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

1 Innledning 2
1.1 Hva er biometri 2
1.2 Biometriske kjennetegn og bruk av biometriske data 2
1.2.1 Fingeravtrykk og håndflateavtrykk 2
1.2.2 Biometriske data som regelmessig analyseres 3
1.2.3 Adferdsbiometri m.m. 3
1.3 Funksjonalitet 3
1.3.1 Hvor sikre er biometriske løsninger? 4
1.3.2 Hvordan benyttes de biometriske dataene i sikkerhetsøyemed? 4
1.3.3 Lagring 4
1.4 Forskjellige bruksområder for biometriske kjennetegn 5
1.4.1 Privat bruk 5
1.4.2 ”Anonyme” løsninger 5
1.4.3 Adgangskontroll til fysiske områder 6
1.4.4 Adgangskontroll til informasjonssystemer og andre tekniske løsninger 7
1.4.5 Registreringsløsninger 7
1.4.6 Publikumsløsninger 7
1.4.7 Overvåkning av publikum 8
1.4.8 Biometri i nasjonale og internasjonale løsninger 8
2 Gjeldende rett 8
2.1 Personverndirektivet (Europa-parlamentets og Rådets direktiv 95/46/EF av 24. oktober 1995) 8
2.2 Personopplysningsloven (Lov om behandling av personopplysninger av 14. april 2000 nr. 31) 9
2.3 Internasjonale organers praksis 9
2.3.1 Artikkel 29-gruppen 9
2.3.2 European Data Protection Supervisor 10
2.4 Andre europeiske datatilsynsmyndigheters behandling av biometrispørsmål 11
2.4.1 Sverige 11
2.4.2 Danmark 11
2.4.3 Finland 11
2.4.4 Frankrike 12
3 Noen problemer ved gjeldende regulering 12
3.1 Personopplysningslovens § 12 benyttet på biometriske kjennetegn 12
3.2 Melde- og konsesjonsplikt 13
4 Forslag til lovendring 13
4.1 Kommentarer til de foreslåtte endringene 13
Til § 2 13
Til § 12 14
Til § 12 a 14
4.2 Dagens ordlyd 15
4.3 Forslag til ny ordlyd 16

1 Innledning

Datatilsynet har i den senere tiden mottatt en rekke henvendelser knyttet til bruk av biometriske kjennetegn. Henvendelsene bærer preg av at teknologi for bruk av biometriske kjennetegn promoteres kraftig fra produsentenes side med sterk fokus på at bruken er enkel og praktisk og at prisene på utstyret går ned. Spørsmål har kommet så vel fra virksomheter som ønsker å innføre løsninger hvor biometriske kjennetegn benyttes, som fra ansatte eller publikum som blir bedt om å avgi biometriske data. Det har særlig vært mange spørsmål knyttet til bruk av fingeravtrykk, men også bruk av andre biometriske kjennetegn har vært nevnt. Spørsmålene strekker seg fra bruk av fingeravtrykk i stedet for garderobelapp, via bruk av fingeravtrykk i forbindelse med tidsregistrering på arbeidsplasser, til bruk av fingeravtrykk og irisskanning for å kontrollere adgangen til lufthavner og andre terrorutsatte områder.

1.1 Hva er biometri

Ordet biometri stammer fra de greske ordene *bios* som betyr liv, og *metron* som betyr mål, ordet biometri betyr med andre ord ”mål av liv”.

Biometri kan defineres som ”vitenskap som går ut på en matematisk behandling av livsytringene i den utstrekning biologiske fenomener kan gjøres til gjenstand for målinger og resultatene uttrykkes i tall, for eksempel beregning av gjennomsnittlig levetid”[1] eller som målbar fysisk karakteristikk av en personlig egenskap, brukt for å gjenkjenne en personidentitet eller bekrefte en påstått personidentitet.

1.2 Biometriske kjennetegn og bruk av biometriske data

Biometriske kjennetegn kan defineres som kjennetegn som utgår fra kroppen og som er unike for den registrerte og samtidig er permanente eller stabile over tid og er egnet for identifisering eller bekreftelse av en påstått identitet. Et fingeravtrykk vil kunne slites som følge av arbeid med hendene, eller bevisst bortetsing av fingeravtrykket. Fingeravtrykk er likevel å anse som stabile over tid. En persons ansikt vil forandre seg med alderen, likevel vil de biometriske data som utledes fra ansiktet kunne sies å være stabile, i det minste i et visst tidsperspektiv.

Det finnes en rekke biometriske kjennetegn som per i dag kan benyttes til identifisering eller bekreftelse av identitet eller begge deler, for eksempel fingeravtrykk, håndflateavtrykk, ansiktsgjenkjenning og irisskanning. De ulike typene har sine fordeler og ulemper i praktisk bruk med hensyn til sikkerhet, integritetsinngrep, funksjonalitet og hvor enkel bruken oppfattes å være.

1.2.1 Fingeravtrykk og håndflateavtrykk

Fingeravtrykk er det biometriske kjennetegn som er mest vanlig i bruk knyttet til identifisering, og er i lang tid benyttet i rettsvesenet. Koplingen mot etterforskning gjør at bruk av fingeravtrykk blant enkelte har blitt betraktet som stigmatiserende. Aksepten for bruk synes likevel å være relativt høy. Et viktig aspekt ved bruk av fingeravtrykk er at fingeravtrykk legges igjen overalt individet ferdes, med mindre det tas skritt for å forhindre dette, for eksempel ved å bruke hansker. Håndflateavtrykk atskiller seg fra fingeravtrykk ved at man sjelden legger igjen gode avtrykk av hele håndflaten med mindre dette er bevisst.

