelevering av barn artikkel 8 nr. 2, er det også satt krav til identifisering av barnet og foreldrene.

Beskyttelse av/tilgang til ID

Flere viktige bestemmelser i lovgivningen beskytter personers identitet. Således gjelder for eksempel en rekke bestemmelser i straffeprosessloven beskyttelse av vitners identitet i tilknytning til anonym vitneførsel.[85] Anonymitet og beskyttet identitet er også garantert i lovgivning vedrørende granskningskommisjoner.[86] Også visse klageres identitet kan være

[75] Lov av 15. juni 2001 nr. 81.
[76] Se forskrift av 15. juni nr. 611.
[77] Se arbeidsmiljøloven § 4-1 med forskrifter.
[78] Se for eksempel forskrift om sikring av havner og havneterminaler mot terrorhandlinger mv (FOR-2007-07-03-825)og FOR-2004-04-30-715 Forskrift om sikkerheten i luftfarten. Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten (2004-04-30).
[79] Se for eksempel hvitvaskingsloven § 5 Identitetskontroll og Verdipapirregisterloven § 6-5 om krav til dokumentasjon av identitet ved registrering av rettigheter til finansielle instrumenter.
[80] Se passloven §§2, 3, 6 og 6a.
[81] Se statsborgerloven § 7 om krav til klarlagt identitet ved søknad om statsborgerskap, jf tilhørende forskrift der hovedregelen er at fremleggelse av pass godtas som identitetsbevis.
[82] Se valgloven § 8-4 om identifisering av velgere.
[83] Se for eksempel politiloven § 10 om rett til å innbringe personer som ikke vil/kan identifisere seg og § 12 om visitasjon for å bringe ID på det rene. Straffegjennomføringsloven § 27 og 32 inneholder flere bestemmelser vedrørende krav og hjemler til identifisering mv overfor Kriminalomsorgen.
[84] Se en rekke meget inngripende bestemmelser i utlendingslovens kapitler 6 og 7, samt utlendingsforskriften § 128 flg.
[85] Se straffeprosessloven §§ 21a, 28, 40, 52, 130a, 234a, 242, 245, 264 og 292.
[86] Se lov om granskingskommisjonen for Mehamn-ulykken § 2, og lov om granskningskommisjonen som skal foreta en bred gjennomgang av utredning, planlegging, prosjektering og utbygging av ny hovedflyplass for Østlandet og Gardermobanen § 2 anonymitet for den som forklarer seg for kommisjonen.

beskyttet i lov.[87] Politiloven inneholder regler om tildeling av fiktiv (falsk) identitet, se dennes kapittel II a.

Spørsmål om beskyttet identitet og anonymitet står særlig sterkt innen de deler av helselovgivningen som gjelder slektskap og opphav til humant materiale mv. Således har bioteknologiloven §§ 2-9 annet ledd en regel om at sædgiver ikke skal gis opplysninger om parets eller barnets identitet, og transplantasjonsloven § 8f har bestemmelser om anonym bruk av fostervev.

Barns identitet er spesielt beskyttet i lovverket. For å verne om rettighetene og interessene til barn som er offer for menneskehandel, prostitusjon og pornografi har Norge forpliktet seg til å beskytte slike barn på alle trinn i den strafferettslige prosessen. Dette gjelder bl.a. ved å "beskytte, der det er hensiktsmessig, de berørte barnas privatliv og identitet, samt treffe tiltak i samsvar med nasjonal rett for å unngå utilbørlig spredning av informasjon som vil kunne føre til at barna blir identifisert."[88]

3.2.3 Lovgivning som spesielt gjelder biometri

Det finnes lovhjemler for bruk av biometri for identifiseringsformål mv i straffeprosessloven, passloven samt i gjeldende[89] og ny[90] utlendingslov. Etter straffeprosessloven § 160 kan det tas fingeravtrykk og fotografi av personer som mistenkes eller er dømt for en handling som etter loven kan medføre frihetsstraff, og personer som er besluttet utvist eller utlevert til fremmed stat.[91] Samme lovs § 160a hjemler opprettelse av sentralt DNA-register til bruk i strafferettspleien og innsamling av humant biologisk materiale fra personer som kan registreres i registeret.[92] Påtaleinstruksen[93] inneholder nærmere regler om innsamling av fingeravtrykk og fotografering av mistenkte (kap. 11) og registrering og bruk av DNA-profiler (kap. 11a). Reguleringen i påtaleinstruksen forutsetter ikke bruk av bestemte biometriske systemer (jf avsnitt 2.4.3, ovenfor). Spørsmålet oppstår derfor om påtalemyndigheten kan gjøre bruk av enhver teknologi for behandling av slike data, for eksempel ansiktsgjenkjenningssystemer.[94]

For pass er det hjemmel til å gjøre bruk av "biometrisk personinformasjon i form av ansiktsfoto", dvs ansiktsformen kan brukes for å verifisere personers identitet, se passloven § 6 annet ledd. Tidligere hadde passforskriftens § 5 også bestemmelser om at fingeravtrykk skulle inngå i pass for personer under 8 år og personer som ikke selv kunne underskrive passboken. Denne bestemmelsen ble imidlertid opphevet ved forskrift av 20. september 2005 nr. 1188. Bakgrunnen var at ansiktsfoto er lite egnet for små barn fordi ansiktsformen raskt endres. Tanken var derfor at fingeravtrykk fra små barn kunne kompensere for denne svakheten. Denne løsningen var

[87] Se diskrimineringsloven, Vedlegg 2. Internasjonal konvensjon om avskaffelse av alle former for rasediskriminering (norsk oversettelse) artikkel 14 nr 6, og lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste § 8 nr 1.
[88] Se menneskerettsloven med valgfri protokoll til konvensjon om barnets rettigheter om salg av barn, barneprostitusjon og barnepornografi, 25. mai 2000, art. 8 nr 1, bokstav e. Protokollen gjelder som norsk lov i hht menneskerettsloven § 2 nr. 4 b og § 3.
[89] Lov av 24. juni 1988 nr. 64.
[90] Lov av 15. mai 2008 nr. 35.
[91] Se nærmere regler i Påtaleinstruksen, kapittel 11.
[92] Det kan også bestemmes at registeret skal brukes til forskning, se strpl § 160a tredje ledd.
[93] Forskrift av 28. juni 1985 nr.1679 om ordningen av påtalemyndigheten.
[94] Jeg har ikke tatt stilling til spørsmålet.

imidlertid ikke grundig vurdert og muligheten for slik bruk av fingeravtrykk trådte aldri i kraft før § 5 ble opphevet.[95]

Det kan tas fingeravtrykk av en rekke kategorier utlendinger, se utlendingsloven § 37 fjerde ledd.[96] Dette gjelder for eksempel utlending som ikke kan dokumentere sin identitet mv, asylsøkere og utlendinger som er utvist eller bortvist. Slike opplysninger kan registreres i et "EDB-basert fingeravtrykkregister" (femte ledd). På visse nærmere vilkår gir utlendingsloven også hjemmel for DNA-testing for å fastslå familierelasjoner, se § 37f. I saker om asyl, arbeidstillatelse og oppholdstillatelse for personer der det ikke er mulig å fastslå alder med rimelig sikkerhet, kan utlendingen anmodes om å la seg underkaste undersøkelse for å bringe alder på det rene (§ 37g). Slik undersøkelse skjer ved å bedømme kjennetegn ved skjelettet, idet ungdommenes tenner og/eller hånd og håndledd røntgenundersøkes.[97] Undersøkelsene kan sies å være biometri i en grunnleggende betydning av ordet, se avsnitt 2.4.2.

I ny utledningslov er det tatt inn hjemmel til omfattende identitetskontroll ved inn- og utreise av Schengen-området, herunder ved anvendelse av biometriske teknikker. Paragraf 15 i loven fastsetter således at det kan "foretas andre former for identitetskontroll, herunder iriskontroll, kontroll av fingeravtrykk og ansiktsgjenkjenning". Oppregningen må trolig forstås som tillatelse til å benytte en ikke uttømmende liste over biometriske identifiseringsteknikker. Andre regler om fingeravtrykk og fotografi er tatt inn i § 93 tredje ledd (asylsøkere) og i kap. 12 (om bl.a. Eurodac-registeret, § 101). Regler om DNA-testing (§ 87) og aldersundersøkelse (§ 88) er også tatt inn i den nye loven.

Lov om iverksetjing av internasjonale, ikkje-militære tiltak i form av avbrot eller avgrensing av økonomisk eller anna samkvem med tredjestatar eller rørsler,[98] regulerer bl.a. andre lands tilgang til visse biometriske systemer, se § 1. Således anses utstyr for "særskilt konstruert fingeravtrykk-utstyr" (fingeravtrykklesere mv) å ha et så stort undertrykkingspotensiale at det inngår i listen over produkter som det er forbudt å sende til visse land med autoritære regimer som er gjenstand for særlige sanksjoner. Dette gjelder land som Usbekistan, Zimbabwe og Burma (Myanmar).[99]

3.2.4 Lovgivning som spesielt gjelder bruk av fødselsnummer

Innføring og bruk av fødselsnummer, D-nummer mv er i første rekke regulert i folkeregisterloven med forskrift. Disse bestemmelsene er det i grove trekk gjort rede for i avsnitt 2.5.2 om bruk av fødselsnummeret og vil derfor ikke bli gjentatt her.

En rekke lover inneholder hjemmel vedrørende innsamling og registrering av fødselsnummer. Dette gjelder for eksempel samvirkelova[100] § 9(2), stiftelsesloven[101] § 8, revisorloven[102] § 10-1, straffegjennomføringsloven[103] § 7a annet ledd, og smittevernloven[104] § 2-3 fjerde ledd. I tillegg

[95] Denne forklaringen vedrørende fingeravtrykk for barn er basert på mail datert 23. september 2008 fra Steinar Talgø ved Juridisk seksjon i Politidirektoratet .
[96] Jf. utlendingsforskriften § 128.
[97] Metoden har vært kritisert for å være for usikker, se for eksempel http://www.klassekampen.no/artikler/nyheter/48340/mod_article/item/null.
[98] Lov av 27. april 2001 nr. 14.
[99] Se henholdsvis forskrifter av 28. april 2006, 15. august 2003 og 4. juli 2003.
[100] Lov av 29. juni 2007 nr. 81.
[101] Lov av 15. juni 2001 nr. 59.
[102] Lov av 15. januar 1999 nr 2.
[103] Lov av 18. mai 2001 nr. 21.

kommer et stort antall bestemmelser vedrørende registrering av fødselsnummer i forskrifter. Jeg har ikke gjort systematiske undersøkelser av disse reguleringene, men søkeresultatene i Lovdata peker i retning av ca 150 bestemmelser vedrørende krav/anledning til registrering mv av fødselsnummer i lover og sentrale forskrifter.

Personopplysningsloven § 12 stiller vilkår for bruk av fødselsnummer, og krever at anvendelse av nummeret både skal være saklig begrunnet og at nummeret skal være nødvendig for sikker identifisering. Datatilsynet kan imidlertid også pålegge bruk av fødselsnummer dersom dette er nødvendig for å sikre tilstrekkelig kvalitet på personopplysningene. Jeg kommer nærmere tilbake til forståelsen av pol § 12 i avsnitt 3.4 nedenfor.

Personopplysningsforskriften setter enkelte grenser for bruk av fødselsnummer. For det første er det gitt en regel i tilknytning til folks rett til å reservere seg mot direkte markedsføring, se pol § 26. Paragraf 5-4 annet ledd i forskriften presiserer således at fødselsnummer ikke kan overføres Reservasjonsregisteret i Brønnøysund i tilknytning til oppdatering av adressatregistre som vaskes/oppdateres mot Reservasjonsregisteret. Slik oppdatering skal skje minst hvert kvartal, se pol § 26 tredje ledd. Bare adressatregistre som fra før inneholder fødselsnummer får med andre ord tilgang til disse fra Reservasjonsregisteret.

Samme forskrifts § 9-2 forbyr bruk av fødselsnummer i postsendinger på måter som gjør nummeret synlig for andre enn adressaten. Bestemmelsen får tilsvarende anvendelse ved bruk av telekommunikasjon, noe som formodentlig innebærer at fødselsnummer ikke skal forekomme der de lovlig kan leses av andre enn avsender og mottaker, dvs. fødselsnummer skal for eksempel ikke vises i emnefeltet på elektronisk post.

3.2.5 Samlet bilde

Samlet sett gir min brede men ufullstendige gjennomgang av lovgivning mv vedrørende identifisering generelt, samt biometri og fødselsnummer spesielt, inntrykk av en rekke spredte bestemmelser som ikke er bygget på noen samlet begrepsforståelse eller systematikk. Slik sett ligger det forholdsvis få føringer i eksisterende lovgivning på systematiske og begrepsmessige valg i eventuelle nye bestemmelser om bruk av fødselsnummer og biometri for identifisering og verifikasjon av identitet.

Regelverksoversikten forteller muligens også noe om spredningspotensialet som biometriske metoder med identifiseringsformål kan ha. Således kan det være grunn til å forvente at det i tilknytning til deler av særlovgivningen som i dag inneholder krav til identifisering og verifikasjon av identitet, kan oppstå krav om å få adgang til å anvende biometriske teknikker. Dersom dette er en holdbar antagelse, vil ikke generelle regler i personopplysningsloven som angir vilkår for bruk av biometri nødvendigvis bli viktigst for ivaretagelsen av personvernet. Tvert i mot kan særreguleringer komme til å dominere på livsområder der vernebehovet vil være størst, for eksempel innen helsesektoren, strafferettspleien, kriminalomsorgen, ved sikring av transportmidler, utlendingsadministrasjonen og i spørsmål om pass og statsborgerskap. Gitt denne antakelsen vil regulering av biometri mv i personopplysningsloven få betydning for annen spredt anvendelse av biometriske teknikker, for eksempel innen adgangskontroll, pålogging på datamaskinsystemer mv.

[104] Lov av 5. august 1994 nr. 55.

På områder som i dag omfattes av særlovgivning men som ikke har regler vedrørende identifisering, kan det dessuten lett tenkes introdusert slike bestemmelser. Det kan med andre ord ikke utelukkes at antallet lover og forskrifter med bestemmelser om identifisering mv vil øke, og at også disse kan komme til å inneholde bestemmelser om biometri. Jeg kommer nærmere tilbake til de regeltekniske problemstillingene, og særlig om forholdet mellom generelle bestemmelser i personopplysningsloven og bestemmelser i særlovgivningen nedenfor i avsnitt 7.1.2.

3.4 Regulering av fødselsnummer og andre entydige identifikasjonsmidler, personopplysningsloven § 12

3.4.1 Innledning

Pol § 12 regulerer bruk av "fødselsnummer og andre entydige identifikasjonsmidler", og stiller opp krav til saklig behov og nødvendighet for at bruk av slike identifiseringsmåter skal være lovlige. Loven gir imidlertid også kompetanse for Datatilsynet til å pålegge bruk av slike identifikasjonsmidler.

Bestemmelsen tilsvarer ingen bestemmelse i den tidligere personregisterloven (pregl).[105] Fram til ikrafttredelse av personopplysningsloven gjaldt det i mange tilfelle konsesjonsplikt, eller vilkår for og bruk av personregistre var detaljert regulert i forskrift. I tilfelle av konsesjon skulle en bl.a. ta stilling til hvilke opplysningstyper som kunne tas inn i registeret og hvilke vilkår som skulle gjelde for bruken. Spørsmål vedrørende fødselsnummer var blant de forhold loven spesielt påla konsesjonsmyndigheten å vurdere, se pregl § 11 nr. 4. For at fødselsnummer skulle være tillatt å registrere, måtte det med andre ord være gitt en spesifikk tillatelse. Konsesjons-myndigheten kunne både nekte bruk av fødselsnummer og stille vilkår for bruk. I tilfelle der det gjaldt unntak fra konsesjonsplikten, var det i noen tilfelle eksplisitt regulert at fødselsnummer kunne registreres og hva det kunne brukes til. I andre tilfelle var det ikke tillatt å registrere fødselsnummer i konsesjonsfrie registre.[106]

Pol § 12 er gitt med bakgrunn i artikkel 8 i personverndirektivet (95/46/EU) der det heter i nr. 7 at

"Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed."

Artikkel 8 nr. 7 regulerer nasjonale identifikasjonsteknikker som har generell anvendelse. Nasjonalt identifikasjonsnummer er nevnt spesielt, men bestemmelsen omfatter anvendelse av enhver teknikk som kan benyttes i forhold til hele befolkningen eller en ubestemt krets eller ubestemt antall individer i befolkningen. Bestemmelsen er heller ikke avgrenset til å gjelde nummersystemer, men er teknologiuavhengig utformet, og omfatter således trolig også biometriske identifikasjonsmetoder, herunder bruk av fingeravtrykk.[107]

---

[105] Lov av 9. juni nr. 48 om personregistre m.m, opphevet ved ikrafttredelse av personopplysningsloven, se dennes § 52 nr 2, jf dog overgangsreglene i § 51.

[106] Dette gjaldt for eksempel for kunde-, abonnent- og leverandørregistre der en måtte nøye seg med navn, adresse og fødselsdato (se personregisterforskriften § 2-3).

[107] Se Artikkel 29 arbeidsgruppen 2003 avsnitt 3.8 der gruppen uttaler at: "Biometric data are unique and most of them generate a unique template (or image). If used widely, in particular for a substantial proportion of a population, biometric data may be considered as an identifier of general application within the meaning of Directive 95/46/EC."

Bestemmelsen er del av Section III, Special Categories of Processing, og gjelder med andre ord en type personopplysning som er viet særlig oppmerksomhet i direktivet på grunn av den mulige skaden for personvernet som slike spesielle opplysningstyper kan medføre. I artikkel 8 nr. 1 er det for øvrig angitt slike opplysninger som i pol § 2 nr. 8 er klassifiserte som sensitive. Det er imidlertid verd å merke seg at direktivet selv ikke benytter betegnelsen sensitiv om noen opplysningstyper, heller ikke om opplysninger om rase, religion, helse mv som er betegnet sensitive etter den norske loven. Etter direktivet er med andre ord bruk av nasjonalt identifikasjonsnummer og andre identifikasjonsteknikker kun eksempler på behandling av en type personopplysning som skal underlegges særlig regulering.

Direktivet angir en forholdsvis detaljert regulering av slike opplysningstyper som er sensitive etter norsk lov, mens det for bruk av nasjonalt identifikasjonsnummer mv kun pålegges at dette reguleres på nasjonalt nivå. Det forutsettes i bestemmelsen at slike identifikasjonsteknikker ikke skal kunne brukes fritt ("shall determine the conditions …"), men det fremgår intet direkte om hvor strenge slike vilkår skal være, eller hvilke typer vilkår som kan settes. Selv om plasseringen av bestemmelsen skaper en forventning om restriktiv regulering, må direktivet antas å gi stor frihet for nasjonal regulering av slike identifikasjonsteknikker.

3.4.2 Oversikt over innholdet av pol § 12

Generelt

Bestemmelsen lyder i sin helhet:

> **"§ 12.** *Bruk av fødselsnummer m.v.*
>
> Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.
>
> Datatilsynet kan pålegge en behandlingsansvarlig å bruke identifikasjonsmidler som nevnt i første ledd for å sikre at personopplysningene har tilstrekkelig kvalitet.
>
> Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer og andre entydige identifikasjonsmidler."

Forarbeidene gir ingen nærmere forklaring av "identifikasjonsmidler", men eksemplifiserer ved også å nevne biometri.[108] Heller ikke spørsmål om autentisering tas opp til diskusjon, og det er lite trolig at distinksjonen mellom identifisering og autentisering var tema da loven ble forberedt. Etablert praksis i Personvernnemnda (se avsnitt 4.3.3, nedenfor), bygger imidlertid på den forståelse at bestemmelsen også kan anvendes på spørsmål om autentisering. I tillegg omfattes identifisering i vanlig betydningen, dvs. å sette navn på og å finne frem til hvem en person er,[109] for eksempel med tanke på å sammenstille personopplysninger fra flere kilder. Da person-opplysningsloven ble forberedt var slike samkjøringsmuligheter viktige og en vesentlig del av motivasjonen for bestemmelsen i § 12. Årsaken var at samkjøring etter personregisterloven var avhengig av konsesjon, mens det etter personopplysningsloven ikke var slike krav til forhånds-tillatelse. Derfor var redusert tilgang til fødselsnummer som universell koplingsnøkkel viktig.

Article 8, §7 of Directive 95/46/EC would then be applicable and Member States would have to determine the conditions of their processing.

[108] Se merknadene til § 12: "Bestemmelsen gir en generell regulering av bruk av fødselsnummer og andre entydige identifikasjonsmidler som for eksempel fingeravtrykk og andre biometriske data."

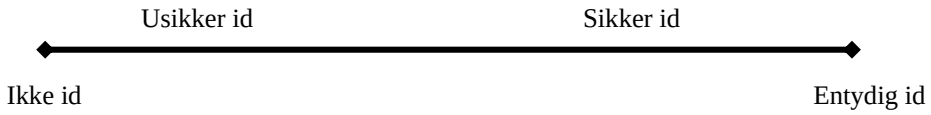
[109] Jf avsnitt 2.2 ovenfor.

Bestemmelsen regulerer bruk av fødselsnummer og "andre entydige identifikasjonsmidler" under ett. I departementets merknader i ot.prp. nr. 92 (1998-1999) til § 12 eksemplifiseres dette uttrykket med "fingeravtrykk og andre biometriske data", men uttrykket blir ikke videre forklart eller drøftet. Det er imidlertid liten tvil om at "andre biometriske data" må forstås som henvisning til enhver fremgangsmåte som gjør det mulig entydig å identifisere personer ved hjelp av biometri. Bestemmelsen regulerer dermed ikke bare biometri i form av fingeravtrykk, men også iris- og stemmegjenkjenning kan i utgangspunktet være omfattet under forutsetning av at teknikken gir entydig identifisering. Biometri brukes bare som eksempel i forarbeidene, og det er derfor ikke viktig om identifiseringsteknikker kan klassifiseres som biometriske eller ikke så lenge det kan skje sikker identifisering. Bestemmelsen gjelder med andre ord flere til dels meget forskjelligartede teknikker, og særlig er det stor forskjell mellom bruk av fødselsnummer og anvendelse av medfødte/naturlige kroppslige kjennetegn, jf avsnitt 2.4 (ovenfor).

"Saklig behov for sikker identifisering"

Pol § 12 første ledd stiller opp to kumulative vilkår for bruk av entydige identifiseringsmidler. For det første må det være saklig behov for sikker identifisering av personer. Denne behovsvurderingen må bl.a. skje ut i fra lovens formålsbestemmelse, dvs det må kunne begrunnes at det er behov for sikker identifisering for dermed å kunne ivareta grunnleggende personvernhensyn. Et slikt saklig behov kan ofte begrunnes ut i fra mange hensyn (økonomiske, effektivitetsmessige mv.), herunder ut i fra personvernhensyn, jf § 12 annet ledd. Flere av de øvrige bestemmelsene i loven forutsetter jo nettopp at den behandlingsansvarlige er sikker på hvem han forholder seg til, og det er således ikke anledning til å gi innsyn i personopplysninger (pol § 18 annet ledd) eller gi informasjon til registrerte (pol § 20), uten at det foreligger sikker identifikasjon. Utgangspunktet er med andre ord at det ofte er saklig behov for sikker identifisering; spørsmålet er imidlertid *hvor sikker* identifiseringen skal være, og når de sterkeste/entydige identifikasjonsmidlene kan benyttes?

