PERSONVERNHENSYN VED BRUK AV BIOMETRISKE KJENNETEGN I PASS OG VISUMSØKNADER

Kandidatnummer: 382

Veileder: Jens Petter Berg

Leveringsfrist: 27.11.2006

Til sammen 17 953 ord

07.06.2007

Innholdsfortegnelse

1 INNLEDNING

1.1 Tema

Samfunnet har endret seg dramatisk de siste 10 – 15 årene når det gjelder bruken av teknologi for å kunne kontrollere områder og mennesker. Enkelte vil hevde at utviklingen har gått for langt, og at vi i altfor stor grad er underlagt en kontroll fra myndighetenes side med kameraovervåkning og andre former for kontroller, som elektroniske billetterings- og betalingssystemer. Andre vil si at dette er en nødvendig utvikling for at vi kan bevege oss fritt og trygt, og at det er et gode for borgerne å utsettes for en stadig større overvåkning. Spørsmålet er hvorvidt dette kan beskytte oss fra kriminalitet, og ikke minst det som har blitt det store temaet etter 11. september 2001 – terror. Etter hendelsen i New York ønsket man å innføre tiltak for at noe slikt aldri skulle kunne skje igjen. Terrorattentatene i Spania 2004 og i England i 2005 har ikke gjort problemstillingen noe mindre aktuell.

Hva er egentlig mest skadelig for den enkelte borger? Er det terrorfaren, eller en stadig større inngripen i den enkeltes privatliv? Ivaretas den enkeltes rettsikkerhet i stor nok grad i utviklingen?

Biometriske kjennetegn[1] er et resultat av en teknologisk utvikling som vil kunne gjøre det lettere for den enkelte å søke reisetillatelser og å reise ved at man behøver færre reisedokumenter, men er det så enkelt? Noen føler seg kanskje tryggere med vissheten om at det gjennomføres en omfattende kontroll med personopplysninger. Samtidig behandles stadig mer informasjon om den enkelte, og det er tilnærmet umulig å holde oversikt over hvilke opplysninger som er lagret om en. Har en samtykket til en spesiell bruk av opplysninger om seg selv, er det svært vanskelig å undersøke om de avgitte opplysningene senere blir benyttet til andre formål enn det opprinnelige, såkalt sekundærbruk. Sett fra et

[1] For nærmere definisjon av biometriske kjennetegn, se avsnitt 1.5.2.

juridisk perspektiv er det heller ikke uproblematisk at den teknologiske utviklingen skjer så fort, da lovgiver lett blir hengende etter og man hele tiden må prøve å være i forkant av en utvikling som er vanskelig å forutsi. Det kan føre til at reglene blir for vage til å fange opp alle mulige tenkelige og utenkelige situasjoner, og grensedragningene mellom hva som er tillatt og ikke blir vanskelig.

Tolv av Storbritannias mektigste IT-sjefer var av IT-publikasjonen Silicon.com samlet for å debattere fremtidens sikkerhets- og identifikasjonsformer. Nesten alle trodde at biometrisk teknologi vil utradere dagens sikkerhetsløsninger i løpet av noen få år.[2] Bruk av biologiske kjennetegn til identifiseringsformål er imidlertid ikke noe nytt. Allerede i 1812 ble det i Frankrike åpnet et detektivbyrå med bruk av fysiske bevis[3], og bruk av fingeravtrykk som teknisk bevis i straffesaker har blitt brukt i over 100 år. Selv om fingeravtrykk har vært brukt i strafferettspleien, er det imidlertid noe helt nytt å benytte biometriske kjennetegn, som fingeravtrykk, til et identifiserings- eller legitimeringsformål utenfor dette området, særlig i så stor skala som nå er tenkt i pass og visum. Det er personverntrusler rettet mot denne bruken det vil fokuseres på i denne oppgaven. Derimot kan det oppstå et spørsmål i forhold til blant annet strafferettspleien, hvis slike innsamlinger av biometriske kjennetegn benyttes til andre formål enn det som først var tenkt, for eksempel ved at fingeravtrykksregister for pass benyttes til kriminalitetsbekjempelse.

1.2 Problemstilling

Jeg vil konsentrere meg om den delen av teknologien som går på bruk av biometriske kjennetegn. Problemstilingen i min oppgave vil til dels være en problemstilling som alltid vil oppstå når man drøfter den enkeltes personvern; nemlig at hensynene til den enkeltes personvern må avveies mot det man vanligvis betegner som behandlingsformålene. Denne oppgaven vil undersøke disse formålene, samt drøfte de kryssende hensyn som gjør seg gjeldende. Kanskje foreligger det så tungtveiende samfunnshensyn at hensynet til den

[2] http://www.steria.no/?id=11002858 lest 10.11.2006.

[3] http://www.ridgesandfurrows.homestead.com/landmark.html.

enkeltes personvern må vike. Samtidig er viktige samfunnshensyn til vern for samfunnsborgerne, og det er til fordel for medlemmene av samfunnet at det igangsettes sikkerhetstiltak. Spissformulert kan det sies at det i enkelte tilfeller vil være viktigere å beskytte liv enn privatliv.

Denne oppgaven vil drøfte hvorvidt problemstillinger rundt personvernhensyn alltid vil være et argument mot bruk av biometriske kjennetegn, eller om bruken av biometriske kjennetegn i enkelte tilfeller kan styrke den enkeltes personvern. Der det som utgangspunkt er nødvendig og hensiktsmessig å benytte biometriske kjennetegn kan forekomme at man benytter flere opplysninger om den enkelte enn det som det er behov for, såkalt "overkill", og at opplysningen benyttes til andre og nye formål, sekundærbruk. Er fordelene ved et omfattende fingeravtrykksregister store nok til å rettferdiggjøre risikoen?

Jeg vil også undersøke om det er noen store forskjeller når det gjelder den enkeltes personvern ved innføring av fingeravtrykk i pass i forhold til bruk av fingeravtrykk ved visumsøknader.

1.3 Aktualitet

De som har fått nye pass etter høsten 2005 har fått implantert en RFID-brikke i passet som lagrer personopplysninger og bilde. Fra senest juni 2009 er fingeravtrykk tenkt implantert i passene. Fra begynnelsen av 2007 er det meningen at alle visum skal få integrert biometrisk data. Dette innebærer at alle som søker visum må avgi fingeravtrykk og bilde.[4]

Hovedregelen for hvem som må søke visum er hjemlet i utlendingsloven[5] (utl.) § 25 første ledd. Det gjelder en visumplikt for alle utlendinger, med mindre Kongen har gjort unntak fra visumkravet, jf utl. § 25 første ledd. På grunn av Norges deltakelse i Schengen-samarbeidet, gjelder visumplikten ikke for borgere av Schengen-land, og heller ikke en del

[4] Opplysninger fra Tom Halvorsen, prosjektleder i Innvandringsavdelingen, Arbeids- og inkluderingsdepartementet 03.11.2006.

[5] Lov om utlendingers adgang til riket og deres opphold her (utlendingsloven) 24.juni 1988 nr. 64.

andre land Norge har inngått visumfrihetsavtaler med, deriblant USA. Det følger av utlendingsforskriften[6] § 105 hvilke utlendinger som er unntatt fra visumplikt. De som vil måtte avgi fingeravtrykk i visumsøknader er personer som kommer fra land utenfor Schengen-området og som det ikke gjelder visumfrihetsavtaler med, og som skal reise inn i Norge/Schengen, med andre ord tredjelandsborgere. Tredjelandsborgere som har fått visum til et annet Schengen-land kan reise uhindret inn i Norge. Det er ikke snakk om lang tid før alle som på et eller annet tidspunkt vil ut å reise over landegrenser må finne seg i å avgi fingeravtrykk i pass og/eller visumsøknader. Plikten til å avgi fingeravtrykk i pass gjelder alle borgere av et Schengen-land, det er kun visumplikten man er unntatt, ikke passplikten. Debatten rundt innføring av fingeravtrykk og andre biometriske kjennetegn har ikke vært overveldende i folks dagligliv, og når det diskuteres er det ofte teknologien som er i fokus, og ikke personvernet. For eksempel er enkelte bekymret for om irisskanning kan skade øynene over tid, og hva med uten hender? Siden innføringen av biometri er en prosess som pågår nå og derfor i aller høyeste grad er aktuell, finner jeg det interessant å drøfte de personvernmessige hensyn som taler for og imot en slik innføring.

1.4 Avgrensning av oppgaven

Fødselsnumre har en del likhetstrekk med biometriske kjennetegn, først og fremst ved at de er unike, altså at ingen personer har samme fødselsnummer og ved at fødselsnumrene er digitaliserbare. Men biometriske kjennetegn skiller seg fra bruken av fødselsnumre ved at biometriske kjennetegn er velegnet for å verifisere den man hevder å være, mens fødselsnumre derimot ikke har denne egenskapen. Jeg vil derfor ikke komme inn på fødselsnumre i andre sammenhenger enn når jeg sammenligner det med bruk av biometriske kjennetegn.

På grunn av oppgavens omfang vil jeg ikke diskutere bruk av sentrale databaser sammenliknet med lokale databaser. Det viktige i forhold til oppgavens tema er de

[6] Forskrift 21.12.1990 nr. 1028 om utlendingers adgang til riket og deres opphold her (utlendingsforskriften).

personverninteresser som gjør seg gjeldende når man lagrer biometrisk data og har adgang til å avlese disse.

Det finnes mange ulike biometriske kjennetegn eller biometriske mønstre. Blant annet ansiktsbiometri, håndavtrykk, DNA, stemme, øreform, lukt, ganglag, signatur, netthinne, regnbuehinne (iris) og fingeravtrykk. Irisskanning gir visstnok en sikrere form for verifikasjon/identifikasjon enn bruk av fingeravtrykk da feilmarginene ikke er så store som for fingeravtrykk. Ingen mennesker har like mønstre rundt delen av øyet. Per dags dato er det imidlertid ikke aktuelt å benytte irisskanning verken i pass eller ved søknad om visum fordi et amerikansk foretak sitter på patentet. Alle land må enkeltvis kjøpe utstyr fra det amerikanske foretaket for å kunne benytte irisskanning. Dette vil være en betydelig økonomisk kostnad som foreløpig har fått myndighetene til å legge bort tanken på å benytte seg av den teknologien. Jeg vil av den grunn ikke gå nærmere inn på bruk av irisskanning, men i den videre fremstilingen vil konsentrere meg om fingeravtrykk.

Dette er utvilsomt et område hvor de tekniske aspektene ved utviklingen er svært viktig for ivaretakelsen av personvernet, ikke bare de lover og regler som eventuelt regulerer dette. Jeg vil imidlertid i liten grad gå inn på den tekniske delen av debatten da det ikke er det mest interessante sett fra en juridisk synsvinkel. Samtidig er det viktig å ha i bakhodet at man ikke må ha en uberettiget naiv tiltro til teknologien og dens sikkerhet i forhold til de kontrollformer vi allerede har i dag. Dette vil i så fall kunne føre til at feil ved bruken vil kunne gå hardt utover personvernet til den som rammes av en feil. Selv om oppgaven ikke diskuterer det tekniske ved bruken, er det essensielt at sikkerheten ved de tekniske komponentene som brukes ved generering og kontroll av biometriske kjennetegn er høy. For at det skal kunne være mulig å stole på teknologien som benyttes, burde det være en minimumsstandard på utstyret som benyttes med blant annet spesifikke reguleringer, og som alle landene må forholde seg til (ISO/IEC) [7]. Det bør altså foreligge reguleringer av hvilket utstyr som er godkjent for slik bruk av hensynet til personvernet, og ikke bare regler

[7] ISO/IEC PDTR 24714-1 side 8 2005.

om hva slags bruk som bør tillates. Det er imidlertid det siste som er temaet i denne oppgaven, selv om grensen ikke alltid vil være så klar.

Oppgaven vil ikke drøfte kommersiell bruk av fingeravtrykk. Forholdene oppgaven først og fremst skal undersøke, er av samfunnsmessig karakter, og skiller seg følgelig fra formålene ved kommersiell bruk, som er av mer økonomisk og praktisk art.

På grunn av oppgavens omfang velger jeg å avgrense mot FN-konvensjonen om sivile og politiske rettigheter (SP) av 1966 artikkel 17, da jeg vil komme inn på stort sett de samme hensyn som vil gjøre seg gjeldende etter Den europeiske menneskerettighetskonvensjon (EMK) av 1950 artikkel 8. Rettighetene etter SP artikkel 17 samsvarer med EMK artikkel 8.

Som nevnt ovenfor er bruk av biometriske kjennetegn ikke en ny bevismetode i straffesaker, men en merkelapp på nye metoder for å sikre entydig identifikasjon av fysiske personer ved grensepasseringer og liknende, og det er det siste jeg skal konsentrere meg om. Jeg vil derfor ikke gå noe videre inn på bruk av DNA i strafferettspleien, slik det for eksempel drøftes i NOU 2005:19.

1.5 Begrepsavklaring

1.5.1 Biometri

Ordet biometri kommer fra gammelgresk og er en sammenslåing av bios, som betyr liv, og metron, som betyr mål. Biometri er vitenskapen om behandling av livsytringer i den utstrekning biologiske fenomener kan gjøres til gjenstand for målinger og resultatene uttrykkes i tall, altså digitaliseres, f.eks. beregning av gjennomsnittlig levetid.[8] Biometri kan benyttes til mer enn bare å identifisere et menneske entydig eller verifisere at en person er den han gir uttrykk for. Biometriske egenskaper kan også fortelle noe om selve personen

[8] www.ordnett.no/ordbok.html 11.09.2006.

og avsløre sensitive opplysninger. Dette gjelder særlig ved bruk av DNA, men også ved å benytte biometriske kjennetegn som irisskanning, hvor man i dag skal ha oppdaget at det er mulig å avsløre om personen har diabetes, og ut ifra en persons fingeravtrykk kan man i dag visstnok kunne finne kjennetegn på at personen har psykiske problemer[9].

Når man benytter biometri digitaliseres bestemte punkter i et mønster. De punktene man velger ut beskrives med binære tall. Ved å benytte biometri digitaliserer man unike kjennetegn, for eksempel linjemønstre i et fingeravtrykk. Et fingeravtrykk kan for eksempel bestå av 4000 rekker med nuller og enere, mens med Panasonics kameraer for irisgjenkjenning kan man lagre opp til 100 000 mønstre, jf Ragna Kronstad, 2006.[10] Ifølge Tom Halvorsen planlegger myndighetene å benytte 120 punkter i et digitalisert fingeravtrykk som biometriske kjennetegn i norske pass.

1.5.2 Biometriske kjennetegn

Bruk av biometriske kjennetegn er ikke noe nytt. Vi mennesker har til alle tider benyttet oss av ansiktsbiometri, gjenkjennelse av ansikter. Dette er tilsynelatende enkelt for mennesker, men erfaringsmessig likevel vanskelig nok jo mer flyktig kjennskapen til vedkommende er. Å konstruere et pålitelig ansiktsgjenkjenningsprogram for datamaskiner, har imidlertid vist seg å være vanskelig – påliteligheten per i dag er ikke imponerende, i alle fall ikke målt ut fra de sannsynlighetsprosenter man snakker om som tilstrekkelig for skyldavgjørelser i straffesaker.[11] Derfor er fingeravtrykk mest hensiktsmessig å bruke i en identifiserings- eller verifiseringshensikt. Samtidig er det viktig å poengtere at bruk av biometriske kjennetegn ikke er en eksakt vitenskap, man foretar en sannsynlighetsberegning hvor man på forhånd legger inn hvor store feilmarginer man kan godta:

---

[9] Liu, personvernforelesning, IRI mars 2006.

[10] Teknisk Ukeblad s. 26-27, 153. årgang nr.11 mars 2006.