[1] Kunnskapsforlagets fremmendord og synonymer blå ordbok 5. utgave, Kunnskapsforlaget 2004

1.2.2 Biometriske data som regelmessig analyseres

Kroppsvæsker (spytt, blod, urin, etc.), hud og hår vil alltid inneholde biometriske data som kan være utgangspunkt for analyser, herunder genetiske analyser. Eventuelle analyser vil kunne gi langt flere opplysninger om avgiveren enn det som er formålstjenlig i forskjellige tenkelige bruksituasjoner (overskuddsinformasjon). Innsamlingen av slike prøver vil også av de fleste bli betraktet som mer inngripende enn eksempelvis avlesning av en håndflate.

1.2.3 Adferdsbiometri m.m.

Det finnes programvare som analyserer en PC-brukers tastetrykk, og som for eksempel kan angi sannsynligheten for at det er riktig person som benytter utstyret. I en slik løsning kan det eksempelvis gå en alarm hos sikkerhetsleder dersom det er mer enn 30% sannsynlighet for at feil bruker sitter ved en maskin.

Identifisering ved hjelp av en persons ansikt, stemme eller tastetrykk kan teknisk sett skje uten at vedkommende selv er klar over det. Opplysningene kan med letthet hentes ut av et overvåkningskamera, et opptak av en samtale eller fra datalogger, og bruken av biometrisk analyse er tidsuavhengig i forhold til innsamlingen av den biometriske prøven. Ansiktsgjenkjenning benyttes i dag blant annet på Keflavik Lufthavn på Island.

For ytterligere drøfting av ulike typer biometriske kjennetegn henvises det til Norsk Regnesentrals personvernrapport punkt 9.7.4.

1.3 Funksjonalitet

En rekke parametre kan benyttes i prosessen med å identifisere en person. I prosessen med å bekrefte identitet benyttes tradisjonelt tre parametre som også er aktuelle for ordinær identifisering. Disse er ”det du har”, ”det du vet”, og ”det du er”.

”Det du har” er noe brukeren har som kan benyttes til å bekrefte identiteten, for eksempel en nøkkel eller et adgangskort. Noe du ”har” kan både gis bort, mistes og stjeles.

”Det du vet” er kunnskap brukeren besitter, eksempelvis et passord. Noe du ”vet” kan gis bort eller tapes dersom det skrives ned.

”Det du er” er parametre som er knyttes fysisk til brukerens person, typisk biometriske data. Et annet eksempel kan være tradisjonelle ”har” parametre som er fysisk sikret til den fysiske personen, eksempelvis adgangskort i et håndjern eller RFID-brikke som er operert inn i kroppen.

Hvilke parametre som bør benyttes avhenger av den konkrete situasjon. Der det er lave krav til sikkerhet kan det være tilstrekkelig med bruk av ett parameter, for eksempel en nøkkel. Ved høyere krav til sikkerhet kan det være en fordel å kombinere to eller flere parametre. Tradisjonelt kjenner vi godt til bruk av adgangskort og PIN-kode i fysisk adgangskontroll. Det hevdes ofte at bruk av biometriske data i seg selv innebærer at sikkerheten blir bedre. Dette er imidlertid en sannhet med store modifikasjoner jf. pkt. 1.3.1.

1.3.1 Hvor sikre er biometriske løsninger?

Bruk av biometriske data i identifisering og bekreftelse av identitet er ikke en eksakt vitenskap, men brutal sannsynlighetsberegning, og man må velge hvilken feilrate man godtar.

Man må definere hvilke feilrate man godtar i to sammenhenger; hyppigheten av at systemet aksepterer feil person (False Acceptance Rate – FAR) og hyppigheten av at systemet ikke aksepterer riktig person (False Rejection Rate – FRR). Hvilken feilrate man godtar vil være avhengig av hva man benytter løsningen til. I et system for ansiktsgjenkjenning på en flyplass for å identifisere uønskede personer vil man akseptere en langt større FAR enn i en fysisk adgangskontroll til et bankhvelv.

1.3.2 Hvordan benyttes de biometriske dataene i sikkerhetsøyemed?

I biometriske løsninger sammenligner man som oftest ikke de biometriske prøvene direkte, men bearbeidede utgaver av disse som er egnet for sammenligning. Dette kalles ofte ”templates”. Når en person registreres i et biometrisk system, tas en biometrisk prøve av personen, for eksempel ved at det avgis et fingeravtrykk. Fra denne biometriske prøven velges det ut bestemte målepunkt som bearbeides og lagres i en template. En template har to særskilte egenskaper; den tar vesentlig mindre plass å lagre enn de opprinnelige avleste data og den er egnet for sammenligning. Bruk av templates gjør det unødvendig å oppbevare konkrete måledata, som for eksempel hele fingeravtrykk, i systemet. Siden templates utregnes fra punkter er det vanskelig å reversere utregningen slik at man finner frem til den fullstendige biometriske prøve som er avgitt. I tillegg kan man på forskjellige måter øke sikkerheten mot en eventuell reversering ved å benytte blant annet kryptering.