Etter min mening er det derfor nærliggende å forstå behovsvurderingen i § 12 som et spørsmål knyttet til et kontinuum mellom to ytterpunkter som vist i figur 5. Dersom det ikke er mulig å identifisere, er opplysningene anonyme og loven gjelder ikke. Dersom det er stor grad av usikkerhet med hensyn til muligheten for identifikasjon er vi i gråsonen for lovens saklige virkeområde, se § 3 første ledd, jf § 2 nr 1 og 2. Eksistensen av personopplysninger forutsetter med andre ord en forholdsvis stor grad av sikkerhet mht identifisering, og diskusjonen om behovet for sikker identifisering i § 12 er derfor grovt uttrykt knyttet til 3/4 av den høyre del av figuren nedenfor.



Figur 5: Grader av sikker identifisering

Spørsmålet om behov for sikker identifisering må derfor trolig presiseres til et spørsmål om behovet for å unngå muligheten for personforveksling, innenfor området for relativt sikker identifisering. En slik forståelse peker i retning av risikovurdering i samsvar med § 2-4 i personopplysningsforskriften. I så fall vil spørsmålet av hvor sikker identifiseringen bør være avhenge av en vurdering av hvor alvorlige negative følger forveksling av personer vil kunne

medføre for personvernet. Det er i utgangspunktet skadelige følger for personvernet som inngår i behovsvurderingen. Utelukkende økonomisk skade, skade på helse mv som ikke er knyttet til vurdering av personvernet, har neppe betydning; jf pol § 1 som kun angir beskyttelse av den enkelte "mot at personvernet blir krenket gjennom behandling av personopplysninger" som formål. Loven begrunner for eksempel at post som inneholder personopplysninger skal adresseres slik at bare personer som har rett til å se opplysninger i forsendelsen blir mottakere, men begrunner neppe særlig krav til sikker identifisering dersom posten ikke inneholder personopplysninger.[110] Adressering av post med melding av at en person har vunnet i idrettslagets julelotteri, skaper med andre ord intet stort behov for sikker identifisering som er begrunnet ut i fra personvernet. Muligheten for at slik post ikke kommer frem til rett adressat, skaper med andre ord ikke nevneverdig behov for sikker identifisering ut i fra hensynet til personvern.

Selv om behovet for sikker identifisering direkte refererer til behovet ut i fra ivaretakelse av personvern og ikke (bare) andre behov, er det ikke alltid lett å holde fast ved dette skillet. For det første er selve personvernbegrepet vidt, og det kan derfor være vanskelig å skjelne mellom tilfelle som ligger i kjernen og i randsonen av det. Dersom personforvekslingen både medfører feil i behandling av personopplysninger (et problem som er innenfor lovens formål), og innebærer at feil person blir arrestert (et problem som i seg selv er utenfor lovens formål), er det vanskelig å holde fast ved et skille mellom følgene for personopplysningsvern og rettssikkerhet. Uansett kan det være vanskelig å holde på skillet mellom personvernbehov og andre behov, fordi dette kan oppfattes som urimelig. Selv om de personvernmessige følgene er små kan det derfor forsvares å anslå behovet for sikker identifisering som stort dersom feil identifisering kan følge til helseskader eller store økonomiske tap i tillegg til de negative personvernmessige følgene.

Nærmere om betydningen av risikovurdering ved vurdering av behovet for sikker identifisering

Pol § 12 første ledd innebærer som nevnt krav om at det skal gjennomføres en vurdering av hvilke behov det foreligger for sikker identifisering og som kan begrunnes i hensynet til personvern. Det er imidlertid ikke gitt direkte anvisning på hva slags fremgangsmåte som skal eller kan følges for å gjennomføre slike vurderinger. Samtidig er det på det rene at behovsvurderingen er en type risikovurdering, og gjennomføring av risikovurdering er et krav for ivaretakelse av informasjonssikkerhet etter personopplysningsforskriften (pof) § 2-4, jf pol § 13. Loven definerer imidlertid informasjonssikkerhet på en snever (men tradisjonell) måte, og avgrenser dette til å gjelde spørsmål om personopplysningers integritet, konfidensialitet og tilgjengelighet. Spørsmål om sikker identifisering kan neppe henføres inn under et av disse tre kravene, og faller derfor utenfor det loven regner som informasjonssikkerhet. Av den grunn gjelder heller ikke forskriftens kapittel 2 om informasjonssikkerhet, herunder § 2-4 om risikovurdering direkte for identifiseringsspørsmålene.

Selv om informasjonssikkerhetsbestemmelsene ikke kommer direkte til anvendelse på spørsmål om identifisering, er kravene til internkontroll fullt ut relevante. I pol § 14 om internkontroll er krav til opplysningskvalitet spesielt understreket, og i pof § 3-1 er det nærmere spesifisert krav om at den behandlingsansvarlige skal ha "rutiner for […] vurdering av personopplysningenes kvalitet i forhold til det definerte formålet med behandling av opplysningene, jf.

[110] Unntak kan for eksempel gjelde dersom det er en personvernmessig belastning å motta en sending som gjelder en annen, for eksempel dersom Jan Johansen nr 1 mottar en sendingen som skulle vært sendt til Jan Johansen nr 2, og som angir et klientforhold.

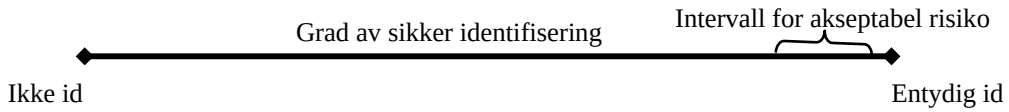
personopplysningsloven §§ 11 bokstav d og e, 27 og 28 […]". Usikker identifisering er eksempel på at opplysninger har utilstrekkelig presisjon, jf pol § 11 bokstav d, og kan således ses som et spørsmål om opplysningskvalitet. Et kvalitetskrav er at personopplysninger skal være tilstrekkelige i forhold til formålet med behandling av opplysninger, dvs ha en tilstrekkelig kvalitet til at det ikke oppstår personvernskade. Et slikt resonnement vedrørende opplysningskvalitet fører med andre ord til samme resultat som resonnementene vedrørende "saklig behov for sikker identifisering", jf forrige avsnitt. Med internkontroll og opplysningskvalitet som utgangspunkt, følger det imidlertid klarere krav til hvorledes den behandlingsansvarlige må jobbe i forhold til pol § 12 for å sikre riktig etterlevelse.

Det heter i pol § 14 om internkontroll at

> "Den behandlingsansvarlige skal 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."

Bestemmelsen innebærer at spørsmålet om behov for entydig identifisering skal være gjenstand for planlagte og systematiske tiltak, når dette er nødvendig for å følge kravene i eller i medhold av loven. Dersom det ikke er åpenbart hvilke krav til identifisering som kreves, må den behandlingsansvarlige med andre ord gjøre systematiske forhåndsvurderinger av spørsmålet. Det følger ikke direkte av lovteksten hva slags systematisk tilnærming som bør velges, men det er nærliggende å gjøre bruk av en type risikovurdering. Forskriften gir som nevnt anvisning på gjennomføring av risikovurdering i spørsmål om informasjonssikkerhet. Selv om denne ikke gjelder direkte for sikring av opplysningskvalitet mv, kan den gi viktige holdepunkter. Særlig kravet til å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd er aktuelt, noe som i sammenheng med pol § 12 innebærer klarlegging av sannsynligheten for og konsekvenser av sviktende identifisering og/eller verifikasjon av identitet.

Risikovurderingen innebærer bl.a. å fastslå differansen mellom beregnet risiko og akseptabel risiko. Er beregnet risiko høyere enn akseptabel risiko må det settes inn tiltak for å redusere risikoen til akseptabelt nivå. Det vil etter dette være mulig å oversette "behov for sikker identifisering" til et bestemt intervall av "akseptabel risiko", for eksempel satt til 5% eller lavere. Dersom den beregnede risikoen (uten fødselsnummer mv) er høyere enn 5%, må det settes inn tiltak. Fødselsnummer og biometri mv kan da være aktuelt dersom slike fremgangsmåter kan anses som *nødvendige*, jf nedenfor.



Figur 6: Grader av sikker identifisering

Problemet med en slik tilnærming er at "akseptabel risiko" er sterkt skjønnsmessig, noe som kan gjøre det enkelt for behandlingsansvarlige å hevde at det første vilkåret i pol § 12 er oppfylt. Det kan riktignok tenkes krav til begrunnelse for det anslåtte nivået for akseptabel risiko, men slike krav vil i flere sammenhenger trolig oppleves som for vanskelige og byråkratiske til at de lar seg forsvare.

"Nødvendig for å oppnå slik identifisering"

Selv om det foreligger et saklig behov for sikker identifisering, er det ikke uten videre adgang til å benytte fødselsnummer og andre entydige identifikasjonsmidler. I forarbeidene uttales det at "[s]like identifikasjonsmidler bør ikke benyttes i utrengsmål."[111] Slike identifikasjonsmidler må derfor i tillegg være *nødvendige* for å oppnå identifiseringen. Utgangspunktet er med andre ord et visst intervall for akseptabel risiko for feil identifisering, sammenholdt med en anslått/beregnet risiko for samme. Dersom den anslåtte risikoen er større enn den akseptable risikoen, oppstår spørsmålet om bruk av fødselsnummer eller andre entydige identifikasjonsmidler er nødvendige for å sikre et akseptabelt sikkerhetsnivå.

Den nevnte vurderingen av nødvendighet inviterer til en bred vurdering av mulige virkemidler, ut over fødselsnummer mv. Det betyr at effekten av mulige tekniske, fysiske, organisatoriske, pedagogiske virkemidler mv må vurderes. Dersom slike andre virkemidler bringer risiko for identitetsforveksling mv ned til et akseptabelt nivå, er fødselsnummer mv ikke nødvendige å bruke, og kravet i § 12 er ikke tilfredsstilt. Bruk av kundenummer, navn og adresse vil for eksempel ofte utgjøre tilstrekkelig identifisering dersom dette kombineres med ett eller flere andre tiltak. Så lenge det kun er tale om informasjonsbehandling innen en virksomhet med samme kundenummer, vil det ikke være små muligheter for at det kan skje feil identifisering dersom en kombinerer med personnavn mv. En annen situasjon oppstår dersom opplysninger skal innhentes fra en organisasjon som ikke benytter kundenummeret, og der en derfor primært har navn og adresse å holde seg til. I en slik situasjon oppstår det en noe høyere risiko for personforveksling. Også slik forhøyet risiko kan imidlertid unngås gjennom andre tiltak enn fødselsnummer mv. Slike krav gir imidlertid ofte resultater som åpenbart vil bli oppfattet som urimelig tungvinte og kostbare. Når spørsmålet om risiko skal vurderes, er det derfor grunn til også å ta hensyn til hvilke kostnader mv som følger av alternative tiltak for å redusere risiko for gal identifisering. Identifisering ved hjelp av fødselsnummer og andre entydige identifikasjonsmidler må derfor muligens anses som nødvendig selv om det kunne vært valgt andre sikre fremgangsmåter, hvis disse alternative fremgangsmåtene er uforholdsmessig dyre, tidkrevende mv.

Forutsetningen for å kunne benytte entydige identifikasjonsmidler er da at disse er nødvendige for å oppnå et akseptabelt risikonivå, dvs en akseptabel risiko for personforveksling mv. Hva som kan anses som en akseptabel risiko er i utgangspunktet avhengig av en vurdering av personvernmessige konsekvenser. I forarbeidene uttales det imidlertid at også samfunnets behov kan tillegges vekt. Dersom (nesten) enhver risiko for slik forveksling er uakseptabel (ut i fra en personvernmessig, eventuelt samfunnsmessig vurdering), vil det være nødvendig å benytte entydige identifikasjonsmidler, og slik bruk vil også være tillatt - og kanskje også *påbudt*, jf neste avsnitt.

Pålegg fra Datatilsynet om bruk av entydige identifikasjonsmidler

Datatilsynets kompetanse til å gi pålegg om bruk av fødselsnummer og andre entydige identifikasjonsmidler er i § 12 annet ledd knyttet spesielt til spørsmålet om å sikre at personopplysningene har tilstrekkelig kvalitet. Hva som menes med kvalitet kan være noe uklart. Begrepet er også anvendt i pol § 14 første ledd, men heller ikke her er kvalitet nærmere forklart. Kvalitet må imidlertid trolig forstås som slike aspekter ved de grunnkravene til behandling av personopplysninger der bruk av fødselsnummer mv kan være til hjelp. Således må pålegg om bruk av fødselsnummer trolig kunne være begrunnet i hensynet til å unngå eller fjerne uriktige opplysninger og til å oppdatere opplysninger som ellers ville ha vært foreldet, jf §

[111] Se ot.prp. nr. 92 (1998-1999), merknadene til § 12.

11 bokstav e. Pålegg om bruk av fødselsnummer kan imidlertid også tenkes å være begrunnet i å sikre at personopplysninger er så fullstendige som formålet krever, se § 11 bokstav d.

Jeg har ikke undersøkt Datatilsynets praksis på området, og kjenner ikke til om bestemmelsen i pol § 12 tredje ledd er i særlig bruk.

4 Retts- og forvaltningspraksis vedrørende fødselsnummer og biometri

4.1 Oversikt

I det følgende gjør jeg kort rede for undersøkelser av norsk forvaltnings- og rettspraksis i sivile saker på området biometri og fødselsnummer. I forhold til rettspraksis har jeg gjort generelle søk som ikke har vært spesielt knyttet til personopplysningsloven. Forvaltningspraksis har kun omfattet Personvernnemndas publiserte avgjørelser. Dette er primært avgjørelser etter personopplysningsloven og -forskrift, selv om nemnda også har kompetanse innen enkelte andre lover.[112]

4.2 Rettspraksis

Jeg har ikke funnet norsk rettspraksis i sivile saker som kan sies å være relevant for problemstillinger om biometri i denne utredningen. En rekke rettsavgjørelser har riktignok spørsmålet om riktig identitet som viktige elementer i grunnlaget for avgjørelsene. Særlig gjelder dette i saker om utvisning mv etter utlendingsloven der fingeravtrykk ikke sjelden danner grunnlag for rettens konklusjon vedrørende de angjeldende utlendingers identitet. Jeg har imidlertid ikke funnet saker der retten tar stilling til adgangen til å benytte fingeravtrykk for identifisering og/eller autentisering og/eller drøfter hvor sikker identifisering ved hjelp av fingeravtrykk kan anses å være. Avgjørelser med slikt innhold kan med sannsynlighet finnes i straffesaker, men slike saker er ikke undersøkt. For uten utlendingssaker, har jeg funnet sivile saker fra spredte felt der fingeravtrykk har spilt en viss rolle uten å være hovedsak (farskap, forsikring, utlegg mv). Sakene gjaldt bruk av fingeravtrykk med tradisjonelle teknikker. Jeg har heller ikke funnet rettspraksis i sivile saker som vedrører fødselsnummer på måter som er relevante for denne utredningen.[113]

Rettspraksis i straffesaker har ikke blitt gjennomgått som ledd i denne utredningen. Det er likevel grunn til å fremheve at avgjørelsen i Rt 1996 s. 1114 har klar relevans for personvernmessige vurderinger knyttet til biometri. Saken gjaldt krav om å legge frem resultater fra løgndetektortest ("polygraf") som bevis i en straffesak. Førstvoterende fremholdt at bevis, helt unntaksvis, kunne nektes ført på ulovfestet grunnlag, selv om det var lovlig ervervet og ønsket ført av siktede. Tungtveiende personvern- og rettssikkerhetshensyn kunne tenkes å begrunne slik nektelse (s. 1119). Førstvoterende la særlig vekt på det sterke press på siktede personer som ville oppstå dersom en åpnet for bruk av løgndetektor, og at det også ville kunne oppstå tilsvarende press i sivile saker der spørsmål om partenes troverdighet står sentralt (s. 1121).

Høyesterett brukte ikke som begrunnelse den tilsidesettelse av evnen til fri selvbestemmelse som bruk av løgndetektorer kan sies å innebære når en måler kroppslige reaksjoner og slik går utenom personens vilje.[114] I stedet ble det lagt vekt på en forventet spredningseffekt som kunne

[112] Se helsregisterloven § 32 tredje ledd og lov om Schengen informasjonssystem § 23 annet ledd.
[113] En sak vedrørende endring av fødselsnummer er av en viss interesse. I sak LB 1997-3246 (RG-1999-671) avsa Borgarting lagmannsrett dom i sak vedrørende endring av registrert fødselsår i Folkeregisteret, jf folkeregistreringsloven § 4. Fødselsår var allerede endret en gang, og saken gjaldt ny endring på grunnlag av annen dokumentasjon enn original og verifisert fødselsattest. Fremlagt skolebevis, id-kort og erklæring fra foreldrene ble ikke ansett troverdig, og kravet om endret fødselsår vant ikke frem.
[114] Men dommen viser at slike resonnementer også kan tenkes å være relevante (s. 1119).

frata andre siktede og parter i sivile saker en reell selvbestemmelsesrett og frihet til å nekte bruk av løgndetektor. Retten peker her på et generelt problem: Selv om personer har formell rett til å nekte samtykke til bruk av for eksempel biometri, vil det kunne oppstå sosialt press mot, og til og med mistenkeliggjøring av personer som benytter retten til å si nei. Dersom det skal være akseptabelt å basere bruk av slik teknologi på samtykke, kan det derfor være grunn til å introdusere tiltak som gjør at retten til å nekte samtykke oppleves som reell. Forslaget til § 12 i avsnitt 7.3.2 (nedenfor) er motivert ut i fra slike betraktninger, se bestemmelsens siste ledd.

4.3 Personvernnemndas avgjørelser vedrørende pol § 12

4.3.1 Generelt

I det følgende vil jeg kortfattet gjennomgå alle avgjorte og publiserte saker vedrørende pol § 12 som har vært behandlet av Personvernnemnda frem til og med 5 oktober 2008. Sakene gjelder enten fødselsnummer eller biometri, og jeg har derfor disponert presentasjonen av sakene i tråd med dette skillet selv om begge typer saker er vurdert etter samme bestemmelse. I avsnitt 4.3.4 gir jeg imidlertid noen samlede vurderinger. I enkelte saker trekker Personvernnemnda frem dansk og svensk praksis, noe som også vil komme til uttrykk i min gjennomgang. Det synes imidlertid ikke som om nemnda har gjort systematiske gjennomganger av disse landenes praksis, og jeg har ikke foretatt supplerende undersøkelser. Dette bildet blir derfor ufullstendig.

4.3.2 Klagesaker vedrørende fødselsnummer

Klagesak 2002/7 Norskespill.no AS
Saken gjaldt klage fra Norskespill.no AS på Datatilsynets vedtak om opphør av bruk av fødselsnummer. Klager benyttet fødselsnummer for å forsikre seg om at spillere var over 18 år. Det skjedde kun kontroll av fødselsår og av at det forelå et gyldig fødselsnummer. Bakgrunnen var krav fra Lotteritilsynet om at spillere bl.a. måtte kunne identifiseres, være over 18 år, ha registrert fast bosted i Norge og ha etablert bankforbindelse. Personvernnemnda kom til at bruk av fødselsnummer ikke gav noen sikkerhet mot at yngre personer deltok i spill, og at det uansett fantes andre metoder for sikker identifisering. Nemnda vektla særlig at konsekvensene av en personforveksling var små, og at samfunnsmessige hensyn ikke tilsa bruk av fødselsnummer. Datatilsynets vedtak ble opprettholdt.

Klagesak 2003/06, vedr. Norsk Rikstoto AS
Saken lignet klagesak 2002/7, og gjaldt pengespill over nettstedet www.rikstoto.no. Spillere måtte oppgi navn, adresse, e-post adresse, telefon, bankkontonummer og fødselsnummer. Spillerne måtte videre være over 18 år, norske statsborgere bosatt i Norge og ha konto i norsk bank. Norsk Rikstoto kontrollerte at fødselsnumrene var gyldige og at spilleren var over 18 år. Ved registrering må spillerne legge inn et spørsmål med svar til bruk for autentisering ved eventuelle senere endringer av opplysninger om spilleren. Nemnda viste i sin avgjørelse til at Norsk Rikstotos bruk av fødselsnummer ikke gav sikker identifikasjon, og at andre fremgangsmåter var like sikre. For øvrig ble det vist til vedtaket i klagesak 2002/7.

Klagesak 2004-08, Finansnæringens Hovedorganisasjon (FNH)
Saken gjaldt flere forhold vedrørende forsikringsselskapenes konsesjon etter personopplysningsloven. Et av spørsmålene gjaldt forsikringsselskapene adgang til å benytte fødselsnummer for å foreta kredittvurdering av kunden som ledd i en risikovurdering.[115]

[115] Konsesjonen tillot bruk av fødselsnummer i enkelte andre tilfelle.

Nemnda la vekt på å diskutere om det forelå saklig grunn til å innhente kredittopplysninger, jf pol § 11 første ledd litra b. Under forutsetning av at dette vilkåret var oppfylt, uttalte nemnda at forsikringsselskapene kunne benytte fødselsnummer for å gjennomføre selve kredittvurderingen. Begrunnelsen synes å være at selskapene var avhengige av å få oppgitt et fødselsnummer for å kunne innhente kredittopplysninger, dvs at kredittopplysningsselskapene krevet slik informasjon. I klagesaken ble denne ordningen imidlertid ikke nærmere redegjort for eller diskutert.

***

De refererte sakene gir ikke vesentlig avklaring av reglene for anvendelse av fødselsnummer. I disse sakene, som i de sakene som er referert nedenfor om fingeravtrykk, er det spørsmålet om den entydig identifiseringsmetoden er nødvendig eller ikke som er avgjørende. Personvern-nemnda legger også tydelig vekt på skillet mellom identifisering og autentisering. Personopplysningsloven § 12 regulerer direkte bare identifisering, men i de to først nevnte sakene gjør nemnda også enkle vurderinger av autentiseringseffekten av fødselsnummer, og kommer til at slike numre ikke har tilstrekkelig slik virkning.

4.3.3 Klagesaker vedrørende bruk av fingeravtrykk

Klagesak 2006-07 Tysvær kommune
Saken gjaldt fingeravtrykk ved pålogging av datasystem på alle bærbare og enkelte stasjonære datamaskiner i Tysvær kommune, for å sikre autorisert tilgang til sensitive opplysninger i kommunens datasystem. Fingeravtrykk for personer som var aktuelle som brukere var registrert på forhånd i form av et biologisk mønster der inntil 75 punkter i avtrykket inngikk. Når en fingeravtrykkskanner på maskinen fant samsvar mellom skannet avtrykk og lagret mønster, autentiserte den brukeren og tildelte den 4 - 5 passord. Passordene gav brukeren tilgang til maskinen med rettigheter til lesing av informasjon mv.