[11] Ansiktsgjenkjenning benyttes likevel i dag, blant annet på Keflavik Lufthavn, Island.

> "Biological Biometric Characteristics: A biometric characteristic based primarily on a anatomical or physiological characteristic, rather then a learned behaviour. All biometric characteristics depend somewhat upon both behavioural and biological characteristic. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry."[12]

1.5.3 Autentisering; verifikasjon versus identifikasjon

Norsk Regnesentral forklarer i sin rapport "Elektroniske spor" verifisering på følgende måte:

> "Biometrisk autentisering har to ulike anvendelser. Den ene er verifisering av en identitet; altså en en-til-en autentisering hvor brukeren selv hevder å ha en bestemt identitet. Den andre anvendelsen er identifisering hvor man ønsker å finne identiteten til en person blant mange."[13]

Verifisering/legitimering er en en–til–en-situasjon hvor man allerede har fremlagt en identitet, og nå skal man benytte seg av et fingeravtrykk for å bekrefte at man er den personen man hevder å være. Identifiseringssituasjonen er en en–til–flere-situasjon. Her har man et fingeravtrykk, men man vet ikke hvem det er sitt, eller fester ikke lit til forklaringen om oppgitt identitet. Da kan man for eksempel gå inn i en fingeravtrykkdatabase og legge inn fingeravtrykket for å finne en match blant alle avtrykk som ligger der fra før av.

I dagligtalens juss sier man at legitimasjon er et bevis for at man er den man utgir seg for å være. Når man legitimerer seg dokumenterer man hvem man er.[14] Men ved å legitimere seg behøver man ikke alltid være den man utgir seg for å være, det er det ytre skinn av rett en

---

[12] NSTC: Taking Today's Biometrics to Meet Tomorrow's Needs s. 7.

[13] Norsk Regnesentral: Elektroniske spor s. 45, 6. juni 2005.

[14] www.ordnett.no/ordbok.html 12.09.2006.

person har til å foreta visse rettslige disponeringer.[15] Dette stiller seg imidlertid annerledes ved bruk av biometriske kjennetegn og biometrisk legitimering/verifisering, altså biometrisk autentisering. Ved å legitimere seg ved å benytte for eksempel fingeravtrykk, kan man ikke være noen annen enn den man utgir seg for å være. Det betyr ikke at innholdet i det jeg fremlegger nødvendigvis er ekte, men ved hjelp av biometriske kjennetegn i en verifiseringsprosess vil man kunne vite at det er riktig person som står foran en. Biometriske kjennetegn er således egnet for et legitimeringsforhold, i motsetning til for eksempel et fødselsnummer, som bortimot hvem som helst kan få tak i.

Autentisering kan baseres på tre typer faktorer, jf Elektroniske spor side 17[16]. For det første kan autentisering baseres på noe du *vet*, en hemmelighet, for eksempel et passord eller en pin-kode (Personal Identification Number). For det andre kan autentisering baseres på noe du *har*, en gjenstand, for eksempel et adgangskort eller en nøkkel. Og for det tredje kan autentisering baseres på noe du *er*, en egenskap ved deg som person, for eksempel et fingeravtrykk. Det er den siste typen av autentisering som kalles biometrisk autentisering, og denne typen autentisering skiller seg fra de andre fordi den er direkte knyttet til deg som person, og det er ikke noe som kan byttes ut eller erstattes med noe annet, som for eksempel et nytt adgangskort eller ny kode. Nettopp derfor egner den siste faktoren seg til et verifiseringsformål fremfor de andre to faktorene, for noe du er kan ikke komme på avveie og forfalskes på samme måte som noe du har eller vet. Du kan ikke gi vekk fingeravtrykket ditt. I forhold til noe du vet eller har, er det ved bruk av noe du *er* langt vanskeligere å stjele, kopiere eller endre.

1.5.4 Fingeravtrykk

Fingeravtrykk er avtrykk av hudlinjene på innsiden av fingrene[17]. Selv om vi vokser og hendene blir større, og daglig bruker og sliter på fingertuppene, regnes fingeravtrykk for å

---

[15] Jusleksikon 1999 s. 167.

[16] Norsk Regnesentral: Elektroniske spor, 6. juni 2005.

[17] Jusleksikon 1999 s. 82.

holde seg uforandret gjennom hele livet. Det er nettopp derfor at man i straffesaker har kunnet benytte seg av fingeravtrykksresultater. Det har visstnok så langt aldri blitt oppdaget to personer med like fingeravtrykk.

1.5.5 RFID

"RFID" er forkortelsen for Radio Frequency Identification.[18] De nye passene som utstedes i Norge i dag inneholder en RFID-brikke. Dette er små brikker for automatisert identifikasjon av objekter ved bruk av radiobølger. I forhold til bruk av biometriske kjennetegn kan man benytte RFID-brikker ved at man lagrer den biologiske informasjonen (fingeravtrykk) i en slik brikke, og avlesere vil kunne se om de data som er lagret om deg i passet stemmer overens med det biologiske mønsteret du viser frem (fingeravtrykk) når du går gjennom passkontrollen og avgir fingeravtrykk ved fremvising av passet. Andre eksempler på bruk av RFID i dag er bomveisystemet Autopass hvor biler gjenkjennes automatisk ved man har utstyr i bomstasjonen som avleser identifikasjonsdata på Autopass-brikken i passerende biler.

National Science and Technology Council[19] skriver dette om RFID:

> "Technology that uses low-powered radio transmitters to read data stored in a transponder (tag). RFID tags can be used to track assets, manage inventory, authorize payments, and serve as electronic keys. RFID is not biometric."

Personvernutfordringer ved bruk av RFID for den bruken som er aktuell for min problemstilling, er først og fremst at man kan spore den enkeltes bevegelser, så lenge man beveger seg med passet på seg.

---

[18] Teknologirådet: Elektroniske spor og personvern s. 68, Rapport 1 2005

[19] National Science and Technology Council (NSTC): Taking Today's Biometrics to Meet Tomorrow's Needs s. 25 August 2006.

1.6 Kort om personvernbegrepet og personvernhensyn

Personvern er et begrep som er litt flytende, i den forstand at vi mennesker ikke har en klar og avgrenset definisjon på hva som ligger i begrepet, til dels legger vi forskjellige forståelser i begrepet, og når det forklares i teorien viser man også til forskjellige interesser og måter å se det på.[20] Men man kan i alle fall si at personvern er en fundamental menneskerettighet som er anerkjent over store deler av verden, på tvers av kulturer og religioner. På engelsk knytter man to ulike begreper til det vi kaller personvern, *privacy* som er knyttet til vern av grunnleggende verdier som integritet, autonomi og privatliv, mens *data protection* mer er vern av personopplysninger.[21] Retten går ikke bare ut på hvilke opplysninger om en person hvilket vedkommende selv ønsker å dele med andre, men også hvilke opplysninger man ønsker å vite om seg selv. Det siste er aktuelt for min oppgave ved at jo mer vi avgir av oss selv, det være seg fingeravtrykk, DNA, osv, jo mer opplysninger om ens egen kropp vil man kunne undersøke. For eksempel vil man ved hjelp av DNA kunne undersøke hvilke sykdommer man er disponert for. Man har i nasjonal og internasjonal personvernrettslig teori lenge anerkjent at det er et sentralt begrepskjennetegn ved personvernbegrepet at den enkelte selv må kunne bestemme ikke bare hvor mye andre skal få vite om for eksempel egne sykdommer (”informational control”), men også hvor mye en skal få slippe å vite om egen sykdom (”the Right not to know”). I norsk personvernteori har man ofte sett personvernet fra tre forskjellige perspektiv, integritetsperspektivet, beslutningsperspektivet og maktperspektivet, og man benytter seg ofte av det som kalles ”interesseteorien” som sier noe om hvilke personverninteresser som har vært utviklet og lagt til grunn de siste 30 år.[22] De personvernhensyn som særlig gjør seg gjelden for oppgavens tema, vil presenteres og drøftes gjennom de vurderinger som blir gjort gjennom hele oppgaven.

---

[20] Schartum, Wiese og Bygrave: Personvern i informasjonssamfunnet, 2004 kapittel 2.

[21] Teknologirådet: Elektroniske spor og personvern, s. 22 Rapport 1 2005.

[22] For mer om dette, se Schartum, Wiese og Bygrave: Personvern i informasjonssamfunnet kapittel 2, 2004.

1.7 Spesielle rettskildemessige utfordringer

Fremstillingen baserer seg på vanlig juridisk metode, slik den er fremstilt av blant annet Eckhoff i hans "Rettskildelære" 5. utgave 2001. De spesielle rettskildemessige utfordringer som først og fremst gjør seg gjeldende i denne oppgaven, er at dette er et område hvor det per i dag ikke eksisterer mye lovgivning. Det som finnes er relativt nytt, eller under arbeid. Det foreligger heller ikke mange andre rettskilder, som for eksempel rettspraksis på området, knyttet direkte til problemstillingen i denne oppgaven. For innføring av biometriske kjennetegn i pass har vi i dag, som jeg kommer tilbake til, lovfestet bruk av digitale ansiktsfoto i passene.

1.7.1 Norsk lov

1.7.1.1 Personopplysningsloven

Lov av 14. april 2000 nr. 31 om behandling av personopplysninger, heretter omtalt som personopplysningsloven eller pol, er den sentrale loven på personvernområdet i Norge. Den inneholder generelle bestemmelser for behandling av personopplysninger. Formålsbestemmelsen i § 1 sier noe om hva som regnes for å være grunnleggende personvernhensyn:

> "behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger."

Personopplysningsloven § 12 regulerer bruk av "Fødselsnummer og andre entydige identifikasjonsmidler", og det fremgår av forarbeidene[23] at fingeravtrykk og andre biometriske data er eksempler på "andre entydige identifikasjonsmidler". Det er dermed klart at biometrisk data faller inn under § 12. Det fremgår videre av § 12 at den regulerer bruk av fødselsnummer eller andre entydige identifikasjonsmidler i et *identifiseringsformål*, det vil si at den kun hjemler bruk hvor man ønsker å finne en persons

[23] Ot.prp. nr. 92 (1998-1999) s.114.

identitet, og ikke i et legitimeringsformål, hvor man ved hjelp av for eksempel fingeravtrykk bekrefter at man er den man hevder å være. Personopplysningsloven inneholder ingen andre regler som hjemler bruk av biometriske kjennetegn i et legitimeringsformål. All slik bruk vil derfor være i strid med personopplysningsloven og dermed ulovlig[24]. I tillegg til at § 12 kun hjemler bruk i et identifiseringsøyemed, foreligger det også vilkår som må være oppfylt for at bruk av biometriske kjennetegn skal være lovlig. For det første må det foreligge et saklig behov for sikker identifisering, og for det andre må metoden være nødvendig for å oppnå en slik identifisering. Implisitt foreligger det et krav til forholdsmessighet; kravet til nødvendighet vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler ikke er tilstrekkelig. I tillegg til disse vilkårene må også de andre vilkårene i personopplysningsloven være oppfylt.

Dette vil si at det skal svært mye til før man etter personopplysningsloven i dag kan benytte biometriske kjennetegn, fordi man i de aller fleste tilfeller kan oppnå en tilfredsstillende identifikasjon ved hjelp av navn, adresse, fødselsdato og kundenummer.

1.7.1.2 Passloven

Lov 19. juni 1997 nr. 82 om pass, heretter omtalt som passloven, inneholder i § 6 en bestemmelse om bruk av ansiktsbiometri i pass til verifisering eller kontroll av passinnehaverens identitet. Det er etter hvert tenkt at passloven også skal regulere bruk av fingeravtrykk i pass. Passloven er lex specialis i forhold til personopplysningsloven, og går således foran ved tolkningen av reglene.

1.7.1.3 Utlendingsloven

Arbeids- og inkluderingsdepartementet sendte i mars 2006 ut et høringsforslag om å innta bruk av biometriske kjennetegn i utlendingsloven (utl), i form av ansiktsfoto og fingeravtrykk i visumsøknader. Det foreslås at den biometriske informasjonen skal

[24] Se www.datatilsynet.no for Datatilsynets praksis på området.

overføres til en sentralenhet for opplysninger om visum, hvor også andre opplysninger som er nødvendige for behandling som søknad om visum skal lagres.

I disse dager foregår siste innspurt på arbeidet med ny utlendingslov som skal fremlegges for Stortinget tidlig i 2007. Forslaget om å innføre ansiktsfoto og fingeravtrykk i visumsøknader er, så vidt jeg kan se, enda ikke innarbeidet i forslaget til ny lov, og jeg forholder meg også av den grunn til gjeldende rett.

Utlendingslovens regler vil på samme måte som passlovens regler gå foran personopplysningsloven ved en eventuell uoverensstemmelse i reglene, da det i forslaget til ny § 37 f tredje ledd sies at personopplysningsloven skal gjelde dersom ikke annet er bestemt i lov eller forskrift.

1.7.2 Forarbeider

Forarbeidene[25] til personopplysningsloven sier lite om bruk av biometriske kjennetegn, annet enn at fingeravtrykk og andre biometriske data faller inn under definisjonen ”andre entydige identifikasjonsmidler” i pol § 12. Men bakgrunnen for § 12 er å forhindre misbruk av personnummer, og regelen er utformet med henblikk på dette. Det er derfor sagt direkte i forarbeidene at fødselsnummer ikke skal benyttes i et legitimeringsformål.

Bakgrunnen for at et fødselsnummer ikke er egnet til et legitimeringsformål er at fødselsnumre er lett tilgjengelige og enkelt for andre enn eieren å benytte seg av. Som det blir sagt i personvernkretser: å oppgi sitt personnummer er bare som å si navnet sitt en gang til. Imidlertid er det her en viktig forskjell på et fødselsnummer og bruk av biometriske kjennetegn, da sistnevnte nettopp er egnet til legitimasjon, hvilket gjør dagens regel lite hensiktsmessig. Jeg vil derfor under avsnitt 3 presentere Datatilsynets forslag til endring av personopplysningsloven § 12.

[25] Ot.prp. nr. 92 (1998-1999).

Forarbeidene til passloven[26] sier at myndighetene skal komme tilbake til bruk av fingeravtrykk når dette er grundigere diskutert og nødvendige undersøkelser er gjort. Videre var fristen fra EU kortere når det gjaldt innføring av digitale foto i pass enn ved fingeravtrykk, og man har derfor avventet å regulere dette.

1.7.3 Praksis

1.7.3.1 Rettspraksis

Jeg viser til lovdatasøk av 24.11.2006. Per 24.11.2006 foreligger det ingen annen rettsavgjørelse som har direkte relevans for mitt område enn en dom fra Høyesterett som omhandler bruk av biologisk materiale (Rt. 2006 s.90). Dommen får ikke direkte anvendelse for min oppgave, men jeg kommer tilbake til den under punkt 5.2 i oppgaven.

1.7.3.2 Forvaltningspraksis

Forarbeider til personopplysningsloven sier lite og endringen i passloven er relativt ny, så praksis på området er derfor relevant for å få belyst rettstillingen. Datatilsynet er i så henseende et tilsynsorgan hvor avgjørelser fattet av dem vil være relevant for vurderingen. Avgjørelser fattet av Personvernnemnda, som er klageinstans for vedtak fattet av Datatilsynet, vil også være av betydning.

1.7.4 Internasjonal rett

1.7.4.1 EMK artikkel 8 og artikkel 6

Personvernlovgivningen som foreligger i Norge og internasjonalt, har sine røtter i internasjonale traktater om menneskerettigheter, særlig artikkel 8 i Den europeiske menneskerettskonvensjonen. Artikkel 8 fastslår at enhver har rett til respekt for sitt privat- og familieliv, sitt hjem og sin korrespondanse. Videre fastslår artikkel 6

[26] Ot.prp. nr. 86 (2004-2005), St.prp. nr. 54 (2004-2005).

uskyldspresumsjonen som er et viktig rettsikkerhetsprinsipp: enhver er uskyldig til det motsatte er bevist.