Bruk av templates er mindre personvernkrenkende enn for eksempel bruk av hele fingeravtrykk, fordi man begrenser muligheten for misbruk.

1.3.3 Lagring

Hvilken lagring som skjer av de biometriske kjennetegnene har betydning for vurderingen av personverntrusselen bruken medfører. En tenkt løsning er at man legger koden for et fingeravtrykk inn i et bankkort. Ved uttak i minibank kontrolleres personenes fingeravtrykk mot fingeravtrykket som er lagret i kortet. Dersom man mister minibankkortet kan det ikke benyttes av andre, fordi de ikke kan fremvise riktig fingeravtrykk. I og med at koden for fingeravtrykket kun er lagret i kortet og kan sies å være ”under den registrertes kontroll”, er personverntrusselen liten.

Dersom dataene lagres lokalt eller sentralt øker personverntrusselen. En sentral database kan for eksempel være en base på nasjonalt nivå, men også en base hos arbeidsgiver. Lagring som skjer i selve kontrollutstyret måtte anses som lokal lagring. Dersom man eksempelvis avgir fingeravtrykk i en garderobe ved avlevering av en jakke, og fingeravtrykket slettes når man på et senere tidspunkt henter jakken, vil det skje en lokal lagring i utstyret. Det vil imidlertid lett oppstå grensetilfeller hvor lagringen vanskelig kan kategoriseres inn under en eventuell definisjon av sentral eller lokal database.

Store sentrale baser utgjør et misbrukspotensial fordi det alltid vil være interessant å benytte opplysningene til annet enn det opprinnelige formålet. Jo større basen blir desto flere potensielle formål vil den kunne oppfylle.

Lokale baser utgjør et misbrukspotensial fordi sikkerheten rundt dem ofte er dårligere enn for sentrale baser. For eksempel vil utstyr som inneholder biometriske data kunne stjeles. Rutiner for å hindre uautorisert adgang til dataene er også ofte mangelfulle.

1.4 Forskjellige bruksområder for biometriske kjennetegn

I det følgende gis en kort oversikt over forskjellige typer bruk som anses relevant i denne sammenhengen. Listen over bruksområder må ikke anses som uttømmende.

1.4.1 Privat bruk

Bruken av biometriske kjennetegn for private formål er økende som følge av at den teknologiske utviklingen går i stor fart og at tilbyderne driver relativt massiv markedsføring av sine produkter, også overfor private. Løsninger for bruk av fingeravtrykk ved pålogging til private datasystemer, PDA'er og mobiltelefoner finnes, og vil antagelig bre om seg i bruk i tiden fremover. Videre tilbys det på det norske markedet løsninger hvor man bruker fingeravtrykk som nøkkel til sitt eget hjem. Fra utlandet kjenner man til løsninger hvor fingeravtrykk benyttes som tenningsnøkkel til bil.

Utstrakt privat bruk av biometriske kjennetegn for private formål bidrar til at personopplysninger blir spredt i stor skala, noe som igjen øker misbrukspotensialet og muligheten for at opplysninger mot brukerens vilje skal komme på avveie.

Bruk av biometriske data for private formål faller utenfor både direktiv 95/46 EF og personopplysningsloven, og regulering av privat bruk og utstyr til privat bruk ligger utenfor Datatilsynets mandat. Men tilsynet har kompetanse og plikt til å informere publikum om eventuelle personverntrusler ved slik bruk.

1.4.2 "Anonyme" løsninger

Biometriske kjennetegn kan benyttes i såkalte "anonyme" løsninger, hvor formålet med bruken ikke inkluderer kunnskap om individets tradisjonelle identifiserende opplysninger som navn, fødselsnummer etc, men kjennskap til at individet er gitt en rettighet. Eksempler på slike løsninger er en garderobe hvor fingeravtrykk benyttes istedenfor en tradisjonell garderobelapp, oppbevaringsboks hvor fingeravtrykk benyttes som nøkkel og bruk av biometriske kjennetegn som bevis på at man har betalt for måltid i en kantine.

Løsningene kan ikke betraktes som anonyme i personvernsammenheng da biometriske kjennetegn kan knyttes til enkeltindividet som har avgitt den biometriske prøven. Spørsmålet er om en slik bruk av biometriske kjennetegn kan betraktes som mindre krenkende enn løsninger der hvor de biometriske kjennetegnene knyttes opp mot tradisjonelle identifiserende opplysninger. Kanskje kan man sammenligne bruken med bruk av avidentifiserte personopplysninger.

Ved innføring av biometriske løsninger i tilknytning til denne typen tjenester beveger man seg bort fra situasjonen i dag hvor disse tjenestene faktisk kan benyttes anonymt. Bruk av biometriske kjennetegn for trivielle formål innebærer derfor en reell begrensning i individenes mulighet til å bevege seg anonymt i samfunnet.

Valg av biometri i slike løsninger bunner som regel ikke i at man har et høyt behov for sikkerhet, men heller i praktiske hensyn, og kan oppfattes som hensiktsmessig også for brukeren. Eksempelvis vil dette eliminere problemet med tapte garderobelapper.

Løsningene kan etableres slik at de biometriske data slettes så snart man er ferdig med å benytte privilegiet, eksempelvis når jakken er hentet. Det er likevel en fare for at man også etter dette tidspunktet kan hevde å ha et behov for videre lagring, eksempelvis for i ettertid å kunne dokumentere at jakken ble levert ut til riktig person.