Personvernnemda traff sin avgjørelse i saken ut i fra gjennomgang av relevante avgjørelser i Sverige og Danmark.[116] Disse landene har ikke bestemmelse tilsvarende pol § 12, og sakene var derfor avgjort på grunnlag av interesseavveininger innenfor rammene av bestemmelser tilsvarende pol § 11 (formål mv), jf § 8 (rettslig grunnlag). To saker gjaldt innlogging med fingeravtrykk på PCer på skoler, en sak gjaldt bruk av fingeravtrykk for å kontrollere at elever hadde betalt matavgift i skolens kantine, og den siste saken gjaldt fingeravtrykk som integrert del av kundekort for kjøp av fergebilletter. I de to først nevnte sakene kom den svenske Datainspektionen til at det forelå brudd på personuppgiftsloven, men at forholdet kunne bringes i orden dersom tilstrekkelig informasjon og samtykke ble innhentet fra barnas foreldre. I de to andre sakene ble hensynet som begrunnet bruk av fingeravtrykk funnet mer tungtveiende enn personvernhensynene. Sakene ble ikke direkte trukket inn i Personvernnemndas argumentasjon i saken vedrørende Tysvær kommune, men inngikk som bakgrunnsinformasjon i sakens anledning.

Personvernnemnda konkluderte med at § 12 kom til anvendelse på fingeravtrykk. Samtidig uttalte nemnda at i motsatt fall ville lovens øvrige bestemmelser komme til anvendelse, og saken

[116] Dette gjaldt Datainspektionen vedtak i sak 555-2004 (Kvarnbyskolan), sak 2105-2003 (Spånga - Tensta skoler), samt Kammarrätten i Stockholms dom av 1.11.2005 (sak nr 1982-05) vedrørende Gymnasieskolan i Uddevalla. I tillegg ble det danske datatilsynets uttalelse av 4. mars 2003 vedrørende BornholmsTrafikken kundekort med fingeravtrykk for betaling av fergebilletter.

måtte i tilfellet bli avgjort på lignende måte som i de svenske og danske sakene. Drøftelsen som ledet ut i konklusjonen om at § 12 omfatter fingeravtrykk, inneholder flere synspunkter vedrørende forståelsen av "entydige identifikasjonsmidler" generelt, og spesielt vedrørende fingeravtrykk. For å være "entydig" la nemnda til grunn at identifikasjonsmiddelet må være egnet til bruk som identifikasjon i flere systemer. Fødselsnummer og fingeravtrykk vil således være et entydig identifikasjonsmiddel, fordi de er egnet som nøkkel til å gjenfinne informasjon i flere ulike systemer. For øvrig understreket nemnda at det er viktige ulikheter mellom fødselsnummer og fingeravtrykk, for eksempel ved at fødselsnummer ikke kan benyttes til autentisering (verifisering av identitet). Generelt stilte nemnda seg kritisk til ønskeligheten av å regulere fødselsnummer og fingeravtrykk felles. De pekte på at anvendelse av pol § 12 på fingeravtrykk kun har grunnlag i én enkelt setning i forarbeidene uten at konsekvensene var utredet. Personvernnemnda fremholder videre at:

> "Biometriske metoder til bruk for identifikasjon eller autentisering har vært i sterk utvikling siden loven ble vedtatt. Nemnda har merket seg at Datatilsynet har fremmet forslag om særlig regulering av biometriske metoder, og stiller seg sterkt positiv til at dette blir gjort, og blir gitt prioritet i revisjonsarbeidet."

Denne uvanlig klare rettspolitiske uttalelsen, sammen med Datatilsynets forslag om særlig regulering av biometriske metoder, er bl.a. grunnlag for denne utredningen. Saken vedrørende Tysvær kommune danner imidlertid også grunnlag for etablering av en praksis som har bidratt til å klargjøre anvendelse av pol § 12 i forhold til fingeravtrykk, jf nedenfor.

I det konkrete tilfellet vedrørende Tysvær kommune, drøftet Personvernnemnda andre, alternative rutiner for tilgangskontroll, men kom til at pålogging med brukernavn og passord i praksis ikke gav tilfredsstillende sikkerhet. De anså det dessuten for usikkert om pålogging med smartkort ville være akseptabelt. Konklusjonen ble etter dette at fingeravtrykk måtte ses som nødvendig, og derfor representerte lovlig bruk av entydig identifikasjonsmiddel.

Klagesak 2006-08 Oxigeno Fitness
Treningssenteret Oxigeno Fitness gjorde bruk av adgangskontrollsystemet IdentX basert på fingeravtrykk. Systemet lager og lagrer et biologisk mønster basert på 50 punkter i hvert fingeravtrykk, og mønsteret lagres i en lokal database. Når personer skulle autentiseres ble det gjort søk etter et mønster i databasen som stemte overens med det fingeravtrykk som ble avlest i adgangskontrollen. Ved samsvar gav databasen informasjon om ”kunde-id”, dvs navn og andre personalia på personen som var gjenstand for adgangskontroll. Fingeravtrykkene fra hver passering ble ikke lagret, og sensoren som ble brukt til å lese mønstrene som ledd i adgangskontrollen hadde intet minne. Skulle sensoren komme på avveie, forelå det derfor ingen fare for uautorisert spredning av mønstrene. Når et medlemsskap i treningssenteret opphørte, ble mønstrene og kunde-id slettet fra databasen.

Personvernnemnda kom etter en konkret vurdering til at det i dette tilfellet ikke var nødvendig med fingeravtrykk for å oppnå sikker identifisering. Nemnda fremholdt at enkelte personer opplevde bruk av fingeravtrykk som et integritetsinngrep, bl.a. fordi slike avtrykk tradisjonelt sett er blitt brukt av politiet i forbindelse oppklaring av straffbare forhold. Det at politiet benytter fingeravtrykk i alvorlige kriminalsaker kan gi en opplevelse av mistenkeliggjøring dersom man må avgi slike avtrykk i dagligdagse situasjoner. Fingeravtrykk legges dessuten igjen som spor i det daglige liv, og nemnda fremholdt at det kan være fare for at dataene kan brukes til andre formål enn de opprinnelig ble samlet inn for.

Klagesak 2006-09 Oslo trimsenter
Saken lignet meget på klagesaken vedrørende Oxigeno Fitness. Personvernnemndas klarlegging av den aktuelle teknologien, rettslige resonnementer og den konkrete vurdering av om fingeravtrykklesing var nødvendig tilsvarte langt på vei nevnte sak. Oslo trimsenter ble således nektet å bruke fingeravtrykkavlesning som ledd i adgangskontrollen. I nemndas avgjørelse ble det imidlertid gjort rede for ytterligere en dansk sak[117]. Også i denne avgjørelsen fra det danske Datatilsynet,[118] var det tale om adgangskontroll til et mosjonssenter ved hjelp av fingeravtrykkskanner. Her ble mosjonssenteret nektet å bruke fingeravtrykk, bl.a. med den begrunnelse at opplysningene ble lagret utenfor de registrertes kontroll, og ikke i et kundekort som i en annen sak vedrørende Bornholmerkortet.[119] Personvernnemnda knyttet imidlertid ingen kommentar til denne argumentasjonen, men det at den eksplisitt nevnes, kan trolig ses som et uttrykk for at nemnda har ansett spørsmålet om kontroll med lagringsmediet å være relevant.

Klagesak 2006-10 Esso Norge AS
Saken gjaldt bruk av fingeravtrykk som del av adgangskontrollen ved fire forskjellige tankanlegg for petroliumsprodukter. Innrullering og bruk av fingeravtrykk skulle skje på grunnlag av ansattes skriftlige samtykke. Ansatte kunne alternativt benytte pinkode i kombinasjon med kort, og bl.a. av den grunn ble samtykkene ansett som frivillige og gyldige, jf pol § 8 første ledd og § 2 nr 7.

Kort med magnetstripe eller mikroprosessor ble brukt for å fastslå hvem som skulle autentiseres ved hjelp av fingeravtrykk. Bruken av kortet styrte med andre ord bruk av fingeravtrykk som var registrert og lagret på forhånd. Det lagrede fingeravtrykkmønsteret ble sammenlignet med det fingeravtrykket som ble skannet ved passering inn til tankanleggene. Identifisering av personene og verifikasjon av identitetene ble med andre ord gjennomført i to operasjoner, men Personvernnemnda valgte å se det samlede tekniske opplegget som en helhet.

Den valgfrihet Esso Norge AS gav sine ansatte, og som var forutsetning for gyldig samtykke (jf krav til frivillighet), kunne etter flertallet av medlemmene i Personvernnemndas syn ikke utelukke at bruken av fingeravtrykk kunne anses å være "nødvendig" slik pol § 12 krever. Den motsatte konklusjonen ville medføre at samtykke ikke kunne være mulig rettslig grunnlag for bruk av entydige identifikasjonsmidler, noe flertallet mente var i dårlig samsvar med formålet med loven, jf § 1. Nemnda gjorde derfor en helhetsvurdering av ordningene med fingeravtrykk og kort med pinkode mv, og kom til at denne ordningen *samlet sett* kunne anses nødvendig for å oppnå sikker identifisering. Klagen ble derfor tatt til følge, og bruk av den etablerte ordningen med fingeravtrykk akseptert.[120]

Klagesak 2006-11 REMA 1000
Saken gjaldt systemet KRONOS 4500 der det skulle genereres en biologisk mønster fra fingeravtrykk. Mønsteret skulle lagres lokalt i en terminal. Ansatte skulle registrere seg i terminalen ved å taste inn sitt ansattnummer eller id-nummer. Deretter blir vedkommende bedt om å legge en finger på leseplaten/sensoren for å verifisere at det er tastet riktig nummer, dvs det nummer som i terminalen er knyttet til fingeravtrykkmalen. Metoden var valgt for å sikre at ansatte registrerer timene sine korrekt og ikke bruker hverandres stemplingskort og koder.

[117] I tillegg til de som ble nevnt i avgjørelsen vedrørende Tysvær kommune, klagesak 07.2006 (jf ovenfor).
[118] Avgjørelse av 26.11.2004 i sak 2004-219-0208.
[119] Saken er referert ovenfor under saken vedrørende Tysvær kommune.
[120] Nemnda kom til at § 12 ikke hjemlet vedtak om vakthold og andre fysiske sikringstiltak mv som eventuelt kunne overflødiggjøre bruk av fingeravtrykk.

Personvernnemnda mente det forelå saklig grunn til sikker identifisering. Imidlertid var nemnda av den oppfatning at timeregistrering ved hjelp av fingeravtrykk innebar en unødvendig mistenkeliggjøring av de ansatte, og derfor ville bidra til å svekke, heller enn å styrke, tillitsforholdet mellom ansatt og arbeidsgiver. I avgjørelsen er det imidlertid ikke klarlagt på hvilken måte spørsmålet om mistenkeliggjøring og svekket tillitsforhold er relevant ved fortolkningen av pol § 12. Nemnda la uansett til grunn at det forelå adekvate alternativer som var sikre nok for butikkjedens formål og behov, og tok således ikke klagen fra REMA 1000 til følge.

4.3.4 Samlet bilde av Personvernnemndas praksis

Gjennomgangen viser at det er flest saker vedrørende fingeravtrykk og at spørsmål om fødselsnummer sjelden har vært oppe til avgjørelse i Personvernnemnda. Det er mulig denne fordelingen mellom sakstypene viser noe om hvor omstridt fødselsnummer og fingeravtrykk er. Allmenn bruk av fingeravtrykkteknologi er noe nytt, mens fødselsnummer har vært brukt i 45 år, noe som innebærer en viss grad av tilvenning. Forholdsvis stor grad av tilvenning og aksept av fødselsnummer generelt, betyr imidlertid ikke at rådende praksis på området er uproblematisk, se avsnitt 2.5.3 (ovenfor).

Sakene med fødselsnummer sammenlignet med sakene vedrørende fingeravtrykk, viser klart forskjellen på de to fremgangsmåtene. Bruk av fødselsnummer gjelder kun spørsmålet om identifisering, samtidig som det brukes i en sammenheng som synes å forutsette en autentiseringseffekt (men uten at dette er direkte behandlet). Fingeravtrykk gjelder primært autentisering.

Kravet til saklig behov for sikker identifisering byr ikke på tvil i noen av sakene, og alle saker er derfor avgjort ut i fra nødvendighetskriteriet i pol § 12. Jeg kan ikke se at Personvernnemnda har lagt klare generelle retningslinjer for hvorledes spørsmålet om nødvendighet skal vurderes. Nødvendighetsvurderingen må derfor fremdeles - generelt sett - sies å være svært åpen og skjønnsmessig, og utenfor de sakstyper som er behandlet, kan det ikke sies å være stor forutberegnelighet. Likevel er flere av de avgjorte sakene svært like hverandre, og innen sakstypen er det lett å identifisere en konsekvent praksis.

5 Personvernmessige konsekvenser av biometriske løsninger

5.1 Innledning

I dette og det følgende kapittelet skal jeg generelt diskutere hvorledes bruk av biometri og fødselsnummer kan sies å krenke personvernet. Selv om det er flere felles trekk ved vurderingen av biometri og fødselsnummer, er det etter min mening likevel så mange forskjeller at jeg har valgt separate gjennomganger.

Det er en utfordring å skjelne mellom de spørsmål som direkte gjelder fødselsnummer og biometri, og de videre, tilknyttede personvernspørsmålene. Det er for eksempel ikke nødvendigvis bruk av biometri i seg selv som skaper personvernproblemer, men indirekte følger, mulige smitteeffekter osv. Jeg har valgt å konsentrere meg om direkte/nærliggende følger, samtidig som jeg på utvalgte punkter også prøver å illustrere mer indirekte konsekvenser.

Et vesentlig moment i vurderingen av fødselsnummer og biometri gjelder skillet mellom enkeltstående tilfelle, og en praksis som summerer seg opp til en omfattende aggregert og intensiv bruk. Dette aspektet gjør at jeg har funnet det riktig å gjøre noen forutsetninger vedrørende sannsynlige trekk ved den relevante teknologiske og samfunnsmessige utviklingen, se neste avsnitt.

Når jeg nedenfor gjennomgår mulige personvernmessige konsekvenser av biometriske id-systemer, er det viktig å understreke at ikke alle momenter nødvendigvis er relevante for all anvendelse. Hvilken vekt personvernvurderingene bør tillegges, er uansett et åpent spørsmål, både generelt og konkret vurdert.

Ved analyse av personvernspørsmål kan en velge å gjøre bruk av ulike systematikker som er utviklet for å beskrive de interesser, verdier mv som kan sies å være involvert. Personvernprinsippene innen europeisk personvernrett og fremstillinger av personverninteresser og -krav er to sentrale eksempler på slik tilgjengelig systematikk. Når jeg i fortsettelsen ikke har valgt å legge slike ordnede systemer til grunn for min drøftelse, er det dels fordi slike gjennomganger vil bli svært omfattende, og dels fordi jeg er i tvil om hvor fruktbart og treffsikkert en slik tilnærming vil være. De følgende gjennomgangene er derfor skrevet på et friere grunnlag.

5.2 Anslag vedrørende fremtidig bruk av biometrisk id-teknologi

Når jeg skal anslå noe om biometrisk id-teknologi i fremtiden, er det åpenbart for alle at slike prediksjoner er grunnleggende usikre. Samtidig har samfunnet etter hvert ganske mye erfaring med utvikling og bruk av informasjons- og kommunikasjonsteknologi de siste 50 årene som det kan være mulig å resonnere ut i fra. Særlig tror jeg utvikling og bruk av PC, Internett og mobiltelefoni kan være relevant å se hen til når mulig videre utvikling på området biometri skal vurderes.

Det første spørsmålet med usikkert svar er om bioteknologi for identifiserings- og autentiseringsformål vil komme til et markert teknologisk gjennombrudd eller ikke. Jeg mener det faktum at denne teknologien er tilgjengelig på et vanlig forbrukermarked i dag, indikerer at slike teknologiske løsninger kan øke i antall og utbredelse. Nyhetssakene som kort er vist til i avsnitt 2.4.5 og klagesakene for Personvernnemda i avsnitt 4.3.3 viser dessuten at biometri er

anvendt innen vidt ulike bransjer og har en rekke - til dels fantasifulle - anvendelser. I tillegg og viktigere, er at vi lever i en tid med meget stor vekt på sikkerhet, herunder informasjons-sikkerhet. Jeg vil ikke her ta opp spørsmålet om denne vektleggingen er vel begrunnet. Uansett skaper gjennomførte terrorhandlinger og faren for nye, samt internasjonal organisert kriminalitet usikkerhet og frykt. Innen Den europeiske unionen skaper også nedbygging av landegrensene med fri bevegelse av mennesker ekstra utfordringer for kriminalitetsbekjempelse og sosial kontroll. Samlet sett gir trolig trekk ved denne samfunnsutviklingen grobunn for teknologier som kan sies å øke sikkerheten.

Fortsatt stor vekt på sikkerhet kan legge forholdene til rette for at nye sikkerhetsteknologier får et stort marked og dermed et teknologisk og kommersielt gjennombrudd. Biometrisk id-teknologi er blant disse sikkerhetsteknologiene. Slike teknologiers hjelp til å vite hvem vi forholder oss til er ikke minst viktig i et åpent samfunn med svært mobile mennesker. Jeg mener med andre ord det er grunn til å anta at biometrisk teknologi som anvendes for identifiseringsformål vil komme til å bli langt vanligere enn i dag, og kanskje også allestedsnærværende slik PCer og mobiler mv har utviklet seg til å bli. Når en eventuelt gjennomfører en rettslig regulering av biometriske systemer for identifiseringsformål mv, bør en ha gjort seg opp en mening om det som reguleres vil være et marginalt eller et sentralt teknologisk element i fremtidens samfunn.

Det ligger i min forutsetning om mulighet for betydelig større spredning enn i dag, at biometrisk id-teknologi vil kunne bli fremstilt industrielt og med stadig lavere priser. Det åpner opp for at teknologien også vil være del av den forbrukerteknologi som vil bli tilbudt. Biometrisk pålogging på PC og fingeravtrykkleser i dørhåndtak, er eksempler på dette. Biometrisk id-teknologi handler derfor neppe bare om offentlige myndigheter, kommersielle aktører og andre mektige organisasjoners bruk, men også om bruk i samkvemmet mellom vanlige borgere.

Den neste antagelsen jeg vil gjøre, er at biometrisk id-teknologi i stadig større grad vil bli *integrert* i annet utstyr. Dette kan for eksempel være en effekt av at teknologien blir mindre i størrelse samtidig som den blir mer robust i bruk. Dessuten kan det hevdes å være mest "brukervennlig" å unngå teknologi som innebærer særskilt og eksplisitt bruk. I tillegg vil integrasjon i andre gjenstander kunne gi mer effektiv bruk. I den grad biometrisk id-teknologi blir liten og godt integrert i andre gjenstander, vil det kunne innebære en trivialisert bruk, dvs hyppig bruk som oppleves som vanlig og selvfølgelig.

På bakgrunn av de foregående antagelsene, mener jeg det er grunn til å tro at biometrisk id-teknologi i hvert fall vil bli aktuell på mange områder der det i dag er en rettslig regulering av krav til identifisering mv, jf den anslagsvise oversikten i avsnitt 3.2. Jeg tolker det faktum at id-bruken i dag er rettslig regulert som en indikasjon på at den er viktig nok til at en vil ønske å investere i nyere teknologi. Dersom teknologien blir billig og integrert, kan en tenke seg en helt allmenn utbredelse, for eksempel i hjem, på arbeidsplasser, ulike serviceinstitusjoner, i biler osv. Jeg tror trykket vil komme til å bli stort, og mener derfor det er behov for å skille vesentlige fra mindre vesentlige anvendelser. Et kjernespørsmål er etter min mening hvem som kontrollerer teknologien og hvilken relasjon det er mellom vedkommende og de som registreres i systemene. Jeg antar det kan være grunn til å legge vekt på noen klassiske konfliktrelasjoner i samfunnslivet; nemlig offentlige myndighet - borgere, næringsdrivende - forbrukere, og arbeidsgivere - arbeidstakere.[121] Det er primært slike relasjoner jeg har som utgangspunkt i den følgende diskusjonen av personvernmessige konsekvenser.

[121] Også andre relasjoner der det kan hevdes å være et misforhold mellom partenes innflytelse kan være aktuelt å prioritere, for eksempel i forholdet mellom fanger og fengselsmyndigheter og mellom skolemyndigheter og elever.

5.3 Kontroll med eget liv og selvbilde

5.3.1 Innledning

Personvern kan helt grunnleggende sett sies å gjelde ivaretakelse av enkeltindividers autonomi og integritet. Populært sagt kan vi kanskje uttrykke dette som å være "sjef i eget liv". Både faktisk og opplevet autonomi og integritet kan sies å være viktig. Dersom bruk av fingeravtrykk feilaktig oppleves som sterkt integritetskrenkende fordi teknologien og bruken av et slikt id-system er dårlig forklart, kan også dette sies å være et problem for personvernet.

Et sikkert utgangspunktet for diskusjonen om identifisering og autentisering, er at den sosiale praksisen på området er varierende. Vi opptrer forholdsvis ofte på måter som kan etterlate tvil om personers identitet. I noen sammenhenger er kunnskaper om identiteter lite vesentlig eller det er vesentlig å være anonym; for eksempel i vanlig sosial omgang med andre i det offentlige rom. Nettopp den følelse av anonymitet som kan fremkalles av å ferdes i folkemyldret uten å bli gjenkjent, har vært fremhevet som en kvalitet ved det urbane livet i motsetning til livet i små bygdesamfunn der alle vet hvem alle er, og alle vet alt om alle. Også i mange situasjoner med direkte interaksjon mellom mennesker skjer omgangen uten at noen av partene vinner sikker kunnskap om andres identiteter. Dette er for eksempel ofte situasjonen ved kjøp av varer og tjenester, enten kjøpet skjer kontant eller med betalingskort.[122]

I andre tilfelle er det av stor betydning å kjenne identiteten. Jeg vil ikke her forsøke å angi hva som kjennetegner slike situasjoner på en uttømmende måte, men et felles trekk er at personforveksling/falsk identitet kan føre til et betydelig tap av økonomisk, ideell eller sikkerhetsmessig verdi. For eksempel har treningsstudioet behov for å sikre økonomiske interesser ved å sørge for at kun medlemmer bruker deres lokaler; skolen trenger å etablere sammenheng mellom den eleven som er oppmeldt til eksamen og vedkommende som møter til eksamen, og forvaltningsorganet trenger å etablere sammenheng mellom en adressat og en innsynsberettiget person. Enkle handlinger, som skjer direkte, ansikt til ansikt, skaper i utgangspunktet ingen slike behov. Når en person vinner i lotteri og kan forevise vinnerloddet, er det i utgangspunktet ikke behov for noe navn/identitet.[123]

5.3.2 Biometriske mønstre som nøkkel for sammenstilling og gjenfinning

Personvern kan bl.a. sies å omfatte et behov for selv å kunne velge hvorledes en ønsker å fremstå overfor andre mennesker, herunder i hvilken grad og på hvilken måten en ønsker å røpe sin identitet. Bruk av biometri brukt for identifiseringsformål, for eksempel i form av ansiktsgjenkjenning av personer for å fastslå deres identitet uten personens medvirkning, kan sies å komme i konflikt med et slikt behov. Det er grunn til å anta at slike "fredsforstyrrelser" av mange vil bli oppfattet som mer inngripende enn bruk for rene autentiseringsformål, jf uttalelser i Europarådet 2005, gjengitt i avsnitt 5.5.