1.7.4.2 EUs personverndirektiv 95/46/EF

Av mer direkte betydning for den lovgivning vi har i Norge i dag på personvernområdet er det først og fremst EUs personverndirektiv 95/46/EF av 24. juli 1995 ”Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger” som er av betydning, da personopplysningsloven i hovedsak bygger på dette direktivet. Det kan derfor være naturlig i enkelte tilfeller å se hen til direktivet ved tolkningen av personopplysningsloven. EUs personverndirektiv bygger igjen på prinsipper nedfelt i Europarådets personvernkonvensjon av 28. januar 1981 nr. 108. Formålet med personverndirektivet er harmonisering av de nasjonale lovene for å avskaffe regler som gjør at personopplysninger ikke kan flyte fritt mellom landene. Samtidig oppstiller direktivet en minimumsstandard for personvernet i det enkelte landet, og sørger for å ha et forholdsvis høyt nivå på personvernet. I ”Personvern i informasjonssamfunnet” vises det til at direktivet er et av de første EU-rettslige instrumenter som eksplisitt gir fremtredende plass til beskyttelse av menneskerettigheter.[27]

Personverndirektivet 95/46/EF definerer i artikkel 2 a hva som menes med personopplysninger, og det innbefatter all type informasjon som kan knyttes til en identifisert eller mulig identifiserbar person. Inn under dette nevnes elementer som er særegne for personens fysiske, fysiologiske og psykiske identitet. Videre nevnes det i fortalens punkt 26 at når det skal avgjøres om en person er identifiserbar, ”bør alle hjelpemidler vurderes som det er rimelig å ta i bruk for å identifisere vedkommende”. Jeg finner det ikke tvilsomt at biometrisk data faller inn under denne definisjonen.

[27] Schartum, Wiese og Bygrave: Personvern i informasjonssamfunnet s. 8, 2004

Det ble i forbindelse med direktivet nedsatt en arbeidsgruppe etter artikkel 29. Artikkel 29-gruppen har lagt til grunn at biometrisk data og biometrisk data som digitalt er omformet til et *template (mønster)* som hovedregel er en personopplysning.[28]

Direktivets artikkel 8 nr. 7 er "bakgrunnen" for § 12 i personopplysningsloven.

[28] Datatilsynet: Notat fra Datatilsynet – forslag til revisjon av personopplysningsloven § 12 og ny bestemmelse om bruk av biometrisk data s. 10.

2 GJELDENDE RETT OM BRUK AV BIOMETRISKE KJENNETEGN I PASS OG VISUMSØKNADER

2.1 Føringer fra personopplysningsloven

Personopplysningsloven § 12 åpner for bruk av biometriske kjennetegn for å identifisere en person, men derimot ikke for å legitimere seg. Bakgrunnen for dette er at regelen i første omgang ble lagd med tanke på fødselsnummer, og bruk av biometriske kjennetegn er så vidt nevnt i forarbeidene.

I Datatilsynets forslag[29] til ny lovhjemmel i personopplysningsloven, § 12 a, hevdes det at biometriske data som utgangspunkt ikke er å anse som sensitive personopplysninger, jf personopplysningsloven § 2 nr. 8, men at biometriske kjennetegn i enkelte tilfeller kan analyseres på en slik måte at sensitive opplysninger om den enkelte avdekkes. Blod og urin er nevnt som eksempler. Derimot mener Schartum og Bygrave[30] at opplysninger knyttet til biometri kan være sensitive personopplysninger etter personopplysningslovens § 2 nr. 8 bokstav c, opplysninger om helseforhold, men utdyper ikke dette noe videre. Jeg mener at reelle hensyn tilsier at biometriske data bør regnes for å være sensitive opplysninger fordi dette vil begrense bruken av slike opplysninger og særlig fordi vi i dag i liten grad kjenner til hvilke konsekvenser slik bruk vil få for den enkelte. Ved å karakterisere biometriske data som sensitive personopplysninger vil man i større grad gi Datatilsynet kontroll over bruken og den enkelte vil kanskje tenke mer igjennom å avgi et fingeravtrykk når man vet at dette regnes for å være en sensitiv opplysning på linje med for eksempel andre helseforhold.

---

[29] Datatilsynet: Elektronisk lagring av biometrisk personinformasjon – forslag til endring i passloven av 24.06.2005 s. 9.

[30] Wiese Schartum og Bygrave: Utredning av behov for endringer i personopplysningen 2006 s. 82.

2.2 Passloven § 6, § 6a og § 8 med forarbeider

Passloven ble endret av Stortinget i juni 2005.[31] Endringene går i all hovedsak ut på at passloven i dag åpner for elektronisk lagring av ansiktsfoto i pass. Endringen er et resultat av implementeringen av Rådsforordning 2252/2204/EF av 13.12.2004 om krav om biometri i EU/Schengen-borgernes pass (heretter omtalt som rådsforordningen). Prosessen om innføring av biometri i pass skyldes i stor grad påvirkning fra USA for fortsatt visumfri innreise dit. Myndighetene i USA krever biometrisk informasjon i alle pass utstedt etter 26. oktober 2005, reisende med pass utstedt før denne dato kan benytte disse ved innreise til USA så fremst passet har maskinlesbar tekst.[32] Endringen av passloven ble innført uten de store diskusjonene, verken i Stortinget eller i media. Internasjonale datatilsynsmyndigheter var blant de som etterlyste debatt om bruk av biometri pass.[33] Formålet er først og fremst å hindre forfalsking og bruk av uriktige pass ved grensekontroll, jf St.prp. nr. 54 (2004-2005) avsnitt 1. Dette er, i følge samme dokument, viktige tiltak for å hindre terrorisme og annen alvorlig grenseskridende kriminalitet. Videre fremheves det at man ved bruk av biometrisk personinformasjon kan hindre identitetstyveri. Pass brukes ofte ved identitetstyverier som ledd i internasjonale bedragerier, for å hvitvaske penger eller, rett og slett for å få innreise til et land og så søke asyl.

Det fremkommer av rådsforordningens artikkel 2 at pass og reisedokumenter skal ha et lagringsmedium som skal inneholde ansiktsbilde og fingeravtrykk. Det er satt en lengre tidsfrist for innføring av fingeravtrykk enn ansiktsfoto, og det fremkommer videre av Ot.prp. nr. 86 at Justis- og politidepartementet (JD) valgte å ikke foreslå en lovhjemmel for elektronisk lagring av fingeravtrykk i passet da den lange fristen gjør at man grundigere kan utrede viktige personvernspørsmål før saken igjen fremlegges Stortinget.

Det fremkommer av rådsdirektivet at personverndirektivet 95/46/EF skal gjelde i forhold til de personopplysninger som behandles i forbindelse med pass og reisedokumenter.

---

[31] http://odin.dep.no/jd/norsk/aktuelt/nyheter/012101-210167/dok-bu.html.

[32] Ot.prp. nr. 86 (2004-2005) Kapittel 1.

[33] http://www.datatilsynet.no/templates/Page____1199.aspx.

I det følgende vil jeg gjennomgå innholdet i de to av de nye bestemmelsene i passloven, § 6 annet ledd og § 6a, og i tilknytningen til innføring av biometriske kjennetegn også gå innom § 8 som ikke er ny, men som det kan stilles spørsmålstegn ved om vil/kan få et endret innhold etter innføringen av biometriske kjennetegn i pass. Justis- og politidepartementet har uttalt[34] at lagring av biometrisk informasjon i et sentralt passregister "vil kunne åpne for andre bruksområdet enn den verifiseringen som skjer i passkontrollen" og dette krever at det settes klare rammer for bruken og at det gis en særskilt hjemmel for slik lagring. Kravet til hjemmel er viktig ved inngripen i den privats sfære. Dette vil altså si at § 8 ikke kan benyttes til slik lagring, slik den er utformet i dag. Lovens § 1 har også blitt endret ved at loven har fått større anvendelsesområde, tidligere var blant annet ikke diplomatpass omfattet, men § 1gjøres ikke til gjenstand for noen videre drøfting.

Nytt annet ledd i § 6 hjemler bruk av innhenting og lagring av biometrisk personinformasjon i form av ansiktsfoto i passet. Dette skal brukes til verifisering eller kontroll av passinnehaverens identitet. Det er altså ikke åpning for å oppta fingeravtrykk i pass etter dagens lovgivning, kun ansiktsfoto. Videre sier bestemmelsen noe om hvordan lagringen skal skje uten å oppstille konkrete tekniske krav, annet enn at informasjonens ekthet, integritet og konfidensialitet skal ivaretas.

Ny *§ 6a første ledd* gir passinnehaveren rett til innsyn i personopplysningene som er innført i passet og en rett til å kreve at uriktig informasjon slettes eller endres. Rett til innsyn er en av de viktigste rettighetene vi har innenfor personvern, nettopp fordi innsynsretten er en viktig vei hva gjelder hvilken kunnskap man selv skal ha om opplysninger som er lagret om seg. Men for at denne retten skal ha noen betydning, må passinnehaveren være klar over at

[34] Justis- og politidepartementet: Forslag til endring av passloven m.m. (elektronisk lagring av biometrisk personinformasjon i pass m.v.) s.7 mars 2005.

han har en slik rett. Videre er retten til innsyn en forutsetning for at man skal kunne få rettet eller slettet feilopplysninger om seg selv.

§ 6a annet ledd fastsetter en plikt for utstederen av passet til å slette biometrisk personinformasjon innhentet ved utstedelsen av passet så snart passet er oversendt eller utlevert til passinnehaveren. Dette vilkåret er med på å forhindre at den biometriske informasjonen som innhentes fra den enkelte kan benyttes til andre formål. *§ 6a tredje ledd* hjemler innhenting av biometrisk informasjon (ansiktsfoto) av alle som passerer et grensekontrollsted. *§ 6a fjerde ledd* fastsetter en plikt til å slette biometrisk personinformasjon som er innhentet ved passkontroll så snart vedkommendes identitet er verifisert.

Det fremkommer av rådsforordningen at deler av spesifikasjonene ved utarbeidelsen kan gjøres hemmelig. Spørsmålet er om det her åpnes en bakdør for sentral lagring av fingeravtrykk, uten at det er hjemlet i lov. Rådsforordningen artikkel 4 nr. 3 oppsummerer de godtatte bruksformålene med fingeravtrykk i pass, og sentral lagring av fingeravtrykk er ikke hjemlet i rådsforordningen. Før endringene om innføring av biometri kom, forelå det hjemmel i passlovens § 8 som åpner for at det kan opprettes et nasjonalt passregister. I et høringsnotat[35] fra JD vurderes fordeler og ulemper ved lagring av biometrisk personinformasjon i sentralt passregister, og det vurderes en ny § 8a som åpner for å lagre ansiktsbilde og fingeravtrykk i en slik database. Denne hjemmelen er foreløpig ikke vedtatt. Blant annet skyldes det at man per i dag ikke har innført og lovfestet bruk av fingeravtrykk i pass, og det fremkommer av Ot.prp. 86 (2004-2005) under avsnitt 3.1 at spørsmålet om et sentralt passeregister ikke ble behandlet i proposisjonen da det vil være behov for ytterligere utredninger og forberedelser. Det er svært viktig å ha klart for seg at dette ikke er hjemlet i forordningen som hele endringen av passloven så langt bygger på, og at Norge dermed går langt ut over det som kreves i forhold til Schengen-avtalen hvis en

[35] Justis- og politidepartementet: Forslag til endring av passloven m.m. s. 7, mars 2005.

slik database vedtas. Myndighetene sier følgende i forarbeidene[36] om lagring av biometrisk data:

> ”Lagring av biometrisk data opnar for at denne personinformasjonen kan brukast utanfor det føremålet han er innhenta for. Rådsforordninga gjev difor reglar som avgrensar bruken av slike data, i tillegg til at gjeldande reglar om vern av personopplysningar skal nyttast.”

Å innføre et sentralt passregister hvor biometrisk data lagres, vil føre til mer inngripende tiltak for den enkelte enn det fra EUs side legges opp til. I alle fall vedrørende lagring av fingeravtrykk hvor et slikt register kan få utilsiktede bruksområdet, og da er det i første omgang bruk ved etterforskning i straffesaker jeg tenker på. I høringsnotatet fra JD fremheves det flere positive virkninger av et slikt sentralt fingeravtrykksregister, blant annet når det utstedes nytt pass på grunn av tyveri eller tap. Etter egen mening vil det ikke være så tids- og kostnadsbesparende å innehente opplysningene på nytt at det veier opp for å lage et sentralt register. Videre nevnes det i notatet at registeret kan benyttes til å kontrollere identiteter ved utstedelse av andre id-kort, både i offentlig og privat sektor. Jeg er svært skeptisk til at finansielle institusjoner uten videre skal kunne benytte seg av et register hvor det ligger lagret biometrisk personinformasjon om egen person. Selv om det legges til grunn at den enkelte må samtykke for å gi andre denne tilgangen, mener jeg at man allerede her argumenterer for en sentral database med andre formål enn selve verifiseringen som skal gjennomføres ved en grensekontroll. Man benytter altså sekundærformål som begrunnelse for å opprette et slikt register, noe jeg mener i seg selv er en grunn til nettopp ikke å opprette et sentralt passregister. Det vil i så fall ikke være et passregister, men et register med biometrisk data om den enkelte som kan benyttes i mange praktiske øyemed, og som det tilfeldigvis faller inn under passloven. Jeg håper at det ved en eventuell utredning drøftes nøye om de positive virkningene kan måles opp mot de ulempene et slikt register vil føre med seg, og at utredningen vil gå på nødvendigheten av

[36] St.prp. nr. 54 (2004-2005) avsnitt 1.

et slikt register i forhold til sikker verifisering av passinnehaveren. I følge Datatilsynet[37] er det bred enighet blant personvernmyndigheter i EØS at både nasjonale og internasjonale databaser bør forbys.

2.3 Føringer fra Den europeiske menneskerettskonvensjon (EMK)

Vi har et internasjonalt menneskerettighetsvern, først og fremst gjennom EMK, som ble inkorporert i lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21. mai 1999 nr. 30. Jf menneskerettsloven § 2 gjelder EMK som norsk lov. Loven ble vedtatt fordi man ønsket at sentrale menneskerettigheter skulle inkorporeres for å styrke menneskerettighetenes stilling i norsk rett. Lovens § 3 sier at konvensjonene med de tilhørende protokoller ved motstrid skal gå foran annen lovgivning. Dette vil i klartekst si at Norge har plikt til å følge de rettighetene som følger av disse konvensjonene. Ved en eventuell motstrid mellom en inkorporert konvensjonsbestemmelse og annen norsk rett viser praksis at dette ikke kan løses ved hjelp av et generelt prinsipp om forrang, men må bero på en nærmere tolkning av de aktuelle rettsregler.[38]

Møse skriver følgende om menneskerettighetsvernets alminnelige innhold:[39]

> ”Kort og upresist kan det defineres som visse grunnleggende forestillinger om forholdet mellom individ og stat. Det dreier seg om rettigheter for individet uansett retts- eller samfunnssystem.”

Som jeg skal komme inn på, fremgår det blant annet at den enkeltes personvern regnes for å være en menneskerettighet, jf blant annet EMK art. 8 og retten til privatliv. Personopplysningsvern (”protection of personal data”) er ikke direkte nedfelt i EMK, men

---

[37] Datatilsynet: Notat til Justisdepartementet av 03.10.2005 Forslag til endring av passloven – elektronisk lagring av personinformasjon i pass mv. – Endringenes personvernmessige problemer s. 2.