Dersom bruk av biometriske kjennetegn gjøres obligatorisk for bruk av tjenester hvor kravet til sikkerhet er lite, kan det bli oppfattet som unødvendig inngripende av enkelte brukere. Dersom bruken baseres på brukerens samtykke medfører dette at det må foreligge alternative løsninger. Det er ikke tilstrekkelig å vise til at det er frivillig å benytte seg av tjenesten, for eksempel at det er frivillig å henge fra seg en jakke i garderoben. Dersom det ikke finnes alternative løsninger, for eksempel anledning til å benytte vanlig graderobelapp, vil det at en person nekter å avgi biometrisk prøve i denne sammenhengen ha som negativ konsekvens at garderoben ikke kan benyttes. Dermed er personopplysningslovens krav til frivillighet ikke oppfylt. Når det stilles krav til at det skal foreligge alternativer til den biometriske løsningen kan dette imidlertid ha som konsekvens at effektivitetsgevinsten ved innføringen av biometriske løsninger reduseres.

1.4.3 Adgangskontroll til fysiske områder

Bruk av biometriske løsninger i tilknytning til adgangskontroll til fysiske områder fremstilles av produsentene av løsningene som særlig sikkert, effektivt og kostnadsbesparende. Biometriske kjennetegn kan benyttes sammen med andre identifikasjonsmetoder, for eksempel manuell eller elektronisk kontroll av ID kort, kontroll av passord/PIN-kode osv. Enkelte henvendelser Datatilsynet har mottatt tyder imidlertid på at man også vurderer løsninger hvor biometriske kjennetegn benyttes som eneste identifikasjons middel.

I forhold til adgangskontroll synes det hensiktsmessig å skille bruken i tre deler, adgangskontroll for områder med høyt sikkerhetsbehov, for eksempel ved adgangskontroll til terrorutsatte områder, adgangskontroll for områder med et ordinært sikkerhetsbehov, for eksempel ordinære arbeidsplasser, og adgangskontroll for områder med lavt sikkerhetsbehov hvor formålet mest er å kontrollere at adgangen er betalt, for eksempel adgangskontroll til treningssentre. Det vil lett oppstå usikkerhet med hensyn til kategoriseringen av et bestemt område i de forskjellige gruppene. Flyplasser anses som særlig terrorutsatte områder hvor man aksepterer høye krav til sikkerhet i adgangskontrollen, samtidig som en jernbanestasjon kan være et like egnet terrormål, uten at man aksepterer innføring av de samme sikkerhetsrutiner for adgang til jernbanestasjonen.

1.4.4 Adgangskontroll til informasjonssystemer og andre tekniske løsninger

Det finnes i dag en rekke løsninger hvor biometriske kjennetegn benyttes i pålogging til dataløsninger for eksempel for å sikre at passord ikke blir avgitt (frivillig eller ufrivillig) til andre som ikke skal ha adgang til bestemt informasjon. Det finnes videre løsninger hvor biometriske kjennetegn avkreves før adgang gis til andre tekniske løsninger, for eksempel løsninger hvor kassepersonalet må avgi fingeravtrykk for å få tilgang på pengene i kassen.

Bruk av biometriske prøver i adgangskontroll til informasjonssystemer og andre tekniske løsninger må i utgangspunktet betraktes likt med bruk i fysisk adgangskontroll. Spesielt for informasjonssystemer er at passord lett kommer på avveie, bevisst eller ubevisst, og at man har mindre fysisk kontroll med brukerne. Bruk av biometriske kjennetegn i slike sammenhenger kan være hensiktsmessig. For eksempel innen helsesektoren vil bruk av fingeravtrykk bedre kunne sikre at det er riktig bruker som eksempelvis får tilgang til å lese en pasients journal.

1.4.5 Registreringsløsninger

Dette omfatter tidsregistrering på arbeidsplasser hvor stemplingsuret aktiveres ved bruk av fingeravtrykk og andre løsninger hvor biometrisk prøve avkreves for å bekrefte oppmøte eller tilstedeværelse.

Det kan argumenteres med at ansattes ID-kort og koder kan byttes, slik at man stempler inn og ut for hverandre og slik uberettiget får utbetalt lønn og evt. overtid. Biometriske løsninger oppfattes av arbeidsgivere som en god metode for timeregistrering som er vanskelig å forfalske. Ansattes oppfatning av slik bruk av biometriske løsninger strekker seg fra at dette er praktisk og ønskelig, til at det er svært inngripende i den ansattes integritet.

1.4.6 Publikumsløsninger

De tidligere presenterte bruksområder har, med unntak av de anonyme løsningene, i hovedsak arbeidstakere som målgruppe. I det videre omtales løsninger som har fokus på det store publikum. Generelt kan disse deles i to grupper, de som man har en reell valgmulighet om man skal benytte eller ikke, og de som ikke gir oss en valgmulighet.

Det er i dag ikke et reelt alternativ for den jevne nordmann å gi avkall på minibankkort og gå over til kun kontant betaling. Dersom bankene skulle beslutte at man fra et gitt tidspunkt obligatorisk skal benytte biometriske data ved uttak i minibank og betaling med kort, vil dette i realiteten bli påtvunget oss alle, selv om det er frivillig å ha minibankkort. Dersom en eventuell innføring baseres på samtykke, innebærer dette at det må foreligge reelle alternative løsninger. Dersom de alternative løsningene belemres med større egenandel ved tap eller lignende fordi de anses som mindre sikre, vil ikke samtykket være frivillig jf. personopplysningsloven 2 nr. 7.