Personvern kan også begrunne at den enkelte person skal ha bestemmelsesrett over hva som behandles av opplysninger om ham eller henne, herunder hvilke opplysninger som sammenstilles. Biometriske mønstre kan tenkes brukt for uønsket sammenstilling av

[122] Skjer betalingen med kort, kan jeg fremdeles være anonym overfor betjeningen. Identiteten til den som er innehaver av kortet blir kun kommunisert til et maskinelt betalingssystem.
[123] Skal utbetalingen skje i ettertid til vinnerens bankkonto, oppstår derimot behov for sikker identifisering.

personopplysninger fra ulike kilder, ved for eksempel å sammenholde alle innsamlede fingeravtrykk (som direkte gir opplysning om oppholdssted og tid), eventuelt med andre tilknyttede opplysninger. Slike muligheter er imidlertid avhengig av at hver fingeravtrykkenhet er kompatible med hverandre og del av samme system, slik at de biometriske mønstrene faktisk lar seg sammenstille rent teknisk/praktisk. Dette lar seg åpenbart gjøre,[124] men uansett vil slike muligheter for sammenstilling av opplysninger ved hjelp av biometri være klart dårligere enn med for eksempel fødselsnumre.

5.3.3 Muligheten for å motsi

Retten til kontradiksjon, dvs til å motsi ved å hevde sine egne meninger om faktiske, rettslige og andre forhold, er en grunnleggende del av rettssystemet, og er også basalt for ytringsfrihet og alt sosialt liv. Dersom noen har rett/anledning til å fastslå sannheten om faktiske forhold, dvs fremsette påstander om faktiske forhold på måter som det er umulig å motsi, får de åpenbart stor makt. Biometriske id-systemer kan sies å angå slik etablering av sannhet, fordi biologiske spor framstår som spesielt troverdige. Når opplysninger kun er knyttet til et betalingskort eller et kjøretøy jeg er eier av, er sannsynligheten stor for at opplysningene sier noe om meg, men opplysningene kan også være resultatet av at kortet/bilen er stjålet, bortlånt, registreringsskiltet og kortet kan være forfalsket osv. Det oppstår da et rom av tvil, for motsigelse og forhandling om hva som skal anses som sant.

Vanlige elektroniske spor nagler ikke den enkelte opp til helt bestemte historier om tidligere hendelser. Med biometrisk id-teknologi har de elektroniske sporene også blitt biologiske. Biometriske spor åpner tilsynelatende ikke for troverdige alternative forklaringer som gir meg mulighet til å motsi koplingen til min person. Eksistensen av biologiske spor kan skape frykt for at det kan "bevises" ting om hva jeg har foretatt meg, uten at jeg kan bestride riktigheten av forholdet. Er bruken av de biometriske metodene nær 100% sikre, er dette en irrasjonell frykt som det kanskje ikke vil blitt tatt hensyn til. I avsnitt 2.4.3 er det imidlertid tatt inn opplysninger som viser at det er en usikkerhet også knyttet til biometriske metoder, og for noen metoder er usikkerheten større enn andre. Likevel er sannsynligheten for feil meget liten (ofte mindre enn 1%), noe som kan gi forventningen om at muligheten for andre sannheter enn det de biometriske metodene viser, kun vil bli tatt hensyn til dersom følgen av feil og forvekslinger er særdeles stor. Er biometri utslagsgivende for 21 års fengsel vil usikkerheter trolig bli nøye gjennomgått, men kanskje ikke dersom følgen er oppsigelse av arbeidsforholdet eller bøtestraff. I trivielle saker oppstår faren for at den som motsier riktigheten av opplysninger fra biometriske metoder blir sett på som kverulanter. De færreste mennesker vil uansett ha kunnskaper som gir mulighet for å sannsynliggjøre feil.

Muligheten til reelt å kunne motsi, er knyttet til personopplysninger og kan dermed betraktes som et personvernproblem. Kontradiksjon er særlig viktig i sammenheng med offentlig myndighetsutøvelse med tilhørende sanksjoner og innskrenkning av rettigheter. Slik sett kan disse spørsmålene om biometri like gjerne ses på som spørsmål om rettssikkerhet. Muligheten for å kunne motsi er imidlertid også viktig overfor enkelte private aktører som forvalter vesentlige velferdsgoder. Slik kan det for eksempel hevdes at rettssikkerhetstenkningen også er relevant i forhold til biometri brukt som grunnlag for forsikringsoppgjør.

[124] Det kan for eksempel tenkes at et vaktselskap introduserer låsesystemer basert på fingeravtrykk til alle sine kunder i hele landet, og med mulighet for direkte oppkopling til selskapets vaktsentraler.

5.3.4 Informasjonsubalanse

Et utslag av vid mulighet til å kople personopplysninger ved hjelp av entydige identifikatorer som fingeravtrykk, er at det kan settes sammen informasjon til store bilder av folks liv og fortid. Dette vil dels være opplysninger som mange mennesker har glemt eller har usikker/ufullstendig erindring om, mens den som setter sammen opplysningene tilsynelatende har tilgang til sikker og sann informasjon om de aktuelle personene. Et hvert informasjonssystem gir imidlertid et meget lite og begrenset bilde av de situasjoner og hendelser de anvendes i. Samtidig kan de være eneste kilde til kunnskap om tidligere hendelser, noe som kan gjøre at dette utvalget likevel blir tillagt stor vekt når det i ettertid er behov for å finne ut hva som faktisk har skjedd. Det er den som har anskaffet og/eller bruker informasjonssystemet som har styring med denne informasjonen. Dermed kan det oppstå en informasjonsubalanse mellom den som står bak systemet og de som blir registrert i det.

Informasjonsubalansen oppstår også pga. de forståelses-/tolkningsspørsmål som oppstår når opplysninger fra ulike kilder settes sammen ved hjelp av fingeravtrykk eller på annen måte. Problemet er at alle opplysninger har blitt til i en bestemt saklig kontekst, til en bestemt tid osv. Sammenstillingen kan gjøre at opplysninger som i utgangspunktet er knyttet til vidt forskjellige situasjoner fremstår som noe samlet og enhetlig. Den enkelte som opplysningene beskriver kan ha store problemer med å huske og tolke slike opplysninger: Dørsystemet har registrert at du låste deg inn på adressen A, men du kan ikke huske den legitime grunnen for dette; Bilen kan bare startes av deg, og du blir derfor ikke trodd når du hevder at en ukjent person stjal den mens motoren var i gang (osv).

Et ytterligere poeng er at de opplysninger som blir sammenstilt i datamaskinsystemer ofte vil være strengt formaliserte, noe som gjør dem uegnet til å fortelle den "sanne" historien. Samtidig kan personene det gjelder ha problemer med å huske og sannsynliggjøre nyanser og forklaringer til disse opplysningene. Dermed er det kun et strengt formalisert bilde som gjenstår og som vi har å forholde oss til, noe som kan gi urettferdige og lite akseptable resultater. Desto strengere formalisering av opplysninger, desto lengre tilbake i tid, og desto bredere og forskjelligartet saksfelt opplysningene er hentet fra, desto større kan slike problemer antas å være.

Informasjonsubalansen gjelder med andre ord både mengden opplysninger og den antatte/opplevde sannhetsgehalten slike opplysninger gir. Den som sammenstiller opplysninger om deg, har flere opplysninger enn du selv har. Disse opplysningene kan ha en sannhetsgehalt du bestrider men som du ikke lett kan motsi med overbevisningskraft fordi du ikke har tilsvarende sikre og harde data å vise til.

5.3.5 Sosiale identiteter og roller

For noen mennesker avviker den sosiale og registrerte identiteten fra den biologiske, jf avsnitt 2.3. Det kan være at personen kjenner til sitt biologiske opphav, men velger å hemmeligholde det, og det kan være at personen ikke er kjent med avviket mellom biologisk og sosial identitet. Biometri kan tenkes å bidra til å avdekke at biologisk identitet og slektskapsforhold ikke er i overensstemmelse med de sosiale identitetene og relasjonene. Dette gjelder for eksempel for barn som adopteres og for voldsofre og andre som skifter identitet som ledd i et beskyttelsesbehov, jf politiloven kap. IIa. Fingeravtrykk og irismønstre er permanente, og ved å sammenholde dette med gammel og ny registrert identitet, vil identitetsskiftet kunne avdekkes. I tilfelle der biologisk identitet reetableres for personer som har fått fiktiv identitet pga. trusler om vold eller lignende, vil effekten både være at et pseudonym/alias kompromitteres og at

voldsbeskyttelsen faller bort/svekkes. Slikt bortfall av vern vil også kunne ramme andre personer i husstanden som er berørt av den fiktive identiteten (for eksempel barn av den som har beskyttelsesbehov), se politiloven § 14a, tredje ledd.

En del av kontrollen over eget liv er muligheten for å gå inn i ulike sosiale roller som i større eller mindre grad synliggjør din personlighet. I noen situasjoner er identiteten falsk/skjult, noe som tillater at personen spiller en helt annen rolle enn i livet ellers. Kjerneeksempelet er personer som i prategrupper mv på Internett utgir seg for å ha et annet kjønn, alder, sosial bakgrunn mv enn i virkeligheten. Dette gir både mulighet for livsutfoldelse og for (forberedelse til) kriminelle handlinger, jf for eksempel "grooming".[125] Muligheten til å spille en bestemt rolle i en sosial sammenheng, kan også være knyttet til riktig men ufullstendig identitet. Du er for eksempel bare "Geir" som er lidenskapelig opptatt av å bekjempe menneskehandel, og ingen vet nøyaktig hvem du er, hvor du bor, og du er gift har barn mv. Med slik beskyttelse av biologisk og offentlig registrert identitet vil en kunne føle seg tryggere i kommunikasjon og meningsutveksling med andre. Slike sosiale situasjoner gjør det også mulig å fremheve sider ved eget liv, samtidig som (de fleste) andre sider ved livet får liten eller ingen oppmerksomhet. Etablering av en "sann" og uomtvistelig identitet ved å måtte logge på maskiner eller digitale tjenester med fingeravtrykk eller lignende kan fjerne eller redusere denne muligheten. Dermed reduseres også enkelte muligheter for livsutfoldelse.

5.3.6 Krenkende sosiale assosiasjoner

Identifisering ved hjelp av fingeravtrykk har i løpet av de siste hundre årene primært foregått som ledd i etterforskningen av alvorlige straffesaker. Dette trekkes spesielt frem i Personvernnemndas avgjørelse klagesak 2006-08 (Oxigeno Fitness) i tilknytning til bruk av fingeravtrykk som del av adgangskontrollen til treningsstudio. Også identifisering ved hjelp av DNA har tidligere vært spesielt knyttet til alvorlige straffesaker som drap og voldtekt.[126] På en slik bakgrunn kan det sies å være krenkende å bli utsatt for samme metoder som alvorlig kriminelle blir utsatt for. Mot dette kan det anføres at dette mest er et spørsmål om tilvenning. Registrering i DNA- med det tilhørende identitetsregisteret kunne fra 1. september 2008 for eksempel skje uten at det er begått alvorlig kriminalitet, og registrering kan derfor hevdes å bli mindre belastende enn tidligere. Uansett kan biometrisk id-teknologi som brukes hyppig av borgerne kunne ha en trivialiserende effekt som vil gjøre slik identifisering dagligdags og mindre støtende og kontroversiell enn i dag.

5.3.7 Fare for spredning og illegitim bruk av identitetsmerker

Det er forskjell på biologiske identitetsmerker ved at noen er mer tilgjengelige enn andre. Lett tilgjengelig er for eksempel humant biologisk materiale av ulik slag (spytt, blod, hudceller mv) som kan brukes for å identifisere personer ved hjelp av DNA-analyse. I dag er denne teknologien forholdsvis dyr, tidkrevende og lite tilgjengelig at det trolig er meget liten fare for misbruk. Dersom jeg imidlertid forutsetter en teknologisk utvikling som skissert i avsnitt 2.4.3, vil det kunne bli en reell fare for at biometriske mønstre og nødvendig utstyr vil kunne bli

[125] Dvs å etablere sosial/følelsesmessig kontakt med en mindreårig for å oppnå seksuell omgang, se http://en.wikipedia.org/wiki/Child_grooming og strl 201a.
[126] Se strpl § 160a slik den lød før endringen av 27 juni 2008 nr. 67.

tilgjengelig for personer med uhederlige hensikter, og som kan tenkes å benytte teknologien til personovervåking, planting av biologiske spor på åsteder mv.[127]

En viss fare for spredning og illegitim bruk foreligger i dag ved bruk av fingeravtrykkskannere. Slike avtrykk vil kunne avsettes på steder og måter som gjør dem tilgjengelige for personer som ønsker å tilegne seg dem for å opptre som vedkommende person, jf "skimming"[128]. Hvor stor denne faren vil kunne bli, ligger utenfor min kompetanse å bedømme. Spørsmålet er imidlertid både avhengig av kvaliteten av biometriske id-systemer i ulike brukssituasjoner, samt hvilke hjelpemidler som blir tilgjengelige for å identifisere og avlese fingeravtrykk som andre personer har avsatt.

5.3.8 Ulydighet og motstand i krigs- og krisesituasjoner

I ekstreme situasjoner vil alle mennesker kunne ha en legitim grunn til å skjule sin virkelige identitet og enten ikke fremstå som en bestemt person (være anonym) eller fremstå med falsk identitet (pseudonym). I motstandskamp under krigs- og krisesituasjoner kan muligheten til å unngå korrekt identifisering være helt avgjørende. Et samfunn som har bygget opp en omfattende infrastruktur av identifiseringsmekanismer ved hjelp av biometri mv, dvs der hyppig og sikker identifisering er uunngåelig for den som vil leve et tilnærmet normalt liv, vil ødelegge eller vesentlig redusere denne muligheten for ulydighet mot illegitime makthavere.

Det oppstår her en vanskelig avveining mellom på den ene side hensynet til effektivt å kunne bekjempe aktører som ønsker å omstyrte vårt demokratiske styre, og hensynet til å unngå å gi illegitime makthavere midler som gjør at de kan bruke illegitim makt. Grunnlaget for en slik diskusjon blir enda vanskeligere dersom vi ikke forutsetter krig eller revolusjon, men holder muligheten åpen for en gradvis omdanning av samfunnet i en udemokratisk og illegitim retning. Jeg går ikke her nærmere inn på slike muligheter, og grensene for når motstand vil være legitim. Også denne eventualiteten bør imidlertid inngå som en relevant del av den samlede diskusjonen. Risikoen for slik dramatisk samfunnsutvikling er imidlertid for tiden så liten, at slike argumenter trolig vil tillegges liten vekt.

5.4 Informasjonssikkerhet

Ovenfor har jeg kommentert enkelte spørsmål som systematisk hører inn under informasjonssikkerhetsspørsmål. Her vil jeg - kortfattet - vie slike spørsmål samlet oppmerksomhet.

Informasjonssikkerhet handler bl.a. om ivaretakelse av konfidensialitet, integritet og tilgjengelighet ved behandlingen av personopplysninger. Konfidensialitetskravet innebærer at personopplysninger ikke skal tilflyte andre enn de som er autorisert til å få tilgang, herunder at de ikke spres videre fordi ingen har slik autorisasjon. Biometriske teknikker kan for det første brukes av de personer som opplysningene gjelder for å "låse" opplysningene og dermed gjøre dem utilgjengelig for andre. Pålogging på PC ved hjelp av fingeravtrykk eller lignende vil gi større kontroll for vedkommende person til opplysninger som ligger på maskinen sammenlignet ved om innlogging skulle skje med bruker og passord. Teknologien vil gi tilsvarende god

[127] Visse former for DNA-testing vedrørende slektskap mv er tilgjengelig for alle mot betaling, se for eksempel http://www.dna-worldwide.com/.

[128] Dvs. ulovlig kopiering av biologiske mønstre ved hjelp av uautorisert leser. Tilsvarende teknikker har vært brukt i minibankterminaler for å lese pin-kode fra bankkort.

beskyttelse i situasjoner der personen velger å gi andre digital tilgang til opplysningene, dvs når mottakeren bruker biometriske teknikker for å skaffe tilgang til tilsendte opplysninger.

At opplysningenes integritet er beskyttet, betyr at opplysningene bare kan endres av personer som er autoriserte til å foreta endringer. Biometriske teknikker kan åpenbart være viktig for å styre tilgang til å gjøre endringer, tilsvarende som for ivaretakelse av konfidensialitet. Slik kan sikkerhetsnivået økes i forhold til endring av opplysninger på grunnlag av pålogging med bruker og passord.

Når det gjelder sikring av tilgjengelighet til personopplysninger, er virkningene av biometrisk id-teknologi trolig mer indirekte. Dersom vi legger til grunn at konfidensialitets- og integritetsvernet er bedre med biometri enn med tradisjonelle påloggingsmetoder, kan en tenke seg at biometriske id-systemer for tilgangsstyring blir argument for å gjøre tilgjengelig *flere* personopplysninger for de personene opplysningene gjelder, jf pol § 18 annet ledd. Slik kan biometri tenkes å bidra til større grad av åpenhet og mer omfattende tilgang til opplysninger om egen person hos offentlige myndigheter og private selskaper. Noen *nødvendig* konsekvens av å anvende biometri er dette imidlertid ikke.

Samtidig som biometriske teknikker i utgangspunktet kan sies å ha positive virkninger for informasjonssikkerheten, kan flere slike teknikker muligens også gi større sårbarhet i forhold til fysisk tvang. Således kan det hevdes å være langt lettere å tvinge noen til å plassere tommelen med fingeravtrykket på en leser enn det er til å tvinge noen til å oppgi bruker/passord. Dette kan spesielt ha betydning på skjermede steder, for eksempel i hjem og andre private områder. Selv om det sikkerhetsmessige generelle utgangspunktet er positivt, kan den konkrete slutt-vurderingen likevel bli negativ.

5.5 Anbefalinger fra Europarådets rådgivende komite

Europarådets Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD) ferdigstilte i 2005 en "Progress report" vedrørende anvendelse av prinsippene i Europarådskonvensjonen om personvern nr 108 av 1981 (Europarådet 2005). Rapporten konkluderer i form av tolv punkter med særlige understrekninger og forståelser vedrørende personopplysningsvern og biometri. Jeg har ikke funnet andre tilsvarende uttalelser i Europarådet ellers eller i EU, og velger derfor kort å gjengi innholdet av denne konklusjonen. I gjengivelsen har jeg omformet innholdet til en sammenhengende tekst, og har herunder endret på rekkefølgen av punktene for å gruppere disse slik at punkter som saklig sett henger sammen gjengis i sammenheng. Fordi nyanser kan ha gått tapt i omskrivingen, gjengir jeg den originale nummererte teksten i fotnoter.

Komiteen mener at biometriske opplysninger skal anses å være en særlig form for personopplysning fordi de er hentet fra menneskekroppen og fordi de ofte er uforanderlige hele livet.[129] Slike teknikker bør ikke velges bare fordi det er lettvint, og en bør ta hensyn til at bruken kan berøre spørsmål om menneskelig verdighet, herunder motvilje mot at kroppen brukes

[129] 1. Biometric data are to be regarded as a specific category of data as they are taken from the human body, remain the same in different systems and are in principle inalterable throughout life. They might be altered, however, for instance through aging, illnesses or surgical interventions.

som redskap.[130] Før en søker biometriske løsninger bør den behandlingsansvarlige gjøre en avveining mellom de registrertes privatliv og den behandlingsansvarliges formål med bruken av biometri. Av foreliggende alternativer bør en velge det som er minst inngripende for den enkeltes privatliv.[131] En sentral avveining gjelder systemarkitektur og spørsmålet om biometriske opplysninger bør lagres på lagringsmedium som den enkelte har, i desentral database eller i sentral database. Denne vurderingen må også skje ut i fra hensynet til informasjons-sikkerhet.[132] Er verifikasjon av identiteter tilstrekkelig, bør ikke den biometriske løsningen omfatte identifikasjonsmuligheter. Gjelder bruken kun verifikasjon, bør løsningen fortrinnsvis være basert på lagringsmedium som den enkelte har (smartkort eller lignende).[133]

Formålsbestemthetsprinsippet gjelder for biometriske personopplysninger og andre tilknyttede personopplysninger, noe som bl.a. innebærer at det alltid skal foreligge spesifikke, eksplisitte og legitime formål for behandlingen av slike opplysninger.[134] Opplysningene må alltid være tilstrekkelige, relevante og ikke være overflødige i forhold til formålet for behandlingen. Er innsamling og lagring av utvalgte biologiske mønstre tilstrekkelig, bør ikke hele mønsteret behandles.[135]

I anbefalingene vedrørende rett til innsyn og informasjon, går Komiteen forholdsvis detaljert til verks, og angir et nivå for slike individuelle rettigheter som er i overensstemmelse med Personverndirektivet art. 10.[136] I tillegg sier en eksplisitt at retten til innsyn i egne opplysninger, samt retting, sletting og blokkering av opplysninger også bør gjelde for biometriske opplysninger, og andre opplysninger som kan være knyttet til disse, jf art 12(b).[137] I tillegg uttaler komiteen at det bør gjelde egne rettigheter for den registrerte i tilfelle enkelte feilsituasjoner. Dette gjelder for det første tilfelle der den registrerte blir avvist, dvs. autentiseringen ikke gir positivt resultat. I slike tilfelle anbefaler komiteen at den registrerte skal

[130] 3. Biometrics should not be chosen for the sole sake of convenience. Human dignity might be affected by the use of biometrics. Socio-cultural aspects and possible reluctance towards the instrumental use of the human body, should be taken into account.
[131] 2. Before having recourse to biometrics, the controller should balance the possible advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand, and consider possible alternatives that are less intrusive for private life.
[132] 6. In choosing the system architecture, the controller should balance the advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand. A reasoned choice should be made between storage solely on an individual storage medium, a decentralised database or a central database, bearing in mind the aspects relating to data security.
[133] 7. The architecture of a biometric system should not be disproportionate in relation to the purpose of the processing. Therefore, if verification suffices, the controller should not develop an identification solution. Biometric data that are solely used for verification purposes preferably should be stored only on a secured individual storage medium, e.g. a smart card, held by the data subject only.
[134] 4. The biometric data and any associated data generated by the system must be processed for specific, explicit and legitimate purposes and should not be processed further for purposes that are incompatible with these.
[135] Jf. beskrivelsen av biometriske systemer i avsnitt 2.4.3 (ovenfor) som skjelner mellom tilfelle der det skjer et visst utvalg av det totale mønsteret (et visst antall punkter i fingeravtrykket), og tilfelle da hele avtrykket benyttes. Det er i sist nevnte tilfelle at mønsteret omtales som "picture" i det følgende sitatet: "5. The data should be adequate, relevant and not excessive in relation to these purposes. A technical system using biometric data should be configured to exclude the possibility to collect more biometric or associated data than is necessary for the purposes of the processing. Where templates are sufficient, the collection or the storage of the picture should be avoided."
[136] 8. The data subject should be informed about the purposes of the system and the identity of the controller unless he or she already knows, and about the personal data that are processed and the persons or the categories of persons to whom they will be disclosed as far as the information is necessary to guarantee the fairness of processing.
[137] 9. The data subject has a right of access, rectification, blocking and erasure of the data relating to him or her. These rights extend to the biometric data undergoing automatic processing attached to his identity, possibly associated data (such as date and place of use of the system) and to whom they have been communicated.

kunne be om at det blir gjort nytt forsøk, eventuelt at det tilbys annen form for autentisering. Det bør i tillegg gis informasjon til den registrerte om de rutiner som blir fulgt i tilfelle av negativt resultat fra autentisering.[138]

Komiteen uttaler seg også om krav til informasjonssikkerhet, som i stor grad samsvarer med de krav som generelt gjelder i medhold av art. 17 i personverndirektivet. Forskjellen er at det også kreves at tilknyttede opplysninger beskyttes, noe som tilsvarer kravene etter annet ledd i personopplysningsforskriften §§ 2-11, 2-12 og 2-13.[139] Det rådes videre til at et uavhengig organ gjennomfører sertifisering, overvåkning og kontroll av biometriske systemer, særlig i tilfelle der bruken er omfattende. Kontroll bør utføres i forhold til kvalitetsstandarder for maskin- og programvare, samt for opplæring av ansatte som forestår innrullering av biometriske mønstre, og sammenligning mellom innrullerte og registrerte mønstre. Det anbefales også periodisk revisjon av biometriske systemløsninger.[140]

Deler av den gjengitte uttalelsen bringer etter min mening lite nytt til temaet biometri og personvern fordi den i stor grad henviser til det beskyttelsesnivået som også ellers gjelder for annen behandling av personopplysninger. På enkelte punkter gis det imidlertid uttrykk for synspunkter som bringer nye momenter inn i diskusjonen, og som det etter min mening kan være grunn til å legge vekt på i en fremtidig norsk lovgivning. Dette gjelder for det første tilrådingen om å velge løsninger for lagring som gir best sikkerhet, og at dette ikke automatisk fører til fraråding av å velge sentral lagring. Det klassiske dilemmaet her er at mye innsats kan settes inn for å sikre en sentral biometridatabase, men samtidig vil sikkerhetsbrudd kunne gi ekstremt store skadevirkninger. For lagring hos den enkelte, er det grunn til å anta at situasjonen er den motsatte. Det er også grunn til å merke seg at identifisering anses som klart mer inngripende enn autentisering, og at lagringen bare bør skje hos den enkelte dersom formålet kun er autentisering. Biometriske mønstre anses dessuten å være mindre inngripende å behandle enn biometriske kopier, jf avsnitt 2.4.2 (ovenfor). Også krav om at det skal finnes alternative fremgangsmåter til biometri er av interesse. Det samme gjelder anbefalingen av etablering av sertifiseringsordninger, noe jeg oppfatter som sertifisering av de teknologiske løsningene og metodene.