[38] Rt 2000 s. 996

[39] Møse: Menneskerettigheter s.25 2002.

har gjennom domstolspraksis gradvis blitt utledet av retten til respekt for privatliv etter konvensjonens artikkel 8. Den europeiske menneskerettsdomstol (EMD/MRD) har også uttalt at begrepet ”privatliv” er vidt og ikke kan defineres uttømmende. I nyere EU-instrumenter finner man i dag en særskilt rett til ”protection of personal data”.[40]

I det følgende vil jeg kort vurdere om en plikt til å avgi ansiktsfoto og fingeravtrykk i pass og visumsøknader vil være lovlig etter EMK, da særlig EMK artikkel 8 (2), EMK protokoll 4 (P4) artikkel 2 (3) og EMK artikkel 6 (2).

EMK artikkel 8 (1) fastslår at enhver har rett til respekt for sitt ”privatliv og familieliv, sitt hjem og sin korrespondanse”, kjernen er at artikkelen regulerer den fysiske integriteten. For denne oppgavens tema er det først og fremst retten til privatliv som er av betydning. Særlig i forhold til VIS, hvor den enkelte visumsøker i tillegg til personopplysninger som navn, adresse, osv, må oppgi formål med reisen, hvor man skal og hvor lenge man skal være der, osv. Videre må en eventuell referanseperson som har invitert tredjelandsborgeren også oppgi personopplysninger og opplysninger om han har hatt besøk av tredjelandsborgere før, noe som innebærer at plikten får konsekvenser langt ut over den enkelte person som søker visum. Utlevering av disse opplysningene samt plikten til å avgi noe av seg selv, først og fremst fingeravtrykk, gjør at det kan være grunnlag for å hevde at det er i strid med retten til privatliv, da disse tiltakene forhindrer at man kan være privat. Men ikke ethvert tiltak som har negative virkninger for ens integritet faller inn under bestemmelsen. Foreligger det inngrep etter artikkel 8 (1), må det ses hen til om vilkårene for å gjøre unntak er til stede etter artikkel 8 (2). Da vilkårene for å gjøre unntak etter P4 artikkel 2 (3) er de samme som etter artikkel 8 (2), vil jeg foreta en felles vurdering. Jeg vil derfor først kort si noe om hva P4 artikkel 2 (1) og (2) går ut på.

[40] Schartum, Wiese og Bygrave: Personvern i informasjonssamfunnet s. 80, 2004

P4 artikkel 2 går ut på at enhver har bevegelsesfrihet på en stats territorium, såfremt han befinner seg lovlig på territoriet. ”Lovlig” opphold viser til statenes rett til å regulere utlendingers adgang til riket. Videre stadfester artikkel 2 (2) at enhver skal være fri til å forlate ethvert land, også sitt eget. Innføring av biometriske kjennetegn i reisedokumenter og sentral lagring av opplysninger om reisende er ikke en innskrenkning i bevegelsesfriheten i seg selv, men oppstiller vilkår for at den enkelte skal kunne krysse landegrenser. Men hvis det oppstilles så strenge krav til den enkelte borger at det reelt sett vil være bortimot umulig å oppfylle kravene slik at man ikke kan bevege seg, mener jeg at det vil være et brudd på P4 artikkel 2. Med dette mener jeg for eksempel at det innføres en avgift på 30 000 kr for å få utstedt et pass. Det vil være et vilkår som det for svært mange vil være vanskelig å oppfylle, og innholdet i retten til bevegelsesfrihet blir illusorisk. Videre vil det være et inngrep å ikke utstede pass eller beslaglegge det, jf Møse s. 294.

I artikkel 8 nr. 2 og P4 artikkel 2 nr. 3 gis det en adgang til å gjøre unntak fra rettighetene overfor. For at offentlige myndigheter skal kunne foreta inngrep overfor disse rettighetene må inngrepet være i samsvar med lov og nødvendig av hensyn til nærmere oppregnede formål. Dette vil bli drøftet senere.

Statene har et relativt stort handlingsrom hva gjelder hvilke tiltak de kan igangsette for å beskytte egne borgerer og landets interesser. Adgangen til å gjøre unntak henviser også til en ganske vag ordlyd som åpner for at statene kan innskrenke rettighetene fra alt fra nasjonal sikkerhet til helse og moral. Hvor langt går for eksempel hensynet til ”landets økonomiske velferd” i forhold til den enkeltes rett til privatliv? Det er vanskelig for den enkelte å trekke grensene slik ordlyden er i artiklene, og man må se hen til særlig rettspraksis fra EMD for å kunne se hvor langt statene kan gå i å innskrenke den enkeltes menneskerettighet. Vedrørende innføring av biometrisk data i pass og visumsøknader, begrunnes dette blant annet med at det skal forhindre alvorlig kriminalitet, identitetstyveri og illegal innvandring, altså faller formålet inn under følgende unntak i EMK artikkel 8 nr. 2 og P4 artikkel 2 nr. 3: ”hensyn til den nasjonale sikkerhet, offentlig trygghet eller landets økonomiske velferd, for å forebygge uorden og kriminalitet…eller for å beskytte andres

rettigheter og friheter." Både lovskrav og nødvendighetskrav må være oppfylt og inngrepet må være forholdsmessig. Når det gjelder spørsmålet om noe er "nødvendig i et demokratisk samfunn" for å fremme de formål EMK artikkel 8 (2) angir, har Høyesterett[41] uttalt følgende:

> "… MRD har utviklet en rettssetning om at konvensjonsstatene for så vidt har en skjønnsmargin, en "margin of appreciation", i forhold til konvensjonen og konvensjonsorganene."

Videre følger det av dommen:

> "I ordet "nødvendig" ligger etter konvensjonsorganenes praksis ikke mer enn at det må foreligge et vesentlig samfunnsmessig behov ("a pressing social need")".

Reglene som innføres vil ikke utgjøre en dramatisk forskjell fra hvordan reisekontrollen er allerede i dag, i den forstand at vi til nå ikke har måttet gjennom kontroller ved passering av landegrenser. Vi må legitimere oss med pass når vi er ute og reiser, og tredjelandsborgere må søke visum og innvilges innreisetillatelse til Schengen. De restriksjoner på den fri bevegelse som foreligger i dag, regnes ikke for å være i strid med retten til privatliv etter EMK. Det vil altså si at man før innføringen av biometrisk data ikke påberoper seg å reise anonymt uten å fremvise identifikasjonspapirer eller søke om reisetillatelser. Det som vil bli annerledes, og til dels er forandret ved at det er innført digitale ansiktsfoto, er at passene og visumsøknadene vil inneholde biometrisk data, og man oppretter, i alle fall for visumets del, sentrale databaser hvor det legges inn opplysninger om den enkelte. Det at vi allerede har visse kontrollformer begrunner ikke at man skal kunne innføre strengere tiltak, men jeg finner at vilkårene for unntak uansett er til stede da det vil foreligge lovskrav og minst et av nødvendighetskravene vil være oppfylt. Videre legges det opp til et forholdsmessighetskrav som innebærer at tiltakene man søker å

[41] Rt 1996 s. 551

oppnå må stå i forhold til de ulempene det innebærer for den enkelte. Det er avgjørende at ”inngrepet” står i et rimelig forhold til de negative virkninger det vil ha for den enkelte. For pass og regelverket som er tenkt ved innføringen der, mener jeg det foreligger forholdsmessighet mellom innføring av fingeravtrykk i passene og den sikkerhet man ønsker å oppnå ved legitimeringen opp mot ulempen for den enkelte. Hvis rettstilstanden vil holde seg slik den er i dag, at det ikke opprettes et sentralt register med alle fingeravtrykk i, vil fingeravtrykket måles opp mot passet idet du passerer kontrollen, og det vil ikke skje noen lagring. Altså foretas det en match der og da som slettes rett etterpå. Og jf passlovens § 6a skal den biometriske personinformasjonen som innhentes i forbindelse med utstedelse av passet ”slettes så snart passet er oversendt eller utlevert til passinnehaver”. Derimot synes jeg forholdsmessighetsvurderingen er vanskeligere når det kommer til VIS hvor det skal foreligge en sentral database med langt flere opplysninger om den enkelte enn det som skal lagres i et pass. Det er ikke ulempen ved å stå i registret i seg selv som vekker størst bekymring, men hva et slikt register kan benyttes til, hvem som får tilgang til det, vil det utsettes for sekundærbruk? Vil i så fall den enkelte være klar over hva opplysningene om vedkommende benyttes til?

EMK artikkel 6 nr. 2 inneholder det vi i norsk rett kaller for uskyldspresumsjonen, nemlig at ”enhver som blir siktet for en straffbar handling, skal antas uskyldig inntil skyld er bevis etter loven”. Det er altså påtalemyndighetene som har bevisbyrden for at noen er skyldig. EMK artikkel 6 er ikke aktuell før det eventuelt foreligger en sekundærbruk av den sentrale databasen i VIS eller en eventuell sentral database for lagring av fingeravtrykk. Med dette mener jeg at hvis en slik database benyttes til bruk utenfor reiseforhold, som var formålet, og i stedet benyttes til kriminalitetsbekjempelse, vil artikkel 6 bli aktuell. Da tenker jeg først og fremst på at det skjer en kriminell handling hvor politiet gis tilgang til databasen for å forsøke å identifisere eventuelle gjerningsmenn. Her vil man få en omvendt presumsjon: alle er skyldige inntil det motsatte er bevist. John Major uttalte en gang: ”If you’ve got nothing to hide, you’ve got to fear”. Det som gjør forkjempere for personvern skeptiske til bruk av fingeravtrykk i pass, er at det i passlovens § 8 er hjemlet at man senere kan opprette en sentral database hvor alle fingeravtrykk blir samlet. Siden man først har en

slik fingeravtrykksdatabase, hvor lang tid tar det da før man bestemmer seg for at denne databasen kan benyttes i kriminalitetsbekjempelse?

Samtidig er det slik i dag at hvis ditt fingeravtrykk først blir funnet på et åsted og politiet klarer å finne ut hvem som har vært der, må vedkommende jo i like stor grad som uten et slikt register, gjøre rede for sine handlinger. Hvis det har skjedd en kriminell handling hvor man har et gjerningssted, som for eksempel et innbruddstyveri, vil man sannsynligvis ha mange fingeravtrykk fra andre personer som var der både før og etter hendelsen. Det vil for det første være svært kostbart å sjekke og samle inn alle fingeravtrykk, så sjansen for at dette blir gjort er liten hvis det ”kun” er snakk om et innbrudd. Hvis dette blir gjort, gjør det noe med min rett til privatliv hvis jeg for eksempel har vært i det huset uten at jeg ønsker at det skal være opplyst. Jeg må kunne ferdes til steder hvor ikke alle skal behøve å vite at jeg har vært. Videre kan jeg komme opp i en situasjon hvor jeg må bevise at jeg er uskyldig i stedet for at påtalemyndighetene må bevise at jeg er skyldig, hvis spor av meg blir funnet. Man kan gå så langt som å si at tilstanden endrer seg fra at alle er uskyldige til at alle er potensielt skyldig til det motsatte er bevist. Vil dette likevel være vesentlig forskjellig fra i dag? Finner de først fem fingeravtrykk på stedet, og ved hjelp av undersøkelser kommer frem til at jeg har vært der, vil jeg fortsatt måtte forklare hva mitt ærend der var. Forskjellen er at det er lettere og økonomisk besparende for politiet. Likevel mener jeg at retten til privatliv er en så grunnleggende rettighet som stadig innskrenkes at det skal vesentlig tyngre hensyn og formål til enn ressursbesparelser.

2.4 Er biometriske kjennetegn alltid en personopplysning?

Det er liten tvil om at bruk av fingeravtrykk til et identifiserings- eller verifiseringsformål faller inn under personopplysningsbegrepet i personopplysningsloven § 2 nr. 1 og rådsdirektiv 95/46/EF artikkel 2, som den norske personopplysningsloven bygger på. Poenget er nettopp å etablere entydighet og å knytte fingeravtrykket til én person, og man benytter en identifiserings- og verifiseringsmetode som er unik for den enkelte, og et fingeravtrykk kan i utgangspunktet ikke knyttes til noen andre.

Vedrørende bruk av legitimering ved hjelp av passord/pinkoder, vil man blant annet måtte se hen til hvorvidt det er flere som har tilgang til samme koden, og om det foreligger noen tidsbegrensninger på når den enkelte kan benytte seg av koden. Hvis det er slik at flere har tilgang til samme kode, og til samme tid, vil det tale mot at det kan regnes for å være en personopplysning. Dette vil stille seg annerledes hvor legitimeringen foregår ved hjelp av et fingeravtrykk. Det kan ikke benyttes av andre, og vil i så henseende alltid være en personopplysning. Grensen vil altså her ikke gå på selve bruken, men hva slags biometriske kjennetegn som benyttes, og sikkerheten i bruken. Videre foregår det en diskusjon[42] i fagmiljøer på om biometrisk data alltid er "personal data", jf personverndirektivet artikkel 2 a. Her er det ikke arbeidsmengden og kostnaden som er bakgrunnen for spørsmålet, men skillet mellom det som kalles "biometric image" og "biometric template". For det første tilfellet er det ingen tvil om at det er en personopplysning. Vedrørende "biometric template" har det derimot vært en større diskusjon, da det har vært hevdet at det kan være uidentifiserbart. Det gjelder jo svært detaljerte deler av den enkeltes fingeravtrykk. Men det er like fullt unikt for hvert enkelt menneske, og en EU-rappport bekrefter at begge deler faller inn under personopplysningsbegrepet i personverndirektivet; som nevnt under avsnitt 1.7.5.2 har artikkel 29-gruppen slått fast at selv data som digitalt er omformet til et template er en personopplysning.

2.5 Skille mellom bruk av biometriske kjennetegn for å kunne identifisere en person entydig, og bruk av biometriske kjennetegn som ett av flere identifiserings- og verifiseringsmuligheter.

Ved å ta i bruk biometrisk kjennetegn er målet nettopp entydighet, det samme som ved bruk av fødselsnummer, hvor hver enkelt har sitt unike fødselsnummer. Ved en verifisering oppstår derimot spørsmålet om legitimeringen behøver å være entydig? Det kan være det, men er det nødvendig? Ta for eksempel adgangskort til en arbeidsplass, hvor enkelte adgangskort ikke inneholder mer enn en magnetstripe. Det fremkommer ingen personalia når kortet dras. Det interessante er at innehaveren av kortet har gyldig tilgang til bygget, og

[42] Liu, forelesning i personvern mars 2006.

det holder da at man innehar et kort, verken personalia eller kode er nødvendig. Kortet verifiserer at du har tilgang til bygget. Et annet eksempel på ofte brukt verifisering som man kanskje ikke tenker over i hverdagen, er når man har kjøpt en billett til teater/konsert/opera. Ved å fremvise billett viser du at du har tilgang til forestillingen. Det er ingen som vet hvem du er av den grunn, det er kun alder som kanskje sjekkes hvis det er aldersgrense. Da kommer jeg over på det som er problemet med lovteksten i personopplysningsloven, slik den er utformet i dag. Fordi den er så strengt utformet, kan heller ikke fingeravtrykk benyttes i verifiseringsformål, selv om det ikke er lagret andre personopplysninger i forbindelse med fingeravtrykket enn at du for eksempel har tilgang til bygget.