En tenkt situasjon er at man innfører bruk av fingeravtrykk eller lignende tilknyttet digitale IDer som man benytter ved pålogging til nettjenester eller betaling over nett. Eksempelvis for pålogging til den statlige ”Min side” hvor hver enkelt skal kunne hente og formidle

informasjon om seg selv til det offentlige. Da offentlige tjenester skal være tilgjengelig for alle, uten noen form for diskriminering, er det tvilsomt om en slik løsning kan gjøres obligatorisk. Betalingsløsninger over Internett blir etter hvert like vanlig som bruk av minibankkort, og løsningene bør vurderes på linje med hverandre. Det er grunn til å anta at sikkerhetsløsninger som er knyttet til minibankkort, også kan knyttes til netthandel.

Biometriske kjennetegn benyttes i enkelte andre land i billetteringssystemer, enten for å knytte eier og reisebevis sammen, eller som reisebevis alene. Det er ikke usannsynlig at slike løsninger vil bli fremstilt som ønsket også i Norge.

1.4.7 Overvåkning av publikum

Biometriske kjennetegn kan benyttes for å overvåke publikum med det formål å identifisere eller skille ut mistenkelige personer. Det mest konkrete eksempel her er myndigheters bruk av biometriløsninger på sportsarenaer og flyplasser for å plukke ut hooligans, terrorister og andre uønskede personer. I en del sammenhenger blir det også argumentert for at private bør kunne benytte biometriske løsninger for slike formål, for eksempel at vaktselskaper skal kunne benytte biometriske kjennetegn sammen med fjernsynsovervåkning med formål å plukke ut svartelistede personer.

Det kan argumenteres for at slik registrering skal skje uten publikums kunnskap for å gi best resultat, det er imidlertid svært betenkelig sett ut ifra et personvernståsted.

1.4.8 Biometri i nasjonale og internasjonale løsninger

Biometriske kjennetegn eller data benyttes i stigende grad i tilknytning til offentlige organers myndighetsutøvelse, for eksempel i immigrasjonskontroll og passkontroll. Norske pass er allerede tilrettelagt for innføring av biometriske data og det foreligger planer om innføring av et nasjonalt ID-kort med innlagte biometriske data. I tillegg fører internasjonale regler og forpliktelser til at man i Norge i stigende grad innfører ordninger hvor biometriske data benyttes, for eksempel i tilknytning til visumutstedelse og ID-kort for sjømenn. De nye ”biometriske passene” nevnt ovenfor, kommer også som en konsekvens av internasjonale krav. Felles for slike løsninger er at de involverer et stort antall personer, og at deltagelse i liten grad er frivillig.

2 Gjeldende rett

2.1 Personverndirektivet (Europa-parlamentets og Rådets direktiv 95/46/EF av 24. oktober 1995)

Artikkel 2 a i direktiv 95/46/EF definerer personopplysninger som all slags informasjon som kan knyttes til en identifisert eller mulig identifiserbar enkeltperson….;en identifiserbar person er en som kan identifiseres, direkte eller indirekte, spesielt via et identifikasjonsnummer eller gjennom en eller flere faktorer som er spesielle for vedkommendes fysiske, psykologiske og mentale… identitet . Fortalens resitasjon nr. 26 kommer i tillegg med følgende forklaring av begrepet:”…for å bestemme hvorvidt en person er identifiserbar, skal man også ta i betraktning alle de midler som det er sannsynlig kan bli benyttet av den behandlingsansvarlige eller andre til å identifisere en gitt person…”. Det legges til grunn at biometriske data faller inn under denne definisjonen jf. pkt. 2.3.1 nedenfor

Det følger av direktivets artikkel 8 nr 7 at ”Medlemsstatene skal bestemme hvilke vilkår som må oppfylles for at et nasjonalt identifikasjonsnummer eller andre vanlige midler til identifikasjon kan behandles”. Direktivet er oppfylt gjennom personopplysningslovens § 12.

2.2 Personopplysningsloven (Lov om behandling av personopplysninger av 14. april 2000 nr. 31)

Personopplysningslovens § 12 regulerer bruken av fødselsnummer og andre entydige identifikasjonsmidler. I Ot prp nr 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven) s 114 nevnes fingeravtrykk og andre biometriske data som eksempler på ”andre vanlige midler til identifikasjon”. Det er følgelig klart at biometriske data faller inn under bestemmelsen i § 12. Det har i denne sammenheng ingen betydning om man kun benytter en kode eller templates beregnet ut fra den biometriske prøven, så fremt denne koden kan knyttes til et enkeltindivid. Det har heller ingen betydning om de biometriske dataene eller koden som benyttes, blir kryptert og dermed vanskelig kan misbrukes. Dette er imidlertid krav til sikkerhet som vil kunne komme inn dersom formålet med bruken oppfyller paragrafens vilkår.

Det følger av § 12 at det både må foreligge et saklig behov for sikker identifisering og at det må være nødvendig for å oppnå slik identifisering. Det må være viktig for behandlingsansvarlig og den registrerte at riktig identitet benyttes, og man må se hen til konsekvensene som en personforveksling kan få. Feil i kunderegistre i postordrefirmaer får ikke så alvorlige konsekvenser som en identitetsforveksling av pasienter som skal opereres. Kravet til nødvendighet vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som for eksempel navn, adresse og kundenummer ikke er tilstrekkelig.