5.6 Noen vurderinger av mulige veier videre

Biometri representerer på mange måter et dramatisk skille i den teknologiske utviklingen. Tidligere har informasjonsteknologi vært gjenstander som i en første fase var meget store og svært få ("mainframe" datamaskiner), i neste fase også mindre og spredte (PCer mv), deretter ble teknologien også utviklet til å omfatte bærbart utstyr (mobiltelefon, PDA, GPS mv), og i foreløpig siste fase blir teknologien direkte "koplet på kroppen" primært i tilknytning til identifisering og autentisering (biometri, RFID). Det er nærliggende å tro at det kan følge flere faser, der biometriske teknikker også kan bli integrert med kroppen og både behandle tilstander

[138] 12. If, as a result of a biometric system, a data subject is rejected, the controller should, on his or her request, re-examine the case and should, where necessary, offer appropriate alternative solutions. Procedures should be in place and made known to the data subject in the case of an allegedly false result of the system.

[139] 10. The controller should foresee adequate technical and organisational measures that aim to protect biometric and associated data against accidental or deliberate deletion or loss, as well as against illegal access, alteration or communication to unauthorised persons or any other form of illegal processing.

[140] 11. A procedure of certification and monitoring and control, if appropriate by an independent body, should be promoted, particularly in the case of mass applications, with regard to the quality standards for the software, the hardware and the training of the staff in charge of enrolment and matching. A periodic audit of the system's performance is recommendable.

som har betydning for identitet og andre tilstander og egenskaper vedrørende helsetilstand, kognitive prosesser mv.

Selv om forestillingen om kybernetiske organismer[141] (cyborg) fremdeles fortoner seg som science fiction, kan det se ut som om vi også på dette området er i ferd med å bevege oss fra fiksjon til virkelighet. Således har for eksempel medisinsk teknologi innen området brain-computer interface (BCI), gjort det mulig å kople seg direkte på prosesser i hjernen for å bedre synsfunksjonen og gi bevegelse til kroppsdeler med lammelser.[142] Med et slikt utgangspunkt er det etter min mening ikke usannsynlig at informasjonsteknologi og ulike typer medisinsk digital teknologi mv, vil komme til å integreres og totalt endre forholdet mellom menneske og maskin.

Jeg vil understreke at en ikke må forholde seg til biometri og annen (lignende) informasjons-teknologi som direkte koples på menneskekroppen, som om det var *ett* spørsmål. Om noen år vil bruk av biometri til identifisering og autentisering trolig komme til å være et forholdsvis uskyldig eksempel på informasjonsteknologibruk som direkte gjelder menneskers kropp. Slike fremtidige teknologier og anvendelser er det etter min mening ikke grunn til å prøve å regulere på forhånd. Forventet teknologisk utvikling gir imidlertid grunn til tydelig å angi hva gjeldende lovgivning faktisk regulerer. Derfor er det grunn til tydelig å avstå fra og regulere biometri generelt, men helt eksplisitt angi både teknologien og *formålet*. Det betyr at en tydelig bør angi at reguleringen kun gjelder bruk av biometri for identifisering og autentisering av enkeltindivider. I dette ligger det en dobbelt presisering idet en tydelig utelukker annet enn identifisering/autentisering, og samtidig understreker at identifiseringen/autentiseringen kun gjelder tilfelle der en bruker opplysninger som direkte eller indirekte kan knyttes til en enkeltperson, og som derfor involverer personopplysninger. I så fall regulerer en ikke all autentisering, for eksempel ikke autentisering av roller når denne ikke samtidig kan røpe identitet, jf avsnitt 2.2.

Samtidig som en tydelig angir et begrenset formål med reguleringen må relevante myndigheter følge med på teknologiutvikling og -bruk innen det biometriske og beslektede forskningsfelt for løpende å vurdere behovet for lovgivning eller bruk av andre virkemidler for å beskytte individers integritet og autonomi. Ytterligere regulering av biometri, kan for eksempel gjelde måling av andre egenskaper og tilstander ved den menneskelige kropp enn det som direkte gjelder identitet mv. Det kan eksempelvis bli mulig å måle egenskaper som kan si noe om personer er påvirket av ulovlige stoffer (alkohol, narkotika, medisiner mv) eller sinnstilstander mv (jf for eksempel løgndetektor) ved hjelp av apparatur som ligner på dagens iris- og fingeravtrykklesere mv, dvs uten tidkrevende laboratoriumsanalyser. I fremtiden vil det kunne bli aktuelt også å regulere slik annen anvendelse av biometri. I så fall vil det imidlertid lett være helt andre lover enn personopplysningsloven som vil være det mest aktuelle regimet å plassere bestemmelsene i (særlig helselovgivning). Poenget er at biometri kan brukes på et teknologiområde som trolig komme til å bli langt bredere enn i dag, og at det derfor antagelig trengs variert og målrettet lovgivningsmessig og annen respons på den videre teknologiske utviklingen.

Den grensesprengende overgangen fra teknologi som ting som ikke er koplet til mennesker, til teknologi som leser menneskekroppen, kan lett skje i relativ stillhet fordi de praktisk viktigste formålene i dag (identifisering og autentisering) er nyttige, og teknologien er rasjonell i bruk. Dramatikken ligger imidlertid i det prinsipielle: Biometrisk id-teknologi innebærer at en går

[141] Se http://en.wikipedia.org/wiki/Cyborg.
[142] Se for eksempel http://en.wikipedia.org/wiki/Brain-computer_interface.

utenom personens egen fremstilling av seg selv, og dermed hans vilje og kontroll over egen situasjon.[143] Et slikt poeng er det ikke lett å gjøre tydelig med en teknologi som for eksempel bare skal brukes for å bekrefte sannheten i utsagn om identitet, og avsløre noen ganske få løgnere. Dersom vi i stedet tenker oss at biometrien gjaldt å måle tilstander som sikkert viste noe om sannhet og løgn for en lang rekke utsagn (jf løgndetektor[144] og Cognitive Performance Biometric Systems), kan vi ane konturene av at tankene våre i fremtiden ikke lenger er helt fri og beskyttet av vår vilje.[145] Slike foruroligende anelser er trolig alt for ekstreme, usikre (og noen vil kanskje si useriøse og spekulative) til å bli tatt alvorlig i en politisk og saklig debatt om "uskyldig" bruk av biometri for autentiseringsformål, men kan kanskje bli mer akseptert i debatter om identifisering og overvåkning (jf ansiktsgjenkjenning på offentlig sted). Uansett kan følelsen av å stå i fare for å miste kontroll over egen kropp og eget liv være grunn til "irrasjonell", dvs. ikke rasjonelt formulert, motstand mot dagens biometriske teknologi.

Eksempler på bruk av teknologi for andre primærformål enn identifisering mv, viser også at det i ett perspektiv ikke er grenser for hva som bør tåles av integritetskrenkelser som har fornuftige begrunnelser. I USA er det for eksempel utviklet et system for håndhygiene som er basert på id-opplysninger i en RFid-brikke, og som gjør det mulig å kontrollere at helsearbeidere vasker hendene og hvordan de gjør det. Formålet er åpenbart godt, nemlig å unngå sykehusinfeksjoner som hvert år krever et stort antall menneskeliv.[146] Det store dilemmaet er imidlertid at det nesten ikke er grenser for hvilke "forbedringer" vi kan ønske for menneskelig adferd, og dermed er det kanskje heller ikke grenser for hva slags bruk av teknologi vi kan legitimere ut i fra slike gode formål.

[143] Alterman 2003 s. 146 legger vekt på den fremmedgjørende effekten av at teknologi brukes direkte på personen: "The degree to which the body is objectified by the process, suggest[s] that biometric identification alienates a part of the embodied self. The body becomes an object whose identity is instantly determinable by purely mechanical means, and subject to external controls on that basis; while those means themselves are removed from the control of the subject. The representations are infinitely reproducible by their owner, but are not even accessible to the subject whose body they represent. The embodied person now bears, more or less, a label with a bar code, and is in this respect alienated from her own body as well as from the technology used to recognize it. If having an iris scan on file is not quite like being incarcerated in the world at large, being made known to mechanical systems wherever they may be is still a tangible loss of privacy that is not precisely paralleled by any other kind of information technology".

[144] Se http://en.wikipedia.org/wiki/Lie_detector.

[145] Jf. den tyske motstandssangen fra 1820-tallet om "Die Gedanken sind frei".

[146] Se http://www.rfidjournal.com/article/view/3425/. I dette systemet brukes id-nummer, men også biometriske data kan anvendes for slike formål.

6 Personvernmessige konsekvenser av fødselsnummeret

6.1 Fødselsnummer som identifikator og nøkkel for sammenstilling av personopplysninger

I utgangspunktet må personvernet forstås slik at den enkelte i størst mulig grad selv må kunne bestemme over opplysninger om egen person, herunder om og på hvilken måte personopplysninger skal sammenstilles.[147] Det følger ikke av personvernet at sammenstilling ikke bør skje, bare at den enkelte selv skal kunne nekte sammenstilling og eventuelt stille krav til gjennomføringen. Et slikt ideelt utgangspunkt er imidlertid så langt fra den praktiske virkeligheten at det kanskje ikke er hensiktsmessig.

For det første er det på det rene at det når det gjelder fødselsnummer i liten grad er realistisk mulig å ha særlig grad av selvbestemmelse og valgfrihet for den enkelte. Dette skyldes primært at offentlig forvaltning har sterkt behov for å sy sammen en virksomhet som før øvrig er hierarkisk organisert, for på den måten å sikre informasjonsflyt og sammenheng mellom sidestilte organisatoriske enheter. For det andre viser erfaringer oss at det for den enkelte ofte kan være vanskelig å utøve bestemmelsesrett gjennom ordninger med samtykke.[148] I den grad det eksisterer rett til selv å bestemme for den enkelte, kan det derfor være en utfordring å få reell effekt av slike ordninger.

Selv om det ideelle utgangspunktet er selvbestemmelsesrett, kan det reelt sett være grunn til å anta at personvernet ofte vil være best tjent med preseptorisk lovgivning vedrørende bruk av fødselsnumre for sammenstilling av personopplysninger. En slik tilnærming vil gi klarere politisk ansvar for rettstilstanden, og vil dessuten i større grad stimulere til demokratisk, politisk debatt enn med mer "privatiserte" løsninger.

6.2 Fødselsnummer som "passord" og verifikasjon av identitet

Fødselsnummer brukes av enkelte virksomheter som passord for å verifisere identiteter. Jeg har ingen nærmere dokumentasjon på omfanget av denne praksisen. Likevel antar jeg at eksistensen av en slik praksis er så allment kjent at jeg legger dette til grunn for den videre diskusjonen. Bruken er knyttet til situasjoner der noen henvender seg på telefon, epost eller lignende og på grunn av den fysiske avstanden ikke lett kan fremlegge identitetsbevis. Dersom det ikke er avtalt noe hemmelig passord/kode eller lignende, kan det være fristende å bruke fødselsnummer som "passord", eventuelt i sammenheng med andre opplysninger som er knyttet til samme person (adresse, telefonnummer).

Det er så vidt jeg kan forstå to mulige forutsetninger som alene eller i kombinasjon kan begrunne en slik praksis. Den ene mulige forutsetningen er at fødselsnummer er så utilgjengelig at det primært er vedkommende person selv som kjenner nummeret. En slik forutsetning er åpenbart uholdbar. For det første kan Folkeregisteret i en rekke situasjoner lovlig gi ut opplysning om fødselsnummer, se avsnitt 3.2.4. For det andre brukes fødselsnummer i så mange offentlige og private sammenhenger at det neppe er vanskelig å skaffe seg kunnskap om nummeret for den som søker slik informasjon. Blant annet er fødselsnummer ofte en del av innloggingsrutinen for

[147] Jf NOU 1997: 19, avsnitt 3.4.2.

[148] I Ravlum 2005 s 35 blir det således konkludert med at en god del mennesker trolig gir sitt samtykke til at personopplysninger skal bli behandlet, selv om de egentlig ikke ønsker det.

nettbank, og står ikke sjelden på korrespondanse fra forvaltningsorganer. For det tredje er fødselsnumre spredd til uvedkommende gjennom ulike typer tabber, særlig i offentlig sektor.

Den andre mulige forutsetningen for at nevnte bruk av fødselsnummer kan være forsvarlig, er at det som skal beskyttes ikke er underlagt taushetsplikt, og at formålet med å kreve fødselsnummer er å unngå at det gis opplysninger om uriktig person. Dette kan tenkes å være rasjonelt begrunnet, for eksempel dersom jeg ønsker å kontrollere at NAV-kontoret har registrert riktige personalia på meg. Selv om det ikke er taushetsplikt for slike opplysninger, vil det være viktig for den som svarer å unngå personforveksling, noe bruk av fødselsnummeret kan bidra til. Selv om det kan være rasjonelt begrunnet, bør en imidlertid unngå å bruke fødselsnummeret på denne måten.

Dersom det foreligger taushetsplikt, men brudd på denne typisk antas å gi små negative virkninger vil en viss grad av kontroll med identitet være nødvendig. Her kan det ikke helt utelukkes at risikoen for å gi opplysninger til uvedkommende blir akseptabelt liten dersom en anvender fødselsnummer for verifisering av identitet sammen med andre teknikker. Kan risikoen sies å være akseptabel, vil praksisen også innebære en tilfredsstillende informasjonssikkerhet, jf kravene til risikovurdering i personopplysningsforskriften § 2-4. Situasjonen kan for eksempel være at det antall personer som kan ringe å etterspørre informasjon er lite, den som svarer kjenner de fleste (lokale, små forhold), og den informasjonen som kan gis har lite skadepotensiale. Jeg tror derfor ikke enhver bruk av fødselsnummer for å verifisere identitet på denne måten vil være uforsvarlig. Slik bruk av fødselsnummer vil imidlertid være klart unødvendig og dermed ulovlig etter pol § 12, jf gjennomgangen i avsnitt 3.4.2.

Etter min mening er det neppe grunn til å tillate bruk av fødselsnummer som passord for å få tilgang til informasjon, tjenester mv. Begrunnelsen er ikke at slik praksis alltid gir for dårlig sikkerhet for uautorisert spredning av personopplysninger, men at sikkerheten *ofte* blir for dårlig, og at det uansett er uheldig å bruke og dermed spre fødselsnummer på en slik måte, jf forrige avsnitt.

6.3 Fødselsnummer for å sikre personopplysningenes kvalitet

Fødselsnummerets funksjon som entydig identifikator innebærer at opplysninger om samme person fra flere kilder sikkert kan sammenstilles. Forutsatt at opplysninger skal sammenstilles må denne egenskapen sies å være positiv for personvernet. Årsaken er selvsagt at personvern begrunner krav til kvalitet på personopplysninger, jf § 11 første ledd bokstav e. Uriktig sammenstilling av datasett som innebærer sammenblanding av opplysninger fra flere personer, vil selvsagt gi sviktende opplysningskvalitet. Slik sett kan fødselsnummeret sies å fremme personvernet.

Som tidligere nevnt kan imidlertid også andre identifikatorer enn fødselsnummeret gi sikring mot feilkopling av personopplysninger, i hvert fall internt i en organisasjon. Dersom slike identifikatorer gir en tilfredsstillende sikkerhet,[149] vil ikke bruk av fødselsnummer gi den løsningen som samlet sett er optimal for personvernet. Årsaken er at fødselsnummer samtidig legger til rette for omfattende sammenstilling av personopplysninger. I forhold til personvernet er det med andre ord grunn til å foreta sammenstilling av personopplysninger bare når dette er begrunnet i forbedret kvalitet på personopplysninger. Derfor vil en velge identifikatorer som gir tilstrekkelig kvalitet, og dette vil ikke alltid tilsi bruk av fødselsnumre.

[149] Jf. personopplysningsforskriften § 2-4 om risikovurdering, jf pol § 13.

7 Behov for lovendringer og forslag til nye bestemmelser

7.1 Innledning

7.1.1 Om forholdet til tidligere forslag til endringer av personopplysningsloven

Det er tidligere utarbeidet forslag til endringer av flere bestemmelser i personopplysningsloven for Justisdepartementet, herunder bestemmelsen i § 12 om entydige identifikasjonsmidler.[150] I utredningen ble det dels tatt utgangspunkt i et "radikalt" og dels et "moderat" forslag, betegnelser som indikerer at endringene er større i førstnevnte enn i sistnevnte forslag. I det radikale forslaget ble det tatt høyde for separat regulering av henholdsvis biometri og fødselsnummer, men det ble ikke fremmet forslag til bestemmelse om biometri fordi dette lå utenfor mandatet. Forslaget lød:

"§ 11. Bruk av biometriske identifikasjonsteknikker
[...]

§ 12. Bruk av fødselsnummer

Fødselsnummer kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og bruk av fødselsnummer er nødvendig for å oppnå slik identifisering.

Datatilsynet kan pålegge en behandlingsansvarlig å bruke fødselsnummer for å sikre at det ikke skal skje forveksling av identitet.

Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten. Tilsvarende gjelder sendinger som formidles ved hjelp av telekommunikasjon.

Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer. "

Heller ikke bestemmelsen om fødselsnummer var i seg selv omfattet av mandatet. Bestemmelsen ble derfor kun vurdert og foreslått ut i fra regelstruktur. Forslaget hadde således kun bakgrunn i ønsket om å flytte en bestemmelse i personopplysningsforskriften vedrørende fødselsnummer opp i lovens § 12.[151] De forslag jeg her fremmer tar utgangspunkt i forslaget til struktur i nevnte utredning, og inneholder i tillegg forslag til ny rettslig regulering av både biometri og fødselsnummer. Jeg har imidlertid valgt å snu på rekkefølgen slik at fødselsnummer reguleres i § 11 og biometri i § 12. I tillegg mener jeg det er behov for enkelte andre bestemmelser i personopplysningsloven, se avsnitt 7.4.

7.1.2 Noen regeltekniske overveielser

Mandatet for denne utredningen er knyttet til personopplysningsloven. Jeg har likevel tillatt meg å gå noe videre til verks ved bl.a. å danne et mye bredere bilde av lovgivning vedrørende biometri og fødselsnummer enn det som eksisterer og/eller kan gjøres til en del av personopplysningsloven, jf redegjørelsene i avsnittene 3.2 og 3.3. En slik oversikt er avgjørende for spørsmålet om lovgivningsstrukturen eller -arkitekturen og "arbeidsdelingen" mellom ulike deler av lov- og forskriftsverket.

[150] Se Schartum og Bygrave 2006.
[151] Se avsnitt 12.5.3.2 i utredningen.

Utgangspunktet mitt har vært iakttagelsen av at det allerede finnes spesiallovgivning som regulerer bruk av biometri og fødselsnummer i spesielle situasjoner. I avsnitt 3.2.5 antok jeg også at dette vil være et tiltagende fenomen. Jeg mener særlovgivning på området er viktig for å sikre lovregulering som er godt tilpasset ulike brukssituasjoner, og tror en slik reguleringsform vil kunne gjøre det lettere å balansere hensynene til fleksibilitet og forutberegnelighet på en god måte. Dessuten vil særlovgivning gi flere rettspolitiske diskusjoner, og dermed bedre demokratisk deltakelse og engasjement enn hva tilfelle vil være dersom spørsmål om biometri mv primært reguleres i personopplysningsloven. I lovforslagene jeg presenterer i avsnittene 7.2.2 og 7.3.2 (nedenfor), er utgangspunktet derfor at personopplysningsloven primært skal være "bakgrunnsrett", dvs. inneholde regulering som gjelder med mindre annet er bestemt i særlovgivning. Et slikt opplegg legger etter min mening til rette for forholdsvis restriktive og enkle bestemmelser i personopplysningsloven. Med ett unntak vedrørende sikring av fødselsnumre, forutsetter jeg heller ikke nærmere forskriftsregulering til personopplysningsloven av spørsmål vedrørende fødselsnummer og biometri. I stedet mener jeg at særlige spørsmål bør bli regulert i lov og/eller forskrift til særlovgivning.

