

Specialeafhandling
Det Juridiske Fakultet
Københavns Universitet

Biometri

Emnebeskrivelse: Vurdering af biometri i gældende ret. Indkredsning af hensyn mv. til persondatanedømmelse af brugen af biometri.

Af Bénédicte Lunde-Christensen

København 2010

Abstract

In Denmark a number of companies, amusement parks and discotheques use biometry in connection with access control. The term biometry refers to a number of technologies for verification or identification of a person using unique biological characteristics. One can distinguish between two main categories of biometric techniques, depending on whether stable data or dynamic behavioral data are used.

The main object of this paper is to assess the use of biometry under current Danish law, including the identification of potential privacy risks regarding the use of biometry.

The processing of biometrical data, e.g. reading a person's fingerprint(s), and the following use of this information, is to be regarded as a processing of personal data which is regulated by the Danish *Act on Processing of Personal Data (Act No. 429 of 31 May 2000)*. The controller must therefore ensure when using a biometrical solution that the provisions in the Danish *Act on Processing of Personal Data* are respected. The controller must among other consider whether or not the use of a biometric solution is necessary, or whether or not the purpose can be achieved in a less intrusive way by using other methods.

Biometric technologies can create certain challenges for both the users and the creators of the systems. Due to the incorporated tolerance levels two major types of recognition errors may arise: a false reject and a false match. False rejects will according to *Biometrics at the Frontiers* cause unnecessary inconvenience to innocent individuals whereas false matches are more insidious as they allow a fraudulent individual to pass, but the mistake goes unnoticed by the system.

Biometry is like other technologies not directly mentioned either in the *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* or in the Danish *Act on Processing of Personal Data*. Consideration should be made in order to clarify some of the provisions in the Danish *Act on Processing of Personal Data* when preparing a code of conduct according to art. 74 in the Danish *Act on Processing of Personal Data* or when implementing a sector oriented regulation.

Indholdsfortegnelse

1.	Indledning.....	4
2.	Biometri.....	6
3.	Den retlige ramme	8
4.	Personoplysningsloven.....	10
4.1	Indledende bestemmelser.....	10
4.1.1	Personoplysninger.....	10
4.1.2	Behandling	11
4.2	Den dataansvarlige og databehandleren.....	12
4.3	Behandlingsregler	13
4.3.1	Grundlæggende principper.....	13
4.3.1.1	Princippet om god databehandlingsskik	14
4.3.1.2	Principper for indsamlingen	14
4.3.1.3	Princippet om formålsbestemthed (finalité-princippet).....	14
4.3.1.4	Relevans- og Proportionalitet	15
4.3.1.5	Princippet om sikkerhed	16
4.3.2	Behandlingsbetingelser	17
4.3.2.1	Almindelige ikke-følsomme oplysninger	17
4.3.2.1.1	Samtykke	18
4.3.2.1.2	Interesseafvejning.....	18
4.3.2.2	Følsomme oplysninger.....	19
4.4	Registreredes rettigheder.....	19
4.5	Anmeldelse.....	20
5.	Biometriske systemer	22
6.	Teknologiske udfordringer	24
6.1	False Rejection og False Acceptance.....	24
6.1.1	Omfanget af den dataansvarliges oplysningspligt over for den registrerede	25
6.2	Bestandighed	27
6.3	Er behandling af nogle biologiske kendetegn potentielt mere integritetskrænkende end andre?	29
6.4	Uenighed om sikkerheden.....	29
7.	Biometri i natlivet.....	31
7.1	Datatilsynets afgørelse i Crazy Daisy-sagen.....	31
7.1.1	Sammenfatning	33

7.2	Betænkning nr. 1504 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud.....	33
7.2.1	Udvalgets overvejelser og anbefalinger.....	34
7.2.1.1	Individuel underretning af restauratøren	34
7.2.1.2	Oprettelse af et centralt register over personer med restaurationsforbud	34
7.2.1.3	Tilvejebringelse af en klar lovhjemmel for politiet til at videregive oplysninger om personer med restaurationsforbud til restauratøren	35
7.2.2	Sammenfatning	35
7.3	Høringssvar fra Institut for Menneskerettigheder og Forbrugerrådet vedrørende Betænkning nr. 1504.....	36
7.3.1	Central eller decentral lagring.....	36
7.3.2	Iagttagelse af personoplysningslovens samtykkekrav	37
7.3.3	Sammenfatning	39
8.	Fremmed ret (skandinavisk).....	40
8.1	Norge.....	40
8.1.1	Specialbestemmelse	40
8.1.2	Administrativ rekurs	42
8.2	Sverige	42
8.3	Bemærkninger til praksis i de skandinaviske lande	44
9.	Teknologineutral regulering	45
9.1	Adfærdskodeks.....	45
9.2	Sektororienteret regulering	46
9.3	Afsluttende bemærkninger.....	47
10.	Konklusion (med sammenfatning).....	48
11.	Litteraturfortegnelse.....	51

1. Indledning

Herhjemme anvender flere danske arbejdspladser, forlystelsesparker og diskoteker biometri til at verificere eller identificere deres medarbejdere/kunder. Biometriske systemer generer imidlertid en særlig form for oplysninger. Der er tale om oplysninger baseret på noget fysiologisk, f.eks. et fingeraftryk, eller adfærdsmæssigt, f.eks. gangart, hvilket muliggør en unik og livslang identificering.¹ Grundet specialets omfang fokuseres primært på fingeraftryks aflæsning.

Hovedsigtet med dette speciale er at vurdere biometri i gældende ret, herunder indkredsning af hensyn m.v. til persondatabelømmelsen af brugen af biometri. Indledningsvis berøres selve begrebet biometri og de bestemmelser og principper, som er relevante i forbindelse med biometriske løsninger. I forbindelse med indkredsning af hensyn m.v. skal den dataansvarlige ved etablering af en biometrisk løsning bl.a. overveje, om den påtænkte foranstaltning har til hensigt at verificere eller identificere personer, herunder hvorledes de indsamlede personlige oplysninger skal lagres.

Ved anvendelse af biometri kan teknologien skabe visse udfordringer for henholdsvis brugerne og skaberne af systemerne. Biometriske systemer har f.eks. en indbygget tolerance, der sikrer mod upræcis brug af teknologien og mod forskelle i de forhold, hvorunder de biometriske oplysninger præsenteres. Denne tolerance medfører imidlertid en risiko for, at der opstår afvisning af autoriserede personer eller accept af uautoriserede personer. Herudover berøres biologiske kendetegns bestandighed, spørgsmålet om behandling af nogle biologiske kendetegn kan opfattes som potentielt mere integritetskrænkende end andre, og hvorvidt det er muligt at genskabe det oprindelige billede af en persons biologiske kendetegn² ud fra templatens jf. nærmere kapitel 6.

Fordi lovgrundlaget for behandling af personoplysninger er meget lig hinanden i de skandinaviske lande, er det fundet nærliggende også at fremhæve praksis i forbindelse med behandling af biometriske oplysninger fra Norge og Sverige. Herudover er det værd at bemærke, at medens norske og svenske administrative afgørelser fra henholdsvis Datatilsynet og Datainspektionen i visse tilfælde er blevet indbragt for administrative rekursorganer eller domstole, er der ikke i Danmark tradition for, at Datatilsynets afgørelse indbringes for domstolene jf. nærmere kapitel 8.

¹ I nærværende arbejde benyttes biometriske systemer og biometriske løsninger som synonymer.

² I nærværende arbejde benyttes biologiske kendetegn, biometriske kendetegn og biometriske oplysninger som synonymer.

Afslutningsvis fremhæves fordele og ulemper ved teknologineutral regulering samt mulige tiltag, der kan overvejes i denne forbindelse.

2. Biometri

Biometri³ er den samlede betegnelse for en række teknologier til verifikation eller identifikation af personer ved hjælp af unikke biologiske kendetegn. Disse unikke biologiske kendetegn er bl.a. karakteriseret ved at være *universelle*, *entydige* og *bestandige*.⁴ I forbindelse med sidstnævnte vil det imidlertid være mere korrekt at sige, at biologiske kendetegn oftest ikke ændrer sig over tid jf. nærmere kapitel 6, afsnit 6.2.

Der skelnes mellem to hovedtyper af biometriske teknologier afhængigt af, hvorvidt der anvendes faste data eller dynamiske adfærdsmæssige data.⁵

For det første findes der fysiske og fysiologisk baserede teknologier, som bestemmer en given persons fysiologiske karakteristika, herunder f.eks.:

- Ansigtsgenkendelse
- DNA-analyse
- Fingeraftryksaflysning
- Håndscanning
- Irisgenkendelse
- Kropsduftanalyse
- Retinas scanning (nethinde)
- Venescanning
- Øreformsanalyse

For det andet anvendes adfærbaserede teknologier, der måler en given persons adfærd, herunder f.eks.:

- Ganganalyse
- Signaturanalyse
- Stemmegenkendelse
- Tastedynamik⁶

³ Ordet biometri kommer fra græsk og er en sammensætning af ordene bios, som betyder liv, og metron, der betyder mål.

⁴ Se i denne forbindelse *Biometrics at the Frontiers: Assessing the Impact on Society*, Teknisk rapport udgivet af EU Kommissionen, oktober 2005, hvor der arbejdes med de såkaldte "Seven Pillars of Biometric Wisdom", som ud over de allerede nævnte omhandler *muligheden for indsamling, systemets performance, accept af metoden og modstandsdygtighed i fht. omgåelse*. Se endvidere Jain, Anil K. m.fl., *Biometrics. Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999, s. 15.

⁵ Nogle teknologier kan både være fysiologiske og adfærdsmæssige.

⁶ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 3.

Det afgørende er således ikke noget personen **har**, eller **ved**, men derimod noget personen **er**.⁷

Den autentificering af personer, som opnås ved brug af biometri, stammer ikke direkte fra personens biologiske krop, men beror på en matematisk gengivelse af et biologisk kendetegn (template), der eksempelvis lagres på en chip. En template er en sekvens af 0- og 1-taller, som det biometriske system danner hver gang det præsenteres for eksempelvis en persons pegefinger, hånd eller ansigt.⁸

Biometri anvendes i stigende omfang til personidentifikation i forbindelse med adgangs- og sikringssystemer, og efter begivenhederne den 11. september 2001 er biometri ofte blevet fremhævet som et middel til at forbedre den offentlige sikkerhed.⁹

I Danmark bruger politiet biometri i deres registre over DNA og fingeraftryk. På foranledning af Rådets forordning (EF) nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometriske indikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder, indeholder alle nye danske pas siden 2006 biometriske data, som er lagret på en chip.^{10 11}

Herudover er der utallige anvendelsesmuligheder for biometri. Teknologien vil bl.a. kunne anvendes til at skabe øget bekvemmelighed i log-in-situationer, hvor det ikke er nødvendigt at anvende password eller PIN-koder, men hvor et biometrisk bruger-ID er tilstrækkeligt. Mange bærbare computere leveres f.eks. i dag med indbygget fingeraftryksflæser.

⁷ Se endvidere Davies, Simon G., *Touching Big Brother – How biometric technology will fuse flesh and machine*, Information Technology & People, 1994, Vol 7, No. 4, s. 38-47.

⁸ Teknologirådets rapporter 2010/2, *Anbefalinger*, s. 6-11, s. 7.

⁹ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 2.

¹⁰ Forordningen er behandlet af Artikel 29-gruppen i WP 112: Udtalelse 3/2005 om gennemførelsen af Rådets forordning (EF) nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometriske indikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder, vedtaget den 30. september 2005.

¹¹ I skrivende stund er implementeringen af fingeraftryk i alle nye pas i Danmark endnu ikke sket grundet Rigspolitiets planer om en digital pasløsning til kommunerne, Pas 2.0. Torsdag den 27. maj 2010 annullerede Justitsminister Lars Barfoed udbuddet af Rigspolitiets forsinkede pasløsning, Pas 2.0., til fordel for en ny pasløsning fra Rigspolitiet, som tilgodeser det faktum, at omkring en femtedel af landet kommuner allerede nu har indført et alternativt passystem uden om Rigspolitiet. Ifølge Justitsminister Lars Barfoed er vurderingen stadig, ”at systemet skulle kunne være fuldt etableret i andet halvår af 2011.” jf. følgende URL: <http://www.version2.dk/artikel/14989-millionspild-afvaerget-minister-skrorter-politiets-pas-loesning>.

3. Den retlige ramme

Den almindelige persondataretlige lovgivning er baseret på Europaparlamentets og Rådets direktiv om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.¹² Direktivet trådte i kraft den 24. oktober 1998 og blev med betydelig forsinkelse implementeret i dansk ret ved Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger¹³, som er baseret på Justitsministeriets betænkning nr. 1345/1997 om behandling af personoplysninger. Loven trådte i kraft den 1. juli 2000. Databeskyttelsesdirektivet har markant præget personoplysningslovens udformning, idet denne hovedsageligt er udfærdiget tæt op af direktivets tekst. Det er herved søgt sikret, at loven er i overensstemmelse med direktivet, og at de EU-retlige forpligtelser dermed bliver overholdt.

Den omstændighed, at personoplysningsloven er baseret på databeskyttelsesdirektivet, indebærer, at kompetencen til at fastlægge den definitive fortolkning af de grundlæggende regler er placeret hos EU-domstolen.¹⁴

I medfør af databeskyttelsesdirektivet er der nedsat en gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger, den såkaldte '*Artikel 29-gruppe*'. Kort fortalt er Artikel 29-gruppen et uafhængigt EU-rådgivningsorgan vedrørende databeskyttelse og beskyttelse af privatlivets fred. Artikel 29-gruppen består af en repræsentant for den eller de tilsynsmyndigheder, som hver medlemsstat har udpeget, og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og –organerne, samt af en repræsentant fra Kommissionen.¹⁵ Artikel 29-gruppens opgaver er beskrevet i databeskyttelsesdirektivets artikel 30 og artikel 15 i direktiv 2002/58/EF.

Artikel 29-gruppen har udarbejdet en lang række arbejdsrapporter og anbefalinger. Selvom disse ikke er juridisk forpligtende for medlemsstaterne, har de betydelig indflydelse på retsudviklingen og

¹² Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. I det følgende betegnet som databeskyttelsesdirektivet.

¹³ I det følgende betegnet som personoplysningsloven.

¹⁴ Domstolen hed tidligere EF-domstolen. Ved Lissabontraktatens tiltrædelse ændrede domstolen navn til Den Europæiske Unions Domstol med virkning fra den 1. december 2009.

¹⁵ Jf. følgende URL: <http://www.datatilsynet.dk/internationalt/artikel-29-gruppen/>.

udgør på denne måde en vigtig retskilde også i dansk persondatabeskyttelsesret.¹⁶ Artikel 29-gruppens arbejdsdokument om biometri vil løbende blive inddraget i nærværende arbejde.¹⁷

Ifølge Artikel 29-gruppen skaber en omfattende og ukontrolleret udnyttelse af biometri bekymring med hensyn til beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder.¹⁸ Denne fremhævelse hænger nøje sammen med databeskyttelsesdirektivets formålsbestemmelse, hvoraf det bl.a. fremgår, at medlemsstaterne i forbindelse med behandling af personoplysninger skal sikre beskyttelsen af disse rettigheder, herunder især retten til privatliv.¹⁹

Personoplysningsloven gengiver ikke direkte kravet om beskyttelse af privatlivets fred, men ifølge bemærkningerne til personoplysningslovens § 2, stk. 2, anføres det, at andre grundlæggende rettigheder, herunder artikel 8 i den Europæiske Menneskerettighedskonvention (EMRK), også skal overholdes.

EMRK's artikel 8, stk. 1, fastsætter, at *"[e]nhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance"*. Beskyttelsen i EMRK's artikel 8, stk. 1, er dog ikke absolut, idet det i stk. 2, er angivet, under hvilke omstændigheder privatlivet må krænkes.