Hvis det er umulig eller urimelig vanskelig å oppnå sikker identifisering på annen måte, og det er av stor betydning at den registrerte er sikkert identifisert, kan biometriske kjennetegn benyttes. I de fleste tilfeller vil man imidlertid oppnå en tilfredsstillende identifikasjon av de registrerte ved bruk av navn, adresse og fødselsdato, eventuelt med tillegg av et egendefinert kunde- eller medlemsnummer.

I de tilfeller hvor vilkårene i § 12 er oppfylt, må den behandlingsansvarlige i tillegg oppfylle de øvrige kravene i personopplysningsloven. Dvs. at det må foreligge et gyldig behandlingsgrunnlag jf. personopplysningslovens § 8 og evt. § 9 og at grunnkravene i § 11 må være oppfylt. I tillegg må informasjonssikkerheten oppfylle kravene i § 13.

Biometriske data er som utgangspunkt ikke å anse som sensitive personopplysninger jf. personopplysningslovens § 2 nr. 8, men biometriske kjennetegn kan i enkelte tilfeller analyseres på en slik måte at sensitive opplysninger avdekkes (dette er blant annet tilfelle for blod og urin). I disse tilfellene vil bruken som utgangspunkt være underlagt konsesjonsplikt jf. personopplysningslovens § 33. Bruk av biometriske data eller biometriske kjennetegn for øvrig er som utgangspunkt meldepliktig jf. personopplysningslovens § 31. Det er imidlertid mange unntak fra denne hovedreglene.

2.3 Internasjonale organers praksis

2.3.1 Artikkel 29-gruppen

Gruppen er nedsatt ved Europa-parlamentets og Rådets direktiv 95/46/EF av 24. oktober 1995, som henviser til direktivets artikkel 29 og artikkel 30, nr. 1, litra a), og artikkel 30, nr.

3, som henviser til gruppens forretningsorden, særlig artikkel 12 og 14. Gruppen er et rådgivende organ for Kommisjonen i personvernspørsmål og skal i korte trekk beskytte fysiske personer i forbindelse med behandling av personopplysninger, og omtales som artikkel 29-gruppen.

En av gruppens formål er å se til at personverndirektivet tolkes på samme måte i alle EU/EØS-land. Artikkel 29-gruppen legger til grunn at biometriske data og biometriske data som digitalt er omformet til et template (mønster), som hovedregel er å anse som personopplysninger.

Art. 29-gruppen har i flere av sine uttalelser omhandlet spørsmålet om bruk av biometriske data, herunder uttalelser om bruk av biometri i reisedokumenter (pass) og visa (VIS)[2]. Det finnes også et eget arbeidsdokument om biometri som ble vedtatt 1. august 2003.

Art. 29-gruppen fremhever viktigheten av å følge en del grunnleggende prinsipper ved vurderingen av om biometriske data skal tillates benyttet, og trekker særlig frem kravet til formålsbestemthet og proporsjonalitet. Det understrekes videre at de grunnleggende friheter og menneskerettigheter må respekteres. Dersom formålet kan oppnås ved hjelp av mindre inngripende metoder skal disse foretrekkes. Art. 29-gruppen legger videre vekt på hvilken type biometriske data som ønskes benyttet, og uttaler at man fortrinnsvis skal benytte biometriske data som ikke etterlater spor, for eksempel skal man unngå bruk av fingeravtrykk og heller bruke håndflateavtrykk. Det legges blant annet også vekt på informasjon til den registrerte og mulighet for den registrerte til selv å sjekke de data som er lagret elektronisk. Det fremheves at eventuell lagring av de biometriske dataene bør skje på et lokalt lagringsmedium eksklusivt tilgjengelig for den registrerte, fremfor i sentrale databaser. Eventuelle sentral lagring, bør etter gruppens vurdering være gjenstand for forhåndskontroll av personvernmyndighetene.

Art. 29 gruppen peker på en rekke mulige personverntrusler ved bruk av biometriske data. Bl.a. faren ved at enkelte biometriske data legges igjen som spor i det daglige liv og dermed kan samles inn uten den registrertes kjennskap (fingeravtrykk og DNA). Innsamlingen av denne typen data innebærer kun små fysiske inngrep, noe som igjen kan medføre stor bruk av mer eller mindre pålitelige data, og i verste fall identitetstyveri med den følge at de biometriske data i lang tid fremover kan knyttes til feil identitet og skape alvorlige problemer for de biometriske datas rettmessige eier.

2.3.2 European Data Protection Supervisor

European Data Protection Supervisor (EDPS) er EUs personvernombud som ble opprettet i 2004. EDPS har som oppgaver å overvåke behandlingen av personopplysninger i EUs institusjoner og organer, gi råd med hensyn til personvernlovgivning og -prinsipper og samarbeide med lignende organer for å sikre et helhetlig personvern.