Datatilsynet har i flere tilfeller behandlet søknader om bruk av biometriske kjennetegn, da først og fremst fingeravtrykk. Dette gjelder blant annet treningssentre som SATS som ønsket å innføre tommelfingeravtrykk for å gjøre det enklere for kunden, som slipper å ha med treningskort. Avgjørelsene fra Datatilsynet og Personvernnemnda som omhandler bruk av biometriske kjennetegn skiller seg fra bruken som jeg har som fokus i min oppgave fordi formålene i deres avgjørelser er annerledes enn formålet for bruk av fingeravtrykk i pass og visumsøknader. Myndighetenes formål med bruken er av samfunns- og sikkerhetshensyn, mens formålet i de sakene som har versert for tilsynet mer har dreid seg om å forenkle adgangssystemer, og ikke et presserende, nødvendig samfunnsbehov. Bedrifter har også ønsket å innføre fingeravtrykk som et kontrolltiltak for å undersøke når den ansatte kommer på jobb og går hjem. Datatilsynet har likevel ikke funnet at bruken står i forhold til formålet (forholdsmessighetsprinsippet). For å benytte biometriske kjennetegn må det foreligge et saklig behov for sikker identifisering, og metoden må være nødvendig. SAS ønsket å benytte fingeravtrykk av sikkerhetsgrunner, men fikk avslag fordi personopplysningsloven i dag ikke hjemler bruk av entydige identifikasjonsmidler til et legitimeringsformål, mens for bruk av ansiktsbiometri i pass foreligger det egen hjemmel som tillater bruk av biometrisk data i et legitimeringsformål. Jeg finner det derfor riktig å avgrense forvaltningspraksis til det Datatilsynet har uttalt generelt i forhold til bruk av

biometriske kjennetegn, høringsuttalelser og lovforslag, og vil i det følgende i liten grad gå inn på enkeltsaker.

Har utviklingen gått dit hen at det i dag er nødvendig å benytte biometriske kjennetegn for å kunne foreta en sikker identifisering? Er det ikke tilstrekkelig lengre med for eksempel navn, bilde, adresse og fødselsnummer?

3 PRESENTASJON OG VURDERING AV FORSLAG TIL LOVENDRINGER SOM ÅPNER FOR UTVIDET BRUK AV BIOMETRISKE KJENNETEGN

3.1 Presentasjon og vurdering av Datatilsynets forslag til ny § 12a i personopplysningsloven

Den 31.03.2006 oversendte Datatilsynet til JD et forslag til endring av personopplysningsloven knyttet til bruk av biometriske kjennetegn.[43] Datatilsynet ser i hovedsak to problemer med dagens regulering av bruk av biometri. For det første er gjeldende lovgivning for streng, da pol. § 12 etter tilsynets oppfatning setter et tilnærmet totalforbud mot bruk av biometriske kjennetegn på en rekke områder der bruken kan være nyttig samtidig som personverntrusselen er liten. For det andre gir dagens regulering liten oversikt og kontroll med bruken, da reglene om melding og konsesjon er uoversiktlige.

Datatilsynets forslag til ny § 12a i personopplysningsloven åpner for å kunne benytte biometriske kjennetegn for legitimeringsformål. Bakgrunnen er at den någjeldende bestemmelsen ikke tar høyde for at biometriske kjennetegn er egnet ikke bare for et identifiseringsformål, men også for et legitimeringsformål. Da forslaget ble oversendt JD, kunne Datatilsynet ikke gi praktiske eksempler på bruk av biometrisk data som kan aksepteres etter gjeldende lovgivning. Det viser at ”andre entydige identifikasjonsmidler” i pol § 12 ikke lenger er en egnet formulering, i og med at alle aktuelle eksempler på ønsket av bruk gjelder fingeravtrykk for legitimeringsformål. Eksempler på søknader hvor Datatilsynet har måttet avslå trass i at formålet har vært legitimering, ikke identifisering, og hvor tilsynet mener at det i enkelte av sakene har foreligget et saklig behov, er blant annet søknaden om irisskanning i adgangskontrollen for ansatte ved Oslo Lufthavn Gardermoen, bruk av fingeravtrykk ved innsjekking av bagasje på fly, fingeravtrykk for å registrere timer på arbeidsplasser, fingeravtrykk som alternativ til garderobelapp.

[43] http://www.datatilsynet.no/upload/Dokumenter/saker/2006/Revisjon_12_biometri.pdf.

I tillegg til en hjemmel for bruk av biometriske kjennetegn for legitimeringsformål, foreslår Datatilsynet å innta en definisjon av hva som menes med ”biometri” og ”biometrisk kjennetegn” i pol § 2.

Jeg synes forslaget til ”biometriske kjennetegn” er mest klargjørende, lettere for en ”utenforstående” å forstå, og den forklarer mer enn forslaget til definisjon av ”biometri”. Samtidig synes jeg at definisjonene kunne benyttet terminologien ”identifisere” og ”legitimere/verifisere”, slik at forskjellen allerede kommer tydelig frem her, og at de som skal benytte seg av dette er kjent med begrepene. I stedet foreslår tilsynet under biometridefinisjonen ”brukt for å gjenkjenne en personidentitet eller bekrefte en påstått personidentitet”. Under definisjonen av ”biometriske kjennetegn” er ordlyden følgende: ”egnet for identifisering eller bekreftelse av en påstått identitet”. Jeg ville foreslått at § 2 også burde inneholdt en definisjon av hva autentisering er, og forskjellen identifisering versus verifisering. Dette er ikke aktuelt bare i forbindelse med biometriske kjennetegn. Det har tidligere oppstått forvirring ved bruk av fødselsnummer hvor det har vært ønsket brukt som legitimering i blant annet et tippesystem på internett. Kanskje er det ikke så lett ved første øyekast å se forskjellen på identifisering og legitimering når det ikke fremgår noen steder i loven hva det er, eller forskjellen på det.

For å kunne benytte biometriske kjennetegn til et identifiserings- eller legitimeringsformål etter tilsynets forslag, må det etter forslaget til *§ 12a første ledd* for det første foreligge et ”saklig behov” for bruken, og for det andre må behandlingen være tillatt etter lovens § 11. Forslaget skiller seg således ut fra dagens ordlyd i § 12 ved at det ikke etter § 12a oppstilles et krav om nødvendighet. Dette skyldes ikke at Datatilsynet ikke mener det skal foreligge et nødvendighetskrav, men ved at man sier at behandlingen skal være tillatt etter § 11, som igjen viser til at behandlingen må oppfylle vilkårene i § 8 og § 9, vil dette være et tilleggsvilkår som allerede ligger inne i bestemmelsen og således vil det være en gjentakelse. Likevel mener jeg at det vil være en viss lemping av kravene, og Datatilsynet åpner her for at biometriske kjennetegn kan benyttes i sammenhenger hvor det ikke er

nødvendig, men hvor for eksempel personvernrisikoen er liten og hvor vedkommende det gjelder har samtykket. Dette kan være ved bruk av fingeravtrykk i stedet for garderobelapp, hvor ingen person opplysninger om deg lagres, annet enn fingeravtrykket. Samtidig stiller kravet til saklig behov en nedre grense for hva som skal tillates. Det må være et saklig behov for en ”sikker …. bekreftelse av en påstått identitet”, og dette er en vesentlig endring fra gjeldende rett, som ikke har inneholdt noe om behov for en sikker bekreftelse av en oppgitt identitet, kun behovet for en sikker identifisering.

Etter forslaget til *§ 12a annet ledd* fremgår det at bruk av biometriske kjennetegn/biometri som innebærer behandling av sensitive opplysninger krever konsesjon fra Datatilsynet, som også for andre sensitive opplysninger etter loven, jf § 33. Men forslaget skiller seg fra annen bruk av sensitive opplysninger ved at man etter § 12a ”uten unntak” krever konsesjon. Slik er det ikke for øvrig bruk av sensitive personopplysninger etter loven. Det følger av § 33 annen setning at kravet om konsesjon ikke gjelder for sensitive opplysninger som er avgitt uoppfordret. § 12a oppstiller ikke noe slikt unntak fra konsesjonsplikten.

Etter forslaget til *§ 12a tredje ledd* oppstilles det vilkår for lagring av biometriske kjennetegn/biometri. Dette kan bare skje med hjemmel i lov, jf litra a, eller med samtykke fra den registrerte og konsesjon, jf litra b eller når det følger av personopplysningsforskriften, jf litra c. Det skal mer til for å kunne *lagre* biometriske kjennetegn, enn ved bare å *benytte* biometriske kjennetegn/biometri. Forslagets tredje ledd skiller seg fra de andre reglene i loven, hvor det enten må foreligge samtykke, hjemmel i lov eller nødvendighet, blant annet jf § 8. § 12a oppstiller en snevrere åpning for *lagring* enn for *bruk* av biometri, og den behandlingsansvarlig har etter § 12a tredje ledd ikke selv en adgang til å vurdere og bestemme at lagring av biometri er nødvendig. Videre er det ikke nok at den registrerte samtykker, det må også foreligge konsesjon fra Datatilsynet, så fremst det ikke er lovfestet med hjemmel i lov eller i personopplysningsforskriften.

Lagring av biometriske kjennetegn kan benyttes til langt mer og andre ting enn hvor et fingeravtrykk avgis og slettes rett etterpå, sekundærbruk og overkill. Idet et fingeravtrykk

ligger lagret er faren for misbruk til stede, og faren for at andre ”bryter seg inn” og benytter seg av informasjonen om den enkelte. Et skille mellom *behandling* og *lagring* av dataen legger opp til at slik data faktisk slettes med en gang den er avgitt. Spørsmålet er hvor realistisk et slikt skille faktisk er. Ved å avgi et digitalisert fingeravtrykk som garderobelapp vil dette måtte lagres i garderobesystemet slik at man ved på ny å avgi fingeravtrykk når man skal hente jakken, faktisk blir gjenkjent som den riktige eieren av jakken og ”garderobelappen”. Poenget med et verifikasjonssystem er nettopp å sammenlikne biometrisk data som ble avgitt av riktige innehaver av jakken for så å på ny avgi fingeravtrykk for å foreta en verifisering av at dataene stemmer. Det vil ikke være nødvendig med en sentral lagring, men en lokal lagring. Er likevel mulighetene for videre bruk av fingeravtrykket borte av den grunn? Det kan være viktig med et skille som Datatilsynet foreslår, men det bør klargjøres nærmere hva som menes med forslagets tredje ledd. Det kan være en god grunn å opprette forslaget hvis man skiller lagring av data fra *bruken* av et biometrisk verifiseringssystem. For eksempel bruk av fingeravtrykk i stedet for adgangskort på treningssentre. Her burde lagring av data fra bruken slettes. Man ligger lagret i systemet som kunde, men informasjonen om hvor ofte og lenge man trener, som registreres når man går inn og eventuelt ut, slettes automatisk. Videre er det et rettspolitisk spørsmål om det for enkelte former for lagring burde stilles strengere krav enn andre. I den sammenheng kan det være hensiktsmessig å skille mellom områder hvor man i dag ferdes anonymt, men hvor innføring av et biometrisk adgangskontrollsystem vil føre til at anonymiteten forsvinner, for eksempel ved bruk av fingeravtrykk for å gå inn på trikken for å vise at man har betalt.

I forslaget *§ 12a fjerde ledd* forslår Datatilsynet en hjemmel for å kunne gi pålegg om bruk av biometriske kjennetegn/biometri. To vilkår må være oppfylt for at Datatilsynet skal kunne påby en slik bruk. For det første må bruk av biometri anses for å være nødvendig for sikker identifisering eller bekreftelse (verifisering) av påstått identitet, og for det andre må bruken være nødvendig av sikkerhetshensyn. Hva som ligger i ”sikkerhetshensyn” utdypes ikke. Pol. *§ 12a femte ledd* åpner for at det i forskrift kan gis nærmere regler om bruk av biometri.

Fordelen med å hjemle bruk av biometriske kjennetegn i personopplysningsloven er at man får en generell hjemmel som myndighetene og privatforetak kan benytte, og man slipper å måtte lovfeste bruken i enkeltsituasjoner i spesiallover som passloven og utlendingsloven. Samtidig kan det være en fordel å regulere bruken i enkeltlover da dette synliggjør et bestemt formål for bruken, og kanskje i større grad forhindre sekundærbruk eller "overkill".

3.2 Presentasjon og vurdering av Arbeids- og inkluderingsdepartementets forslag til ny § 37 f i utlendingsloven

3.2.1 Generelt

Arbeids- og inkluderingsdepartementet (AID) sendte i mars 2006 ut et høringsforslag om å innføre en lovhjemmel for å implementere et felles europeisk informasjonssystem, Visa Information System (VIS).[44] Bakgrunnen for forslaget er Norges rettslige grunnlag for deltakelse i EU/Schengen-samarbeidet, og siden deler av samarbeidet består av avskaffelse av personkontroll på medlemsstatenes felles grenser, som igjen fører til at alle som oppholder seg på det europeiske territoriet kan bevege seg fritt over grensene innenfor territoriet, må alle medlemslandene ha et felles og ensartet regelverk som håndheves likt av alle landene. VIS skal inneholde felles prosedyrer for utveksling av informasjon om visumsøkere mellom medlemslandene for å kunne behandle en søknad om visum inn til et Schengen-land. Ikke alle slags opplysninger om personer skal kunne legges inn i systemet, men nødvendige opplysninger om som navn, fødselsdata, nasjonalitet og biometriske data, i tillegg til at VIS skal inneholde avgjørelsene som landene foretar i behandlingen av en visumsøknad. Det er også tenkt at VIS skal inneholde opplysninger (navn og adresse) om personer tilhørende et Schengen-land som inviterer en tredjelandsborger som er visumpliktig inn i Schengen.[45] I høringsbrevet fremgår det at man mener at det er

[44] Høringsbrev, endring i utlendingsloven av 06.03.2006 Referansenr. 200600492.

[45] AIDs høringsbrev s. 4.

nødvendig å behandle biometrisk data i VIS for å sikre nøyaktig verifikasjon og identifikasjon av visumsøkere, og VIS skal inneholde ansiktsfoto og fingeravtrykk. Det er kun det enkeltes lands autoriserte visummyndigheter som har rett til å legge inn, endre og slette opplysninger i VIS. Andre autoriserte myndigheter vil ha lesetilgang til systemet, men ikke ha mulighet til å gjøre noe med opplysningene som ligger der. Informasjonen om enkeltpersoner blir slettet etter fem år, eller tidligere dersom en visumsøker erverver statsborgerskap i et EU/Schengen-land. Det fremkommer av departementets høringsbrev at personverndirektivet vil gjelde for enhver tilgang til og bruk av systemet. Det foreligger i dag ingen bestemmelser om å registrere og lagre biometrisk informasjon i forbindelse med visumsøknader.

Et hensyn bak innføringen av VIS er at systemet skal forebygge trusler mot statenes indre sikkerhet. Andre formål som fremheves er at VIS skal avverge "visashopping", det vil si at en søker strategisk velger å søke visum i det landet hvor han tror sjansene er størst for å innvilget visum, VIS skal lette identifikasjon og tilbakesendelse av ulovlig innvandrere og gjøre jobben med å ta forfalskninger enklere. Videre har formålet blitt utvidet underveis, og nå opplysninger skal kunne benyttes av "rette myndigheter" for å sikre intern sikkerhet ved å "forhindre, avdekke eller etterforske kriminelle handlinger, spesielt terrorisme".[46]

Någjeldende utl. § 37 omhandler identifisering, og departementet fant det hensiktsmessig å plassere ny hjemmel for implementering av VIS-forordningen i tilknytning til § 37, og har foreslått en ny bokstav f i § 37.