I hvilket omfang biometriske løsninger indebærer en behandling af personoplysninger præciseres nedenfor i kapitel 4, afsnit 4.1.

¹⁶ Blume, Peter, *Databeskyttelsesret*, 3. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag 2008, s. 88-89.

¹⁷ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003. I denne forbindelse er det relevant at fremhæve, at Artikel 29-gruppen i henhold til sit arbejdsprogram for 2010-2011 (WP 170) har til hensigt at ajourføre WP 80.

¹⁸ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 2.

¹⁹ Jf. Databeskyttelsesdirektivets artikel 1, stk. 1.

4. Personoplysningsloven

4.1 Indledende bestemmelser

Personoplysningsloven gælder ifølge lovens § 1, stk. 1, for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Loven gælder tillige for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, der med rimelighed kan forlanges underdraget offentligheden, jf. § 1, stk. 2.

Ved anvendelse af biometriske løsninger er der således indledningsvis to grundlæggende persondatarelige spørgsmål, som skal besvares, nemlig for det *første* om biometriske oplysninger er personoplysninger, og for det *andet* om anvendelsen af biometriske løsninger er en behandling i personoplysningslovens forstand.

4.1.1 Personoplysninger

Ifølge personoplysningslovens § 3, nr. 1, defineres personoplysninger som ”*[e]nhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)*”.

Databeskyttelsesdirektivets artikel 2, litra a, eksemplificerer yderligere denne definition med at tilføje, at der ved identificerbar person forstås ”*en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet*”.

For at afgøre, om en person er identificerbar, fremgår det af databeskyttelsesdirektivets præambel (betragtning 26), at den registeransvarlige eller enhver anden person kan tage alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende.

Omfattet af begrebet personoplysninger er herefter oplysninger, som kan henføres til en fysisk person, selv om dette forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer.

Biometriske oplysninger eller de digitale udgaver heraf (templates) vil således være omfattet af begrebet personoplysninger. Dette fremgår bl.a. også af Artikel 29-gruppen's arbejdsdokument om

biometri²⁰ og af Datatilsynets første afgørelse på det biometriske område²¹, som blev truffet på baggrund af en forespørgsel om BornholmsTraffikkens anvendelse af fingeraftryk til identifikation i forbindelse med indførelse af nyt id-kort til pendlere. Af afgørelsen fremgår det, at ”[d]et er Datatilsynets vurdering, at den værdi af kundens fingeraftryk, som ligger lagret i chippen, er at betragte som en personoplysning omfattet af persondataloven”²².

Se endvidere Datatilsynets afgørelse fra 2005 vedrørende behandling af oplysninger hos Projekt Janus. Af denne afgørelse fremgår det, at ”oplysninger, som foreligger i form af billede, personens stemme, fingeraftryk eller genetiske kendetegn” ligeledes vil være omfattet af begrebet personoplysninger.²³

Slutteligt skal blot følgende passus i Artikel 29-gruppens arbejdsdokument om biometri nævnes: ”I tilfælde, hvor de biometriske data ligesom skabelonerne lagres på en sådan måde, at den registrerede ikke kan identificeres af den registeransvarlige eller en anden person, betragtes dataene ikke som personoplysninger.”²⁴

4.1.2 Behandling

Ifølge personoplysningslovens § 3, nr. 2, defineres behandling som ”[e]nhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for”.

Behandlingsbegrebet dækker således over alt, hvad der kan foretages i forbindelse med en personoplysning fra denne indsamles til oplysningen slettes eller arkiveres.^{25 26}

I forbindelse med en forespørgsel fra Scandinavian Airlines Danmark (SAS) om selskabets påtænkte behandling af flypassagerers biometriske oplysninger i form af en template af deres fingeraftryk har Datatilsynet udtalt følgende: ”Det er Datatilsynets opfattelse, at der såvel i forbindelse med indsamling (indrollering) af aftrykket af passagerens fingeraftryk, som ved den

²⁰ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 5.

²¹ Se endvidere Datatilsynets journalnummer 2005-291-0295 hvor Registertilsynets hidtidige praksis vedrørende adgangskontrol baseret på biometriske oplysninger sammenfattes.

²² Jf. Datatilsynets journalnummer 2003-212-0143.

²³ Jf. Datatilsynets journalnummer 2004-54-1508.

²⁴ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 5, note 11.

²⁵ Databeskyttelsesdirektivets definition indeholder en eksemplificering af behandlingsbegrebet, jf. artikel 2, litra b.

²⁶ Blume, Peter, *Personoplysningsloven*, 1. udgave, 1. oplag 2000, Greens&Jura, Akademisk Forlag A/S. s. 43.

efterfølgende brug (matchning) af templatens af aftrykket i forbindelse med den biometriske løsning, er tale om behandlinger af personoplysninger omfattet af persondataloven.”²⁷

Indsamling og den efterfølgende brug af biometriske oplysninger (templates) er en behandling i personoplysningslovens forstand.

4.2 Den dataansvarlige og databehandleren

Personoplysningslovens pligtssubjekt er den dataansvarlige jf. lovens § 3, nr. 4. Bestemmelsen fastsætter, at der ved begrebet *den dataansvarlige* forstås den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.²⁸ Den dataansvarlige har således ansvaret for, at personoplysningslovens bestemmelser opfyldes og skal således forud for ibrugtagning af en biometrisk løsning sikre sig, at personoplysningslovens bestemmelser overholdes.

I forbindelse med den ovennævnte definition har det ingen betydning, hvem der faktisk foretager behandlingen, idet dette kan ske af en databehandler jf. personoplysningslovens § 3, nr. 5. Ifølge personoplysningslovens § 3, nr. 5, forstås der ved begrebet *databehandleren* den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne. Det centrale er således, at databehandleren behandler oplysninger på den dataansvarliges vegne, således at det er den dataansvarlige og ikke databehandleren, der er direkte ansvarlig over for den registrerede jf. hermed bl.a. bestemmelsen om erstatningsansvar i personoplysningslovens § 69.²⁹

Organisatorisk differentiering i både den offentlige og den private sektor, udviklingen af informations- og kommunikationsteknologi samt globaliseringen af persondatabehandlingen har ifølge Artikel 29-gruppen øget kompleksiteten af den måde, som personoplysninger behandles på. Artikel 29-gruppen har således med henblik på at sikre en effektiv anvendelse og overholdelse af begreberne om den dataansvarlige og databehandleren vedtaget WP 169.³⁰

²⁷Jf. Datatilsynets journalnummer 2006-219-0370.

²⁸I stedet for begreberne den registeransvarlige og registerføreren jf. herved databeskyttelsesdirektiver artikel 2, litra d og e, tales der i personoplysningsloven om *den dataansvarlige* og *databehandleren*. I det følgende anvendes begreberne den dataansvarlige og databehandleren.

²⁹Waaben, Henrik, Kristian Korfits Nielsen, *Lov om behandling af personoplysninger*, 2. udgave, 1. oplag, Jurist- og Økonomforbundet 2008, s. 119.

³⁰WP 169: Udtalelse 1/2010 om begreberne ”registeransvarlig” og ”registerfører”, vedtaget den 16. februar 2010.

Ifølge WP 169 udløser fastlæggelsen af *formålet* med en behandling kvalificeringen som (reelt) dataansvarlig. Derimod kan fastlæggelsen af *hjælpe midlerne* ved en behandling uddelegeres af den dataansvarlige for så vidt angår tekniske eller organisatoriske spørgsmål. Væsentlige spørgsmål, som er afgørende for lovligheden af en behandling – som f.eks. de oplysninger, der skal behandles, opbevaringsperioden, adgang mv. – skal dog fastlægges af den dataansvarlige.

Sondringen mellem den dataansvarlige og databehandleren har især til formål at skelne mellem de involverede personer, der er ansvarlige som de dataansvarlige, og dem, der kun handler på disses vegne.³¹

4.3 Behandlingsregler

Personoplysningslovens kapitel 4 indeholder bestemmelser om, i hvilket omfang behandling af personoplysninger må finde sted. Kapitlet indeholder lovens centrale bestemmelser, der gælder for alle former for behandling, medmindre der andetsteds er fastsat særlige bestemmelser.

4.3.1 Grundlæggende principper

Den persondataretlige regulering er baseret på en række grundlæggende principper, der samlet tilvejebringer et udgangspunkt for, under hvilke betingelser personoplysninger må behandles. Disse principper er hovedsageligt fastsat i personoplysningsloves § 5.³²

Principperne i personoplysningslovens § 5 giver ikke den dataansvarlige et selvstændigt retligt grundlag for at foretage en bestemt behandling af oplysninger, men hvis en behandling kan finde sted på grundlag af en af de øvrige regler i loven eller eventuelt i særlovgivningen, skal de grundlæggende principper altid være opfyldt.

De enkelte principper er ikke rangordnede og må alle tages i betragtning med samme styrke.³³ Et udvalg af disse principper vil i det følgende blive fremhævet.

³¹For en nærmere analyse af begreberne se WP 169: Udtalelse 1/2010 om begreberne ”registeransvarlig” og ”registerfører”, vedtaget den 16. februar 2010.

³² Blume, Peter, *Databeskyttelsesret*, 3. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag 2008, s. 123-124.

³³ Blume, Peter, *Databeskyttelsesret*, 3. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag 2008, s. 125.

4.3.1.1 Princippet om god databehandlingskik

Ifølge personoplysningslovens § 5, stk. 1, skal oplysninger behandles i overensstemmelse med god databehandlingskik. Heri ligger ifølge bemærkningerne til bestemmelsen, at behandlingen skal være rimelig og lovlig.³⁴

4.3.1.2 Principper for indsamlingen

Ifølge personoplysningslovens § 5, stk. 2, skal indsamlingen af oplysninger ”ske til udtrykkeligt angivne og saglige formål”.

Ifølge bemærkningerne til bestemmelsen ligger der i kravet om udtrykkelighed, ”at den dataansvarlige i forbindelse med indsamlingen skal angive et formål, som er tilstrækkelig veldefineret og velafgrænset til at skabe åbenhed og klarhed omkring behandlingen.”³⁵

Indsamlingen af oplysninger skal endvidere ske til et eller flere saglige formål. I kommentaren i Karnovs lovsamling til bestemmelsen anføres det, at et formål bl.a. vil være sagligt, ”hvis indsamlingen sker til administrative formål, som det ligger inden for en offentlig myndigheds område at varetage. Tilsvarende gælder for en privat virksomheds indsamling af oplysninger inden for det virksomhedsområde, som den udøver.”³⁶ Der må med andre ord være en nærliggende sammenhæng mellem den dataansvarliges virksomhed eller område og de oplysninger, der bliver indsamlet.

4.3.1.3 Princippet om formålsbestemthed (finalité-princippet)

Personoplysningslovens § 5, stk. 2, indeholder endnu et selvstændigt princip. Efter bestemmelsen må senere behandling af oplysninger ikke være uforenelig med de(t) formål, hvortil oplysningerne er indsamlet.

Princippet tager dels sigte på at fremme åbenhed, dels at tilvejebringe en vis kontrol med persondataanvendelsen. Dette sker ved, at der lægges begrænsninger på de dataansvarliges senere persondataanvendelse, der må foregå inde for den ramme, formålet medfører.³⁷

Ifølge Charlotte Bagger Tranberg (Adjunkt, ph.d., Aalborg Universitet) vil specifikationen af formålet have en øget betydning, når der er tale om behandling af personoplysninger ved hjælp af

³⁴ Lovforslag nr. 147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

³⁵ Lovforslag nr. 147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

³⁶ Eyben, Bo Von, Jan Pedersen, Thomas Rørdam (red.), *Karnovs Lovsamling*, 4. bind, 22. udgave, Forlaget Thomson 2007, s. 7155, kommentar nr. 40.

³⁷ Blume, Peter, *Databeskyttelsesret*, 3. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag 2008, s. 128.

biometriske løsninger. Dette skyldes ifølge Charlotte Bagger Tranberg, at den biometriske oplysnings værdi i mange tilfælde er stationær over tid.³⁸ Se nærmere herom i kapitel 6, afsnit 6.2.

Afslutningsvis skal det nævnes, at personoplysningslovens § 5, stk. 2, ikke i sig selv indebærer noget krav om, at den dataansvarlige skriftligt formulerer formålet med en bestemt indsamling. Den dataansvarlige har blot en pligt til at gøre sig det klart, hvad formålet er med enhver indsamling af oplysninger, der er omfattet af loven. I hvilket omfang, der påhviler den dataansvarlige en pligt til i forbindelse med indsamlingen at oplyse den registrerede om indsamlingen og dens formål, følger af bestemmelserne i personoplysningslovens kapitel 8 om den dataansvarliges eller dennes repræsentants oplysningspligt over for den registrerede.

4.3.1.4 Relevans- og Proportionalitet

Personoplysningslovens § 5, stk. 3, stiller indholdsmæssige krav til de indsamlede oplysninger. I lighed med den netop omtalte bestemmelse i personoplysningslovens § 5, stk. 2, omfatter bestemmelsen i stk. 3 to principper.

De indsamlede oplysninger skal for det *første* være *relevante og tilstrækkelige*. Ifølge bemærkningerne til bestemmelsen sigtes der med udtrykkene relevante og tilstrækkelige, at oplysningernes art skal svare til det formål, der tilsigtes med behandlingen.³⁹

For det *andet* er det en forudsætning, at den dataansvarlige sikrer, at der er proportionalitet mellem formålet og de oplysninger, der behandles.⁴⁰ Ifølge bemærkningerne til bestemmelsen må behandling af oplysninger ikke gå videre end, hvad der kræves til opfyldelse af de(t) formål, som den dataansvarlige er berettiget til at forfølge, jf. herved også bestemmelsen i stk. 2.

Datatilsynet har i forbindelse med en anmodning om vurdering af et adgangskontrolsystem, som byggede på biometrisk identifikation udtalt følgende: ”På dette grundlag er det imidlertid Datatilsynets umiddelbare vurdering, at den i denne sag beskrevne behandling ikke vil kunne ske inden for rammerne af persondatalovens regler. Datatilsynet lægger herved vægt på, at formålet med behandlingen ikke synes at stå mål med, hvor indgribende en behandling der er tale om. Hensynet til at etablere en adgangskontrol i et motionscenter uden brug af kort kan efter Datatilsynets umiddelbare opfattelse ikke retfærdiggøre behandlingen af matchværdier i en central

³⁸Tranberg, Charlotte Bagger, *Biometriske personoplysninger*, Erhvervsjuridisk Tidsskrift 2007, s. 105-115, s. 108-109. Se også Tranberg, Charlotte Bagger, *Persondata og biometri i Skandinavien*, Lov & Data 2007, s. 1-6, s. 2.

³⁹ Lovforslag nr. 147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

⁴⁰ Blume, Peter, *Databeskyttelsesret*, 3. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag 2008, s. 131.

database. Det er Datatilsynets vurdering, at det ønskede formål kan forfølges med mindre indgribende midler.”⁴¹

Proportionalitetsprincippet betydning i forbindelse med biometriske løsninger understreges også i Artikel 29-gruppens arbejdsdokument om biometri. Ifølge Artikel 29-gruppen har proportionalitet været det vigtigste kriterium for næsten alle de beslutninger, som tilsynsmyndighederne har taget om behandling af biometriske oplysninger. Artikel 29-gruppen understreger endvidere princippet betydning i forbindelse med verifikation jf. nærmere herom kapitel 5.⁴²

Med henblik på det ovenfor nævnte skal den dataansvarlige således bl.a. overveje, om det er nødvendigt at anskaffe en biometrisk løsning, eller om formålet kan nås på en mindre indgribende måde ved brug af andre metoder. Hvis en biometrisk løsning anvendes har det yderligere ud fra en integritetssynsvinkel betydning, hvilke biologiske kendetegn der skal anvendes, eftersom behandling af nogle biologiske kendetegn kan opfattes som potentielt mere integritetskrænkende end andre jf. nærmere herom i kapitel 6, afsnit 6.3.