EDPS har i spørsmål om bruk av biometriske data fremhevet viktigheten av proporsjonalitet mellom metode og formål, at adgangen til de biometriske dataene begrenses og at det må settes i kraft nødvendige sikkerhetstiltak for å sikre de biometriske dataene. EDPS fremhever det som en personverntrussel at menneskets kropp i seg selv gjøres maskinlesbar og har blant

[2] Se for eksempel Opinion 7/2004.

annet fremhevet at utvidet bruk av biometriske data vil ha stor innvirkning på samfunnet og at det derfor bør gjennomføres en debatt om dette, før bruk tillates på generelt nivå og før lovgivere foreslår bruk av dette i ulike sammenhenger. EDPS har også pekt på at biometriske datas uforanderlighet gjør at konsekvensene ved misbruk, "tap" og lignende vil kunne bli større enn ved tap av et passord.

EDPS har som et behandlingsprinsipp at det pga faren for feil eventuelt må innføres likeverdige prosedyrer som kan brukes istedenfor identifikasjon vha biometri

2.4 Andre europeiske datatilsynsmyndigheters behandling av biometrispørsmål

2.4.1 Sverige

Det foreligger ingen spesielle bestemmelser for bruk av biometriske data og de vanlige reglene i Personuppgiftslagen (PuL) legges til grunn ved vurderingen av om bruken av biometriske data skal godkjennes. Den svenske Datainspektionen har fattet en rekke avgjørelse med hensyn til bruk av biometriske data. Blant annet er det vurdert at bruk av fingeravtrykk innebærer en risiko for integritetskrenkelse som kan være vanskelig å overskue i det daglige. Det er derfor ikke ansett som relevant og hensiktsmessig å benytte fingeravtrykk for å kontrollere ansattes tilstedeværelse på arbeidsplassen. Datainspektionen har videre vurdert at det er i strid med PuL dersom man i skolekantinen avkrever elevenes fingeravtrykk i tallerkenautomaten for å kontrollere om måltidet er betalt. Datainspektionens vedtak ble omgjort av Kammarretten, og saken er i skrivende stund innklaget for Høgsta domstolen.

Datainspektionen har imidlertid åpnet for at biometriske data kan benyttes for å starte tekniske innretninger og i tilknytning til adgangskontroll. Det er slått fast at mindre inngripende metoder alltid skal vurderes. Det er påpekt at dersom bruk av biometriske data baseres på samtykke fra den registrerte, innebærer dette at det må foreligge alternative til bruk av biometriske data.

2.4.2 Danmark

Det foreligger ikke spesielle bestemmelser for bruk av biometriske data, og bruken vurderes etter de vanlige prinsipper i Persondataloven.

Det danske Datatilsynet har blant annet akseptert bruk av fingeravtrykk (template) i ferjekort på Bornholm.

2.4.3 Finland

Det foreligger ingen spesielle bestemmelser for biometri. Dataombudsmannens byrå har imidlertid laget retningslinjer for bruk av biometriske data. I retningslinjene har man blant annet understreket at dataene må krypteres tifredsstillende, at man skal unngå sentral lagring og at biometriske data bør benyttes sammen med andre tradisjonelle identifikasjonsmetoder. Det er også fremhevet at bruken bør ha grunnlag i den enkeltes samtykke.

2.4.4 Frankrike

All bruk av biometri krever forhåndstillatelse fra det franske Datatilsynet (CNIL). Biometrisk gjenkjennelsesteknologi som ikke krever lagring av templates i databaser innebærer etter CNILs oppfatning ikke de store vanskelighetene når det gjelder personvern og datasikring. Ved sentral lagring, kan bruk av biometri ha betydning for personvernet. Dette gjelder særlig biometriske kjennetegn som legges igjen som spor i hverdagen. Proporsjonalitetsprinsippet er da avgjørende.

Ved ubetinget krav om høy sikkerhet, har CNIL likevel godtatt bruk av biometriske data og sentral lagring. Dette gjelder for eksempel for bruk i adgangskontroll til atomanlegg og til enkelte rom i den Franske Nasjonalbank. Også i tilfeller hvor det ikke er særlige krav til sikkerhet har CNIL godtatt bruk av med biometriske data som ikke etterlater spor (eks. håndflateavtrykk), til tross for sentral lagring.

3 Noen problemer ved gjeldende regulering

Det er Datatilsynets oppfatning at dagens regulering på den ene side er for streng, i det man har et tilnærmet forbud mot bruk av biometriske kjennetegn. Samtidig gir dagens regulering liten oversikt og kontroll med bruk av biometriske kjennetegn, i det reglene for melding og eventuell konsesjon er uoversiktlige.

3.1 Personopplysningslovens § 12 benyttet på biometriske kjennetegn

Personopplysningslovens § 12 tillater kun bruk i følge med sikker identifisering. Begrepet identifisering er vidt, og det må vurderes hva dette er ment å favne. Begrepets mulige bredde kan kategoriseres i:

a) Angi et entydig individ (identitet). Slik benyttes tradisjonelt fødselsnummer, for eksempel for å sikre at man rapporterer skattetrekk på riktig individ.
b) Avdekke et gitt individs identitet. Dette er prosessen i å komme frem til hvem et individ er, for eksempel ut ifra et fingeravtrykk.
c) Bekrefte et gitt individs antatte identitet (autentisering). Dette er prosessen i å bekrefte at individet er det man tror eller påstås å være, f. eks ved hjelp av et passord eller kontroll av individets legitimasjonspapirer.