Fordi jeg forutsetter særlovgivning, mener jeg det er viktig at den sentrale begrepsbruken i all lovgivning innen feltet er forsvarlig harmonisert. Jeg har imidlertid ikke funnet noe godt utviklet begrepsapparat i eksisterende særlovgivning som kan danne mønster for begrepsbruken i personopplysningsloven.[152] Derfor har jeg valgt å stå forholdsvis fritt ved valg av begreper og formuleringer ellers. De begrepsmessige og systematiske valg som gjøres i personopplysningsloven, bør etter min mening gi føringer for tilsvarende valg i fremtidig særlovgivning. Jeg har imidlertid ikke hatt tid til å gjøre nærmere analyse av slike mulige hensyn.

7.1.3 Minimalitetsprinsippet som utgangspunkt

I europeisk/internasjonal personopplysningsrett eksisterer det et *minimalitetsprinsipp* dvs. et utgangspunkt om at behandling av personopplysninger ikke skal skje i større utstrekning enn det formålet eller formålene for behandlingen begrunner.[153] Samtidig er det imidlertid få begrensninger for hvilke formål som kan formuleres for behandling av personopplysninger som tilfredsstiller kravene til rettslig grunnlag mv.[154] Dersom det foreligger et saklig behov for identifisering og/eller autentisering vil det med andre ord være tillatt å behandle slike personopplysninger som er nødvendige for dette formålet, jf dog begrensningene i pol § 12 vedrørende bruk av fødselsnummer og biometri. Minimalitetsprinsippet setter med andre ord ikke i seg selv noen begrensning i adgangen til å ha identifisering og autentisering som formål.

Et underliggende premiss for personvernlovgivningen er at det beste personopplysningsvernet oppnås dersom det ikke finnes personopplysninger, for eksempel ved at opplysninger ikke er knyttet til bestemte identiteter. Det er derfor viktig for ivaretakelsen av personvernet at det om mulig ikke brukes identifikatorer, dvs. at opplysningene blir mer eller mindre anonyme. I helseregisterloven har dette hensynet slått igjennom ved at det i § 11 annet ledd, annen setning kreves at "Det skal alltid begrunnes hvorfor det er nødvendig å benytte personidentifiserbare

[152] Begrepsforklaringene i høringsnotatet til forslag om ny passlov er de eneste jeg har identifisert. De aktuelle definisjonene er imidlertid etter vår mening for omstendelige til å bli anvendt i personopplysningsloven, se begrepsoversikten i http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2005/Horing-forsalg-til-endringer-av-passloven-mm/3.html?id=98152.
[153] Prinsippet kommer bl.a. til uttrykk i personverndirektivet art. 6 første ledd bokstav c, samt i artiklene 7 og 8.
[154] Jf pol § 11 første ledd bokstav b, jf a.

opplysninger." Jeg mener en slik begrunnelsesplikt er bevisstgjørende og er en god retningslinje som kan sies å støtte opp under minimalitetsprinsippet (i utvidet forstand, jf ovenfor). Blant annet vil slik plikt kunne stimulere til å benytte roller mv som grunnlag for identifisering, snarere enn hele identiteter (jf avsnitt 2.2 og forslag i avsnitt 7.4).

7.1.4 En eller to bestemmelser?

Innledningsvis er det grunn til å spørre om det i det hele tatt er behov for bestemmelser som nåværende § 12 i personopplysningsloven og mer detaljerte og presise bestemmelser om fødselsnummer og biometri? Drøftelsen av saken vedrørende Tysvær kommunes bruk av biometri (avsnitt 4.3.3) illustrerer hvordan en i andre nordiske land løser spørsmål vedrørende biometri ved hjelp av de generelle bestemmelsene i personopplysningslovgivningen. Dette er åpenbart en mulighet også i Norge. Jeg er likevel ikke i tvil om at en særlig vurdering klart er å foretrekke. På den måten blir det tydelig at disse viktige personvernspørsmål er underlagt rettslig regulering, det blir lettere å forstå hvilke vurderinger som er avgjørende, og vurderingstemaene blir mer konkrete. Til sammen er det grunn til å tro at dette gir større forutberegnelighet.

I mandatet for denne utredningen bes det spesielt om vurdering av om dagens pol § 12 bør beholdes som én bestemmelse som både omfatter fødselsnummer og biometri, eller om disse to spørsmålene bør reguleres i hver sine bestemmelser. Etter min mening er den sist nevnte løsningen klart å foretrekke. Årsaken er primært at fødselsnummer og biometri for identitetshåndtering reiser forskjelligartede spørsmål. Fødselsnummer gjelder primært spørsmål om bruk av en identifikator innen offentlig og offentlig relatert virksomhet for sikkert og entydig å knytte opplysninger til enkeltpersoner, herunder å sammenstille opplysninger om enkeltpersoner. Identifiseringsspørsmålene i tilknytning til fødselsnumre er derfor primært knyttet til navnefunksjonen, dvs det å etablere og bruke en entydig binding mellom et individ og et identifikasjonsmiddel, jf avsnitt 2.2. I biometrisammenheng er identifisering primært aktuelt i betydningen å gjenkjenne personer blant flere mulige personer (i et en-til-mange forhold). Når det gjelder autentisering, dvs verifisering av en påstått identitet, er fødselsnummer lite egnet, mens dette er en hovedanvendelse for bruk av biometriske identifikatorer.

Selv om reguleringen av fødselsnummer og biometri for identitetshåndtering i personopplysningsloven i utgangspunktet bør plasseres som to separate bestemmelser, er slektskapet likevel så nært at bestemmelsene bør følge etter hverandre. I tillegg er det etter min mening behov for å gjøre endringer i enkelte andre spredte bestemmelser for å sikre tilstrekkelig effekt av hovedbestemmelsene, se om dette avsnitt 7.4.

7.2 Behov for endring av § 12 om fødselsnummer

7.2.1 Nærmere om behov og begrunnelse for forslag til endret lovregulering

Fødselsnummeret var i seg selv kontroversielt da det ble innført i 1964. Undersøkelser viser at nummeret fremdeles er kontroversielt i den forstand at mange mennesker mener det er viktig å beskytte fødselsnummeret mot innsyn/spredning. I den store personvernundersøkelsen i 2005 svarte hele 90% at det var veldig viktig (74%) eller litt viktig (16%) å beskytte personnummer[155]

[155] Undersøkelsen brukte ikke "fødselsnummer", dvs 11 siffer, kun "personnummer" som er de fem siste sifrene i fødselsnummeret. Svarene i undersøkelsen hadde neppe blitt særlig annerledes dersom "fødselsnummer" var brukt i stedet, fordi de to begrepene i stor grad oppfattes som synonyme i daglig tale.

mot innsamling og videre bruk.[156] Mange mente videre det var langt viktigere å sikre dette nummeret enn å sikre flere av de opplysningstypene som er spesielt beskyttet i dagens lovgivning ved at de er gjort sensitive, se pol § 2 nr. 8. Dersom en legger personvernprinsippet om rimelig og rettferdig behandling av personopplysninger til grunn,[157] er det grunn til å legge vekt på rimelige forventninger og samstemte oppfatninger i befolkningen. Slik sett kan dagens vern av fødselsnumre neppe sies å stå i et rimelig forhold til de ønsker om vern som en nesten unison befolkning synes å ha.

I tillegg til relativt dårlig rettslig beskyttelse av fødselsnumre, har det vært meget betydningsfulle tilfelle av brudd på gjeldende regler som har ført en meget stor mengde fødselsnumre med tilhørende personalia på avveie. Det er her nok å minne om en nylig skandale der Skattedirektoratet hadde sendt ut nesten 4 millioner fødselsnumre mv på cd-rom til 14 mediebedrifter, uten å oppdage fadesen før det var gått ca 6 uker. Selv om det i utgangspunktet ikke er grunn til å mistenke konkrete personer for å kopiere dette materialet, er det helt åpenbart så stor risiko for at dette kan ha skjedd at en ikke kan se bort ifra en slik mulighet. Dessuten kommer dette tilfellet i tillegg til annen, mindre omfattende ulovlig eksponering av fødselsnumre, der numrene har vært tilgjengelig for verden på Internett.[158]

Jeg mener det primært er grunn til å vurdere om i) det bør gjennomføres lovendringer som reduserer antall behandlingsansvarlige som lovlig kan ha tilgang til fødselsnumre, ii) om det bør legges restriksjoner på hva fødselsnumre kan brukes til, og iii) hvilke krav som bør gjelde for sikring av fødselsnumre.

***

Den primære funksjonen for fødselsnummeret er som unik identifikator for hver person i folkeregisteret og andre offentlige registre.[159] Funksjonen som identifikator innebærer muligheten for effektiv og trygg innhenting og sammenstilling av personopplysninger fra flere kilder. Også sammenstilling på grunnlag av andre opplysninger som navn og adresse gir muligheter for å sammenstille. Faren for feilskrift, manglende oppdatering av opplysninger ved navne- og adresseendringer mv, gjør imidlertid sammenstilling på grunnlag av navn mv langt mer usikker og kostbar.

Tidligere var kopling/samkjøring av personregistre, dvs sammenstilling av personopplysninger fra flere kilder, underlagt spesiell regulering. Hovedregelen var at det trengtes konsesjon fra Datatilsynet for at dette skulle være tillatt. [160] I tilfelle der det var gitt unntak fra konsesjonsplikt, var det i henhold til forskriften til personregisterloven kun gitt adgang til samkjøring av personregistre i spesielt angitte tilfelle. I personopplysningsloven er spørsmål om kopling og annen sammenstilling av personopplysninger ikke spesielt regulert, og er tillatt dersom de generelle kravene til behandling av personopplysninger er tilfredsstilte. Innsamling av

[156] Se Ravlum 2005, tabell 4.1.
[157] Jf. personverndirektivet art. 6 første ledd bokstav a og Europarådskonvensjonen om personvern art. 5 bokstav a.
[158] Således hadde for eksempel Universitetet i Oslo ca 3400 fødselsnumre og navn tilgjengelig for alle på Internett i en periode på ca to måneder, se http://www.universitas.no/nyhet/49165/.
[159] D-nummeret har en lignende funksjon, men jeg kommer ikke her spesielt inn på personvernmessige implikasjoner av dette nummeret. Jeg antar mange av de vurderinger jeg her gjør i forhold til fødselsnummeret også gjelder for D-nummeret.
[160] I den første perioden med personvernlovgivning ble det lagt liten vekt på selvbestemmelse og stor vekt på hva som generelt var ansett å være til folks beste. Derfor var begrensninger av tilgangen til personopplysninger et mål i seg selv, selv om registrerte personer ville kunne gå med på at personopplysninger ble gjort tilgjengelig.

personopplysninger og sammenstillingen mv av disse må med andre ord ha et rettslig grunnlag[161] (samtykke, lovhjemmel eller "nødvendig grunn"), skje for et bestemt formål,[162] tilfredsstille krav til opplysningskvalitet,[163] skje med tilfredsstillende informasjonssikkerhet[164] mv.

Bestemmelsen i pol § 12 og § 21 om bruk av personprofiler har direkte bakgrunn i den vide muligheten til å sammenstille personopplysninger som oppstod da det gamle regimet i personregisterloven ble erstattet med dagens mer liberale regulering. Personopplysningsloven § 12 reduserer muligheten for effektiv sammenstilling av personopplysninger fordi den begrenser muligheten for å bruke fødselsnummer, mens pol § 21 tar sikte på å redusere muligheten for at sammenstilling skal resultere i manipulerende henvendelser.[165]

Innenfor den behandlingsansvarliges egen organisasjon antar jeg at det som oftest er mulig å bruke interne kundenummer og/eller legge så stor vekt på riktige og oppdaterte navne- og adresseopplysninger, at disse blir egnet for tilstrekkelig sikker kopling *internt*. Fødselsnummeret er imidlertid særlig viktig dersom en skal kople opplysninger fra ulike eksterne kilder, dvs. kilder som ligger utenfor den behandlingsansvarliges kontroll.

Etter min mening er det relevant at besittelse av fødselsnummer også gir økt fare for ulovlig sammenstilling av personopplysninger. Den såkalte "virksomhetsundersøkelsen" fra 2005[166] viser generell meget dårlig etterlevelse av personopplysningsloven blant virksomheter i offentlig og privat sektor. Situasjonen gjør at en vanskelig kan forutsette at virksomheter kjenner til og etterlever de regler som gjelder. Jeg tror likevel at en restriktiv politikk med hensyn til bruk av fødselsnummer, vil kunne redusere muligheten for ulovlig sammenstilling av person-opplysninger. Årsaken er at en stor andel av befolkningen mener at fødselsnummeret er viktig for personvernet. Mange mennesker kan derfor forventes å være kritiske til krav om at nummeret skal registreres og stille spørsmål om lovligheten av bruken.[167] Forutsetningen for at folk flest kan ha slik kontrollfunksjon er imidlertid trolig at lovreguleringen vedrørende fødselsnummer blir mindre skjønnsmessig enn i dag, slik at folk sikrere kan gjøre seg opp en mening om hva som er tillatt.

Fødselsnummeret har bakgrunn i offentlig sektor, og er en viktig forutsetning for at forvaltningen skal kunne utføre sine oppgaver på tvers av en hierarkisk inndelt forvaltningsorganisasjon. Nummeret benyttes imidlertid også av private organisasjoner uavhengig av om dette er begrunnet i deres kontakt med det offentlige. Således anvender for eksempel flere nettbanker fødselsnummer som brukernavn ved innlogging til personlige banktjenester.

Det er etter min mening grunn til å vurdere en rendyrking av fødselsnummeret som et hjelpemiddel for offentlig sektor. Konsekvensen vil være at private bare kan bruke fødselsnummer der dette er nødvendig for sikker identifisering av personer som ledd i privates kommunikasjon med offentlige forvaltningsorganer og tjenesteytere. En videre konsekvens vil være at private ikke kan bruke fødselsnummer kun for sine interne formål eller i kommunikasjon

[161] Pol §§ 8 og 9, jf § 2 nr 7.
[162] Pol § 11 første ledd bokstavene b og c.
[163] Pol § 11 første ledd bokstavene d og e, jf § 14 første ledd.
[164] Pol § 13, jf personopplysningsforskriften kap. 2.
[165] Bestemmelsen fastsetter krav til varsling og informasjon ved bruk av personprofiler. Personprofiler forutsetter sammenstilling av opplysninger, for eksempel ved hjelp av fødselsnummer.
[166] Se Ravlum 2005b.
[167] Se nærmere om tallene fra undersøkelsen i avsnitt 7.2.1.

med andre private. En slik innstramning vil være i tråd med mange menneskers sterke vektlegging av fødselsnummerets betydning for personvernet.

En mulig innskrenkning av privates adgang til å bruke fødselsnumre uavhengig av offentlig sektor, vil skape behov for strengere krav til oppdatering av og kvalitetssjekk med navn og andre personalia som må benyttes som identifikatorer. Det kan trolig også bli større behov for å innføre kundenumre og andre identifikatorer i private virksomheter. Generelt vil kostnadene i tilknytning til autentisering av personer og kopling av personopplysninger innen privat sektor øke.

Til tross for at personvernhensyn etter min mening taler for å begrense bruken av fødselsnummer til offentlig sektor og utveksling av personopplysninger mellom privat og offentlig sektor, har jeg valgt ikke å fremme et konkret forslag om slik lovendring. Årsaken er primært at jeg ikke har oversikt over hvilke konsekvenser en slik endring vil få for private virksomheter. Jeg vil likevel anbefale at departementet ser nærmere på denne muligheten.

Selv om en ikke reduserer private virksomheters adgang til å bruke fødselsnumre, mener jeg det generelt er grunn til å gjøre vilkårene for å bruke fødselsnumre klarere og mindre skjønnsmessige enn i dag. Dette gjelder både offentlig og privat sektor. En mulig teknikk vil være mer detaljert å angi innholdsmessige vilkår for at fødselsnumre skal være nødvendige å bruke for å oppnå sikker identifisering. Jeg tror imidlertid dette vil være en lite farbar vei. Årsaken er at det er vanskelig å forutse de situasjoner som kan begrunne bruk av fødselsnummer. En annen tilnærming vil være å sette visse prosessuelle vilkår for lovlig bruk av fødselsnummer. Dette er etter min mening langt mer realistisk og kan dessuten skje på en måte som bygger på prosessuelle krav som allerede er del av personopplysningsloven med forskrifter (jf risikovurdering, se neste avsnitt).

Selv om fødselsnummer i mange tilfelle vil være lovlig å behandle, er det etter min mening behov for å forby bruk av slike numre til å autentisere identiteter på usikre måter. Et slikt forbud bør gjelde generelt innenfor personopplysningslovens virkeområde, og med andre ord være uavhengig av om den behandlingsansvarlige er del av offentlig eller privat sektor. Et forbud vil kunne redusere mulige skadevirkninger av at de fleste fødselsnumre, trolig på uopprettelig måte, er spredt til aktører som ikke burde ha tilgang til dem.

Til slutt vil jeg peke på det jeg mener er behov for bedre sikkerhetsrutiner knyttet til fødselsnumre. Dette gjelder spesielt for sikring av konfidensialitet. Jeg er ikke sikker på om fødselsnumre objektivt sett er spesielt mer beskyttelsesverdige enn enkelte andre opplysningstyper som i dag ikke er regnet som sensitive og derfor ikke har spesielt vern,[168] men mener det kan være grunn til å ta konsekvensen av at folk flest mener beskyttelse av fødselsnumre er viktig for ivaretakelsen av deres personvern. Det kan etter dette være behov for å endre reglene om informasjonssikkerhet, jf pol § 13 med tilhørende forskrifter.

7.2.2 Forslag til endret lovregulering vedrørende bruk mv av fødselsnummer

I utredningen vedrørende etterkontroll av personopplysningsloven i 2006, ble det foreslått endring av den rettslige reguleringen av fødselsnummer mv, jf avsnitt 7.1.1. Forslaget ble formulert på grunnlag av mandatet som la vekt på spørsmål om regelverksstruktur mv. Det ble

[168] Jf pol § 2 nr 8. Opplysninger om private økonomiske forhold er for eksempel ikke regnet som sensitive, samtidig som folk flest mener slike opplysninger er meget beskyttelsesverdige.

derfor ikke gjort noen selvstendig materiell vurdering av bestemmelsen. På bakgrunn av vurderingene i forrige avsnitt og mandatet for denne utredningen (jf avsnitt 1) vil jeg i tillegg til de strukturelle endringene som ble forslått i 2006, også foreslå visse innholdsmessige endringer:

> **§ 11. Bruk av fødselsnummer**
>
> Fødselsnummer kan bare brukes dersom det er saklig behov for sikker identifisering og bruk av fødselsnummer er nødvendig for å oppnå slik identifisering.
>
> Før fødselsnummer samles inn, må den behandlingsansvarlige ha gjennomført en risikovurdering som klart viser slik nødvendighet som nevnt i første ledd, jf § 13 og videre krav i forskrift til vurdering av risiko.
>
> Datatilsynet kan pålegge en behandlingsansvarlig å bruke fødselsnummer for å sikre mot at det kan skje personforveksling.
>
> Det er forbudt å benytte fødselsnummer som bevis for at en person er den han eller hun utgir seg for å være (autentisering), unntatt når det samtidig benyttes opplysninger som ikke er åpent tilgjengelige (koder, passord e.l.).
>
> Enhver forsendelse som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten.
>
> Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer.

Her vil jeg bare kommentere de elementene i lovteksten som er nye i forhold til utredningen fra 2006.

Første ledd innebærer en videreføring av gjeldende § 12 første ledd i personopplysningsloven. Det er imidlertid gjort en viktig presisering i annet ledd av hvorledes den behandlingsansvarlige må gå frem for å kunne konkludere med at bruk av fødselsnummer er nødvendig. Poenget er å innføre et krav til gjennomføring av slik risikovurdering som i dag fremgår av personopplysningsforskriftens § 2-4. Henvisningen til "§ 13 og videre krav i forskrift til vurdering av risiko" er imidlertid lite ideell, både fordi nødvendighetsvurderingen etter forslaget til § 11 ikke er en vurdering av informasjonssikkerhet i streng forstand, og fordi risikovurderingen ikke direkte fremgår av § 13, men av tilhørende forskriftsbestemmelse (§ 2-4). En henvisning til § 14 om internkontroll hadde alternativt vært mulig, men til denne bestemmelsen er det ikke gitt regler om risikovurdering. Lovens §§ 13 og 14 har så vidt jeg vet ikke vært evaluert. Etter min mening ville det vært mulig å endre ordlyden i disse bestemmelsene slik at kravet til risikovurdering fremgikk direkte av loven uansett om spørsmålet kan anses å gjelde informasjonssikkerhet eller internkontroll. Annet ledd i forslaget til § 11 annet ledd ville i så fall kunne uttrykkes enklere og klarere.

Datatilsynets kompetanse etter forslagets tredje ledd gjelder kun for å motvirke personforveksling og ikke som i dag sikring av opplysningskvalitet. Kvalitetsaspektet kan uansett ivaretas i samsvar med den generelle inngrepskompetansen i § 46 jf § 11 bokstavene d og e. Det er grunn til å mene at også Datatilsynets pålegg om bruk av fødselsnummer bør være basert på en risikovurdering, lignende den som den behandlingsansvarlige må foreta i medhold av forslaget til § 11 annet ledd.

I fjerde ledd er det foreslått et nytt forbud mot kun å benytte fødselsnummer for å autentisere identiteter. Etter forslaget kan nummeret fremdeles benyttes sammen med andre opplysninger som ikke er åpent tilgjengelige. Jeg tenker her primært på koder, passord og andre opplysninger som er ment å ha autentiseringsfunksjon. Derimot vil kombinasjon med åpne opplysninger som ikke er ment å ha slik funksjon være forbudt. Forslaget innebærer for eksempel at det ikke vil være lovlig å autentisere identiteter ved å spørre om fødselsnummer og boligadresse, personnavn

mv.[169] Forslaget kan indirekte bidra til å redusere skadefølgene av at et meget stort antall fødselsnumre har kommet på avveie. Særlig forslaget i fjerde ledd antas å ha betydning for muligheten til å gjennomføre identitetstyveri ved hjelp av fødselsnummeret.

Jeg gjør for ordens skyld oppmerksom på at forslaget ikke innebærer forbud mot å bruke fødselsnummer *vedrørende andre personer* ved krav om utlevering av åpne personopplysninger om disse personene, jf diskusjonen i avsnitt 6.2. Dette gjelder ikke "bevis for at personer er den han eller hun utgir seg for å være (autentisering)", men kun bruk av fødselsnummer som merke/navn for å angi en bestemt person. Et annet spørsmål er imidlertid om fødselsnummer alene bør være tilstrekkelig grunnlag for utlevering av personopplysninger i slike tilfelle. Jeg tror spørsmålet ofte må besvares med et nei, men den behandlingsansvarlige bør uansett ta konkret stilling til dette i tilknytning til etterlevelse av kravene i pol § 13 med forskrifter.