4.3.1.5 Princippet om sikkerhed

Personoplysningslovens kapitel 11 indeholder bestemmelser, som tager sigte på at øge sikkerheden for at oplysninger alene undergives behandling i overensstemmelse med den dataansvarliges lovlige intentioner herom.

Ifølge personoplysningslovens § 41, stk. 3, 1. pkt., skal den dataansvarlige ”*træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.*” Om disse foranstaltninger fremgår det nærmere i databeskyttelsesdirektivets artikel 17, stk. 1, at de ”*under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse*” skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer og arten af de oplysninger, som skal beskyttes. Bestemmelsen opstiller hermed de overordnede krav til den dataansvarliges behandlingssikkerhed.

⁴¹ Jf. Datatilsynets journalnummer 2004-219-0208.

⁴² WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 11.

Ifølge Artikel 29-gruppen skal de nødvendige sikkerhedsforanstaltninger gennemføres allerede fra begyndelsen af behandlingen, og de er især vigtige i *registreringsfasen* hvor de biometriske oplysninger omdannes til skabeloner (templates) eller billeder.⁴³

Udformningen af de præcise sikkerhedskrav er mere et teknisk end et juridisk spørgsmål. På lovniveau er det ikke muligt at specificerer de krav, som skal opfyldes, og selvom andre retsforskrifter kan udfylde lovens principper,⁴⁴ er det først om fremmest Datatilsynet, der i konkrete afgørelser og i forbindelse med inspektioner må sikre, at sikkerhedsniveauet er tilstrækkeligt. Ifølge dansk ret kan Datatilsynet foretage inspektioner uden retskendelse og uden at den dataansvarlige varsles herom.

4.3.2 Behandlingsbetingelser

De ovennævnte principper gælder som nævnt for enhver behandling af personoplysninger, men besvarer ikke spørgsmålet om, hvornår en konkret behandling kan finde sted. Svaret herpå er fastlagt i et katalog af behandlingsbetingelser, der regulerer forholdet mellem de registreredes og de dataansvarliges informationsinteresser.

Personoplysningsloven er struktureret således, at alle oplysningstyper, der ikke specifikt er opregnet i personoplysningslovens §§ 7 og 8 eller som personnummeret er særligt reguleret i personoplysningslovens § 11, er omfattet af personoplysningslovens § 6, der således gælder for de fleste personoplysninger.

4.3.2.1 Almindelige ikke-følsomme oplysninger

Ifølge Datatilsynet må et fingeraftryk eller en matematisk værdi af et fingeraftryk (template) anses for en almindelig ikke-følsom oplysning omfattet af personoplysningslovens § 6.⁴⁵

Behandling af oplysninger efter personoplysningslovens § 6 forudsætter imidlertid, at én af betingelserne i bestemmelsens stk. 1, nr. 1-7, er opfyldt. I det følgende fremhæves to af disse.

⁴³ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003. s. 9.

⁴⁴ Se bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, og bekendtgørelse nr. 535 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for domstolene. I tilknytning til bekendtgørelse nr. 528 er der udstedt en vejledning, der nærmere beskriver reglerne i bekendtgørelsen. Se VEJ nr. 37 af 2. april 2001. Derudover har Datatilsynet i samarbejde med Indenrigs- og Sundhedsministeriet (nu Velfærdsministeriet) samt KL udgivet en publikation om datasikkerhed i borgerservicecentre.

⁴⁵ Jf. bl.a. Datatilsynets journalnummer 2006-219-0370.

4.3.2.1.1 Samtykke

Behandling af almindelige ikke-følsomme oplysninger kan bl.a. ske, hvis den registrerede har givet sit udtrykkelige samtykke hertil jf. personoplysningslovens § 6, stk. 1, nr. 1.

I personoplysningslovens § 3, nr. 8, er den registreredes samtykke defineret som enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

At et samtykke skal være *frivilligt* betyder, at samtykket ikke må være afgivet under tvang. Dette gælder ifølge bemærkningerne til bestemmelsen, uanset om det er den dataansvarlige selv eller andre, der øver pression over for den registrerede.⁴⁶ Forudsætningen om frivillighed er dog ikke nogen ideel norm. Særligt må fremhæves, at samtykket er frivilligt, selvom det gives for at opnå en eller anden ydelse.⁴⁷ Se nærmere herom kapitel 7, afsnit 7.3.2.

I kravet om et *specifikt* samtykke ligger, at samtykket skal være konkretiseret i den forstand, at det klart og utvetydigt fremgår, hvad det er, der meddeles samtykke til. Det skal således af et meddelt samtykke fremgå, hvilke typer af oplysninger der må behandles, hvem der kan foretage behandling af oplysninger om den samtykkende, og til hvilke formål behandlingen kan ske.

I kravet om, at samtykket skal være *informeret*, ligger, at den samtykkende skal være klar over, hvad det er, vedkommende meddeler samtykke til. Den dataansvarlige må således sikre sig, at der gives den registrerede tilstrækkelig information til, at den pågældende kan vurdere, hvorvidt samtykke bør meddeles.⁴⁸

Det skal dog bemærkes, at den registrerede på et hvilket som helst tidspunkt kan tilbagekalde et samtykke efter bestemmelsen i personoplysningslovens § 38.

4.3.2.1.2 Interesseafvejning

Behandling kan endvidere finde sted, hvis behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse jf. personoplysningslovens § 6, stk. 1, nr. 7.

⁴⁶ Lovforslag nr. 147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

⁴⁷ Blume, Peter, *Personoplysningsloven*, 1. udgave, 1. oplag 2000, Greens§Jura, Akademisk Forlag A/S. s. 47, samt Waaben, Henrik, Kristian Korfits Nielsen, *Lov om behandling af personoplysninger*, 2. udgave, 1. oplag, Jurist- og Økonomforbundet 2008, s. 125-126.

⁴⁸ Lovforslag nr. 147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

Ifølge bemærkningerne til bestemmelsen er det en betingelse for at kunne anvende bestemmelsen, at den dataansvarlige har foretaget en vurdering af, hvorvidt hensynet til den registreredes interesser overstiger hensynet til de interesser, der ønskes forfulgt med behandlingen, og at denne vurdering falder ud til fordel for de interesser, der ønskes forfulgt.⁴⁹

4.3.2.2 Følsomme oplysninger

Nogle oplysninger er af natur følsomt materiale. Det gælder f.eks. oplysninger om racemæssig eller etnisk baggrund og oplysninger om helbredsmæssige forhold.⁵⁰

Nogle biometriske løsninger kan medføre fremkomsten af sådanne oplysninger, herunder i forbindelse med irisgenkendelse hvor man af øjets regnbuehinde bl.a. kan aflæse oplysninger om racemæssig baggrund og om kortvarige eller længerevarende sygdomme som f.eks. infektioner eller diabetes,⁵¹ og ifølge Artikel 29-gruppen kan biometriske løsninger baseret på ansigtsgenkendelse f.eks. behandle oplysninger om racemæssig eller etnisk baggrund.⁵²

Det er blevet påpeget, at det i biometrisk sammenhæng kun er i registreringsfasen, hvor de biometriske oplysninger optages, og der dannes biometriske templates på baggrund af oplysningerne, at oplysningernes følsomme indhold er direkte tilgængeligt. Når de originale oplysninger er digitaliseret, er det derimod tvivlsomt, om rubriceringen som følsomme oplysninger kan fastholdes, hvilket der dog endnu ikke er taget stilling til i dansk ret.⁵³ Se dog kapitel 6, afsnit 6.4 om hvorvidt det er muligt at ”spole tilbage” fra den digitaliserede til den oprindelige form.

4.4 Registreredes rettigheder

Personoplysningsloven indeholder en række bestemmelser, som giver den registrerede forskellige rettigheder over for den dataansvarlige. Reglerne har til formål at styrke den registreredes retsstilling, bl.a. ved at skabe åbenhed omkring behandlingen af oplysninger og ved at give den

⁴⁹ Lovforslag nr.147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

⁵⁰ Personoplysningslovens § 7, stk. 1, fastsætter et forbud mod, at visse typer af følsomme personoplysninger gøres til genstand for behandling. Undtagelse fra dette forbud gøres dog i bestemmelserne i stk. 2-7.

⁵¹ Gulddal, Jesper, Mette Mortensen (red.), *PAS. Identitet, kultur og grænser*, Forfatterne og Informations Forlag 2004, Olesen, Birgitte Kofod, *Passet og (u)sikkerheden om biometri og integritetsbeskyttelse*, s. 145-156, s. 151.

⁵² WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 10.

⁵³ Gulddal, Jesper, Mette Mortensen (red.), *PAS. Identitet, kultur og grænser*, Forfatterne og Informations Forlag 2004, Olesen, Birgitte Kofod, *Passet og (u)sikkerheden om biometri og integritetsbeskyttelse*, s. 145-156, s. 151-152.

registrerede adgang til at gøre indsigelse over for nærmere bestemte former for behandling af oplysninger.⁵⁴

Disse rettigheder omfatter kort fortalt følgende:

- ret til at modtage besked fra den dataansvarlige om, at der indsamles oplysninger om en selv,
- ret til indsigt i de oplysninger, der behandles om en selv,
- ret til at gøre indsigelse mod, at behandling af oplysninger finder sted, og hvis indsigelsen er berettiget, skal databehandlingen ophøre,
- ret til at gøre indsigelse mod, at oplysninger om en selv videregives med henblik på markedsføring,
- ret til at gøre indsigelse mod, at man undergives afgørelser, der har retsvirkninger for eller i øvrigt berører en selv i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling,
- ret til at få oplysninger, der er urigtige eller vildledende, rettet, slettet eller blokeret, samt i den forbindelse at forlange, at andre, der har modtaget oplysningerne, orienteres om dette,
- ret til at tilbagekalde et samtykke, og
- ret til at klage til Datatilsynet over behandling af personoplysninger om en selv.⁵⁵

4.5 Anmeldelse

Spørgsmålet om, i hvilket omfang der påhviler den dataansvarlige myndighed eller virksomhed mv. en pligt til inden iværksættelsen af en behandling af personoplysninger at anmelde behandlingen til tilsynsmyndighederne, dvs. til Datatilsynet eller Domstolsstyrelsen, er reguleret i personoplysningslovens kapitel 12-15.

Personoplysningslovens kapitel 12-14 beskriver anmeldelsesordningen for behandlinger af oplysninger, som foretages for henholdsvis den offentlige forvaltning, private dataansvarlige og domstolene. Desuden indeholder kapitel 15 regler om offentlige og private databehandlers anmeldelsespligt med hensyn til elektronisk databehandling, der udføres for andre (edb-

⁵⁴ Jf. Vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.

⁵⁵ Jf. Datatilsynets Informationspjece om personoplysningsloven s. 24-25 som er at finde på følgende URL: <http://www.datatilsynet.dk/publikationer/informationspjece/>.

servicebureauer), samt generelle regler om offentlig tilgængelighed af behandlinger af oplysninger.⁵⁶

Anmeldelsesordningerne tjener to formål. For det *første* giver anmeldelserne Datatilsynet mulighed for at sikre den fornødne kontrol med behandlingerne, dels i forbindelse med iværksættelse af den enkelte behandling, dels i forbindelse med Datatilsynets efterfølgende tilsynsvirksomhed. For det *andet* skaber anmeldelsesordninger åbenhed om behandlingerne. Dette skyldes, at Datatilsynet ifølge personoplysningslovens § 54 skal føre en offentlig tilgængelig fortegnelse over de anmeldte behandlinger.⁵⁷

Som udgangspunkt skal enhver behandling af personoplysninger, der foretages for en offentlig myndighed, anmeldes til Datatilsynet. Dette udgangspunkt er dog ikke ubetinget og i Justitsministeriets bekendtgørelse nr. 529 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning er de typer af behandlinger, som er undtaget, nævnt.

De dataansvarlige i den private sektor skal i nogle tilfælde også foretage anmeldelse til Datatilsynet.⁵⁸ De typer af behandlinger, som er undtaget fra anmeldelse fremgår af personoplysningslovens § 49 samt Justitsministeriets bekendtgørelse nr. 534 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig.⁵⁹

⁵⁶ Lovforslag nr.147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

⁵⁷ Se følgende URL: <http://www.datatilsynet.dk/blanketter/generelt-om-anmeldelse/>.

⁵⁸ I Crazy Daisy-sagen, som er omtalt i kapitel 7, afsnit 7.1, skulle diskoteket foretage anmeldelse til samt indhente tilladelse fra Datatilsynet efter personoplysningslovens § 50, stk. 1, nr. 1.

⁵⁹ Se følgende URL: <http://www.datatilsynet.dk/blanketter/generelt-om-anmeldelse/>.

5. Biometriske systemer

Biometriske systemer gør det muligt at foretage automatisk verifikation eller identifikation af en fysisk person.

Ifølge Artikel 29-gruppen besvarer verifikation spørgsmålet: Er jeg den, jeg udgiver mig for at være? Det biometriske system bekræfter en given persons identitet ved at sammenligne det præsenterede biologiske kendetegn med en tidligere registreret reference skabelon (template), og spørgsmålet besvares med ja eller nej ("én-til-én"-sammenligning). Identifikation besvarer derimod spørgsmålet: Hvem er jeg? Det biometriske system genkender spørgeren ved at skelne vedkommende fra andre personer, hvis reference skabeloner (templates) ligeledes er lagret i systemet, og svarer, at spørgeren er X ("én-til-mange"-sammenligning).⁶⁰

Navnlig i forbindelse med verifikation medfører overholdelsen af proportionalitetsprincippet, ifølge Artikel 29-gruppen, at der foretrækkes anvendt biometriske løsninger, hvor de biometriske oplysninger ikke lagres centralt.⁶¹ Dette hænger sammen med, at det i princippet ikke er nødvendigt at lagre biometriske oplysninger til verifikation i en central database, idet der er tale om en "én-til-én"-sammenligning. De biometriske oplysninger kan f.eks. lagres på et smart card, som er et plastikkort på størrelse med et kreditkort med indbyggede chip. Når en person forsøger at bruge kortet, sammenlignes det præsenterede biologiske kendetegn med reference skabelonen (templaten), der ligger gemt på kortet.

Datatilsynet har tilsluttet sig ovennævnte og har i forbindelse med en konkret forespørgsel anført, "at løsninger med lagring på et smart card, set i lyset af hensynet til beskyttelse af personoplysninger, ofte vil være at foretrække, da den registrerede i sådanne tilfælde har oplysningerne i sin varetægt." Ifølge Datatilsynet kan der imidlertid "også foreligge tilfælde, hvor der er et sagligt behov for behandling af oplysninger i en database, og hvor hensynet til de registrerede ikke overstiger hensynet til den dataansvarliges interesse heri."^{62 63}

⁶⁰ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 3. Se endvidere *Biometrics at the Frontiers: Assessing the Impact on Society*, EUR 21585 EN, Teknisk rapport udgivet af EU Kommissionen, oktober 2005, s. 38-39.

⁶¹ Der henvises i denne forbindelse til den engelske version af WP 80 (side 11), idet der formentlig er en fejl i den danske oversættelse.

⁶² Jf. Datatilsynets journalnummer 2005-219-0295.

⁶³ Se endvidere kapitel 4, afsnit 4.3.