Forslaget til *§ 37 f første ledd* innebærer at visumsøkere ned til (sannsynligvis) 6 år skal registreres med ansiktsfoto og fingeravtrykk, og den biometriske informasjonen skal overføres til VIS-databasen. En stor internasjonal database kan gjøre det vanskelig for den enkelte å gjøre seg kjent med sine rettigheter og hvor man skal henvende seg for å gjøre

[46] AIDs høringsbrev s. 7.

disse gjeldende. Datatilsynet anfører i sitt høringsforslag[47] at de synes det er svært betenkelig at barn skal avkreves fingeravtrykk. Forslaget til nytt *§ 37 f andre ledd* hjemler at nødvendige opplysninger som innehentes for å kunne behandle en visumsøknad og opplysninger tilknyttet utfallet av søknaden, samt annullering, tilbakekall og forlengelse, skal overføres til VIS. I forslagets *§ 37 tredje ledd* fremkommer det at personopplysningsloven skal gjelde dersom ikke annet er bestemt ved forskrift eller lov. Videre foreslås det hjemlet at man i forskrift kan gi nærmere regler om behandling av opplysningene som innsamles, hvilke myndigheter som skal ha tilgang til hvilke opplysninger og for hvilke formål.

Det foreslås ikke å lovfeste hvilke myndigheter som skal ha tilgang til den sentrale VIS-enheten, eller hvilke opplysninger og til hvilke formål de skal ha tilgang til. Dette skal fremkomme av en eventuell forskrift. Med tanke på at det fremkommer av forslagets andre ledd at opplysninger som er "nødvendige" for behandling av søknad om visum skal legges inn, og det ikke nærmere er spesifisert hva slags opplysninger dette konkret dreier seg om, og heller ikke lovfester hvem som skal ha tilgang opplysningene og til hvilket formål de kan benytte disse opplysningene, kan det være grunn til å stille spørsmålstegn ved hvor egnet dette forslaget er til å ivareta den enkeltes personvern og rettssikkerhet. Det burde komme klart frem av bestemmelsens andre ledd hva slags opplysninger den enkelte plikter å oppgi, og av tredje ledd hvem som har tilgang på disse opplysningene, og hva de kan benyttes til. Datatilsynet skriver i sin høringsuttalelse[48] at lovregulering vil være et tiltak for å forhindre at andre samfunnsaktører enn de som opprinnelig var tiltenkt tilgang til store databaser i ettertid fremmer mer eller mindre legitime behov for tilgang, noe som fort vil komme i konflikt med formålet for opprettelsen av databasen. Videre er det viktig å ha avklart ansvarsforholdet slik at man vet hvem som har ansvaret for å oppfylle kravene i

[47] Datatilsynet: Høringsuttalelse – endring i utlendingsloven – innføring av lovhjemmel for å implementere et felles europeisk visum informasjonssystem – visa information system (VIS) s. 2 av 24. april 2006.

[48] Datatilsynet: Høringsuttalelse – endring i utlendingsloven – s. 3.

personopplysningsloven og utlendingsloven. Det burde stilles høye krav til bestemmelsene, ikke bare på nasjonalt plan, men også i Schengen. Når regelverket først er ferdig utarbeidet, kan det føre til norske myndigheter må godta tiltak som er mer vidtrekkende enn det nasjonalt er behov for.

3.2.2 Innebærer lovutkastet en lovfesting av helautomatiske avgjørelser i strid med pol. § 25?

Jeg kan ikke se at det i forslaget til endringer i utlendingsloven vurderes om det å avgi fingeravtrykk i grensekontrollen er en helautomatisk avgjørelse. Det vil si at det ikke har vært noen individuell vurdering av saken, se til eksempel ”Personvern i informasjonssamfunnet” side 156. ISO/IEC 24714-1 fremhever under avsnitt 4.2.3 at det bør foreligge en del prinsipper ved bruk av biometri, og sier på side 6 følgende om bruk av helautomatiske avgjørelser:

> ”Where biometric systems are used to make significant and fully automated decisions about individuals, a mechanism to request the intervention of a person should be provided. Individuals should be notified of such automated decisions.”

Det er en maskinell behandling som avgjør om ditt fingeravtrykk matcher med det som ble lagt inn da du søkte visum. Det er anledning til å foreta automatisk behandling jf personopplysningsloven § 22, men det fremgår av personopplysningsloven § 25 første ledd, som bygger på EUs personverndirektiv, at en person som utsettes for en automatisert avgjørelse, ”kan kreve at avgjørelsen overprøves av en fysisk person.” Retten som innrømmes etter første ledd gjelder ikke dersom visuminnehaverens ”personverninteresser varetas på en tilstrekkelig måte og avgjørelsen er hjemlet i lov”, jf § 25 annet ledd. Det kan stilles spørsmålstegn ved om personverninteressene ivaretas på en tilstrekkelig måte når man risikerer å bli avvist på grensen ved at en maskinell operasjon ikke klarer å identifisere deg fordi du kanskje har en rift i fingeren. Hvilken myndighet har man tenkt å tillegge personen som sitter i kontrollen? Hvis vedkommende skal vurdere om du fremstår som troverdig nok til at man velger å slippe deg gjennom, vil ikke dette systemet være så sikkert

som målet er. Slik VIS er utformet per i dag, vil det være en sentral database hvor det legges inn opplysninger med blant annet fingeravtrykk. Når en med innvilget visum går gjennom kontrollen og legger på fingeren, vil dette fingeravtrykket sendes til databasen, som da foretar en sjekk for å se at avtrykkene matcher med oppgitt identitet, og at visum er utstedt. Problemet i så henseende er at et fingeravtrykk aldri vil gi et 100 prosent treff, og at man da må sette en grense for hvor mye som må stemme. Jo lavere den grensen settes, jo større sjanse er det for at det oppstår en ”false acceptance”, og jo høyere grense, jo større sjanse for at det oppstår en ”false rejection”. Det anslås (Tom Halvorsen, AID) at det innen 5 – 6 års tid vil foreligge 70 millioner fingeravtrykk i VIS-databasen. Da er det ikke umulig å tenke seg at 1000 personer vil kunne ha 80 prosent treff på samme fingeravtrykk. Jo større database, jo større mulighet for at flere oppnår samme gjenkjenning. Dette er jo i seg selv ikke en ukjent problemstilling. FBI har jo benyttet seg av samme metode i mange år, og har om lag 40 millioner fingeravtrykk i sin database. Men hvis FBI får opp et treff på et fingeravtrykk, vil de ikke automatisk utvise eller fengsle personen som er identifisert på avtrykket. Der vil avtrykket bli gjennomgått av en ekspert som knytter dette fingeravtrykket til andre omstendigheter i saken. Dette kan også sammenlignes med KRIPOS i Norge. Finner de et fingeravtrykk på et åsted for en kriminell handling, vil eksperter gjennomgå avtrykket og også undersøke om det er flere holdepunkter på stedet som kan knytte vedkommende til hendelsen. Problemet med VIS er at det ikke vil være en person som kan vurdere fingeravtrykket mitt og for eksempel gå god for at jeg virkelig er meg, men har kuttet meg i fingeren siden avtrykket ble tatt første gang og lagt inn i databasen. I det jeg står der og ikke får et treff som meg selv (false rejection) har jeg ingenting jeg skal ha sagt, for maskinen har allerede avslått meg og i verste fall knyttet meg til en annens identitet.

Dette vil kun gjelde for tredjelandsborgere, da det enda ikke er sendt ut forslag om fingeravtrykk i pass. Hvis det er slik at det å slippe gjennom pass- og visumkontrollen kan regnes for å være et enkeltvedtak i forvaltningslovens forstand, selv om det i seg selv er et formløst vedtak, vil personopplysningslovens regler om automatiske avgjørelser gjelde for

tredjelandsborgere så lenge de befinner seg på norsk territorium, jf forvaltningsloven § 2 første ledd bokstav b, jf pol. § 4 første ledd.

Jeg mener ut i fra det jeg har sagt over at det i alle fall fra myndighetens side bør vurderes om dette vil være å innføre en helautomatisk avgjørelse og drøfte de hensyn som gjør seg gjeldende i så henseende.

4 RETTSPOLITISK DRØFTELSE

4.1 Personlig frihet kontra effektiv utlendingskontroll

Det å avgi fingeravtrykk er noe mange forbinder med kriminell aktivitet, da fingeravtrykk har blitt benyttet for å kunne knytte gjerningsmenn til gjerningssted. Imidlertid er fingeravtrykk i dag på vei til å bli assosiert med mer positiv identifikasjon av den lovlydige borger, blant annet fordi det i dag finnes treningssentre (blant annet Oxigon i Oslo) hvor man avgir tommelavtrykk for å vise at man er medlem. Idet utviklingen har ført til at fingeravtrykk benyttes for å legitimere hvem man er, det være seg i pass eller adgangskort, vil også stigmatiseringen og forbindelsen til kriminalitet ved bruk av teknologien etterhvert forsvinne.

Faren ved at teknologien stadig utvikles og benyttes til å føre kontroll med mennesker er at vår atferd endres i tråd med overvåkingen. Vi har en rett til å være privat, og dette rører ved den rettigheten. I ytterste konsekvens kan det vurderes om stadig overvåking vil ha betydning for vårt forhold til ytringsfriheten. Vil vi legge bånd på oss selv når vi vet at alle våre bevegelser, reiseruter, e-postkorrespondanser med venner og familie, og så videre, blir oppfattet av andre og lagret?

En annen utfordring er ikke faren for feil, men en økt fare for liv eller helse ved utvidet bruk av biometri. Er det godet du får tilgang til ved å avgi fingeravtrykk stort nok, er ikke tanken på at noen vil kutte av deg fingeren for å få tilgang utenkelig. I forhold til kontroll ved grensepassering er det derfor viktig at det ikke bare er maskiner som leser passet og avtrykket ditt, men at en fysisk person ser at det er samme person som går igjennom, som er eier av fingeravtrykket. Myndighetene har allerede vurdert dette og det skal skje en personlig kontroll ved utenriksstasjonene og på grensekontrollene.

Ett av hensynene bak forslaget om fingeravtrykk i pass og visumsøknader er at man på grunn av faren terror ønsker å stille høye krav til sikkerheten på flyplasser. Dette er et forståelig synspunkt. Datatilsynet[49] har likefullt et godt poeng når de sier at en jernbanestasjon kan være et like godt egnet terrormål som en flyplass, uten at det aksepteres at de samme sikkerhetsrutiner innføres for adgang til jernbanestasjonen. Til argumentet om at man ved bruk av biometriske kjennetegn i pass skal kunne stanse terrorister ved passering av grense, uttalte Kastrups Lufthavns sikkerhetssjef Anders Maegaard at "man ikke kan se på iris om folk har en pistol i baglommen". Han mener at biometri ikke har en "berettigelse sikkerhedsmæssigt".[50]

4.2 Bedre beskyttelse mot identitetstyveri

Ved å legitimere seg ved hjelp av noe du har fysisk på kroppen din, reduserer du muligheten for at noen kan misbruke din identitet. Det er ikke nok å lære seg en kode eller stjele et kort for å kunne utgi seg for å være en annen, kalt identitetstyveri. Bruk av fingeravtrykk sammen med annen teknologi som allerede benyttes i bankkort/pass, kan kombinasjonen gjøre det umulig for andre å stjele eller forfalske pass eller bankkort. Dette kan gjøres ved at man setter bankkortet inn i minibanken, og i stedet for å taste en pinkode, legitimerer man seg ved å avgi et fingeravtrykk. Dette vil ikke forhindre ikke tvangstilfeller som at en person blir truet og tvunget til å oppgi pinkoden sin. Det samme kan skje ved bruk av fingeravtrykk. I stedet for å tvinge deg til å avgi noe du *har* og *vet*, tvinges du til å avgi noe du *er*, ved at man setter inn sitt kort og avgir et fingeravtrykk mens noen står og venter klar for å ta pengene som kommer ut. Samtidig vil du jo bli konfrontert med det faktiske forhold med en gang og være klar over at du har blitt svindlet, i motsetning til i dag hvor det kan benyttes utstyr hvor kortet forsvinner og man tror det har skjedd en bankfeil.

---

[49] http://www.datatilsynet.no/upload/Dokumenter/saker/2006/Revisjon_12_biometri.pdf s. 6.

[50] (Det danske) Teknologirådets nyhedsbrev til folketinget: På vej mod biometriske pas nr. 198 januar s. 5 2005.

For den enkelte kan det fremme personvernet at vedkommendes pass og visumetikett inneholder ett av ens fingeravtrykk. Dette gjør at når man har søkt visum og fått tillatelse til å reise, kan ingen stjele visumet og reise i vedkommendes navn, for fingeravtrykkene vil ikke matche. Videre vil bli mindre attraktivt å stjele eller selge pass, siden ingen andre likevel kan benytte seg av det. Personverneffekten er at identitetstyver ikke vil kjenne til eller kan benytte andres personalia, og man kan i større grad beskytte sitt privatliv.

På den ene siden er det jo slik at bruk av teknologien og fingeravtrykk til en viss grad kan avhjelpe identitetstyveri. På den annen side er det slik at systemer ikke nødvendigvis blir sikrere av at det legges inn et fingeravtrykk. Hvis noen først søker om pass eller visum og oppgir mine personalia, men avgir sitt eget fingeravtrykk, og får innvilget et visum i mitt navn, men med sitt fingeravtrykk, vil ikke en verifiseringskontroll forhindre vedkommende i å krysse landegrenser. Den kontrollen vil bare kunne sjekke at det er en fingeravtrykksmatch, og at vedkommende har en gyldig tillatelse. Kontrollen vil ikke kunne avdekke om det i systemet er lagt inn falske eller uriktige opplysninger. Legger man uriktige opplysninger inn i systemet, vil dette følge hele prosessen. Har en person fått utstedt identitetsdokumenter i mitt navn, men med sitt fingeravtrykk, vil det kunne være vanskelig for meg å bevise at det er min identitet, og at mitt fingeravtrykk er det riktige til den identiteten. Det må nevnes at dette særlig vil gjelde land hvor man ikke har en fungerende sentralmyndighet hvor man kan sjekke navn opp mot registre, som for eksempel Somalia. Samtidig ligger det ikke bilde av meg i folkeregisteret, så stjeler noen min identitet, er det ikke utopisk å se for seg at dette kan skje i Norge også. Konsekvensene av at det skjer en feil mye større. Du kan få et nytt bankkort og ny kode, men ikke et nytt fingeravtrykk.

Det kan foreligge gode personvernhensyn til grunn for å innføre biometriske kjennetegn mot faren for identitetstyveri. Får man frastjålet sin identitet og noen legitimerer seg som deg overfor banken, ligningskontoret og andre, vil tyven få tilgang til sensitive opplysninger om deg, og kan foreta disposisjoner i ditt navn. Det er et problem at enkelte banker i dag godtar personnummer som legitimering over telefon, men så lenge det skjer

vil misbruk fortsette. Det betyr ikke at vi skal gå mer dramatisk til verks istedet for å drive opplysningskampanje om hva et personnummer egentlig er og hvor enkelt det er ved bare noen få tastetrykk å få tak i en annen persons personnummer, men biometriske kjennetegn vil i stor grad forhindre det misbruket av den enkeltes personvern et identitetstyveri faktisk er. Kanskje kan det gjøre bransjen mindre lukrativ. Dette vil være til gunst for den enkeltes personvern, særlig den grunnleggende rett til privatliv og å selv disponere over opplysninger om seg selv. Det er viktig å se at bruk av biometriske data ikke bare vil være til gunst for myndighetenes del, men som også kan fremme den enkeltes vern mot inngrep i den private sfære. Myndighetenes og borgernes forhold tatt i Norge i betraktning, er det per idag ikke myndighetsmisbruk vi har å frykte, men et stadig større, internasjonalt nettverk av kriminelle som misbruker andres identitet i blant annet økonomiske vinnings hensikt, og for selv å kunne skjule sin egen identitet for å skjule kriminelle handlinger.