7.3 Behov for ny bestemmelse om biometriske metoder mv i personopplysningsloven

7.3.1 Nærmere om behov og begrunnelse for forslag til endret lovregulering

Datatilsynet har i brev til Justis- og politidepartementet den 31. mars 2006[170] fremmet forslag til nye bestemmelser i personopplysningsloven vedrørende biometri. Forslaget bygger i utgangspunktet på samme struktur som nåværende § 12, men i tillegg er det foreslått en egen bestemmelse om lagring av biometriske kjennetegn.

Jeg er grunnleggende enig med Datatilsynet i at det bør kunne være vid adgang til bruk av biometri når formålet kun er autentisering, og at det for øvrig bør gjelde strengere bestemmelser når formålet er identifisering, dvs. når biometri brukes for å bringe en ukjent persons identitet på det rene. Datatilsynet skjelner imidlertid ikke klart mellom ulike formål med bruk av biometri, men anvender både formål (i første ledd), spørsmål om sensitivitet (annet ledd), og lagring (tredje ledd). Jeg mener man klarere bør skjelne mellom formålene autentisering og identifisering, og stille tilleggskrav for hver av disse to kategoriene.

Datatilsynets forslag lyder slik:

> *§ 12a Biometriske kjennetegn/ biometri* (Ny paragraf)
> Biometriske kjennetegn /biometri kan bare nyttes når det er saklig behov for sikker identifisering eller bekreftelse av en påstått identitet og behandlingen er tillatt etter § 11.
>
> Behandling av biometriske kjennetegn/biometri som innebærer behandling av sensitive personopplysninger krever uten unntak konsesjon fra Datatilsynet. Øvrig behandling av biometriske kjennetegn skal meldes til Datatilsynet.
>
> Lagring av biometriske kjennetegn/ biometri hos den behandlingsansvarlige eller databehandlere kan bare skje
> a. med hjemmel i lov,
> b. med den registrertes samtykke og konsesjon fra Datatilsynet eller
> c. når det følger av personopplysningsforskriften.
>
> Datatilsynet kan pålegge en behandlingsansvarlig å bruke biometriske kjennetegn/biometri som nevnt i første ledd der dette anses nødvendig for sikker

[169] Men adresse kan selvsagt være passord, dvs adressen kan være svar på spørsmål om hva som er passord.
[170] Ref 06/00518 -1 /AFL.

identifisering eller bekreftelse av en påstått identitet og bruken er nødvendig av sikkerhetshensyn.

Kongen kan gi forskrift med nærmere regler om bruk av biometriske kjennetegn/ biometri.

Den foreslåtte lovteksten vil trolig være krevende å anvende og kan gi opphav til uklarheter og fare for dårlig etterlevelse. Datatilsynet legger tilsynelatende en noe annen begrepsbruk til grunn enn den jeg har anvendt i denne utredningen. Således står det i forklaringen av forslaget til § 12a: "Med identifisering menes bruk av biometriske kjennetegn der bruken knyttes opp mot tradisjonelt identifiserende opplysninger, for eksempel der fingeravtrykk kontrolleres opp mot fingeravtrykk lagret i et adgangskort med navn. I tillegg er det hensikten at identifisering skal omfatte bruk av biometriske kjennetegn i såkalte "anonyme løsninger", for eksempel brukt som alternativ til garderobelapp uten at det skjer noen registrering av andre tradisjonelt identifiserende opplysninger."

Det Datatilsynet her kaller "identifisering", vil etter min begrepsbruk være autentisering så lenge det gjelder bekreftelse av en påstått identitet. Enhver påstand om en bestemt identitet vil jo innebære at navn eller lignende røpes. I det Datatilsynet beskriver som "anonyme løsninger" foreligger det ingen påstand om en bestemt identitet, bare et tegn på at samme (ofte anonyme) person opptrer. I slike tilfelle vil det etter min mening per definisjon ikke foreligge personopplysninger, og forholdet vil derfor normalt falle utenfor personopplysningslovens virkeområde. Jeg viser for øvrig til det som er skrevet om autentisering mv av roller, se avsnitt 7.1.3, jf avsnitt 2.2.

Datatilsynets forslag bygger på en henvisning til de vilkår som følger av § 11, noe som innebærer en påminnelse om at krav til rettslig grunnlag i §§ 8 og 9, krav til formål i § 11 bokstavene b og c, og krav til opplysningskvalitet i § 11 bokstavene d og e, må være tilfredsstilte. Praksis fra Personvernnemnda (se avsnitt 3.1) viser etter min mening at saklighetskravet i dagens § 12 har meget liten betydning som skranke mot bruk av biometri, og jeg antar derfor at dette kriteriet vil ha ytterst liten effekt i en ny bestemmelse. Samtidig er henvisningen til nevnte krav i §§ 8, 9 og 11 uheldig. For det første er henvisningen indirekte ved kun å vise til § 11, som igjen viser videre til §§ 8 og 9 i § 11 bokstav a. For det andre kan det være misvisende å kun vise til § 11 når også lovens øvrige bestemmelser får anvendelse og betydning.

Forslaget stiller opp en ny konsesjonsplikt for "Behandling av biometriske kjennetegn/biometri som innebærer behandling av sensitive personopplysninger …" og meldeplikt for øvrig bruk av biometriske kjennetegn. Det er uklart om en tenker seg at bruken av biometriske opplysninger i seg selv kan innebære behandling av sensitive personopplysninger, for eksempel slik at ansiktsform, iris-mønstre eller lignende kan gi grunnlag for å slutte noe om personens helsetilstand. Jeg har ikke undersøkt om slike indikasjoner kan være mulig, men antar at et slikt kriterium uansett vil være krevende å praktisere. En annen forståelse av forslaget er at konsesjonsplikt skal gjelde dersom tilknyttede personopplysninger er sensitive. Sensitive personopplysninger er jo i utgangspunktet konsesjonspliktige etter § 33, og forslaget innebærer derfor at unntakene fra konsesjonsplikt i forskriften ikke skal gjelde dersom det er anvendt biometri som ledd i behandlingen av (bl.a.) sensitive personopplysninger. I så fall kan dette trolig formuleres klarere og enklere enn i forslaget.

Jeg er også skeptisk til plasseringen av regler om melde- og konsesjonsplikt som del av § 12a. Særlige bestemmelser om dette bør i størst mulig grad fremgå av §§ 31 - 35 der bestemmelser om dette for øvrig er plassert, eventuelt også i personopplysningsforskriften kap. 7.

For tilfelle der det skjer lagring av biometriske kjennetegn hos den behandlingsansvarlige og/eller databehandler, foreslår Datatilsynet at dette bare kan skje med lov- eller forskriftshjemmel, eventuelt konsesjon. Jeg kan ikke forstå at det kan skje bruk av biometri uten slik lagring, dvs uten innrullering av fingeravtrykk eller lignende i et biometrisk system som skal tjene som sammenligningsgrunnlag ved bruk, jf avsnitt 2.4.3 (ovenfor).

Fjerde ledd i Datatilsynets forslag gjelder tilsynets mulighet til pålegge bruk av biometri. At slikt pålegg skal kunne gis både i tilfelle av identifisering og autentisering gir mening. Det påfølgende kumulative kravet om at bruken av biometri skal være "nødvendig av sikkerhetshensyn", innebærer at slike pålegg må være knyttet til sikring av opplysningenes konfidensialitet, integritet og tilgjengelighet (jf § 13). Dermed faller hensynet til ivaretakelse av opplysningskvalitet ut, til tross for at dette er det eneste som i dag ivaretas i dagens § 12. Uansett kan imidlertid Datatilsynets vide kompetanse til å gripe inn i samsvar med § 46, sammenholdt med bestemmelser om informasjonssikkerhet, opplysningskvalitet mv,[171] sies å gi dekkende hjemmel for Datatilsynet til å gi pålegg.

Min konklusjon er etter dette at det ikke vil være hensiktsmessig å bygge på Datatilsynets forslag om ny bestemmelse vedrørende biometri. I neste avsnitt har jeg derfor valgt å fremme et selvstendig forslag. Forslaget er i stor grad preget av uttalelser fra Europarådets Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD).[172]

7.3.2 Forslag til endret lovregulering vedrørende bruk mv av biometriske metoder

Jeg mener, slik jeg også forstår Datatilsynet, at de viktigste personvernhensynene er knyttet til bruk av biometri for å identifisere/gjenkjenne personer. Med dette sikter jeg til situasjoner der en person ikke har påstått en bestemt identitet, men likevel blir identifisert ved hjelp av ansiktsgjenkjenning, fingeravtrykk, iris, DNA eller på andre måter. Situasjonen er med andre ord at mennesker forstyrres i situasjoner der de opptrer mer eller mindre anonymt.

Jeg mener samtidig at mulige identifiseringsformål gjelder så vidt mange og forskjelligartede situasjoner at det vil være uforsvarlig og uhensiktsmessig å forsøke og regulere disse tilfellene ved hjelp av én sentral bestemmelse i personopplysningsloven. Den hovedsakelige innsatsen på lovgivningsområdet bør derfor skje innen den aktuelle særlovgivningen. Hovedbegrunnelsen er at slike spørsmål er kontekstavhengige og må vurderes konkret. Spørsmålene er også i utgangspunktet kontroversielle og bør derfor være gjenstand for en informert og demokratisk debatt som ledd i lov- eller forskriftsarbeid. Mitt forslag til regulering av biometri for identifiseringsformål (se nedenfor, annet ledd), er av nevnte grunner gjort strengt, noe som vil skape et press i retning av særregulering. Jeg har imidlertid ikke gjennomgått særlovgivning og vurdert behov for særlige hjemler.

Når det gjelder autentiseringsformålene, har vi med en rekke forskjelligartede situasjoner å gjøre. Datatilsynet forslår et skille mellom tilfelle der personalia som knyttes til autentiseringsprosessen er lagret hos den behandlingsansvarlige eller hos den registrerte selv. Dersom den registrerte selv er bærer av biometriske data og andre personalia mv i et kort, må dette kortet etter det jeg forstår være utstedt av behandlingsansvarlige eller hos dennes databehandler. Dette gjelder både

[171] Jf. for eksempel §§ 11, 13 og 14.
[172] Se Europarådet 2005 og avsnitt 5.5 (ovenfor).

ved første gangs utstedelse og dersom kortet blir mistet eller ødelagt. En behandlingsansvarlig og/eller databehandler må derfor *uansett* ha registerert/lagret denne informasjonen. Jeg antar det derfor ikke er holdbart å bruke lagring som et hovedkriterium i reguleringen.

I stedet for lagring vil jeg foreslå at loven bruker angir hvilke opplysningstyper som kan knyttes til autentiseringen. Lett adgang til bruk av biometri for autentiseringsformål bør etter min mening være begrenset til å gjelde tilfelle der kun relevant personalia om den aktuelle personen blir lagret. Jeg er åpen for at andre opplysningstyper enn de jeg har forslått bør kunne godtas, men mener reguleringen på dette punktet bør være streng. Forslaget mitt innebærer at det blir forbudt å kople opplysningene som brukes i autentiseringsrutiner med andre opplysninger som den behandlingsansvarlige har, se tredje ledd bokstav b. Autentiseringsrutinen for adgangskontroll i et treningsstudio kan etter dette ikke koples til opplysninger om hvem som har betalt medlemsavgift, for på den måten å stoppe personer som ikke har betalt.

> **§ 12 Biometriske metoder og identiteter**
>
> Med biometriske metoder menes her enhver innsamling og videre bruk av personopplysninger som skjer ved å måle egenskaper ved personers fysiologi eller adferd.
>
> Bruk av fingeravtrykk og andre biometriske metoder for å avdekke en persons identitet (identifisering), er ikke tillatt med mindre dette klart er hjemlet i lov.
>
> Innsamling og bruk av fingeravtrykk og andre biometriske mønstre for å finne ut om en bestemt person er den han eller hun selv utgir seg for å være (autentisering), er tillatt når dette
>
> a) klart er hjemlet i lov eller det foreligger samtykke, og
> b) det ikke er koplet andre opplysninger til behandlingen enn de som følger av lovhjemmelen eller må anses som nødvendige for å autentisere personen.
>
> Samtykke etter tredje ledd skal samsvare med kravene i § 2 nr 7. Informasjonen som gis skal være i samsvar med § 19. Samtykket kan bare anses som frivillig dersom det eksisterer alternative fremgangsmåter til bruk av biometriske metoder som ikke innebærer vesentlige ulemper for den som ikke samtykker.

Definisjonen av biometriske metoder er tatt inn i § 11 fordi dette er den eneste bestemmelsen der begrepet er foreslått anvendt i personopplysningsloven. Definisjonen er videre formulert enn det direkte behovet i loven tilsier, ved at formålet med bruken av biometriske metoder er holdt utenfor selve definisjonen i første ledd og i stedet er tatt inn i handlingsreglene i andre og tredje ledd ("for å …"). Dette gir en kortfattet definisjon og bidrar til å fremheve de to formålene. Som nevnt i avsnitt 2.4.2 kan biometri i ordets generelle betydning anvendes for flere formål enn det som er knyttet til menneskers identiteter, og det er derfor viktig å fremheve de aktuelle formålene.

Både i andre og tredje ledd av forslaget til § 12 er fingeravtrykk brukt som eksempel på biometriske metoder som kan fremme formålene identifisering og autentisering. Dette er valgt fordi jeg antar fingeravtrykkteknologi vil være blant de mest vanlige teknologiene på området. Samtidig er det klart at enhver biometrisk teknologi som kan fremme formålene i annet og tredje ledd er omfattet av bestemmelsen, og gir derfor rom for betydelig teknologisk utvikling.

Forslaget innebærer regulering av en rekke tekniske løsninger, bl.a. tilfelle der biometrisk informasjon er lagret på RFID-brikke. Bestemmelsen tar derimot ikke sikte på å omfatte annen bruk av RFID og lignende teknologier med identifiseringsøyemed, dvs teknologi som innebærer at en fester en elektronisk brikke/sender med andre identifikatorer enn biometri til mennesker for identifiserings- eller autentiseringsformål (for eksempel ved å feste til kroppen eller integrere i kroppen på annen måte). Jeg har heller ikke foreslått en egen bestemmelse for slike tilfelle.

Årsaken er primært at jeg anser spørsmål som bare gjelder RFID for å falle uten for mandatet. På den annen side mener jeg det bør være et generelt forbud mot slik bruk av RFID, også innen rent private forhold og uansett om formålet er knyttet til ytringsfrihet, jf. unntakene for personopplysningslovens saklige virkeområde i §§ 3 og 7. Spørsmålet krever uansett en nærmere vurdering, bl.a. i forhold til eksisterende bestemmelser i straffeloven, og forholdet til forskrift til lov om straffegjennomføring,[173] kapittel 7 om straffegjennomføring med elektronisk kontroll. Selv om jeg bestemt mener det rettslige utgangspunktet bør være forbud, er jeg i tvil om den mest hensiktsmessige lovtekniske løsningen.

Jeg mener det er viktig å benytte alminnelige ord for å uttrykke identifisering og autentisering, samtidig som disse begrepene settes i parentes som stikkord for personer med fagkunnskaper på området. Kun bruk av autentisering vil trolig gjøre bestemmelsen vanskelig å forstå for mange mennesker. Dessuten er autentisering brukt alene strengt tatt upresist, bl.a. fordi dette ikke bare er identiteter som kan være autentiske, men også for eksempel roller, jf avsnitt 2.2 (ovenfor).

Annet ledd fastsetter i utgangspunktet et forbud mot bruk av biometriske metoder for å identifisere personer, dvs for å fastslå identitet til personer som ikke selv har identifisert seg. Her må det trekkes en grense mellom identifiserings- og autentiseringstilfellene. Jeg foreslår at grensen trekkes ved først klart å definere autentiseringstilfellene. Forslaget i tredje ledd beskriver dette som "å finne ut om en bestemt person er den han eller hun selv utgir seg for å være". Avgjørende her er hva som legges i det å utgi seg for å være en bestemt person. Jeg mener disse tilfellene bare bør omfatte tilfelle der personen selv klart fremsetter en påstand om identitet, og ikke de tilfellene der personen kun gjennom sin adferd opptrer under forutsetning av at han er en bestemt person eller tilhører en avgrenset krets av personer. Personer som oppholder seg i lokaler med adgangsbegrensning vil for eksempel ikke kunne være gjenstand for autentisering fordi personen ikke direkte har presentert seg som en person med lovlig tilgang til lokalet. Andres påstand om en persons identitet skaper ikke en autentiseringssituasjon. Identifiseringstilfellene kan etter dette avgrenses til situasjoner der en forsøker å fastslå en persons identitet uten at denne personen selv direkte har fremsatt en påstand om sin identitet.

Forutsetningen for bruk av biometri for autentiseringsformål (tredje ledd) bør etter min mening være at det på forhånd er innhentet samtykke fra personer som er omfattet av ordningen og som det derfor er innhentet et fingeravtrykk eller lignende fra. Konkretiseringen av samtykkekravene vedrørende informasjon og frivillighet er viktige, og trolig en forutsetning for at samtykkekrav vil ha særlig reell betydning. Uten slikt samtykke bør det etter min mening ikke være mulig å bruke annet rettslig grunnlag enn lovhjemmel. "Nødvendighetsgrunnene" som er regnet opp i § 8 bokstavene a - f og § 9 bokstavene a - h, bør ikke kunne tjene som grunnlag fordi de er for åpne og skjønnspregede og derfor trolig vil innebære et lettvint grunnlag som mange behandlingsansvarlige vil bruke.

I en del tilfelle vil det kunne være personer som ikke ønsker å samtykke, men som likevel ønsker å benytte en tjeneste eller lignende som den biometriske metoden er knyttet til. Enkelte flypassasjerer vil for eksempel ikke ønske å benytte biometri for å knytte bagasjen til egen person. I slike tilfelle mener jeg det er viktig å sikre en reell valgmulighet ved at den behandlingsansvarlige pålegges å gi tilbud til denne gruppen som ikke innebærer vesentlige ulemper. Jeg viser her til Europarådet 2005 som i punkt 12 bl.a. uttaler at: "If, as a result of a biometric system, a data subject is rejected, the controller should, on his or her request, re-examine the case and should, where necessary, offer appropriate alternative solutions." Jeg

[173] Se forskrift av 22. februar 2002 nr 183.

mener slike alternative fremgangsmåter bør kunne kreves selv om det ikke skjer uriktig avvisning av en person.

Jeg har ikke foreslått at identifisering av personer skal kunne skje på basis av samtykke, se forslaget til tredje ledd. Årsaken er at slik bruk av biometri vil være inngripende, samtidig som det kan være vanskelig - generelt - å påstå at det reelt sett vil foreligge mulighet for å gjøre frie og informerte valg for den enkelte. Samtidig vil jeg ikke avvise at samtykke bør kunne brukes innen avgrensede saksområder, men dette bør i så fall reguleres/hjemles i særlovgivning.

7.4 Øvrige spørsmål vedrørende personopplysningsloven

I dette avsnittet vil jeg kortfattet foreslå enkelte spredte bestemmelser som jeg mener er nødvendige for å få tilstrekkelig sammenhengende og dekkende regulering av fødselsnummer og biometri i personopplysningsloven.

Legaldefinisjon av biometriske opplysninger

"Biometriske opplysninger" er foreslått anvendt i ny § 28a og ny § 49 tredje ledd, se nedenfor. Jeg antar derfor det bør tas inn en definisjon av dette begrepet i sammenheng med de øvrige legaldefinisjonene i loven som anvendes i mer enn én bestemmelse.

Jeg foreslår følgende definisjon:

> "Med biometriske personopplysninger forstår en i denne loven; opplysningstyper som gjelder målbare egenskaper ved en persons fysiologi eller adferd."

Definisjonen er tilpasset definisjonen av biometrisk metode i forslaget til § 12 første ledd, se forrige avsnitt.

Dersom en slik bestemmelse skal settes inn i det radikale lovforslaget i Schartum og Bygrave 2006,[174] bør definisjonen inn i § 2 tredje ledd. De fire første leddene[175] vil da lyde:

> **"§ 2. Personopplysning og personregister**
>
> Med personopplysning forstår en i denne loven: opplysninger og vurderinger som direkte eller indirekte kan knyttes til en levende, identifiserbar, fysisk enkeltperson.
>
> Med sensitive personopplysninger forstår en i denne loven; opplysningstyper som er egnet til å åpenbare
>
> 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.
>
> Med biometriske personopplysninger forstår en i denne loven; opplysningstyper som gjelder målbare egenskaper ved en persons fysiologi eller adferd.
>
> Personopplysninger kan komme til uttrykk som skrift, bilde, lyd eller andre signaler.
> […]"

Dersom en i stedet velger å videreføre nåværende system med legaldefinisjoner i pol § 2, bør definisjonen føyes til som § 2 nr 9. I så fall bør ordlyden endres noe i tråd med de någjeldende legaldefinisjonene og det moderate lovforslaget:[176]

---

[174] Se s 190.

[175] Øvrige ledd i forslaget forskyves tilsvarende.

Biometriske personopplysninger; opplysningstyper som gjelder målbare egenskaper ved en persons fysiologi eller adferd.

Plikt til å begrunne hvorfor behandling av personidentifiserbare opplysninger er nødvendig

Det er som nevnt et viktig poeng å unngå at det uten nødvendig grunn samles inn og behandles personopplysninger. Således vil det kunne foreligge muligheter for å anonymisere opplysningene og i stedet for eksempel autentisere i forhold til roller, se avslutningen av avsnitt 2.2. Helseregisterloven (hrl) har i § 11 annet ledd, annen setning en bestemmelse som er ment å motvirke unødvendig behandling av helseopplysninger: "Det skal alltid begrunnes hvorfor det er nødvendig å benytte personidentifiserbare opplysninger." Jeg mener det kan være grunn til å ta inn en lignende bestemmelse for på den måten å sikre en moderat praksis, bl.a. i forhold til bruk av biometriske metoder, jf forslaget til pol § 12. Tilsvarende bestemmelse som i helseregisterloven kunne for eksempel tas inn som siste setning i pol § 14 første ledd:

> **§ 14. Internkontroll**
> Den behandlingsansvarlige skal 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. Det skal alltid begrunnes hvorfor det er nødvendig å benytte personidentifiserbare opplysninger.
> […]

Sletting av biometriske opplysninger

Regulering av biometriske systemer kan etter mitt syn ikke begrenses til spørsmål om registrering (jf innrullering, avsnitt 2.4.3) og videre aktiv bruk av opplysningene. I tillegg må en regulere "utrullering", dvs sletting av biometriske opplysninger fra aktuelle systemløsninger. Dette gjelder for det første tilfelle der formålet ikke lenger tilsier lagring, jf pol § 28. Her er det neppe grunn til å ha særlige regler for biometriske opplysninger. Når det imidlertid gjelder opplysninger vedrørende døde personer, kan fortsatt eksistens av disse tenkes å gi misbruk og identitetstyveri. Jeg antar for eksempel at det kan være mulig å lage latex-avtrykk eller lignende av fingeravtrykk og således brukes avdødes identitet. Uansett antar jeg det ikke kan være noen særlig grunn til å beholde biometriske opplysninger om avdøde personer annet enn i sammenhenger der det uansett gjelder særlige regler (for eksempel når det gjelder pass, og for flyktninger og asylsøkere).