I modsætning til verifikation nødvendiggør identifikation, at reference skabelonerne (templates) lagres i en central database, idet der er tale om en "én-til-mange"-sammenligning. I denne forbindelse henvises til *Biometrics at the Frontiers* hvor det meget præcist er anført, at "[s]ince the system checks against a database of enrolled templates [...], the maintenance of the integrity of the database is essential in protecting individuals from identity theft".⁶⁴

Manglende integritet, fortrolighed og tilgængelighed i forbindelse med en central database kan være ødelæggende for alle fremtidige applikationer, der bygger på oplysninger fra denne database, og vil også kunne tilføje de registrerede uoprettelig skade jf. nærmere kapitel 7, afsnit 7.3.1.

Under henvisning til at det i forbindelse med verifikation ikke er nødvendigt at lagre biometriske oplysninger i en central database, og at det således er muligt at sikre den registrerede kontrol over sine biometriske oplysninger, anses verifikation i persondataretlig forstand for en mindre indgribende foranstaltning end identifikation.⁶⁵

⁶⁴*Biometrics at the Frontiers: Assessing the Impact on Society*, EUR 21585 EN, Teknisk rapport udgivet af EU Kommissionen, oktober 2005, s. 39.

⁶⁵ Se endvidere Tranberg, Charlotte Bagger, *Biometriske personoplysninger*, Erhvervsjuridisk Tidsskrift 2007, s. 105-115, s. 107 samt Tranberg, Charlotte Bagger, *Persondata og biometri i Skandinavien*, Lov & Data 2007, s. 1-6, s. 2.

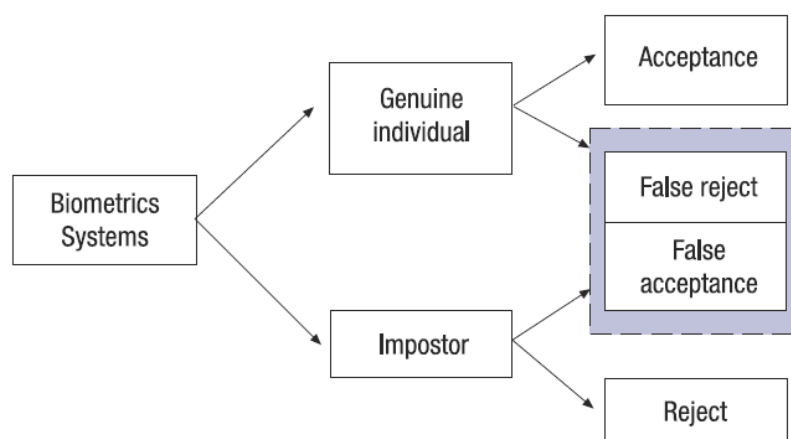
6. Teknologiske udfordringer

Ved anvendelse af biometri kan teknologien skabe visse udfordringer for henholdsvis brugerne og skaberne af systemerne. I nærværende kapitel vil en række af disse udfordringer blive fremhævet.

6.1 False Rejection og False Acceptance

Biometriske systemer har en indbygget tolerance, der sikrer mod upræcis brug af teknologien og mod forskelle i de forhold, hvorunder de biometriske oplysninger præsenteres. Det kan bl.a. fremhæves, at selv minimale forskelle i position og tryk i forbindelse med fingeraftryks aflæsning vil medføre forskelle i den matematiske gengivelse af fingeraftrykket.⁶⁶

Ovennævnte tolerance medfører imidlertid en risiko for, at der opstår afvisning af autoriserede personer eller accept af uautoriserede personer. I *Biometrics at the Frontiers* beskrives forskellen mellem afvisning af autoriserede personer og accept af uautoriserede personer på følgende måde: ”False rejects will cause unnecessary inconvenience to innocent individuals whereas false matches are more insidious as they allow a fraudulent individual to pass, but the mistake goes unnoticed by the system.”⁶⁷ Se endvidere figur 1.



Figur 1. Biometrisk system (EUR 20823 EN, 2003)⁶⁸

⁶⁶ Teknologirådets rapporter 2010/2, *Introduktion til biometriske teknologier*, s. 12-15, s. 13.

⁶⁷ *Biometrics at the Frontiers: Assessing the Impact on Society*, EUR 21585 EN, Teknisk rapport udgivet af EU Kommissionen, oktober 2005, s. 38.

⁶⁸ *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, EUR 20823 EN, udgivet af EU Kommissionen, juli 2003, s. 46.

Tolerancen måles i 'False Rejection Rate' (FRR) og 'False Acceptance Rate' (FAR), som er indbyrdes afhængige. Det vil sige, at en lav afvisningsrate af autoriserede personer følges af en høj acceptrate af uautoriserede personer – og omvendt.⁶⁹

Både afvisning af autoriserede personer og accept af uautoriserede personer kan ud fra en integritetssynsvinkel give anledning til betænkeligheder, hvilket præciseres i det følgende.

Eftersom biometriske systemer kan skabe en illusion af, at verifikation eller identifikation af en person altid er korrekt, vil mangel på en anstændig procedure for, hvordan systemets operatører skal behandle både korrekt og forkert afviste personer på, kunne opleves meget krænkende for den forkert afviste person.

Accept af uautoriserede personer kan derimod give tredjemand adgang til f.eks. de samme bygninger og/eller faciliteter som den autoriserede person uden dog at være berettiget hertil.

Mulige løsningsmodeller kan eventuelt være multibiometriske systemer, som indeholder kombinationer af forskellige biometriske teknologier. Det kan bl.a. fremhæves, at man i visse systemer både anvender ansigtsgenkendelse og stemmegenkendelse.⁷⁰ En anden mulighed er at kombinere biometriske teknologier med en bestemt viden (f.eks. et password eller en PIN-kode) og/eller en bestemt ting (f.eks. et smart card).

6.1.1 Omfanget af den dataansvarliges oplysningspligt over for den registrerede

I forbindelse med afvisning af autoriserede personer er det imidlertid interessant nærmere at undersøge omfanget af den dataansvarliges oplysningspligt.

Uanset om personoplysninger indsamles direkte hos den registrerede eller indhentes fra andre kilder skal det oplyses, hvem den dataansvarlige er, og hvad der er formålet med den påtænkte behandling jf. personoplysningslovens § 28, stk. 1, nr. 1 og 2, samt § 29, stk. 1, nr. 1 og 2.⁷¹ Herudover skal den dataansvarlige give alle *yderligere oplysninger*, der ud fra den konkrete situation skønnes

⁶⁹ Gulddal, Jesper, Mette Mortensen (red.), *PAS. Identitet, kultur og grænser*, Forfatterne og Informations Forlag 2004, Olesen, Birgitte Kofod, *Passet og (u)sikkerheden om biometri og integritetsbeskyttelse*, s. 145-156, s. 152.

⁷⁰ WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003, s. 4.

⁷¹ Oplysningspligten gælder dog ikke ubetinget, idet de dataansvarlige i så fald ville blive påført betydelige omkostninger, som ikke i alle tilfælde ville stå mål med det udbytte, en registreret person har af at modtage underretning om, at der indsamles oplysninger om vedkommende jf. Waaben, Henrik, Kristian Korfits Nielsen, *Lov om behandling af personoplysninger*, 2. udgave, 1. oplag, Jurist- og Økonomforbundet 2008, s. 358.

nødvendig for at opfylde oplysningspligtens formål jf. personoplysningslovens § 28, stk. 1, nr. 3, og § 29, stk. 1, nr. 3.⁷²

Under henvisning til sidstnævnte vil der være meget som taler for, at den dataansvarlige i visse tilfælde skal underrette den registrerede om, at de biometriske oplysninger vil blive gjort til genstand for en automatiseret afgørelse, og at den registrerede i den forbindelse har indsigelsesret efter personoplysningslovens § 39. I det følgende præciseres dette nærmere.

Ifølge personoplysningslovens § 39, stk. 1, skal der for det første være tale om ”*afgørelser, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad*”. Hvor biometri anvendes i forbindelse med adgangs- eller sikringssystemer til at verificere om der kan tildeles en fysisk person adgang til eksempelvis en bestemt bygning eller et it-system, vurderes dette at udgøre en afgørelse i bestemmelsens forstand. Det kan bemærkes, at der ikke er megen hjælp at hente i bemærkningerne til bestemmelsen eller vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger pkt. 4.5.

Der skal endvidere være tale om afgørelser, der ”*alene er truffet på grundlag af elektronisk databehandling*”. Bestemmelsen omhandler dermed kun den situation, at der uden videre gøres brug af resultater, som et edb-system leverer jf. bemærkningerne til bestemmelsen⁷³ og vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger pkt. 4.5. Hvor et adgangs- eller sikringssystem udelukkende er baseret på biometri, vurderes dette krav at være opfyldt.

Endelig skal der være tale om edb-behandling af ”*oplysninger, der er bestemt til at vurdere bestemte personlige forhold*”. Ifølge kommentaren i Karnovs lovsamling til bestemmelsen kan dette f.eks. være oplysninger om erhvervsevne, kreditværdighed, pålidelighed, adfærd mv. Videre anføres det, at oplysninger om forhold, der er objektivt konstaterbare, falder uden for bestemmelsen.⁷⁴

Under henvisning til at biometriske systemer anvendes til automatisk verifikation eller identifikation af personer ved hjælp af unikke biologiske kendetegn, er der således meget som taler for, at den dataansvarlige bl.a. i forbindelse med adgangs- eller sikringssystemer, som udelukkende er baseret på biometri, skal underrette den registrerede om, at oplysningerne vil blive gjort til

⁷² Opregningen i litra a-c i nærværende bestemmelser er ikke udtømmende.

⁷³ Lovforslag nr. 147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

⁷⁴ Eyben, Bo Von, Jan Pedersen, Thomas Rørdam (red.), *Karnovs Lovsamling*, 4. bind, 22. udgave, Forlaget Thomson 2007, s. 7162, kommentar nr. 197.

genstand for en automatiseret afgørelse, og at den registrerede i denne forbindelse har indsigelsesret efter personoplysningslovens § 39.

Konsekvensen af en indsigelse efter personoplysningslovens § 39 er ikke nødvendigvis, at der bliver truffet en anden afgørelse, men at afgørelsen skal efterses manuelt.

Det skal herudover fremhæves, at hvis en indsigelse mod behandlingen ikke imødekommes har den dataansvarlige pligt til at give den registrerede klagevejledning.⁷⁵

Ovennævnte betragtning aktualiseres endvidere af, at Lene Gisselø, chefkonsulent i Rigspolitiet med ansvar for udvikling og implementering af den kommende version af det biometriske pas i Danmark, i artiklen *Biometriske pas – redskab mod terror og illegal indvandring* har udtalt, ”at det er meget sandsynligt, at automatisk paskontrol på et vist tidspunkt vil blive introduceret i EU-regi.”⁷⁶

6.2 Bestandighed

Et af de karakteristiske træk ved biologiske kendetegn er, at de er bestandige, hvilket muliggør en unik og livslang identificering af en fysisk person. Dette skal bl.a. tages i betragtning både i forbindelse med formålsbestemthedsprincippet i personoplysningslovens § 5, stk. 2, proportionalitetsprincippet i personoplysningslovens § 5, stk. 3 og sikkerhedskravene i personoplysningslovens kapitel 11.⁷⁷

Det vil imidlertid være mere korrekt at sige, at biologiske kendetegn oftest ikke ændrer sig over tid, hvilket illustreres nedenfor.

Ifølge Niels Christian Juul, ph.d. og lektor ved Institut for Kommunikation, Virksomhed og Informationsteknologier på RUC, er der særlige forhold omkring børn, fordi deres biologiske kendetegn ændrer sig massivt, indtil de når en vis alder.⁷⁸

Under henvisning til denne omstændighed har den svenske tilsynsmyndighed Datainspektionen i forbindelse med det svenske justitsministeriums forslag til implementeringen af fingeraftryk i alle

⁷⁵ Waaben, Henrik, Kristian Korfits Nielsen, *Lov om behandling af personoplysninger*, 2. udgave, 1. oplag, Jurist- og Økonomforbundet 2008, s. 369.

⁷⁶ Teknologirådets rapporter 2010/2, *Biometriske pas – redskab mod terror og illegal indvandring*, s. 31-32, s. 32.

⁷⁷ Se endvidere kapitel 4, afsnit 4.3.1.

⁷⁸ Teknologirådets rapporter 2010/2, *Biometri kan ikke løse alle sikkerhedsproblemer*, s. 33-36, s. 34. Se endvidere Tranberg, Charlotte Bagger, *Biometriske personoplysninger*, *Erhvervsjuridisk Tidsskrift* 2007, s. 105-115, s. 109, note 28.

nye svenske pas udtalt, at ”*det ännu är alltför oklart om fingeravtrycken hos yngre barn är tillförlitliga. Inspektionen delar europeiska datatillsynsmannens bedömning att åldersgränsen bör ligga vid 14 år eller möjligen strax under.*”⁷⁹ Dette bør medtænkes i forbindelse med implementeringen af fingeraftryk i alle nye danske pas.⁸⁰

I forbindelse med ovennævnte skal det dog fremhæves at Ringkøbing Bibliotek, hvor man anvender fingeraftryk i stedet for sundhedskort som identifikation ved bogudlån, har løst dette problem ved med jævne mellemrum at opdatere børnenes fingeraftryk.⁸¹

I andre tilfælde kan arbejdsforhold påvirke kroppen så meget, at de biologiske kendetegn ændrer sig markant. Dette kan bl.a. illustreres i forbindelse med BornholmsTrafikkens anvendelse af fingeraftryk til identifikation i forbindelse med selskabets pendlerrabat. BornholmsTrafikkens IT-chef, Peter H. Christensen, har i et interview i DR-programmet ’Viden om’ udtalt, at ”*[f]or enkelte passagerer kan systemet ikke fungere. Det drejer sig om 2,5 %, hvis finger simpelthen slet ikke kan blive scannet i første omgang, når der skal laves en referencescanning til chipkortet. Det er typisk keramikere eller håndværkere, som kan have slidt deres fingeraftryk helt væk af deres arbejde*”. Peter H. Christensen fortæller videre, at ”*[m]an må acceptere, at man med et biometrisk system ikke kan få alle igennem*”.⁸²

Herudover kan det fremhæves at sygdomme som sukkersyge samt nogle øjensygdomme vil kunne aflæses af regnbuehinden, ligesom de vil forårsage ændringer i regnbuehindens overflade i takt med sygdommens udvikling.⁸³ Regnbuehinden anvendes bl.a. i forbindelse med irisgenkendelse.

Ovennævnte eksempler illustrerer endvidere, at det ikke er muligt at skabe et sikkert system, som udelukkende er baseret på biometri.⁸⁴ Der vil altid være behov for et eller flere klart definerede alternativer.⁸⁵

⁷⁹ Se følgende URL: <http://www.datainspektionen.se/press/nyhetsarkiv/2008/hoj-aldergransen-for-registrering-av-barns-fingeravtryck-i-pass/>.

⁸⁰ Der henvises til note 11.

⁸¹ Teknologirådets rapporter 2010/2, *Fremtidig anvendelse af biometri*, s. 16-18, s. 17.

⁸² Se følgende URL: <http://www.dr.dk/DR2/VidenOm/Temaer/Biometri/20070530163036.htm>.

⁸³ Olsen, Birgitte Kofod, *Identifikationsteknologi og individbeskyttelse – en øvelse i juridisk teknologivurdering*, 1. udgave, 1. oplag 1998, Jurist- og Økonomforbundets Forlag, s. 146.

⁸⁴ Andre eksempler kan bl.a. være kirurgiske indgreb eller medfødte fysiske handicap.

⁸⁵ Se endvidere Teknologirådets rapporter 2010/2, *Anbefalinger*, s. 6-11, s. 10-11.