Bruk av fingeravtrykk i reisedokumenter kan i større grad forhindre dokumentforfalskning ved at det blir vanskeligere å forfalske dokumenter på grunn av den teknologien man benytter (for eksempel RFID-brikker), og på den måten vil man i noe større grad kunne forhindre illegal innvandring. Norske utlendingsmyndigheter opplever i dag at noen innvandrere kommer med falske dokumenter. Hele dokumentet forfalsket kan være forfalsket, andre ganger er det ekte dokumenter med falske opplysninger eller falske dokumenter med ekte opplysninger. Slike dokumenter forhindres i stor grad ved å innføre fingeravtrykk, da det vil være svært vanskelig å endre dokumentet i ettertid, i alle fall forverre prosessen med å forfalske dokumenter. I dag finnes det dokumenter med fingeravtrykk som norske myndigheter ikke alltid finner å kunne legge til grunn. Disse dokumentene inneholder ingen RFID-brikke som gjør at vedkommendes fingeravtrykk kan matches med avtrykket i dokumentet, for eksempel statsborgerbevis med fingeravtrykk. Det er også å kunne kontrollere når fingeravtrykkene eventuelt ble satt inn i dokumentet. Så langt det er opplyst, er det ikke per i dag oppdaget forfalskninger i bruk av biometriske pass, kun gamle pass som ikke inneholder biometrisk data. Samtidig er det et poeng at nesten ingen land har tatt i bruk eller innehar utstyr for å lese av et biometrisk pass.

4.3 Effektiv utlendingskontroll

4.3.1 Sikker identifisering

Den eneste sikre måten per i dag for å knytte en identitet til en person, er ved bruk av biometri. Man kan fremlegge ekte dokumenter med ekte opplysninger, men eneste måten å forhindre at en tvilling reiser under sin søskens identitet, er ved bruk av biometriske kjennetegn. Reisende er underlagt diverse kontrollformer. Selv om visumsamarbeidet blant annet går ut på at Schengen-landene skal ha fri bevegelse, er det slik at pass er det eneste godkjente identitetskortet norske borgere har i dag. Til tross for at det ikke er påkrevd å vise pass på de indre grensene i Schengen, må vi likevel ha det med på reiser ut av Norden. Vedrørende bruk av digitale ansiktsfoto og fingeravtrykk i pass og visum, befinner vi oss på et område hvor vi uansett ikke beveger oss anonymt. Dette fordi det allerede før innføringen av biometriske kjennetegn foreligger kontrolltiltak. Vi har pass som allerede inneholder personopplysninger, og når man søker visum oppgir man en rekke opplysninger om seg selv og formålet med reisen. Sånn sett skiller innføringen av biometriske kjennetegn i pass og reisedokumenter seg fra andre områder hvor det ønskes innført, for eksempel til erstatning for garderobelapper på utesteder. Dette fordi man i sistnevnte tilfelle vil avgi opplysninger på et område hvor man i dag er anonym. Når man i dag henger fra seg kåpen i garderoben på et utested, har ikke den ansatte oversikt over hvem jeg er. Ved å benytte fingeravtrykk til slike praktiske formål, foretas det faktisk en reell begrensning i muligheten til å bevege seg anonymt. Det samme vil imidlertid ikke være tilfelle i situasjoner hvor man er pålagt å oppgi sin identitet eller legitimere seg. Ved bruk av fingeravtrykk til praktiske hensyn kan man slette avtrykket så snart jakken er hentet, men de potensielle farer som foreligger ved slik bruk av biometri vil jeg av plasshensyn ikke gå videre inn på. Samtidig må det ses hen til om det å avgi fingeravtrykk baserer seg på samtykke eller om man er forpliktet til det. Spørsmålet videre er om dette er et *reelt* samtykke; hvis man ikke avgir fingeravtrykk får man heller ikke henge av seg jakken i garderoben.

Når man taster en pinkode eller oppgir et passord vil man alltid oppnå en hundre prosent match på at det oppgitte tallet/koden er riktig eller gal. Er koden riktig, betyr det ikke at det er rette vedkommende som oppgir koden/passordet, men vedkommende er legitimert til å utføre tjenesten. Motsatt utfall kan også tenkes, at det er rette vedkommende som taster koden, men at han taster feil, og av den grunn ikke får tilgang. Dette vil kunne stille seg annerledes ved bruk av et fingeravtrykk. Bare den rette eieren av avtrykket kan legitimere seg med det. Samtidig er teknologien slik at man kanskje ikke setter en hundre prosent match som standard, da dette vil kunne ende med at rette vedkommende ikke klarer å legitimere seg ved hjelp av sitt eget fingeravtrykk grunnet for eksempel et sår eller ripe på fingeren. Dette gjør at man kanskje vil måtte sette en lavere prosent enn hundre for at riktige vedkommende faktisk skal kunne legitimere seg som seg selv. Dette kan igjen føre til at systemet ikke blir like sikkert som ved en pinkode eller et passord som man må kunne hundre prosent, ved at noen med et liknende fingeravtrykk kan passere som meg. For pinkoder og passord er altså risikoen at feil person benytter seg av de i et legitimeringsformål, mens for bruk av fingeravtrykk vil man i utgangspunktet ha rette vedkommende, men ikke hvis man må sette ned grensen for prosenttreff. Hundre prosent match ved tastet pinkode kan altså være mer feil enn åtti prosent treff på et fingeravtrykk hvis det avgjørende er at det er riktig person som står bak.

4.3.2 False acceptance versus false rejections

Et av formålene med å innføre fingeravtrykk er at man ønsker å redusere falske innvilgelser, ”false acceptance”, det vil si at personer passerer sikkerhetskontroller med uriktige identitet. Samtidig vil et fingeravtrykk aldri vil gi en hundre prosent match, og ved å stille krav om høy matchprosent risikerer man en ”false rejection”, det vil si at man blir avvist på grensen fordi resultatet av fingeravtrykkssammenlikningen ikke er sikker nok til at det kan legitimere at personen er seg. For det første er det viktig at de som betjener systemet er oppmerksomme på at det kan komme opp situasjoner hvor folk blir avviste som seg selv. Minst like viktig er det at den enkelte blir orientert om at dette faktisk kan skje. Folk flest tror at et fingeravtrykk er hundre prosent pålitelig, slik det er fremstilt i straffesaker. Det må foretas en avveining mellom hva som er å foretrekke – at noen slipper

inn under en annens identitet, eller at rette vedkommende ikke blir legitimert som seg selv? Ved å benytte avtrykk av alle ti fingrene i stedet for en eller to, vil man forminske risikoen betraktelig for at noen kan komme gjennom som deg. Men dette er en svært krevende identifikasjonsmåte og det vil belaste databasen enormt.

4.3.3 Shit in – shit out

Shit in – shit out-problematikken dreier seg om at det ikke kommer mer fornuftig ut av et system enn det man har lagt inn. Et problem man har sett i den senere tid er at personer som ønsker å søke asyl i Norge oppgir ulike identiteter i land de blir stoppet i på tur til Norge for å forsøke å forhindre å bli sendt tilbake til "første asylland". For eksempel vil irakere som har oppgitt flere identiteter, og som det av den grunn foreligger en identitetstvil rundt, i dag få utstedt gyldige og lovlige pass fra for eksempel Den irakiske ambassaden i Stockholm. Norge anerkjenner disse passene som gyldige reisedokumenter, men passene identifiserer likevel ikke hvem du er. Dette fordi det ved utstedelsen av passene ikke foreligger en underliggende god nok kontroll av personens faktiske identitet. Et fingeravtrykk fra eller til vil ikke kunne bekrefte noe mer hvem du faktisk er enn det passet gjorde uten fingeravtrykket. Det er derfor svært viktig at den underliggende kontroll med hvem en person *er* ved utstedelse av et pass eller visum er grundig. Samtidig er det viktig å nettopp være oppmerksom på at et fingeravtrykk ikke nødvendigvis sier noe mer om hvem du er.

Det må påregnes at uansett hvilke tiltak myndighetene setter i gang, vil det alltid være personer som forsøker å omgå reglene. Det kan tenkes at man forsøker å file vekk fingeravtrykkene eller kutter av fingertuppene. Falske fingeravtrykk kan lages ved hjelp av samme ingredienser som man lager gelégodteri med. [51] I 2002 fremla kryptograf og matematiker Tsutomu Matsumoto og forskere ved Yokohama National University falske fingrer lagd av gummibjørnstoff. De testet 11 ulike biometriske fingeravtrykkssensorer, og alle ble lurt ved 80 prosent av forsøkene. Undersøkelsen deres viste at det er billig og

[51] http://www.forskning.no/Artikler/2002/mai/1021978415.94/artikkel_print Lest 08.11.2006.

enkelt å forfalske fingeravtrykk, enten de er lagd av en direkte avstøpning av fingeren, eller fingeravtrykket er hentet fra glass eller andre harde overflater. Inspirert av dette valgte en teknolog ved den tekniska högskolan i Linköping[52] å lage falske fingeravtrykk som sin eksamensoppgave. Hun rekonstruerte et fingeravtrykk fra en kollegas avtrykk på et glass som hun penslet med et fint pulver som størknet på avtrykkets fett. Avtrykket ble flyttet med teip over til et papir og fotografert. Videre fremkalte hun bildet med ultrafiolett lys på en overflate som er lysømfintlig og kobberbelagt som blir til et tredjemisjonalt kort av det originale fingeravtrykket, og som man da skaper en ny avstøpning av. Gelatin har samme fuktighet som en finger og leder varme og elektrisitet nesten som hud. Dermed kan sofistikerte avlesere som har varmesensorer lures. Studenten dro sammen med kollegaen til datamessen Cebit i Hannover der flere fingeravtrykksavlesere var utstilt. Kollegaen avga sitt fingeravtrykk i systemet, og så forsøkte de å logge inn med det den falske gelatinfingeren. Det fungerte utmerket. Den ekte fingeren ble godkjent i 90 prosent av tilfellene, den falske ble godkjent i 86 prosent av forsøkene. Forsøkene viser to ting: for det første at systemene kan omgås, og at sikkerheten rundt disse systemene er svært viktige. For det andre viser det at bruk av noe man *er* i seg selv ikke behøver å være sikrere enn noe man *vet* eller *har*. Det er ikke slik at alle og enhver vil lage gelefingrer, og at man skal forkaste tanken på et slikt system. Samtidig er det slik at bruk av biometrisk data i dag begrunnes i blant annet å hindre kriminalitet og identitetstyverier. Når det er så enkelt å ta med seg en flaske eller et papir noen har tatt på for så å kopiere dette hjemme på kjøkkenbenken, er det gode grunner for å spørre om et system med fingeravtrykk vil stoppe kriminelle. Dette kan stille seg annerledes ved bruk av irisskanning.

4.4 Overkill-problematikken og sekundærbruk/overskuddsinformasjon

I den fysiske verden er det ikke uvanlig at man utgir mer informasjon enn hva som er nødvendig. For eksempel ved å vise legitimasjon på polet for å bekrefte at man er over 20 år for å kjøpe sprit. Det bankkortet man viser for å legitimere at man er over 20 år gir ekspeditøren langt mer informasjon enn han i utgangspunktet har behov for, blant annet får

[52] MAGASIN DIREKT #1/2005 s. 3.

han opplyst ditt fulle navn, personnummer og kontonummer, selv om han i utgangspunktet bare har behov for fødselsdatoen. Men i det daglige regnes ikke dette for å være et problem, da ekspeditøren konsentrerer seg om fødselsdatoen og bildet, og sannsynligheten for at han husker noe mer er svært liten. Slik er det ikke i den elektroniske verden. Her vil alle disse opplysningene bli lagret, og forsvinner ikke av seg selv, og det kan være vanskelig for den enkelte å vurdere risikoen ved å avgi noe man *er*. Sekundærbruk er ikke tillatt såfremt det ikke er i tråd med det opprinnelige formålet, jf. pol § 11, og regelen hjemler et viktig personvernhensyn. Overskuddsinformasjon kan forklares som informasjon som er unødvendig i den aktuelle konteksten.[53]

Når personverninteresserte er bekymret for utviklingen ved bruk av noe man *er* i et legitimeringsformål, er det kanskje ikke først og fremst selve formålet som ligger til grunn for bruken, men tanken om at fingeravtrykket kan benyttes til sekundærbruk og at et fingeravtrykk kan avgi mer informasjon om deg enn det som er påkrevd etter formålet, overskuddsinformasjon. Den danske teknologirådet frykter sekundærbruk ved bruk av fingeravtrykk i pass. Det er utsikten til register og opprettelsen av sentrale databaser som vekker bekymring. I deres rapport siteres Peter Blume, professor i jus fra København universitet:

> ”Vi ved alle, hvordan det vil gå. Først indfører man biometri i pas og når vi så har vænnet os til det, vil man også opprette registre. Når først de er der mangler man bare en alvorlig hændelse med nogle ofre, hvorefter politiet vil sige: Vi har mulighederne, hvorfor ikke bruge dem? Og så vil politikerne sige ja.”

Dette skaper et potensial for intensiv overvåkning av borgerne når de er ute og reiser. Man får et system hvor alt borgerne foretar seg blir synlig for myndighetene, mens borgerne opplever motsatt situasjon, man ser ikke lenger hva personopplysningene brukes til.

[53] Teknologirådet: Elektroniske spor og personvern side 104.

Faren for sekundærbruk oppstår ikke bare i forhold til kriminalitetsbekjempelse og at landets myndigheter ønsker å kunne benytte et slikt fingeravtrykksregister til andre legitime formål enn selve identifiseringen/legitimeringen ved grensekontrollen. Også andre aktører vil kunne ha interesse av personopplysninger som er lagret i registre, blant annet andre lands myndigheter. For eksempel ønsker myndigheter i USA å kunne foreta en DNA-sjekk, og resultater av denne sjekken vil kunne forhindre innreise ved at det fremkommer at vedkommende som sjekkes har en alvorlig sykdom. Allerede i dag må europeiske luftfartsselskaper avgi personopplysninger om alle passasjerer som flyr til USA. Det er kjent at USA har alarmsystemer som ut ifra navn, adresse, telefonnummer, reiseplan, kredittkortnummer, med mer, skal screene flyreisende mot regjeringens terroristlister.[54] I programmet "60 minutes" fikk man se hvordan over 30 amerikanske menn med sammen fornavn og etternavn hadde fått problemer da de skulle ut og reise på grunn av dette alarmsystemet. Det er ikke til å komme utenom at også private aktører kan ha stor interesse av et slikt register, i første omgang arbeidsgivere og forsikringsselskaper.

Ta for eksempel et arbeidssted som anvender fingeravtrykk som autentisering for å verifisere at de som går inn er de som har lovlig tilgang, og ut ifra den informasjonen som vedkommende legger igjen finner ut at personen lider av eller er disponert for en alvorlig sykdom. Er det for fantasifullt å tenke seg at en arbeidsgiver i konkurransen om en forfremmelse velger å gi stillingen til noen andre, fordi sjefen er kjent med at vedkommendes helse i forhold til andre kandidater er mer utsatt for sykdom og trenger mer tilrettelegging? Sett ut fra et kostnadssynspunkt er det mer gunstig å ansette en frisk person.

Et annet eksempel er at et forsikringsselskap har fått tilgang til databaser hvor det er lagt inn biometriske kjennetegn, og ut ifra disse opplysningene finner at du er disponert for en alvorlig sykdom eller har nedsatte evner i dag. Jeg mener at dette ikke ligger langt frem i tid eller er urealistisk med tanke på at forsikringsselskapene allerede i dag vurderer din

[54] Teknologirådets nyhedsbrev til folketinget nr. 198 s. 3 januar 2005

helse i forhold til hvilken forsikringspolis du får. Dette kan eksemplifiseres: den 12.11.2006 opplyste Kanal 24 og Nettavisen[55] at en 9 år gammel gutt ikke fikk forsikring hos Gjensidige Personforsikring fordi han har dysleksi. Gjensidige forsikring ved avdelingsdirektør Kjennevold bekreftet på nyhetene at det kan være vanskelig for enkelte med dysleksi å få forsikring, og gutten på 9 år havnet i et register over problematiske forsikringskunder der han risikerer å bli stående i ti år. Her var det guttens far som selv hadde krysset av på skjemaet at gutten hadde lett dysleksi. Er det urealistisk å tro at forsikringsselskaper vil benytte seg slike registre, hvis de først er tilgjengelige?