> **§ 28a Sletting av biometriske opplysninger**
> Biometriske opplysninger skal alltid slettes når vedkommende person dør. Den behandlingsansvarlige skal minst fire ganger hvert år oppdatere sine opplysninger i forhold til det sentrale folkeregisteret for å sikre at dødsfall fører til slik sletting.

Det er mulig det også vil være behov for klarere generelle slettingsregler for fødselsnumre enn det som følger av § 28 og er fastsatt i medhold av folkeregistreringsloven. Jeg har imidlertid ikke tilstrekkelig grunnlag for å mene noe bestemt om dette, og avstår derfor fra å fremme forslag.

Forholdet til pol § 48 om straff

---

[176] Se Schartum og Bygrave 2006, s 208.

Forslaget til bestemmelser i §§ 11 og 12 (ovenfor) er gjort så konkrete at overtredelse kan belegges med straff. Ulovlig bruk av biometri og fødselsnummer er uansett så inngripende for den enkelte at slike lovbrudd bør anses som klart straffverdige. Jeg vil derfor foreslå at pol § 48 endres slik at §§ 11 og 12 i mitt forslag settes inn i dagens § 48 første ledd bokstav e:

> "(e) behandler personopplysninger i strid med *§ 11, § 12,* § 13, § 15, § 26 eller § 39, eller" (vår kursiv).

Jeg gjør for ordens skyld oppmerksom på at de øvrige paragrafnumre i oppregningen ovenfor er slik den i dag står i loven, og det er ikke tatt hensyn til foreliggende forslag til lovendringer ellers.

Forholdet til pol § 49 om erstatning

Hovedregelen i personopplysningslovens erstatningsregler er skyldansvar med omvendt bevisbyrde, se § 49 første ledd. For kredittopplysninger er et objektivt ansvaret lagt til grunn. Jeg mener ansvaret for enkelte lovstridige handlinger vedrørende fødselsnummer og biometri som har stort skadepotensiale for personvernet, også bør omfattes av objektivt ansvar. Dagens pol § 49 annet ledd lyder:

> "Behandlingsansvarlige som formidler kredittopplysninger og som har meddelt opplysninger som viser seg uriktige eller åpenbart misvisende, skal erstatte skade som er oppstått som følge av den feilaktige meddelelsen, uten hensyn til om skaden skyldes feil eller forsømmelse på den behandlingsansvarliges side."

Jeg foreslår at det dessuten føyes til et nytt tredje ledd i § 49:

> "Erstatningsansvar uten feil eller forsømmelse på den behandlingsansvarliges side gjelder også for skade som har oppstått ved at fødselsnummer (11 siffer) eller biometriske opplysninger har blitt tilgjengelig for personer eller automatiserte informasjonssystemer som ikke har lovlig tilgang til slike opplysninger.

Samtidig blir dagens tredje ledd nytt fjerde ledd.

Bestemmelsen innebærer strenge krav til sikring, og plasserer den økonomiske risikoen for utilstrekkelig sikkerhet mot konfidensialitetsbrudd helt og fullt på den behandlingsansvarlige. Bestemmelsen er ment å dekke hele spekteret fra uautorisert manuell utlevering til én person, til masseoverføring ved hjelp av maskinelle rutiner/hjelpemidler til en ubestemt krets av personer og/eller systemer. Skadeomfanget kan således være lite eller veldig stort. Bestemmelsen er ment å gjelde uansett om kommunikasjonen skjer mellom mennesker eller automatiserte informasjonssystemer. Således dekkes for eksempel tilfelle der programmer ("roboter") trenger seg inn i informasjonssystemer via Internett og på den måten skaffer seg ulovlig tilgang til fødselsnumre eller biologiske mønstre. Den dekker også tilfelle der utvekslingen skjer mellom mennesker, og alle tilfelle der menneske og maskin er i hver sin ende av kommunikasjonen.

Forslagene til endringer av pol §§ 48 og 49 er også begrunnet ut i fra behovet for tiltak som kan demme opp for identitetstyverier. Jeg har ikke vurdert relevante deler av straffelovgivningen som gjelder ulovlig og falsk bruk av identitet, men mener det likevel er grunn til å fremheve at utilstrekkelig sikring av identitetsmidler mv legger til rette for slik alvorlig svindel. Bestemmelser om straff og erstatning som kan bidra til høyere aktsomhetsnivå hos behandlingsansvarlige som bruker slik informasjon, kan derfor antas å ha en god preventiv effekt i forhold til identitetstyveri.

7.5 Mulige økonomiske og administrative konsekvenser av lovforslagene

De økonomiske og administrative konsekvensene av forslagene i avsnittene 7.2.2 og 7.3.2, er trolig av ganske ulik karakter. Den reduserte adgangen til å gjøre bruk av fødselsnummer som er foreslått i avsnitt 7.2.2, vil kunne innebære ekstra utgifter for virksomheter som ikke kan fortsette å anvende fødselsnummer til autentiseringsformål, men må etablere mer betryggende rutiner, jf forslaget til § 11 fjerde ledd.

De foreslåtte endringene vil trolig ha positive effekter ved at de reduserer muligheten for identitetstyveri.[177] Dette gjelder særlig forbudet mot å bruke fødselsnummer for autentiseringsformål og redusert bruk av fødselsnummer som følge av nye prosessuelle krav, jf § 11 annet ledd. Også slike virkninger er imidlertid meget usikre, og det er særdeles vanskelig å fastslå om dette vil gi en samfunnsøkonomisk gevinst, og i tilfelle hvor stor denne gevinsten vil være.

Begrensningene i bruk av biometri har antagelig minst direkte innvirkning fordi bruken fremdeles er lite omfattende. Virksomheter som ønsker å ta i bruk biometriske autentiseringsmetoder vil imidlertid få noe høyere utgifter på grunn av kravet om alternative fremgangsmåter til bruk av slike metoder, se forslaget til § 12 fjerde ledd. Det er imidlertid ikke mulig å si noe generelt om dette kun vil redusere effektiviseringsgevinster som uansett følger innføring av biometri, eller om det samlet sett vil innebære en utgift.

Generelt kan en også anta at de foreslåtte bestemmelsene i større grad kan gi tillit og sikkerhet, og dermed større grad av villighet til å godta bruk av lovlig biometri og fødselsnummer. Også slike mulige effekter kan ha en positiv økonomisk verdi.

Forslagene gir ikke Datatilsynet eller andre nye tilsynsoppgaver, og det er neppe mulig å beregne noen direkte administrativ effekt verken for Datatilsynet, Personvernnemnda eller andre myndigheter.

[177] Dvs for uautorisert innsamling, besittelse, overføring, reproduksjon eller annen manipulering av annen persons personlige informasjon med den hensikt å begå svindel eller annen kriminell handling som involverer bruk av falsk identitet, jf. Lawson 2008.

Litteratur og kilder

- Alterman 2003. Anton Alterman; A Piece of Yourself: Ethical Issues in Biometric Identification, *Ethics and Information Technology*, 2003, bind 5, s. 139–150.
- Artikkel 29 arbeidsgruppen 2003. Artikkel 29 arbeidsgruppen, "Working document on biometrics", 12168/02/EN/final, WP80 (01.08.2003), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf.
- CIPPIC 2008. Canadian Internet Policy and Public Interest Clinic, Internettsider oktober 2008, tilgjengelig fra http://www.cippic.ca/en/.
- Europarådet 2005. Europarådets Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD). Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005).
- FAD 2008. Fornyings- og administrasjonsdepartementet; Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, Fornyings- og administrasjonsdepartementet 2008. Tilgjengelig fra http://www.regjeringen.no/nb/dep/fad/dok/Lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/1.html?id=505874.
- Hornung 2007. Gerrit Hornung; The European Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards. Paper to the European Consortium of Political Research Joint Sessions of Workshops: Privacy and Information: Modes of Regulation, Helsinki 2007.
- Jain et al 2004. A.K.; Ross, A.; Prabhakar, S.; An introduction to biometric recognition. Circuits and Systems for Video Technology, IEEE Transactions on Volume 14, Issue 1, Jan. 2004 Page(s):4 - 20, referred in Wikipedia. http://en.wikipedia.org/wiki/Biometrics, 10.09.2008.
- JD 2007. Justis- og politidepartementet: Nasjonalt ID-kort. Sluttrapport, februar 2007.
- Lawson 2008. Philippa Lawson; Powerpoint-presentasjon om "Identity Theft", Canadian Internet Policy and Public Interest Clinic, University of Ottawa.
- MOD 2005. Moderniseringsdepartementet; Kravspesifikasjon for PKI i offentlig sektor, januar 2005. Tilgjengelig fra http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/Rapporter/2004/Kravspesifikasjon-for-PKI-i-offentlig-se.html?id=106067&epslanguage=NO
- NOU 1997: 19: Et bedre personvern.
- Olsen 2008. Thomas Olsen; Personvernøkende teknologi og identitetsforvaltning, notat i tilknytning til møte i Personvernkommisjonen, Avdeling for forvaltningsinformatikk, 5. juni 2008.
- Ot.prp. nr. 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven).
- Ravlum 2005. Inger-Anne Ravlum; Setter vår lit til Storebror ... og alle småbrødre med?, Transportøkonomisk institutt, TØI-rapport 789/2005.
- Ravlum2005b. Inger-Anne Ravlum; Behandling av personopplysninger i norske virksomheter. En spørreundersøkelse om personvern og personopplysningsloven, Transportøkonomisk institutt, TØI-rapport 800/2005.
- Rt 1996 s 1114.
- Schartum og Bygrave 2004. Dag Wiese Schartum og Lee A Bygrave; Personvern i informasjonssamfunnet, Fagbokforlaget 2004.
- Schartum og Bygrave 2006. Dag Wiese Schartum og Lee A. Bygrave; Utredning av behov for endringer i personopplysningsloven: Utredning skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet, Justis- og politidepartementets rapportserie 2006. Tilgjengelig fra http://www.personvern.uio.no/pvpn/artikler/utredning_personopplysningsloven.pdf.
- Wei and Li 2006. Gang Wei and Dongge Li; Biometrics: Applications, Challences and Future, I: Strandburg and Raicu (eds.)Privacy and Technologies of Identity. A Cross-Disciplinary Conversation, Springer , New York, 2006.
- Wikipedia 2008. http://en.wikipedia.org/wiki/Biometrics, 10.09.2008.

I tillegg er det benyttet en rekke referanser til nyhetsoppslag mv på Internettsider. Disse er ikke ført opp i referanselisten, og jeg henviser derfor til fotnoteapparatet.

Vedlegg

Mandat for utredning av behovet for endringer i personopplysningsloven § 12

1 Bakgrunn

Lov om behandling av personopplysninger (personopplysningsloven) 31. mars 2000 nr. 31 trådte i kraft 1. januar 2001 sammen med forskrifter til loven. Formålet med loven er å beskytte den enkeltes personvern ved behandling av personopplysninger. Loven gjennomfører Europaparlamentets og rådets direktiv 95/46/EF om beskyttelse av personopplysninger (EU-direktivet) i norsk rett. I Ot. prp. nr. 92 (1998-1999) side 100 ble det understreket at reglene skal anvendes på en teknologi som er i stadig utvikling. I forbindelse med vedtakelsen av loven bestemte Stortinget at det skulle finne sted en etterkontroll som skulle påbegynnes fire år etter at loven trådte i kraft (se Innst. O. Nr. 51 (1999-2000) side 26).

En del av spørsmålene i etterkontrollen er av en slik art at Justisdepartementet, som har ansvaret for personopplysningsloven, og Fornyings- og administrasjonsdepartementet, som har ansvaret for forskriftene til loven, har bedt ekstern ekspertise på fagfeltet utrede enkelte spørsmål før et forslag om lov- og forskriftsendringer sendes på høring. På denne bakgrunn avga professor dr. juris Dag Wiese Schartum og førsteamanuensis dr. juris Lee A. Bygrave etter oppdrag fra JD 8. juli 2005, rapporten ”Utredning av behov for endringer i personopplysningsloven”. I ettertid har det vist seg at det også er ønskelig å få vurdert behovet for endringer i personopplysningsloven § 12 om bruk av fødselsnummer mv. Departementet ber Schartum og Bygrave om å utrede spørsmålene som er omtalt i det følgende. (Som sist står utrederne fritt til å dele arbeidet mellom seg slik de finner det hensiktsmessig.)

Mandatet har vært forelagt for Fornyings- og administrasjonsdepartementet og Datatilsynet.

2 Kort om gjeldende rett mv.

Personopplysningsloven § 12 gjelder bruk av fødselsnummer mv. og lyder:

Fødselsnummer og andre entydige identifikasjonsmidler, kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering. Datatilsynet kan pålegge en behandlingsansvarlig å bruke identifikasjonsmidler som nevnt i første ledd for å sikre at personopplysninger har tilstrekkelig kvalitet.
Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer og andre entydige identifikasjonsmidler.

Bakgrunnen for bestemmelsen og bruken av fødselsnummer for sikker identifisering er omtalt i NOU 1997: 19 Et bedre personvern, side 85:

”Fødselsnummer har vært i bruk siden 1964. Fødselsnummeret gir en stor grad av sikkerhet for at personer ikke forveksles. Det er av betydning for en effektiv saksbehandling som bygger på korrekte personopplysninger. På den annen side er fødselsnummeret en nøkkel til de personopplysninger som er samlet i et register, og det er en enkel nøkkel til kobling/samkjøring av opplysninger fra forskjellige registre.

Hovedbegrunnelsen for å innføre fødselsnummeret var et ønske om en enkel og entydig identifikasjon for å lette samordning/sammenstilling og utveksling av informasjon om

enkeltpersoner når dette var nødvendig eller ønskelig ut fra oppgavene institusjonen/bedriften var pålagt.

I debatten om fødselsnummer så langt har det vært en betydelig sammenblanding av begrepene identifikasjon og legitimasjon. Med identifikasjon menes at fødselsnummeret på en relativt entydig måte peker ut en bestemt person. Dette er den funksjonen fødselsnummer primært bør ha. I visse sammenhenger har imidlertid fødselsnummeret blitt sett på som legitimasjon, dvs sannsynliggjøring av at en enkeltperson er den han utgir seg for å være. Fødselsnummer er imidlertid ikke egnet til å tillegges slike legitimasjonsvirkninger, noe som blant annet har ført til en rekke brudd på taushetsplikt fordi taushetsbelagte opplysninger er blitt gitt ut når et fødselsnummer er blitt oppgitt."

Og i Ot.prp. nr. 92 (1998-1999), side 114:

"Bestemmelsen gir en generell regulering av bruk av fødselsnummer og andre entydige identifikasjonsmidler som for eksempel fingeravtrykk og andre biometriske data. Slike identifikasjonsmidler bør ikke benyttes i utrengsmål. Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som f eks navn, adresse og kundenummer ikke er tilstrekkelige. Det vil også ha betydning hvor viktig sikker identifisering er for den registrerte, dvs hvilke konsekvenser en forveksling kan føre til. Også samfunnets behov kan tillegges vekt."

Datatilsynet har i henvendelse til departementet 31. mars 2006 (vedlagt) gitt uttrykk for at dagens lovgivning vanskelig lar seg anvende på saker om bruk av biometriske kjennetegn/data. Datatilsynet har i brevet lagt fram et forslag til endringer av personopplysningsloven § 12. Forslaget går i grove trekk ut på å skille ut en egen bestemmelse om bruk av biometriske kjennetegn/data fra dagens bestemmelse, som i hovedsak er utformet med tanke på bruk av fødselsnummer.

Senere har Personvernnemnda truffet flere vedtak om biometri og personopplysningsloven § 12, som etter departementets oppfatning gir en viss avklaring. Personvernnemnda har lagt til grunn at når bruken av fingeravtrykk faller inn under personopplysningsloven § 12, omfatter bestemmelsen også bruk av fingeravtrykk til autentisering etter at identifisering har funnet sted, fordi autentisering er en bruk som omfattes av sikker identifisering. (Forskjellen mellom identifisering og autentisering/legitimering er kort forklart i forarbeidene til personopplysningsloven som er gjengitt foran.) Nemndas forståelse av § 12 åpner for bruk av fingeravtrykk til legitimasjonsformål der det foreligger saklig behov og bruken er nødvendig. Praksisen så langt tyder på at kravet om saklig behov nokså enkelt vil være oppfylt, og at det er proporsjonalitetsvurderingen – kravet om at bruken skal være nødvendig – som utgjør en reell skranke.

I saken om Tysvær kommune (2006/7) uttalte Personvernnemnda (på side 12):

"Nemnda vil ikke unnlate å peke på at selv om loven må tolkes slik at både fødselsnummer og fingeravtrykk, på bakgrunn av forarbeidenes uttrykkelige eksemplifisering, må anses for å være entydige identifikasjonsmidler, er det store forskjeller på de to tilfellene. Nemnda stiller seg kritisk til hvorvidt det er ønskelig å regulere de to tilfellene på samme måte, særlig når dette bare har grunnlag i en enkel setning i forarbeidene uten nærmere utredning av konsekvenser. Biometriske metoder til bruk for identifikasjon eller autentisering har vært i sterk utviking siden loven ble vedtatt. Nemnda har merket seg at Datatilsynet har fremmet forslag om særlig regulering av biometriske metoder, og stiller seg sterkt positiv til at dette blir gjort, og blir gitt prioritet i revisjonsarbeidet."

3 Oppdraget

Utrederne bes vurdere behovet for lovendringer som tydeliggjør forskjellene mellom fødselsnummer og biometriske kjennetegn/data. Utrederne skal vurdere om det er naturlig å ha separate paragrafer i loven i stedet for en felles bestemmelse som i dag.

Det er grunn til å tro at løsninger som inkluderer bruk av biometri til sikkert å bekrefte identitet, vil øke i omfang, og at de mulighetene som ligger i dette, vil bli ønsket tatt i bruk i stadig flere sammenhenger. Utrederne skal beskrive de teknologiske løsningene og forsøke å angi på hvilke bruksområder denne teknologien er aktuell. Det er ønskelig å få klargjort de personvernmessige konsekvensene av at biometriske løsninger tas i bruk. Utrederne bes gi en redegjørelse for hvilke hensyn og vurderingstema som bør være avgjørende for om bruk av biometriske kjennetegn/data skal aksepteres i det enkelte tilfelle, og sørge for at dette gjenspeiles i eventuelle forslag til lovendringer. Departementet ønsker også en vurdering av om biometriske løsninger i enkelte tilfeller bør være hovedregelen, fordi personvernrisikoen tilsier at det stilles særlig strenge krav til bekreftelse av identitet.

Utrederne bes også kort redegjøre for hvordan biometri og biometriske metoder ligner på og skiller seg fra andre identifikatorer og autentiseringsmidler, særlig med hensyn til koblingsfare, eksponering av overskuddsinformasjon (eks. at behandlingen også omfatter sensitive opplysninger) og vern mot feilautentisering. Som eksempler på slike andre identifikatorer og autentiseringsmidler kan nevnes:

- navn og fødselsdato[1],
- legitimasjon som gjennom bilde eller tekst avslører religion eller etnisk bakgrunn,
- kortlesere som er sårbare for kopierte kort.

Utrederne bes vurdere om de foreslåtte bestemmelser bør forbeholdes biometriske kjennetegn, eller om de bør gjøres generelle og dekke også andre identifikatorer eller autentiseringsmetoder. Utrederne skal som ledd i sine vurderinger og eventuelle forslag til lovendringer også komme med anbefalinger om begrepsavklaring, for eksempel om den aktuelle typen personopplysninger mest naturlig omtales som ”biometiske kjennetegn” eller ”biometriske data” eller annet. Det er også ønskelig med en klargjøring av begrepet ”entydige identifikasjonsmidler” som i dagens lov omfatter både fødselsnummer og biometriske kjennetegn/data. I den grad utrederne mener det er behov for det, vil det også være relevant med klargjøringer knyttet til begrepene ”identifisering”, ”legitimering” og ”autentisering”.

Personopplysningsloven § 12 bygger på forutsetningen fra forarbeidene om at fødselsnummer ikke kan tillegges legitimasjonsvirkninger. Det kan imidlertid se ut til at denne forutsetningen ikke er godt nok kjent eller forstått. Det har i lengre tid vært fokus på uheldig bruk av fødselsnummer, blant annet gjennom en rekke oppslag i pressen. Problemet knytter seg særlig til at fødselsnummer blir brukt, ikke bare som identifikasjonsmiddel, slik § 12 legger opp til, men også for eksempel som autorisasjonskode til systemer eller som legitimasjonsmiddel ved bestilling/kjøp av varer eller tjenester. Feil bruk av fødselsnummer har også vært knyttet til faren for såkalt ”identitetstyveri” – situasjoner der noen krenker en annens identitet ved bruk av dennes fødselsnummer. (For ordens skyld gjør departementet oppmerksom på, at spørsmålet om ”identitetstyveri” skal være straffbart blir vurdert som ledd i arbeidet med ny straffelov.)

[1] 80% av den norske befolkning har et unikt navn. Korrekt skrevet navn, kombinert med fødselsdato, vil unikt identifisere om lag 99,99% av befolkningen.

Utrederne skal vurdere behovet for lovendringer, herunder om det bør fremgå tydeligere av loven hva et fødselsnummer *ikke* skal brukes til. Utrederne bes, i eventuelle forslag til endringer, ta hensyn til at det for den enkelte bruker av loven kan være vanskelig å skille mellom såkalt *identifisering* og *autentisering.* Det er ønskelig med en lovregulering som klarest mulig får frem hva som er lovlig og hva som ikke er lovlig bruk av fødselsnummer.

4 Avsluttende merknader – krav til utforming av forslag

Dersom utrederne kommer til at det er behov for lovendringer, ber departementet om at det utformes forslag til lovtekst. Lovteksten bør i størst mulig grad utformes teknologinøytralt. Alle forslag må være i samsvar med EU-direktivet og andre folkerettslige forpliktelser. Forslag til lov- eller forskriftsbestemmelser skal utformes i henhold til utredningsinstruksen og Justisdepartementets veiledningshefte om Lovteknikk og lovforberedelse, som vedlegges.

Utrederne skal vurdere de økonomiske og administrative konsekvensene av sine forslag. (Minst ett forslag skal være basert på uendret ressursbruk.)

Arbeidet skal fullføres med avgivelse av en samlet utredning innen 31. august 2008.[*] Utrederne disponerer inntil kroner 75.000.[**] Summen skal dekke vederlag til utrederne og andre utgifter som arbeidet eventuelt medfører.

[*] Fristen ble senere forskjøvet til 1. oktober 2008-

[**] Den økonomiske rammen ble senere justert opp til kroner 100.000.

Utgitt av:
Justis- og politidepartementet
www.jd.dep.no

Offentlige institusjoner kan bestille flere eksemplarer av denne publikasjonen fra:
Departementenes servicesenter
Post og distribusjon
E-post: publikasjonsbestilling@dss.dep.no

Publikasjonskode: G-0406 B

Trykk:
Departementenes servicesenter 11/08 - 300