6.3 Er behandling af nogle biologiske kendetegn potentielt mere integritetskrænkende end andre?

Som fremhævet i kapitel 4, afsnit 4.3.1.4 har det ud fra en integritetssynsvinkel betydning, hvilke biologiske kendetegn der skal anvendes, eftersom behandling af nogle biologiske kendetegn kan opfattes som potentielt mere integritetskrænkende end andre.

Fingeraftryks aflæsning er formentlig den mest anvendte biometriske teknologi, men ikke desto mindre kan brugen heraf virke integritetskrænkende, idet afgivelse af fingeraftryk kan lede tankerne hen på politi- og efterforskningsmæssig aktiviteter, hvorved nogle kan føle ubehag ved at skulle afgive deres fingeraftryk.

For at imødekomme denne oplevelse af ubehag kan det i stedet for overvejes at anvende håndscanning hvor håndens geometriske karakteristika anvendes til verifikation eller identifikation af en fysisk person.

Herudover kan det fremhæves, at relativ mange opfatter brug af øjnene som noget ubehageligt.⁸⁶ Dette kan eventuelt begrundes med en opfattelse af, at man går for tæt på den biologiske krop eller at det siges at øjnene er sjælens spejl.

Ny teknologi kræver tid og ikke mindst tålmodighed, men jo mere biometri bliver en del af hverdags billedet, jo mere vil offentligheden også gradvist vænne sig hertil. Opfattelsen af hvad der er privat, er en subjektiv vurdering.

6.4 Uenighed om sikkerheden

Der er uenighed blandt eksperter om, hvorvidt det er muligt at genskabe det oprindelige billede af en persons biologiske kendetegn ud fra templatens.

En template er, som tidligere fremhævet i kapitel 2, en sekvens af 0- og 1-taller, som det biometriske system danner hver gang det præsenteres for eksempelvis en persons finger, hånd eller ansigt.

Templaten beregnes på baggrund af specifikt udvalgte dele af selve det biologiske kendetegn – for eksempel bestemte punkter i et fingeraftryk eller en bestemt rytme knyttet til en persons gangart.⁸⁷

⁸⁶ Teknologirådets rapporter 2010/2, *Teknologierne*, s. 52-66, s.60.

⁸⁷ Teknologirådets rapporter 2010/2, *Sikkerhed*, s. 25-26, s. 26.

Ifølge Niels Christian Juul må man gå ud fra, at der enten allerede er reel mulighed for at spole tilbage fra templatens, eller at det bliver muligt på et senere tidspunkt.⁸⁸ Birgitte Kofod Olsen har udtalt tilsvarende, idet man ifølge hende ikke bør se bort fra den mulighed, at man kan ”gå tilbage” fra den digitaliserede til den oprindelige form.⁸⁹

Andre har udtalt, at komplette biologiske kendetegn, som f.eks. et helt fingeraftryk, ikke kan genskabes på baggrund af biometriske templates, da der netop er tale om en matematisk gengivelse skabt ud fra specifikt udvalgte dele af det biologiske kendetegn.⁹⁰ Sidstnævnte antages også af Datatilsynet, som mener, at det ikke er muligt at regne sig frem til fingeraftrykkets udseende ud fra kendskab til template.⁹¹

Hvis man antager, at det er eller vil blive muligt at ”spole tilbage”, hvorved nogle af de biometriske oplysningers følsomme karakter vil blive gjort tilgængelige jf. kapitel 4, afsnit 4.3.2.2, vil mulige løsningsmodeller kunne være pseudonymisering⁹² eller biometrisk kryptering, som er eksempler på privatlivsfremmende teknologier som også kendes under betegnelsen PETs - **P**rivacy **E**nhancing **T**echnologies. Disse privatlivsfremmende teknologier omtales ikke yderligere i nærværende arbejde.

⁸⁸ Teknologirådets rapporter 2010/2, *Biometri kan ikke løse alle sikkerhedsproblemer*, s. 33-36, s. 33

⁸⁹ Gulddal, Jesper, Mette Mortensen (red.), *PAS. Identitet, kultur og grænser*, Forfatterne og Informations Forlag 2004, Olesen, Birgitte Kofod, *Passet og (u)sikkerheden om biometri og integritetsbeskyttelse*, s. 145-156, s. 152.

⁹⁰ Teknologirådets rapporter 2010/2, *Introduktion til biometriske teknologier*, s. 12-15, s. 13.

⁹¹ Se følgende URL: <http://www.datatilsynet.dk/erhverv/biometri/diskotekers-registrering/>.

⁹² Se i øvrigt Stephan Engberg: *Nøglen til fremtiden – om pseudonymer og virtuelle identiteter* i debatbogen *De overvågede - vores privatliv er truet men der findes løsningsmodeller*, Udgivet i samarbejde mellem DI og Forbrugerrådet, januar 2009, s. 104-121.

7. Biometri i nattelivet

Et område, hvor brug af fingeraftryksaflysning i dag er meget udbredt, er ved adgangskontrol på diskoteker. I det følgende gennemgås Datatilsynets afgørelse vedrørende Diskotek Crazy Daisy i Viborg, dele af Justitsministeriets Betænkning nr. 1504 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud, samt Institut for Menneskerettigheders og Forbrugerrådets høringssvar til Betænkning nr. 1504.

7.1 Datatilsynets afgørelse i Crazy Daisy-sagen

I den konkrete sag var der tale om, at Diskotek Crazy Daisy i Viborg foruden generelle kundeoplysninger, ønskede at registrere en matematisk beregnet værdi af gæstens fingeraftryk samt gæstens billede. Diskoteket ønskede endvidere at registrere oplysninger om eventuelle karantæneforhold og restaurationsforbud udstedt af politiet efter restaurationsloven.⁹³

Af anmeldelsen fremgik det, at gæsteregistreringssystemet indebar, at alle gæster skulle registreres. Det ville således ikke være muligt at være gæst på diskoteket, hvis man ikke lod sig registrere.

Hovedformålet med behandlingen var ifølge diskoteket at sikre et trygt og sikkert natteliv, bl.a. ved bedre at kunne håndhæve forbud udstedt af politiet efter restaurationsloven. Af sikkerhedsmæssige årsager ønskede diskoteket endvidere at foretage en ensartet og hurtig genkendelse af de gæster, som allerede var i systemet, og som derfor umiddelbart kunne tildeles adgang for derved at undgå lange køer uden for diskoteket, da dette ofte fører til optrin og frustrationer.

Ved at flytte karantæne- og forbudsregistreringen over i et biometrisk system forventede diskoteket videre, at antallet af såvel fysiske som verbale overfald på vagtpersonale/dørmænd ville blive reduceret, da dørmændene ikke længere over for gæsten fremstod som den, der administrerer forbud og karantæner.

Datatilsynet tilkendegav i sin udtalelse at diskotekets ønske om at lave en ensartet kontrol af gæsterne inden for en afgrænset periode og at undgå køer uden for diskoteket udgjorde et sagligt formål. Hvis behandlingen baserede sig på et udtrykkeligt samtykke, der lever op til personoplysningslovens krav, ville den påtænkte behandling af oplysninger om fingeraftryk og billede efter Datatilsynets opfattelse kunne ske inden for personoplysningslovens rammer.

⁹³ Jf. Datatilsynets journalnummer 2008-42-0742.

Datatilsynet påpegede dog, at personoplysningslovens regler indebærer, at diskoteket skal slette templatens og billedet, hvis den registrerede tilbagekalder sit samtykke jf. personoplysningslovens § 38.

Datatilsynet gav herudover konkret tilladelse til, at diskoteket med gæstens skriftlige samtykke kunne registrere følsomme oplysninger, f.eks. om strafbare forhold og narkotikamisbrug i forbindelse med, at diskoteket tildeler en gæst en karantæne. Datatilsynet lagde i den forbindelse til grund, at diskoteket havde behov for at registrere karantæneårsagen for senere at kunne forklare eventuelle gæster, hvorfor de ikke kan blive lukket ind på diskoteket i en nærmere afgrænset tidsperiode. Datatilsynet udtalte videre, at det også med hensyn til følsomme oplysninger gælder, at samtykket skal være udtrykkeligt, og at det skal opfylde personoplysningslovens krav hertil. Hvis gæsten tilbagekalder sit samtykke efter personoplysningslovens § 38, skal oplysninger om årsagen til karantænen slettes. Diskoteket vil dog efter en konkret vurdering kunne gemme oplysninger om navn, adresse, samt hvor længe personen er uønsket som gæst i diskoteket.

Vedrørende spørgsmålet om restaurationsforbud bemærkede Datatilsynet følgende:

”Det er Datatilsynets vurdering, at Crazy Daisy uden samtykke kan indsamle, registrere og bruge oplysninger om forbud udstedt af politiet i medfør af restaurationsloven, jf. persondatalovens § 8, stk. 6, jf. 7, stk. 2, nr. 4, og § 8, stk. 4, 2. pkt., samt identifikationsoplysninger, herunder personnummer, på personer, som har fået sådant forbud, jf. persondatalovens § 6, stk. 1, nr. 3 og 7, og § 11, stk. 2, nr. 1. Oplysningerne skal slettes, når forbuddet udløber.”

Datatilsynet tilkendegav videre, at diskotekets behandlingssikkerhed skulle leve op til kravene i personoplysningslovens kapitel 11.⁹⁴ Til uddybning af disse krav stillede Datatilsynet nærmere vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv jf. personoplysningslovens § 50, stk. 5. Datatilsynet stillede bl.a. krav om, at diskoteket skulle give den fornødne instruktion til sine medarbejdere i hvilke krav der efter personoplysningsloven stilles til behandling af personoplysninger herunder indhentelse af samtykke, opfyldelse af oplysningspligten samt håndtering af den registreredes øvrige rettigheder. Endvidere var det et vilkår, at medarbejderne blev informeret om, at deres opslag blev logget, og at loggen kunne bruges

⁹⁴ Der er redegjort for princippet om sikkerhed i kapitel 4, afsnit 4.3.1.5.

til at kontrollere uberettigede opslag samt til stikprøvekontrol jf. *Datatilsynets vilkår om sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger*.⁹⁵

Under henvisning til ovennævnte bemærkes det at tilsidesættelse af vilkår jf. personopplysningslovens § 50, stk. 5, sanktioneres med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning jf. personopplysningslovens § 70, stk. 1, nr. 5.

7.1.1 Sammenfatning

Afgørelsen viser, at diskoteker med gæstens udtrykkelige samtykke kan registrere dennes fingeraftryk (template) og billede. Herudover kan eventuelle karantæneoplysninger med gæstens skriftlige samtykke registreres. Samtykket skal i øvrigt opfylde kravene i personopplysningslovens § 3, nr. 8.

Hvis gæsten tilbagekalder sit samtykke jf. personopplysningslovens § 38, skal diskoteket slette fingeraftrykket (templaten) og billedet, og hvor der er registeret karantæneoplysninger skal oplysninger om årsagen til karantænen slettes. Diskoteket vil dog efter en konkret vurdering kunne gemme oplysninger om navn, adresse, samt hvor længe personen er uønsket som gæst i diskoteket.

Herudover kan diskoteker uden gæstens samtykke registrere oplysninger om restaurationsforbud i forbindelse med deres adgangskontrol. Når et restaurationsforbud udløber, skal forbuddet og alle oplysninger om dette slettes.

Der skal foretages anmeldelse til samt indhentes tilladelse fra Datatilsynet, hvis et diskotek registrer følsomme personoplysninger, herunder oplysninger om strafbare forhold i form af restaurationsforbud udstedt af politiet efter restaurationsloven.⁹⁶

7.2 Betænkning nr. 1504 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud

I sommeren 2008 nedsatte justitsministeren et sagkyndigt udvalg, som skulle foretage en samlet gennemgang og vurdering af, hvordan restaurationer mv. sikres adgang til identitetsoplysninger på personer med restaurationsforbud, uden at en sådan adgang til personfølsomme oplysninger om enkeltpersoner sætter grundlæggende hensyn til persondatabeskyttelsen over styr.

⁹⁵ Vilkårene findes på følgende URL: <http://www.datatilsynet.dk/erhverv/diskoteker/sikkerhedsregler/>.

⁹⁶ Der henvises generelt til kapitel 4, afsnit 4.5.

Det bemærkes i denne forbindelse, at oplysninger om restaurationsforbud ikke kan videregives, ej heller til koncernforbundne virksomheder, medmindre der foreligger et udtrykkeligt samtykke hertil fra gæsten, eller når det sker til varetægelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrundet hemmeligholdelse jf. personoplysningslovens § 8, stk. 5. Personoplysningslovens øvrige bestemmelser skal ligeledes være opfyldt.

Udvalget udgav i 2009 Betænkning nr. 1504 om restaurationsadgang til identitetsoplysninger på personer med restaurationsforbud.⁹⁷ En række af udvalgets overvejelser og anbefalinger vil i det følgende blive fremhævet.

7.2.1 Udvalgets overvejelser og anbefalinger

7.2.1.1 Individuel underretning af restauratøren

Indledningsvis fremhævede udvalget, at alle restaurationer uanset deres karakter, størrelse og geografiske placering bør have adgang til oplysninger om, hvem der har fået et forbud efter restaurationslovens § 31, stk. 2, 1. pkt., mod at komme det pågældende sted samt oplysninger om, hvor længe forbuddet gælder. Ifølge udvalget bør politiet ved en individuel underretning orientere den eller de berørte restaurationer herom. Udvalget bemærkede dog, at en restauratør skal kunne fravælge en sådan individuel underretning, hvis restaurationen er tilsluttet et centralt register med oplysning om restaurationsforbud.⁹⁸

7.2.1.2 Oprettelse af et centralt register over personer med restaurationsforbud

Udvalget overvejede bl.a., om der bør oprettes et centralt register over personer med restaurationsforbud, som den enkelte restauration kan få online adgang til i forbindelse med sin adgangskontrol.

Et sådant centralt register kan eksempelvis oprettes som et centralt offentligt register eller som et centralt privat register.

Ifølge udvalget vil et centralt offentligt register skulle føres af Rigspolitiet, da det er politiet, der er i besiddelse af oplysningerne om udstedte restaurationsforbud. Politiet kan efter de nugældende regler i retsplejelovens kapitel 72 imidlertid kun optage fingeraftryk af en sigtet, hvis det er

⁹⁷ Lovforslag nr. 13 af 7. oktober 2009 til lov om ændring af lov om restaurationsvirksomhed og alkoholbevilling m.v. (Videregivelse og behandling af oplysninger om forbud mod ophold i bestemte virksomheder) som byggede på Udvalget vedrørende restaurationsadgang til identitetsoplysninger på personer med restaurationsforbuds betænkning nr. 1504/2009 og det heri indeholdte lovudkast blev vedtaget af Folketinget ved 3. behandling den 10. december 2009.

⁹⁸ Se endvidere bemærkningerne til lovudkastets § 31, stk. 6 jf. betænkningens s. 98-99.

nødvendigt for efterforskningen, eller hvis der er tale om en alvorlig forbrydelse. Dette indebærer, at en person, der bliver sigtet for en mindre lovovertrædelse begået på en restauration, og som i den forbindelse får et restaurationsforbud, i de fleste tilfælde ikke vil få optaget fingeraftryk af politiet.

Et centralt privat register vil i modsætning til et centralt offentligt register udover navn og CPR-nummer med samtykke fra gæsten også kunne indeholde billeder, fingeraftryk (templates) og andre identitetsoplysninger, som kan anvendes til at sikre en hurtig, effektiv og ensartet adgangskontrol. Mulighederne for at snyde ved hjælp af et forkert CPR-nummer eller fremvisning af et lånt eller stjålet sundhedskort vil endvidere minimeres i denne forbindelse.

Blandt andet under henvisning til muligheden for registrering af fingeraftryk (templates) anbefalede udvalget, at der oprettes et centralt privat register, hvor de restaurationsvirksomheder, som ønsker det, kan få oplyst, om en bestemt person har restaurationsforbud det pågældende sted.