Høyesterett behandlet en sak hvor spørsmålet var om politiet i forbindelse med et grovt ran kunne kreve utlevert biologisk materiale i en biobank fra en avdød.[56] I et obiter dictum i avsnitt 29 ble følgende uttalt:

> "Behovet for personvern for levende og døde er således spesielt sterkt ved at biologisk materiale kan gi tilgang til bestemte personers gener, sykdommer, lyter og andre egenskaper."

Dette gjaldt en straffesak, men likevel kan dette ha overføringsbetydning til bruk av biometrisk data (biologisk materiale som er digitalisert) utenfor strafferettspleien, fordi de samme personvernhensyn vil gjøre seg gjeldende her. Høyesterett poengterte i avsnitt 17 at utlevering av biologisk materiale gir mottakeren tilgang til langt mer informasjon enn det som er nødvendig for å kartlegge avdødes DNA-profil. Samme problem med overskuddsinformasjon oppstår med å benytte biometriske kjennetegn i et identifiserings- eller verifiseringsformål.

VIS var i utgangspunkt tenkt å være et system for at Schengen-landene skulle samarbeide på visumområdet. Ni dager etter 11. september 2001 satte man seg ned for å se på hva man kunne gjøre for å forhindre terrorisme og begynte å se på hvorvidt dette kunne kombineres

[55] Kanal 24: Nyhetssending kl 12.00 og http://www.nettavisen.no/innenriks/article800418.ece.

[56] Rt. 2006 s. 90

med det arbeidet man hadde gjort så langt innenfor VIS. Blant annet begynte man å vurdere teknologien med bruk av for eksempel fingeravtrykk. Landene aksepterte først teknologien, og ettersom arbeidet steg frem begynte man å se også andre nyttige formål ved å bruke teknologien. Kanskje gikk man vekk fra hovedfokuset, visum, til også å inkludere andre formål. Det som fremheves i dag er å forhindre illegal innvandring, kontroll med inn- og utreise, forhindre identitetstvil, kampen mot terrorisme osv. Det er en justering av primærformålet med systemet, blant annet av praktiske årsaker. Det hevdes at personvern har hatt og har stort fokus i utarbeidelsen av VIS, og den aktuelle debatten i landene i dag går på hvem som skal ha tilgang på dette systemet, og hvem som skal definere hvem som er de aktuelle myndighetene. Hva skjer om ett eller flere land bryter personvernreglene og gir flere tilgang enn de som skal ha det til systemet, eventuelt legger inn annen informasjon om personer enn det som er nødvendig? Det siste er ikke en hypotetisk tenkt problemstilling. I dag har landene et samarbeid for å forhindre at Schengen-visum ikke utstedes til personer som er uønsket på Schengen-området. I henhold til SIS art. 96 skal landene legge inn opplysninger om utlendinger som er uønsket i Schengen-området. Vilkårene for å kunne legge inn opplysninger om enkeltpersoner er at de enten er utvist fra et medlemsland eller representerer en fare for den offentlige orden eller sikkerhet. Selv om disse vilkårene for å benytte SIS art. 96 fremkommer klart er det ulik praksis på hvilke personer som blir registrert etter artikkelen. Italia og Tyskland registrerer alle asylsøkere som har fått avslag på asylsøknaden sin, til tross for at de ikke har gjort noe ulovlig, men fordi vilkårene for å få asyl ikke anses oppfylt.[57] Dette medfører i praksis at disse personene nektes innreise i hele Schengen-området. Det kan hevdes at dette er en sekundærbruk av systemet som ikke er tillatt etter SIS. Asylsøkerne har ikke gjort noe ulovlig, og jeg stiller spørsmål ved om dette er et innvandringspolitisk problem i den forstand at utlendinger ikke har den samme reelle muligheten til å krysse landegrenser hvis de har fått avslag på en asylsøknad. Særlig hvis andre land ikke kan se hvorfor vedkommende har fått avslag, annet enn at man er registrert i SIS. Misbruket fortsetter og har så langt ikke gitt noen ringvirkninger for Italia eller Tyskland. Slik VIS er tenkt, vil

[57] http://www.datatilsynet.no/templates/Page____1322.aspx.

systemet inneholde langt flere personopplysninger enn det som ligger inne etter SIS art. 96 i dag. Dette viser at svært klare regler for bruk av systemet er nødvendig for å verne personer mot sekundærbruk og overkill, og det er også viktig at misbruk får konsekvenser. Det hjelper ikke at det ligger mange gode personvernhensynstanker til grunn for systemet, hvis misbruk ikke får konsekvenser.

Argumentet om at innføringen av biometriske kjennetegn blant annet skal forhindre illegal innvandring kan det stilles spørsmål ved. Slik reglene på utlendingsfeltet i dag er regulert, er det slik at å søke visum med den begrunnelse at man er asylsøker, vil føre til avslag. Dette fremkommer ikke direkte av utlendingsloven, som ikke sier noe om vilkårene for å få visum, og dette er et bevisst valg fra lovgivers side. Bakgrunnen er at kriteriene for å innvilge visum er noen av de mest sentrale og virkningsfulle innvandringsregulerende virkemidler myndighetene har fordi returforutsetningene er helt avgjørende for utfallet av saken, og er gjenstand for endringer avhengig av hvem som sitter i regjering. Videre er reglene om blant annet asyl slik at man ikke kan søke fra hjemlandet eller en norsk utenriksstasjon, man må søke fra riket man har tenkt til å søke asyl i. Dette fremkommer av utlendingsloven § 17. Det økonomiske ansvaret for asylsøkere som blir returnert til hjemlandet etter å ha fått et avslag på sin asylsøknad er i dag privatisert, jf utlendingsloven § 46 tredje ledd. Dette innebærer at et flyselskap som tillater en person å fly til Norge uten gyldig visum må dekke det offentliges utgifter for vedkommendes opphold i Norge og tilbakereisen. Dette kan bli en svært kostbar affære for selskapene, som er svært nøye med å undersøke at alle nødvendige dokumenter er i orden. Private selskaper har altså fått ansvaret for utlendingskontrollen. Hvordan kommer da illegale innvandrere til Norge? Mange av dem kommer ikke med fly eller lignende og går ikke gjennom sikkerhetskontroller. De betaler for å bli transportert av privatpersoner i trailere, personbiler og skip. Det er videre velkjent at nitti prosent av asylsøkerne ankommer uten et eneste identitetsdokument. Dette vil de fortsette med så lenge menneskesmugling er eneste måte å komme til Norge for å søke asyl på, for uten å komme hit med falske papirer eller på falskt grunnlag. Jeg kan derfor ikke se hvordan innføring av biometriske kjennetegn skal kunne forhindre all illegal innvandring.

Derimot vil personer som har fått visum med den hensikt å søke asyl lettere kunne stanses ved bruk av fingeravtrykk. Uten at man vet akkurat hvor store tallene er i dag, er det slik at en del som søker visum hopper av og ikke returnerer til hjemlandet slik tillatelsen forutsetter. For disse personene vil fingeravtrykk i visumetiketten avsløre om de har reist på visum tidligere under en annen identitet. Videre har man også sett eksempler på at man benytter samme pass til å hente inn flere familiemedlemmer. Det har forekommet eksempler på at man henter ett og ett barn til Norge ved å sende samme pass i posten, hvor da alle barna reiser inn under samme identitet. Ved bruk av fingeravtrykk vil man avdekke og forhindre at flere personer reiser inn i landet under samme identitet.

Den pågående innføringen av biometriske kjennetegn skjer i stor grad uten at det foregår en offentlig debatt, og man kan stille spørsmål ved hvor bra dette er for den enkeltes rettssikkerhet og i hvor stor grad den enkelte er klar over den utviklingen som pågår.

4.5 Sammenligning av det tenkte visumregelverket og passeregelverket

Likheten mellom innføringen av biometriske kjennetegn i pass og visumsøknader er først og fremst at man har tenkt til å benytte fingeravtrykk og digitale ansiktsfoto begge steder, og at formålene som ligger til grunn for innføringen samsvarer. Det er offentlige myndigheter som står bak, og ikke private aktører. Videre er tiltakene tenkt og delvis innført på et område hvor man ikke beveger seg anonymt, og vil således ikke angripe retten til å være anonym.

Formålet med å innføre digitale ansiktsfoto og fingeravtrykk i pass er å kunne identifisere og verifisere en person, og ikke noe utover det. VIS har et videre formål enn kun identifikasjon og verifikasjon, da også andre opplysninger som er nødvendig for behandling av visum skal legges inn. Dette utgjør det en forskjell for den enkeltes personvern i forhold til passregelverket. Etter VIS har man langt flere opplysninger om den enkeltes bevegelser enn etter passkontrollen, hvor det ikke skal gjøres annet enn å foreta en

sammenligning av fingeravtrykket i passet og det avtrykket du avgir når du passerer kontrollen.

For visumsøkere er det tenkt at opplysningene som samles inn om den enkelte skal lagres i en sentral database som alle Schengen-landene skal ha tilgang til, og også referansepersoner skal registreres. Det vil si at hvis jeg ønsker å invitere en person fra India på besøk, vil jeg bli registrert i VIS, og det vil ligge inne personopplysninger om meg og at jeg eventuelt tidligere har invitert borgere utenfor Schengen til Norge.[58] For pass foreligger det ingen krav fra EU om at biometrisk data i passet også skal lagres eksternt i en database. For den enkelte kan det være vanskelig å ha oversikt over hva som er lagret i VIS og hvor man skal henvende seg for å få innsyn i opplysningene. Videre vil svært mange land ha tilgang på opplysningene som ligger lagret i VIS, og det er vanskelig å kontrollere hvordan andre vil benytte seg av disse opplysningene, og om det vil forekomme sekundærbruk. Dette gjør seg særlig gjeldende så lenge det ikke fremkommer klart hvilke myndigheter som skal ha tilgang på opplysningen i databasen. Dette gjør at VIS kan få større konsekvenser for den enkeltes personvern enn reglene om pass, slik de foreligger per i dag.

Bruk av fingeravtrykk kan for pass og visumsøknader være positivt for personvernet ved at det kan forhindre identitetstyveri og ved at man ved å innføre disse systemene forsøker å hindre alvorlig kriminalitet. Likevel er det viktig å være oppmerksom på at disse tiltakene kan misbrukes, og det er viktig at myndighetene tar seg god tid til å tenke gjennom lovmessige løsninger for å sikre den enkeltes rettssikkerhet og personvern i størst mulig grad.

[58] AIDs høringsbrev s. 4.

5 Henvisninger

5.1 Litteratur

Wiese Schartum, Dag og Bygrave, Lee A: *Personvern i informasjonssamfunnet*, Oslo 2004

Wiik Johansen, Michal, Kaspersen, Knut-Brede og Bergseng Skullerud, Åsta Marie: *Personopplysningsloven Kommentarutgave* Oslo 2001

Bunæs, Runa, Ottesen Kvigne, Kristin, Vandvik, Bjørn (red.*): Utlendingsrett*, Oslo 2004

Møse, Erik: *Menneskerettigheter*, Oslo 2002

5.2 Artikler

Bygrave: Utredning til Personvernnemnda av 22.12.2002

Teknologirådets nyhedsbrev til folketinget: På vej mod biometriske pas, nr. 198 januar 2005

Teknisk Ukeblad side 26-27, 153. årgang nr.11 mars 2006

Datatilsynet: Notat fra Datatilsynet – forslag til revisjon av personopplysningsloven § 12 og ny bestemmelse om bruk av biometrisk data av 04.04.2006

Liu, Yue: Upublisert personvernforelesning, IRI mars 2006

Magazin direkt #1/2005 (svensk)

5.3 Rapporter

ISO/IEC JTC 1/SC 37 Biometrics American National Standards Institute 2005

Teknologirådet: *Elektroniske spor og personvern*, Rapport 1 2005 ISBN 82-92447-05-9

Norsk Regnesentral: *Elektroniske spor* 2005 ISBN-13: 978-82-53-90516-7

Norsk Regnesentral: Personvern: *En forutsetning for samhandling og nye tjenester* 19. oktober 2004, http://publications.nr.no/2004_1015_eLandetNorge_artikkel_Personvern.pdf

National Science and Technology Council (NSTC): Taking *Today's Biometrics to Meet Tomorrow's Needs; Meeting the Challenge Together*, August 2006

Wiese Schartum og Bygrave: *Utredning av behov for endringer i personopplysningen* 2006

Datatilsynet: Notat til Justisdepartementet av 03.10.2005 *Forslag til endring av passloven – elektronisk lagring av personinformasjon i pass mv. – Endringenes personvernmessige problemer*

5.4 Høringer og høringsuttalelser

Arbeids- og inkluderingsdepartementet: Høringsbrev, endring i utlendingsloven av 06.03.2006

Datatilsynet: Elektronisk lagring av biometrisk personinformasjon – forslag til endring i passloven av 24.06.2005
Datatilsynet: Høringsuttalelse – endring i utlendingsloven – innføring av lovhjemmel for å implementere et felles europeisk visum informasjonssystem – visa information system (VIS) av 24. april 2006
Teknologirådets høring om IKT & personvern 1. desember 2003
Justis- og politidepartementet: Forslag til endring av passloven m.m. (elektronisk lagring av biometrisk personinformasjon i pass m.v.) mars 2005

5.5 Internettsider

www.lovdata.no
www.datatilsynet.no
www.personvernnemnda.no
www.statewatch.no
www.norsis.no
www.tu.no
http://www.tu.no/multimedia/archive/00029/Teknisk_Ukeblad_1106_29440a.pdf
http://www.steria.no
www.biometrics.org
www.forskning.no
www.datatilsynet.no/templates/Page____1199.aspx
www.datatilsynet.no/upload/Dokumenter/saker/2006/Revisjon_12_biometri.pdf
www.forskning.no/Artikler/2002/mai/1021978415.94/artikkel_print

5.6 Lover

Lov om behandling av personopplysninger av 14. april 2000 nr. 31
Lov om pass (passloven) av 19. juni 1997 nr. 82
Lov om utlendingers adgang til riket og deres opphold her (utlendingsloven) av 24. juni 1988 nr. 64
Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21. mai 1999 nr. 30

5.7 Forskrifter

Forskrift om behandling av personopplysninger av 15. desember 2000 nr. 1265
Forskrift om pass (passforskriften) av 9. desember 1999 nr. 1263

Forskrift om utlendingers adgang til riket og deres opphold her (utlendingsforskriften) av 21. desember 1990 nr. 1028

5.8 Forarbeider

Ot.prp. nr. 92 (1998-1999) Om lov om behandling av personopplysninger

Ot.prp. nr. 86 (2004-2005) Om lov om endring i passloven (elektronisk lagring av biometrisk personinformasjon i form av ansiktsfoto i pass m.m.)

St.prp. nr. 54 (2004-2005)

5.9 Rettspraksis

Rt 2000.996

Rt 2006.90

Rt 1996.551

5.10 Forvaltningspraksis

PVN-2002-8

5.11 Internasjonal rett

Den Europeiske Menneskerettighetskonvensjon av 1950

FN-konvensjonen om sivile og politiske rettigheter av 1966

EUs personverndirektiv 95/46/EF 24. juli 1995

Rådsforordning (EF) nr. 2252/2004 av 13. desember 2004

5.12 Andre kilder

Tom Halvorsen, Prosjektleder i Innvandringsavdelingen, Arbeids- og inkluderingsdepartementet