7.2.1.3 Tilvejebringelse af en klar lovhjemmel for politiet til at videregive oplysninger om personer med restaurationsforbud til restauratøren

Da justitsministeren nedsatte udvalget tilbage i sommeren 2008, indeholdt restaurationsloven ikke nogen klar hjemmel til, at politiet kunne videregive oplysninger om personer med restaurationsforbud til restauratøren, når en person havde fået et forbud mod at opholde sig som gæst i den pågældende restauration.

Udvalget fandt således, at der burde tilvejebringes en sådan klar lovhjemmel ved, at der i restaurationsloven blev indsat en bestemmelse om, at politiet kan videregive oplysninger til restauratører om hvilke personer, der har fået forbud efter restaurationsloven mod at opholde sig i den pågældende restauration, herunder om at videregivelsen kan ske via et privat register.⁹⁹

7.2.2 Sammenfatning

Restaurationerne spiller en vigtig rolle i forbindelse med håndhævelsen af restaurationsforbud, herunder gennem adgangskontrollen. Det er således væsentligt, at der tilvejebringes en klar hjemmel i restaurationsloven til, at politiet kan videregive identitetsoplysninger på personer med restaurationsforbud. Dette er i mellemtiden sket.¹⁰⁰

⁹⁹ Se det i betænkningen indeholdte lovforslag s. 95 ff.

¹⁰⁰ Se LBK nr. 135 af 18. januar 2010 om restaurationsvirksomhed og alkoholbevilling m.v. (Restaurationsloven).

Restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud kan sikres på flere måder herunder ved individuel underretning af restauratøren eller ved oprettelse af et central register, som den enkelte restauration kan få online adgang til i forbindelse med sin adgangskontrol.

I modsætning til et centralt offentligt register muliggør et centralt privat register med gæstens udtrykkelige samtykke registrering af dennes fingeraftryk (template), som kan anvendes til at sikre en hurtig, effektiv og ensartet adgangskontrol.

7.3 Høringssvar fra Institut for Menneskerettigheder og Forbrugerrådet vedrørende Betænkning nr. 1504.

Betænkning nr. 1504 og det heri indeholdte lovudkast blev efterfølgende sendt i høring. Væsentlige dele af Institut for Menneskerettigheders og Forbrugerrådets høringssvar til betænkningen vil i det følgende blive fremhævet.

7.3.1 Central eller decentral lagring

Institut for Menneskerettigheder bemærkede bl.a. i deres høringssvar, at det nærmere bør undersøges, om oprettelsen af et centralt privat register er nødvendig og proportional, henset til den øgede registrering af biometriske oplysninger og de datasikkerhedsmæssige betænkeligheder et sådant register rejser og det forhold, at de restaurationer, som ønsker at anvende registret, forudsættes at indhente biometriske oplysninger fra alle gæster.

Forbrugerrådet udtrykte i deres høringssvar tilsvarende betænkelighed med hensyn til oprettelse af et centralt register. Man har ifølge Forbrugerrådet ”svært ved at forstå nødvendigheden af, at alle besøgende gæster – dvs. både personer med og uden restaurationsforbud – skal kunne registreres i et centralt register med navn, CPR-nummer, billede og fingeraftryk og mener, at forslaget i høj grad savner proportionalitet.” Forbrugerrådet fremhævede videre ”at, når så mange private oplysninger kumuleres og lagres centralt, øges risikoen for misbrug automatisk.”¹⁰¹

¹⁰¹ Jf. Forbrugerrådets høringssvar vedrørende betænkning nr. 1504/2009 om restaurationers adgang til identitetsoplysninger på personer med restaurationsforbud. Høringssvaret findes på følgende URL: <http://www.forbrugerraadet.dk/svar-alle/hoeringssvar-restaurationers-adgang-til-identitetsoplysninger-paa-personer-med-r/?ref=43>.

Alternativt kunne det ifølge Institut for Menneskerettigheder overvejes, ”om biometriske oplysninger kan lægges ind i et ”gæstemicrochip-kort” eller lignende, således at lagring af større mængder af biometriske oplysninger i databaser i videst muligt omfang søges undgået”.¹⁰²

Sidstnævnte er bl.a. i overensstemmelse med Artikel 29-gruppens bemærkninger i forbindelse med verifikation¹⁰³ og anbefalingerne i Teknologirådets rapport *Biometri – brug af biometriske teknologier i det danske samfund*. Arbejdsgruppen under Teknologirådet har i rapporten bl.a. vurderet, ”at restaurationsbranchens ønsker til brug af biometri er uhensigtsmæssige.” Branchens mål vil ifølge arbejdsgruppen kunne opnås på mindre integritetskrænkende vis, hvor restaurationsgæster selv beholder deres biometri ved for eksempel at udstede chipkort til gæsterne, hvorpå deres biometri lagres. En anden mulighed kunne ifølge arbejdsgruppen være brug af negativlister, hvor kun de uønskede gæster er registrerede med fingeraftryk.¹⁰⁴

Generelt kan det fremhæves, at når personoplysninger lagres centralt øges risikoen for at den personlige integritet kompromitteres. Dette kan bl.a. ske i forbindelse med øget risiko for misbrug og systematisk overvågning. En decentral model sikrer derimod, at den registrerede har kontrol over sine personoplysninger. Sidstnævnte medfører imidlertid at den registrerede udstyres med endnu en form for dokumentation, hvilket i forbindelse med biometri strider lidt imod den praktiske ide, hvorefter det afgørende er noget personen er, og ikke noget personen har eller ved.

Hvis billeder af komplette biologiske kendetegn lagres centralt, som f.eks. et helt fingeraftryk, risikerer man i forbindelse med manglende eller utilstrækkelige sikkerhedsforanstaltninger, at påføre den registrerede uoprettelig skade, idet biologiske kendetegn på grund af deres unikke karakter ikke som et password eller en PIN-kode kan udstedes i en ny kombination. Lagrer man derimod biometriske reference skabeloner (templates) centralt, er det mindre klart hvilke skader manglende eller utilstrækkelige sikkerhedsforanstaltninger vil kunne påføre den registrerede jf. kapitel 6, afsnit 6.4.

7.3.2 Iagttagelse af personoplysningslovens samtykkekrav

For alle oplysningstyper giver personoplysningsloven som udgangspunkt mulighed for, at behandling kan ske, hvis den registrerede har givet sit udtrykkelige samtykke hertil. De nærmere

¹⁰² Jf. Institut for Menneskerettigheders *Bemærkninger til betænkning nr. 1504/2009 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud*, afsnit 2.3.a. Høringssvaret findes på følgende URL: <http://menneskeret.dk/danmark/h%C3%B8ringssvar/2009>.

¹⁰³ Der henvises i det hele til kapitel 5.

¹⁰⁴ Teknologirådets rapporter 2010/2, *Anbefalinger*, s. 6-11, s. 8.

krav til et sådant samtykke findes i personoplysningslovens § 3, nr. 8, hvor et samtykke er defineret som enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling. For en gennemgang af disse krav henvises til kapitel 4, afsnit 4.3.2.1.1.

Institut for Menneskerettigheder og Forbrugerrådet satte begge i deres høringssvar spørgsmålstejn ved iagttagelsen af personoplysningslovens samtykkekrav. Forbrugerrådet fremhævede bl.a. at ”*det er dybt betænkeligt, hvis gæsternes samtykke til at afgive personlige oplysninger, som navn, CPR-nummer, fotografi og fingeraftryk – uanset om det er mundtligt eller skriftligt – indhentes i forbindelse med et konkret restaurationsbesøg. Dels må det formodes at gæsten – efter at have stået i kø i følgeskab med venner – har en stor interesse i at komme ind på diskoteket og derfor vil være tilbøjelige til automatisk at samtykke, dels fordi gæster ofte har indtaget alkohol og derfor kan være [i] en position, hvor vedkommende ikke kan gennemskue konsekvenserne heraf.*”¹⁰⁵

I forbindelse med ovennævnte kan det bemærkes, at et samtykke er frivilligt, selvom det gives for at opnå en eller anden ydelse, herunder f.eks. adgang til en bestemt restaurationsvirksomhed. Det er imidlertid interessant at dvæle ved betydningen af, at et samtykke indhentes i forbindelse med et restaurationsbesøg. Gæster vil ofte være påvirket af alkohol ved ankomsten til en restauration, herunder navnlig diskoteker og natklubber, hvilket indebærer en ikke uvæsentlig risiko for at nogle af gæsterne er i en tilstand, hvor de ikke kan gennemskue konsekvenserne af et meddelt samtykke.

I denne forbindelse kan det fremhæves at Diskotek Crazy Daisy i Viborg i deres anmeldelse til Datatilsynet oplyste, at man i de tilfælde, hvor det ikke ville være muligt at indhente et udtrykkeligt samtykke til registrering af karantæneårsagen, efterfølgende ville indkalde gæsten til et møde på diskoteket, hvor begrundelsen for karantænen ville blive forklaret.¹⁰⁶

Omend eksemplet fra Crazy Daisy i Viborg illustrerer, at der er taget højde for problemstillingen i en vis udstrækning, vil det være ønskeligt, hvis Datatilsynet jf. personoplysningslovens § 62, stk. 3 inspicere nogle af de 40-50 diskoteker, som har fået Datatilsynets tilladelse til at benytte sig af

¹⁰⁵ Jf. Forbrugerrådets høringssvar vedrørende betænkning nr. 1504/2009 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud. Høringssvaret findes på følgende URL: <http://www.forbrugerraadet.dk/svar-alle/hoeringssvar-restaurationers-adgang-til-identitetsoplysninger-paa-personer-med-r/?ref=43>.

¹⁰⁶ jf. Datatilsynets journalnummer 2008-42-0742.

frivillig gæsteregistrering af billede, fingeraftryk og eventuelle karantæneoplysninger,¹⁰⁷ for bl.a. at undersøge om personoplysningslovens samtykkekrav iagttages.

7.3.3 Sammenfatning

Såfremt personoplysningslovens bestemmelser er opfyldt, er der ikke noget til hinder for, at biometriske oplysninger lagres i en central database.

Manglende eller utilstrækkelige sikkerhedsforanstaltninger i forbindelse med en central database indeholdende bl.a. biometriske oplysninger vil imidlertid kunne påføre den registrerede uoprettelig skade.

Alternativt vil biometriske oplysninger kunne lagres decentralt, f.eks. på et smart card, hvorved den registrerede har kontrol over sine personoplysninger. En decentral model vil imidlertid udstyre den registrerede med endnu en form for dokumentation, hvilket i forbindelse med biometri strider lidt imod den praktiske ide, hvorefter det afgørende er noget personen er, og ikke noget personen har eller ved.

Den omstændighed, at man indhenter den registreredes samtykke til at afgive personlige oplysninger i forbindelse med et konkret restaurationsbesøg, kan efter omstændighederne rejse berettiget tvivl om frivilligheden af et meddelt samtykke. Det er således vigtigt, at den dataansvarlig udviser forsigtighed med hensyn til at godtage et samtykke meddelt på et tidspunkt, hvor gæsten har befundet sig i en sådan situation, f.eks. har været (svært) påvirket af alkohol, at vedkommende ikke har kunnet overskue konsekvenserne heraf.

¹⁰⁷ Jf. følgende URL: http://www.itst.dk/sikkerhed/fora/it-sikkerhedskomiteen/copy_of_it-sikkerhedskomiteen/debatdag-oktober-2009/Faktaark%20Biometri.pdf.

8. Fremmed ret (skandinavisk)

I det følgende redegøres for praksis fra Norge¹⁰⁸ og Sverige, hvor databeskyttelsesdirektivet ligeledes er implementeret. I norsk ret ved Lov nr. 31 af 14. marts 2000 om behandling av personopplysninger (personopplysningsloven) og i svensk ret ved Personuppgiftslagen SFS 1998:204.

Det er værd at bemærke, at medens norske og svenske administrative afgørelser fra henholdsvis Datatilsynet og Datainspektionen i visse tilfælde er blevet indbragt for administrative rekursorganer eller domstole, er der ikke i Danmark tradition for, at Datatilsynets afgørelse indbringes for domstolene.

8.1 Norge

8.1.1 Specialbestemmelse

I den norske personopplysningslovs § 12 findes en specialbestemmelse vedrørende brug af ”[f]ødselsnummer og andre entydige identifikationsmidler”. Bemærkningerne til bestemmelsen nævner direkte fingeraftryk og andre biometriske oplysninger som eksempler på, hvad der kan omfattes af begrebet *entydige identifikationsmidler*.¹⁰⁹

Bestemmelsen kræver for det *første*, at der er et sagligt behov for sikker identifikation og for det *andet*, at metoden er nødvendig for at opnå en sådan sikker identifikation. I forbindelse med sidstnævnte følger det af bemærkningerne til bestemmelsen, at nødvendighedskravet vil være opfyldt ”dersom andre og mindre sikre identifikationsmidler, som f.eks. navn, adresse og kundenummer ikke er tilstrækkelig”.¹¹⁰ Kravene er kumulative, hvilket betyder, at begge krav skal være opfyldt, for at fødselsnummer og andre entydige identifikationsmidler kan behandles.

Hverken den danske eller svenske persondataretlige regulering indeholder tilsvarende bestemmelse, hvorfor vurderingen af biometriske løsninger sker efter de almindelige behandlingsregler.

På nuværende tidspunkt arbejdes der i Norge på at indsætte nye bestemmelser i personopplysningsloven vedrørende specifik regulering af biometriske personopplysninger. Det

¹⁰⁸ Det bemærkes at Norge ikke er medlem af EU, men indgår i et tæt samarbejde med EU gennem EØS-samarbejdet.

¹⁰⁹ Jf. Ot.prp. nr.29 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven).

¹¹⁰ Jf. Ot.prp. nr.29 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven).

norske Datatilsynet har bl.a. udformet et lovudkast til ændring af personopplysningslovens § 12.¹¹¹ Hertil har Personvernemnda¹¹² i en konkret sag fra 2006 fremhævet følgende: ”*Biometriske metoder til bruk for identifikasjon eller autentisering har vært i sterk utvikling siden loven ble vedtatt. Nemnda har merket seg at Datatilsynet har fremmet forslag om særlig regulering av biometriske metoder, og stiller seg sterkt positiv til at dette blir gjort, og blir gitt prioritet i revisjonsarbeidet.*”¹¹³

I 2008 udkom rapporten *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12*, som er udarbejdet på foranledning af det norske Justis- og politidepartement. Rapporten foreslår gennemført en række ændringer af personopplysningsloven og anfører bl.a. i forbindelse med biometri, at:

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

- *Bruk av fingeravtrykk og andre biometriske metoder for å avdekke en persons identitet (identifisering), ikke er tillatt uten lovhjemmel.*
- *Bruk av fingeravtrykk og andre biometriske metoder for å autentisere personers identitet er tillatt dersom det foreligger lovhjemmel eller samtykke. Visse krav til gyldig samtykke foreslås presisert, bl.a. at det må tilbys alternative fremgangsmåter for personer som ikke ønsker å bli autentisert ved hjelp av biometri.”*¹¹⁴

I juli 2009 blev rapporten sendt i høring hos en række myndigheder og organisationer med høringsfrist den 1. november 2009.¹¹⁵

Det vil være interessant at følge dette arbejde, såfremt en revision af den danske personopplysningslov en gang i fremtiden måtte komme på tale. Herudover bidrager dette arbejde til

¹¹¹ Notat fra Datatilsynet – forslag til revisjon av personopplysningslovens § 12 og ny bestemmelse om bruk av biometriske data. Udkastet findes på følgende URL:

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

¹¹² Personvernemnda er nærmere omtalt lige nedenfor i afsnit 8.1.2.

¹¹³ Jf. Personvernemndas afgørelse af 20. december 2006 i PVN-2006-7.

¹¹⁴ Jf. Rapport 2008 – *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12*, Professor dr. Juris Dag Wiese Schartum i samarbejde med førsteamanuensis dr. Juris Lee A. Bygrave, Justits- og politidepartementet, s. 2. Rapporten findes på følgende URL: http://www.datatilsynet.no/upload/hoering/2009/POL%20horing_underlag/G-0406.pdf.

¹¹⁵ Se Justis- og politidepartements høringsbrev af 3. juli 2009. Høringsbrevet findes på følgende URL: <http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2009/horing--etterkontroll-av-personopplysning/horingsbrev.html?id=570701>.

at belyse teknologiens mangfoldige facetter, herunder sondringen mellem begreberne verifikation og identifikation jf. nærmere kapitel 5.

8.1.2 Administrativ rekurs

I modsætning til Danmark, hvor Datatilsynets afgørelser ikke kan indbringes for anden administrativ myndighed jf. personoplysningslovens § 61, kan det norske Datatilsyns afgørelser rekurreres til Personvernemnda. I det følgende gennemgås en konkret sag, hvor Personvernemnda underkendte det norske Datatilsyns afgørelse vedrørende adgangskontrol til en kommunes edb-system.

Den konkrete sag handlede om Tysvær kommune, som anvendte fingeraftryks aflæsning som adgangskontrol på alle nye bærbare computere og enkelte stationære computere i forbindelse med pålogging af kommunens edb-system. Formålet var at øge sikkerheden, så uvedkommende ikke fik adgang til følsomme personoplysninger i kommunens edb-system.

Det norske Datatilsyn fandt, at den konkrete behandling opfyldte kravet om sagligt behov for sikker identifikation, men fandt ”*at bruk av fingeravtrykksløsning ikke er nødvendig for å oppnå slik sikker identifisering*”. Ifølge Datatilsynet kunne man ”*oppnå like sikker identifisering av brukerne uten å benytte fingeravtrykk, for eksempel ved brukeridentitet eller ansattnummer.*”¹¹⁶

Afgørelsen blev efterfølgende rekurreret til Personvernemnda, som var enig med Datatilsynet i, at den konkrete anvendelse af biometri opfyldte kravet om det saglige behov for sikker identifikation. Personvernemnda mente imidlertid ikke, at det ville være tilstrækkeligt at anvende brugernavn eller smart card kombineret med password. Personvernemnda fandt derfor, at ”*[b]rug av fingeravtrykk som påloggingsprosedyre for de bærbare maskinene, som blant annet inneholder sensitive opplysninger om tredjepart, vil gi en løsning med ønsket grad av sikkerhet.*”¹¹⁷

Omdrejningspunktet er således nødvendighedsvurderingen i personoplysningslovens § 12.

8.2 Sverige

Den svenske tilsynsmyndighed Datainspektionen har i en række sager beskæftiget sig med anvendelse af forskellige biometriske løsninger i forbindelse med elevers udlevering af mad i skolers kantiner.

¹¹⁶ Se Personvernemndas afgørelse af 20. december 2006 i PVN-2006-7 hvor det norske Datatilsyns afgørelse er refereret.

¹¹⁷ Jf. Personvernemndas afgørelse af 20. december 2006 i PVN-2006-7.

I juni 2004 fastslog Datainspektionen for første gang, at den behandling af personoplysninger, som sker i forbindelse med aflæsning af elevernes fingeraftryk for at kontrollere, at eleverne har betalt for skolemaden, strider mod de grundlæggende krav i Personoplysningsloven § 9, litra e og f.¹¹⁸ Tre af tilsynets medlemmer fandt imidlertid ikke, at der var ”*någon risk för att den personliga integriteten kränks om det finns andra alternativ för den som inte vill lämna sitt fingermönster*”.¹¹⁹ Sagen blev ikke indbragt for domstolene.

Datainspektionen fulgte denne linje i 2005, hvor Datainspektionen forbød tre gymnasier at anvende biometriske løsninger. På gymnasiet i Uddevalla¹²⁰ og på gymnasiet i Lerum¹²¹ anvendes fingeraftryksaflæsning og på gymnasiet i Värnamo anvendes håndscanning.¹²² Sagerne blev alle anket til *Länsrätten* og senere til *Kammerrätten* som i alle tre tilfælde underkendte Datainspektionens afgørelser. Datainspektionen ankede efterfølgende alle tre afgørelser til *Regeringsrätten*, der er den højeste almene forvaltningsdomstol i Sverige.¹²³ Regeringsrätten besluttede dog udelukkende at realitetsbehandle sagen vedrørende gymnasiet i Uddevalla.¹²⁴

Den 16. december 2008 afsagde Regeringsrätten dom i sagen vedrørende gymnasiet i Uddevalla. Regeringsrätten anførte bl.a., at ”*det förhållandet att det är fråga om biometriska data utesluter inte att uppgifterna kan anses adekvata och relevanta i förhållande till det aktuella ändamålet*.” Regeringsrätten fandt således ikke, at behandlingen stred mod de grundlæggende krav i Personoplysningsloven § 9. Videre anførte Regeringsrätten, at ”*[b]ehandling av biometriska uppgifter i identifieringssyfte kan av många uppfattas som känslig*.” Regeringsrätten fandt bl.a. på denne baggrund, ”*då kommunens intresse av att identifiera eleverna torde kunna tillgodoses även med andra metoder[...] att behandlingen kan vara tillåten endast under förutsättning att samtycke inhämtats*.”¹²⁵ Regeringsrätten underkendte således Kammerrättens afgørelse af 1. november 2005 i 1982-05.

¹¹⁸ Personoplysningsloven § 9, litra e og f har følgende ordlyd: *e) de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen, f) inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen.*

¹¹⁹ Jf. Datainspektionens afgørelse af 15. juni 2004 i 42-2004. Afgørelsen findes bl.a. omtalt i *Skolverket*, Nyhetsbrev 9/2004, s. 6 på følgende URL: <http://www.skolmyndigheter.nu/content/1/c4/13/89/Nyhetsbrev0409.pdf>.

¹²⁰ Jf. Datainspektionens afgørelse af 13. januar 2005 i 1601-2004.

¹²¹ Jf. Datainspektionens afgørelse af 13. januar 2005 i 1602-2004.

¹²² Jf. Datainspektionens afgørelse af 9. marts 2005 i 1976-2004.

¹²³ Jf. Datainspektionens journalnummer 1824-2005 (Uddevalla), 1002-2007 (Lerum) og 1009-2006 (Värnamo).

¹²⁴ Se følgende URL: <http://www.datainspektionen.se/press/nyhetsarkiv/2008/regeringsratten-provar-dom-omtallriksautoma/>.

¹²⁵ Jf. Regeringsrättens afgørelse af 16. december 2008 i sag 6588-05

En af dommerne (Annika Brickman) fandt imidlertid under henvisning til ”*kommunens behov av ett säkert och smidigt kontrollsystem, att det inte är fråga om några känsliga uppgifter och att elever som så önskar kan avstå från att ingå i systemet [...] att kommunens kontrollintresse väger tyngre än elevernas integritetsintresse.*” Annika Brickman stemte for at stadfæste Kammarrättens afgørelse af 1. november 2005.¹²⁶

8.3 Bemærkninger til praksis i de skandinaviske lande

I Danmark er der ikke tradition for, at Datatilsynets afgørelser indbringes for domstolene. Det er således tilsynets afgørelser, der på personoplysningslovens område i praksis er endeligt normerende.¹²⁷ Dette er tankevækkende under henvisning til ovennævnte praksis fra Norge og Sverige, hvor tilsynsmyndighedernes afgørelser (i foranstående eksempler) efterfølgende er blevet underkendt.

For den danske model taler, at Datatilsynet gennem årene har oparbejdet den sagkundskab, der er nødvendig for at vurdere konkrete persondataretlige problemstillinger herunder bl.a. anvendelse af biometri.

Herudover medfører retlige standarder, og den teknologiske viden, der i mange tilfælde er nødvendig for at vurdere konkrete sager, at domstolene ikke er et egnet forum, medmindre der er tale om rene retsspørgsmål. Der henvises her til ovennævnte dom fra Regeringsrätten, hvor den dissenterende dommer i modsætning til flertallet fandt, ”*att kommunens kontrollintresse väger tyngre än elevernas integritetsintresse*”.

I forbindelse med indførelse af biometriske løsninger, i såvel den offentlige som i den private sektor, spiller det danske Datatilsyn således en afgørende rolle. Teknologiens muligheder for verifikation og identifikation af personer i mange forskellige situationer står og falder med Datatilsynets afgørelser.

¹²⁶ Jf. Regeringsrätten Avd. II, protokoll 29. oktober 2008, sag nr. 6588-05 Aktbilaga. Se følgende URL: <http://www.regeringsratten.se/Domstolar/regeringsratten/Avg%C3%B6randen/2008-skmening/6588-05.pdf>.

¹²⁷ Datatilsynet er en statslig myndighed, der udøver sine funktioner i fuld uafhængighed jf. personoplysningslovens § 56. Datatilsynet har en finanslovmæssig og personalemæssig tilknytning til Justitsministeriet, men hverken Justitsministeriet eller andre offentlige myndigheder har instruktionsbeføjelse over for Datatilsynet jf. følgende URL: <http://www.datatilsynet.dk/om-datatilsynet/arbejdsopgaver/>.

9. Teknologineutral regulering

Biometri er ligesom andre teknologier ikke direkte omtalt i hverken databeskyttelsesdirektivet eller personoplysningsloven.

Som tidligere fremhævet har den dataansvarlige ansvaret for, at personoplysningslovens bestemmelser opfyldes, og skal således forud for ibrugtagning af en biometrisk løsning sikre sig at personoplysningslovens bestemmelser overholdes.¹²⁸

Mange af personoplysningslovens bestemmelser er imidlertid formuleret som retlige standarder¹²⁹ bl.a. under henvisning til reguleringens bredde. For retlige standarder taler bl.a., at man kan lave mere langtidsholdbare bestemmelser, idet man overlader det til retsanvenderen at vurdere fremtidige tiltags rimelighed ud fra en overordnet norm. Mod retlige standarder taler bl.a., at den retsundergivne har sværere ved at forudsige retstilstanden end tilfældet er med hensyn til mere detaljerede bestemmelser.

Under henvisning til ovennævnte kan det overvejes at præcisere nogle af personoplysningslovens bestemmelser ved udarbejdelse af en adfærdskodeks jf. personoplysningslovens § 74 eller gennemføre sektororienteret regulering. I det følgende fremhæves fordele og ulemper ved sådanne tiltag.

9.1 Adfærdskodeks

Af bestemmelsen i personoplysningslovens § 74 følger, at brancheforeninger eller andre organer, som repræsenterer andre kategorier af dataansvarlige, i samarbejde med Datatilsynet kan udarbejde adfærdskodekser, der skal bidrage til en korrekt anvendelse af bestemmelserne i personoplysningsloven. Det bemærkes, at bestemmelsen alene tilskynder brancheforeninger m.v. til at tage initiativ til, at der i samarbejde med Datatilsynet udarbejdes adfærdskodekser jf. herved formuleringen '*kan*'.

I de tilfælde, hvor der udarbejdes adfærdskodekser, forudsættes det ifølge bemærkningerne til bestemmelsen, at Datatilsynet påser, at kodeksen ikke er i uoverensstemmelse med bestemmelserne

¹²⁸ Der henvises generelt til kapitel 4, afsnit 4.2.

¹²⁹ Der henvises generelt til kapitel 4, afsnit 4.3.1.

i personoplysningsloven samt regler udstedt i medfør heraf.¹³⁰ Der vil således i denne forbindelse være gode muligheder for at fremme et forsvarligt databeskyttelsesniveau gennem dialog mellem de dataansvarlige og Datatilsynet. Det bemærkes dog, at adfærdskodekser ikke behøver at være udformet på grundlag af personoplysningslovens § 74, idet også andre former for selvregulering kan tages i brug. I relation til internettet har man bl.a. udarbejdet certificeringsordninger som e-handelsmærket og Trust.e., der er relateret til et acceptabelt databeskyttelsesniveau.

På dette sted vil det være passende at nævne '*Danish Biometrics*' som en mulig aktør i forbindelse med udarbejdelse af en adfærdskodeks. Danish Biometrics blev stiftet i 2006 og er et interessent- og formidlingsnetværk til fremme af ansvarlig anvendelse af biometri.¹³¹

For udarbejdelsen af en adfærdskodeks taler bl.a., at branchen ved at gøre noget aktivt er med til at fremme databeskyttelsesniveauet, hvilket også kan have en afsmittende konkurrence- og markedsføringsmæssig effekt i stil med dataansvarliges tilslutning til certificeringsordninger. Herudover vil en adfærdskodeks kunne præcisere sikkerhedskravene i personoplysningslovens kapitel 11, der mere er et teknisk end et juridisk spørgsmål.¹³²

Mod udarbejdelsen af en adfærdskodeks taler bl.a., at dominerende markedsaktører kan sætte sig på udarbejdelsen af kodekset ud fra egne økonomiske interesser. Herudover er en adfærdskodeks ikke retlig bindende, hvilket kan medføre problemer i forbindelse med håndhævelsen af kodekset.

Så vidt vides er der endnu ikke udstedt nogen § 74-kodekser i de 10 år personoplysningsloven har været gældende.

Afslutningsvis skal det fremhæves, at Artikel 29-gruppen tilbage i 2003 i deres arbejdsdokument om biometri fremhævede vigtigheden af udarbejdelse af adfærdskodekser. Det vil være interessant at se, om Artikel 29-gruppen følger op på dette i forbindelse med den forestående ajourføring af WP 80.¹³³

9.2 Sektororienteret regulering

Ved sektororienteret regulering forstås en regulering der tager sigte på et nærmere afgrænset emneområde.

¹³⁰ Lovforslag nr. 147 af 9. december 1999, forslag til lov om behandling af personoplysninger.

¹³¹ Se endvidere følgende URL: <http://danishbiometrics.org/>.

¹³² Der henvises generelt til kapitel 4, afsnit 4.3.1.5.

¹³³ WP 170: Arbejdsprogrammet 2010-2011, vedtaget den 15. februar 2010, s. 5.

For sektororienteret regulering taler bl.a. den stigende brug af biometriske løsninger. Der er ikke længere tale om en teknologi, som man udelukkende associerer med action-thriller film som *The Bourne Identity* fra 2002, men derimod om en teknologi man f.eks. kan observere ved samtlige kasseterminaler i den danske supermarkedskæde Fakta. Herudover vil man i forbindelse med udformningen af sektororienteret regulering kunne præcisere bestemmelserne, eftersom de tager sigte på et mere klart afgrænset område. Yderligere vil begreber som verifikation og identifikation med fordel kunne præciseres, hvilket også er tilfældet i de igangværende tiltag i Norge med henblik på en revision af den norske personopplysningslov, herunder lovens § 12.¹³⁴

Mod sektororienteret regulering taler bl.a. en længerevarende lovgivningsproces. Herudover vil sektororienteret regulering i form af en lov næppe bidrage til det fuldstændige overblik over den danske persondatarelige regulering.

9.3 Afsluttende bemærkninger

Det vurderes, at man vil nå længere ved udarbejdelse af en adfærdskodeks bl.a. under henvisning til de gode muligheder, der er for at etablere en frugtbar dialog mellem Datatilsynet og branchen og muligheden for at præcisere sikkerhedskravene i personopplysningslovens kapitel 11.

¹³⁴ Jf. nærmere kapitel 8, afsnit 8.1.1.

10. Konklusion (med sammenfatning)

Biometriske løsninger giver uanede muligheder for verifikation eller identifikation af personer i mange forskellige situationer.

Behandling af biometriske oplysninger, som f.eks. aflæsning af en persons fingeraftryk, og den efterfølgende brug af oplysningerne, er en behandling af personoplysninger, der er omfattet af personoplysningsloven jf. nærmere kapitel 4, afsnit 4.1.1 og afsnit 4.1.2. Den dataansvarlige skal således forud for ibrugtagning af en biometrisk løsning sikre sig, at personoplysningslovens bestemmelser overholdes jf. kapitel 4, afsnit 4.2. Den dataansvarlige skal bl.a. overveje, om det er nødvendigt at anvende en biometrisk løsning, eller om formålet kan nås på en mindre indgribende måde ved brug af andre metoder jf. kapitel 4, afsnit 4.3.1.

Sondringen mellem verifikation og identifikation er væsentlig, hvilket bl.a. også understreges af de igangværende tiltag i Norge med henblik på en revision af den norske personoplysningslov, herunder lovens § 12 jf. kapitel 8, afsnit 8.1.1.

Under henvisning til at det i forbindelse med verifikation ikke er nødvendigt at lagre biometriske oplysninger i en central database, og at det således er muligt at sikre den registrerede kontrol over sine biometriske oplysninger ved at lagre dem decentralt, anses verifikation i persondataretlig forstand for en mindre indgribende foranstaltning end identifikation jf. kapitel 5.

Hvis billeder af komplette biologiske kendetegn lagres centralt, som f.eks. et helt fingeraftryk, risikerer man i forbindelse med manglende eller utilstrækkelige sikkerhedsforanstaltninger at påføre den registrerede uoprettelig skade, idet biologiske kendetegn på grund af deres unikke karakter ikke som et password eller en PIN-kode kan udstedes i en ny kombination. Lagrer man derimod biometriske reference skabeloner (templates) centralt, er det mindre klart, hvilke skader manglende eller utilstrækkelige sikkerhedsforanstaltninger vil kunne påføre den registrerede, idet der er uenighed blandt eksperter om, hvorvidt det er muligt at genskabe det oprindelige billede af en persons biologiske kendetegn ud fra templatens jf. nærmere kapitel 6, afsnit 6.4 og kapitel 7, afsnit 7.3.1.

Biometriske systemer har en indbygget tolerance, der sikrer mod upræcis brug af teknologien og mod forskelle i de forhold hvorunder de biometriske oplysninger præsenteres. Denne tolerance

medfører imidlertid en risiko for, at der opstår afvisning af autoriserede personer eller accept af uautoriserede personer, der ud fra en integritetssynsvinkel kan give anledning betænkeligheder jf. nærmere kapitel 6, afsnit 6.1.

I forbindelse med afvisning af autoriserede personer har det imidlertid været interessant at undersøge omfanget af den dataansvarliges oplysningspligt. Efter en nærmere gennemgang heraf er der meget som taler for, at den dataansvarlige bl.a. i forbindelse med adgangs- eller sikringssystemer, som udelukkende er baseret på biometri, skal underrette den registrerede om, at oplysningerne vil blive gjort til genstand for en automatiseret afgørelse, og at den registrerede i denne forbindelse har indsigelsesret efter personoplysningslovens § 39 jf. nærmere kapitel 6, afsnit 6.1.1.

Et område, hvor brug af fingeraftryksaflysning i dag er meget udbredt, er ved adgangskontrol på diskoteker. Afgørelsen vedrørende Diskotek Crazy Daisy i Viborg viser bl.a., at diskoteker med gæstens udtrykkelige samtykke kan registrere dennes fingeraftryk (template) og billede. Den omstændighed, at man indhenter den registreredes samtykke til at afgive personlige oplysninger i forbindelse med et konkret restaurationsbesøg, kan rejse berettiget tvivl om frivilligheden af et meddelt samtykke. Det er således vigtigt, at den dataansvarlige udviser forsigtighed med hensyn til at godtage et samtykke meddelt på et tidspunkt, hvor gæsten har befundet sig i en sådan situation, f.eks. har været (svært) påvirket af alkohol, at vedkommende ikke har kunnet overskue konsekvenserne heraf.

Under henvisning til ovennævnte vil det derfor være ønskeligt, hvis Datatilsynet jf. personoplysningslovens § 62, stk. 3, inspicere nogle af de 40-50 diskoteker, som har fået Datatilsynets tilladelse til at benytte sig af frivillig gæsteregistrering af billede, fingeraftryk og eventuelle karantæneoplysninger, for bl.a. at undersøge om personoplysningslovens samtykkekrav iagttages jf. kapitel 7.

Det er værd at bemærke, at medens norske og svenske administrative afgørelser fra henholdsvis Datatilsynet og Datainspektionen er indbragt for administrative rekursorganer eller domstole, er der ikke i Danmark tradition for, at Datatilsynets afgørelser indbringes for domstolene. Det er således tilsynets afgørelser, der på personoplysningslovens område i praksis er endeligt normerende, hvorved biometriske løsninger muligheder for verifikation eller identifikation af personer i mange

forskellige situationer står og falder med Datatilsynets afgørelser. Datatilsynet skal således være opmærksom på at se teknologiens muligheder med et nuanceret syn jf. kapitel 8.

Biometri er ligesom andre teknologier ikke direkte omtalt i hverken databeskyttelsesdirektivet eller personoplysningsloven, hvorfor det kan overvejes at præcisere nogle af personoplysningslovens bestemmelser ved udarbejdelse af en adfærdskodeks jf. personoplysningslovens § 74 eller gennemføre sektororienteret regulering.

Det vurderes, at man vil nå længere ved udarbejdelse af en adfærdskodeks bl.a. under henvisning til de gode muligheder, der er for at etablere en frugtbar dialog mellem Datatilsynet og branchen og muligheden for at præcisere sikkerhedskravene i personoplysningslovens kapitel 11 jf. kapitel 4, afsnit 4.3.1.5 og kapitel 9.

Grundet den øgede brug af biometriske oplysninger kan det afslutningsvis overvejes at lancere en landsdækkende oplysningskampagne vedrørende biometri for at gøre offentligheden mere bevidst om værdien af deres biometriske kendetegn. Dette vil også imødekomme Artikel 29-gruppens bekymring med hensyn til beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder jf. kapitel 3.

11. Litteraturfortegnelse

Bøger

Blume, Peter, *Databeskyttelsesret*, 3. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag, 2008.

Blume, Peter, *Personoplysningsloven*, 1. udgave, 1. oplag, Greens&Jura, Akademisk Forlag A/S, 2000.

Eyben, Bo Von, Jan Pedersen, Thomas Rørdam (red.), *Karnovs Lovsamling*, 4. bind, 22. udgave, Forlaget Thomson, 2007.

Gulddal, Jesper, Mette Mortensen (red.), *PAS. Identitet, kultur og grænser*, Forfatterne og Informations Forlag, 2004.

- Olesen, Birgitte Kofod, *Passet og (u)sikkerheden om biometri og integritetsbeskyttelse*, s. 145-156.

Jain, Anil K. m.fl., *Biometrics. Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.

Mortensen, Henning, Valeur, Erik m.fl., *De overvågede - vores privatliv er truet men der findes løsningsmodeller*, Udgivet i samarbejde mellem DI og Forbrugerrådet, januar 2009.

Olsen, Birgitte Kofod, *Identifikationsteknologi og individbeskyttelse – en øvelse i juridisk teknologivurdering*, 1. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag, 1998.

Waaben, Henrik, Kristian Korfits Nielsen, *Lov om behandling af personoplysninger*, 2. udgave, 1. oplag, Jurist- og Økonomforbundet, 2008.

Rapporter

Biometrics at the Frontiers: Assessing the Impact on Society, EUR 21585 EN, Teknisk rapport udgivet af EU Kommissionen, oktober 2005.

- Rapporten findes på følgende URL:
http://www.biteproject.org/documents/EU_Biometrics_at_the_Frontiers.pdf

Biometri – brug af biometriske teknologier i det danske samfund, Teknologirådets rapporter 2010/2.

- Rapporten kan hentes på projektets hjemmeside: www.biometri.info samt på Teknologirådets hjemmeside: www.tekno.dk

Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview, EUR 20823 EN, udgivet af EU Kommissionen, juli 2003.

- Rapporten findes på følgende URL: <http://fiste.jrc.ec.europa.eu/download/eur20823en.pdf>

Utredning om fødselsnummer, fingeravtryk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12, Justis- og Politidepartementet, Udarbejdet af Professor dr. Juris Dag Wiese Schartum i samarbejde med førsteamanuensis dr. Juris Lee A. Bygrave, Rapport 2008.

- Rapporten findes på følgende URL:
http://www.datatilsynet.no/upload/hoering/2009/POL%20høring_underlag/G-0406.pdf

Artikler

Davies, Simon G., *Touching Big Brother – How biometric technology will fuse flesh and machine*, Information Technology & People, Vol. 7, No. 4, 1994, s.38-47.

Lisbjerg, Jakob Vedel, *Fingeraftryk på færgen*, DR's naturvidenskabelige magasin Viden om.

- Artiklen findes på følgende URL:
<http://www.dr.dk/DR2/VidenOm/Temaer/Biometri/20070530163036.htm>

Meister, Mikkel, *Millionspild afværget: Minister skrotter politiets pas-løsning*, Version2 den 27. maj 2010.

- Artiklen findes på følgende URL:
<http://www.version2.dk/artikel/14989-millionspild-afvaerget-minister-skrotter-politiets-pas-loesning>

Tranberg, Charlotte Bagger, *Biometriske personopplysninger*, Erhvervsjuridisk Tidsskrift 2007, s. 105-115.

Tranberg, Charlotte Bagger, *Persondata og biometri i Skandinavien*, Lov & Data 2007, s. 1-6.

Direktiver

Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesdirektivet).

Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation).

Artikel 29-gruppen

WP 80: Arbejdsdokument om biometri, vedtaget den 1. august 2003.

- Den engelske version findes på følgende URL:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf

WP 112: Udtalelse 3/2005 om gennemførelsen af Rådets forordning (EF) nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometriske indikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder, vedtaget den 30. september 2005.

WP 169: Udtalelse 1/2010 om begreberne ”registeransvarlig” og ”registerfører”, vedtaget den 16. februar 2010.

WP 170: Arbejdsprogrammet 2010-2011, vedtaget den 15. februar 2010.

Danske love m.v.

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (Personoplysningsloven).

- Forslag til lov om behandling af personoplysninger (Lovforslag nr. 147 af 9. december 1999).

Bekendtgørelse nr. 529 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning.

Bekendtgørelse nr. 534 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig.

Vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger.

Betænkning nr. 1504 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud.

Høringssvar

Forbrugerrådets høringssvar vedrørende betænkning nr. 1504/2009 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud.

- Høringssvaret findes på følgende URL: <http://www.forbrugerradet.dk/svar-alle/hoeringssvar-restaurationers-adgang-til-identitetsoplysninger-paa-personer-med-r/?ref=43>

Institut for Menneskerettigheders bemærkninger til betænkning nr. 1504/2009 om restaurations adgang til identitetsoplysninger på personer med restaurationsforbud.

- Høringssvaret findes på følgende URL:
http://menneskeret.dk/danmark/h%c3%b8ringssvar/2009/n09_35

Datatilsynet

Datatilsynets Informationspjece om personoplysningsloven.

- Pjecen kan hentes via følgende URL:
<http://www.datatilsynet.dk/publikationer/informationspjece/>

Datatilsynets arbejdsopgaver og funktioner.

- Se følgende URL: <http://www.datatilsynet.dk/om-datatilsynet/arbejdsopgaver/>

Diskotekers registrering af billede, fingeraftryk og karantæneoplysninger.

- Se følgende URL: <http://www.datatilsynet.dk/erhverv/biometri/diskotekers-registrering/>

Generelt om anmeldelse:

- Se følgende URL: <http://www.datatilsynet.dk/blanketter/generelt-om-anmeldelse/>

Datatilsynets vilkår om sikkerhed i forbindelse med diskotekers anmeldelse af registrering af karantæneoplysninger.

- Vilkårene findes på følgende URL:
<http://www.datatilsynet.dk/erhverv/diskoteker/sikkerhedsregler/>

Datatilsynets afgørelser:

Datatilsynets journalnummer 2003-212-0143. (Fingeraftryk på Bornholmerkort)

Datatilsynets journalnummer 2004-54-1508. (Vedrørende behandling af oplysninger hos Projekt Janus)

Datatilsynets journalnummer 2004-219-0208. (Adgangssystem til motionscenter baseret på fingeraftryk)

Datatilsynets journalnummer 2005-291-0295. (Spørgsmål om anvendelse af biometri i sundhedsvæsenet)

Datatilsynets journalnummer 2006-219-0370. (Anvendelse af biometri ved indcheckning af bagage)

Datatilsynets journalnummer 2008-42-0742. (Adgangskontrol på diskoteker og førelse af intern karantæneliste)

Norge

Lov nr. 31 af 14. marts 2000 om behandling av personopplysninger (Personopplysningsloven).

- Ot.prp. nr.29 (1998-99) Om lov om behandling av personopplysninger.

Notat fra Datatilsynet – forslag til revisjon av personopplysningslovens § 12 og ny bestemmelse om bruk av biometriske data.

- Udkastet findes på følgende URL:
http://www.datatilsynet.no/upload/Dokumenter/saker/2006/Revisjon_12_biometri.pdf

Justis- og politidepartements høringsbrev af 3. juli 2009.

- Høringsbrevet findes på følgende URL:

<http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2009/horing--etterkontroll-av-personopplysning/horingsbrev.html?id=570701>

Personvernemndas afgørelse af 20. december 2006 i PVN-2006-7.

Sverige

Personuoppgiftslagen SFS 1998:204.

Udtalelse fra Datainspektionen af 14. maj 2008: Regeringsrätten prövar dom om tallriksautomat.

- Se følgende URL: <http://www.datainspektionen.se/press/nyhetsarkiv/2008/regeringsratten-provar-dom-om-tallriksautoma/>

Udtalelse fra Datainspektionen af 24. november 2008: Höj åldergränsen för registrering av barns fingeravtryck i pass.

- Se følgende URL: <http://www.datainspektionen.se/press/nyhetsarkiv/2008/hoj-aldergransen-for-registrering-av-barns-fingeravtryck-i-pass/>

Svenske afgørelser:

Datainspektionens afgørelse af 15. juni 2004 i 42-2004. (Njurunda)

Datainspektionens afgørelse af 13. januar 2005 i 1601-2004. (Uddevalla)

Datainspektionens afgørelse af 13. januar 2005 i 1602-2004. (Lerum)

Datainspektionens afgørelse af 9. marts 2005 i 1976-2004. (Värnamo)

Datainspektionens journalnummer 1824-2005. (Uddevalla)

Datainspektionens journalnummer 1009-2006. (Värnamo)

Datainspektionens journalnummer 1002-2007. (Lerum)

Kammerrätten i Stockholm. Afgørelse af 1. november 2005 i 1982-05. (Uddevalla)

Regeringsrättens afgørelse af 16. december 2008 i sag 6588-05. (Uddevalla)

- Regeringsrätten Avd. II, protokoll 29. oktober 2008, sag nr. 6588-05 Aktilaga. Se følgende URL: <http://www.regeringsratten.se/Domstolar/regeringsratten/Avg%C3%B6randen/2008-skmening/6588-05.pdf>

Andet:

Den Europæiske Menneskerettighedskonventions (EMRK)

Danish Biometrics

- Se følgende URL: <http://danishbiometrics.org/>

Fakta ark fra It-sikkerhedskomiteen

- Se følgende URL: http://www.itst.dk/sikkerhed/fora/it-sikkerhedskomiteen/copy_of_it-sikkerhedskomiteen/debatdag-oktober-2009/Faktaark%20Biometri.pdf