Metodene b) og c) kan også orientere seg mot å bekrefte at et gitt individ er gitt spesielle rettigheter eller bekrefte et gitt individs tilknytning til en gitt gjenstand uten at man gjør seg kjent med tradisjonelt identifiserende opplysninger.

Personopplysningslovens § 12 er utformet med henblikk på behandling av fødselsnummer, og at man skal forhindre misbruk av dette. Det er derfor sagt direkte i forarbeidene at fødselsnummer ikke skal benyttes som legitimasjon. Biometriske data er nevnt som eksempel på ”entydige identifikasjonsmidler” i forarbeidene, men regelen tar ikke høyde for de egenskaper biometriske data har som gjør dem egnet, ikke bare i forbindelse med identifisering i snever tolkning (situasjon a), men også i forbindelse med bekreftelse av angitt eller antatt identitet (situasjon c). Fødselsnummer er uegnet som legitimasjon eller for å bekrefte identitet, mens en sammenligning av biometriske prøver nettopp er egnet for dette. Dette gjør at regelen er lite hensiktsmessig hva gjelder bruk av biometriske kjennetegn.

I skrivende stund har Datatilsynet ikke praktiske eksempler på bruk av biometriske data som kan aksepteres etter dagens lovgivning. Vedtak er fattet i forhold til bruk av fingeravtrykk og

irisskanning i adgangskontroll for ansatte ved Oslo Lufthavn, bruk av fingeravtrykk ved innsjekking av bagasje på fly, bruk av fingeravtrykk i tilknytning til timeregistrering ved arbeidsplasser, samt bruk av fingeravtrykk i en garderobe som alternativ til bruk av vanlig garderobelapp. I noen av sakene foreligger et saklig behov for sikker identifisering. Identifiseringen skjer imidlertid ved bruk av tradisjonelle metoder, som for eksempel fremvisning av adgangskort, mens de biometriske kjennetegnene benyttes til å bekrefte at den opplyste identiteten er korrekt. Slik bruk faller jf. det som er beskrevet over utenfor begrepet "sikker identifisering" i § 12. Vedtakene kan bli påklaget.

3.2 Melde- og konsesjonsplikt

I dag råder det blant de behandlingsansvarlige usikkerhet med hensyn til om bruk av biometriske kjennetegn eller biometriske data medfører melde eller konsesjonsplikt. Hovedreglene i personopplysningslovens §§ 31 og 33 og unntakene i personopplysningsforskriften fremstår som vanskelig tilgjengelige for de behandlingsansvarlige og dette medfører at mange velger å sende en konsesjonssøknad for å være på den sikre siden. Dette igjen medfører unødvendig merarbeid for Datatilsynet i form av grunnløse konsesjonssøknader. Samtidig er det fare for at Datatilsynet går glipp av viktige opplysninger om bruk av biometriske løsninger, fordi de behandlingsansvarlige i andre tilfeller ikke er kjent med at bruken er meldepliktige, eller fordi bruken er omfattet av et av de mange unntakene i forskriften.

Det er Datatilsynets oppfatning at bruk av biometriske kjennetegn og biometriske data bør være meldepliktig. Det kan for øvrig være naturlig at konsesjonsplikt for behandling av biometriske data som medfører behandling av sensitive opplysninger, kommer klarere til utrykk i loven.

Meldesystemet har i dagens utforming en begrenset funksjon. Dette har ikke bare sammenheng med at det antagelig er en meget stor underrapportering fra de behandlingsansvarlige. Det kan tenkes at bruk av biometriske kjennetegn bør underlegges en særskilt meldeordning, hvor for eksempel antallet steder biometriske data benyttes angis. Det vil gi Datatilsynet en bedre oversikt over den totale bruken av biometriske data i samfunnet, og således være bedre i samsvar med direktivets intensjoner.

4 Forslag til lovendring

Datatilsynet fremmer med dette forslag til endring av personopplysningslovens § 12 og forslag til ny § 12 a. I tillegg fremmes forslag til endring av § 2 ved at det inntas en ny definisjon.

4.1 Kommentarer til de foreslåtte endringene

Til § 2

Forslaget inneholder to alternative definisjoner. I daglig tale har "biometri" festet seg som et samlebegrep for biometriske data og kjennetegn samt bruken av disse. Det kan derfor være hensiktsmessig å forholde seg til denne begrepsbruken i loven. Det er imidlertid Datatilsynets oppfatning at denne begrepsbruken også kan være egnet til misforståelse og sammenblanding i forhold til biometri som vitenskap. Det er derfor laget en alternativ definisjon av "biometriske kjennetegn". Dette begrepet fremstår som mer presist og vil over tid vise seg lettere å håndtere i praksis.

Definisjonen av biometriske kjennetegn er ment å skulle omfatte både det konkrete biometriske kjennetegnet og resultater som utledes av dette, eks. template. Uttrykket ”stabile over tid” viser til at kjennetegnet må ha en viss stadighet ved seg. Det antas å være lite hensiktsmessig å foreta en mer presis tidsavgrensing i loven, da det bør være opp til den behandlingsansvarlige å vurdere hvilken stabilitet som er nødvendig og hensiktsmessig knyttet til konkrete formål.

Til § 12

Biometriske kjennetegn vil ikke falle inn under definisjonen ”lignende” identifikasjonsmiddel”, fordi de i sine egenskaper i stor grad avviker fra fødselsnummer. Det blir på denne måten trukket en klar grense mellom bruk av biometriske kjennetegn som skal følge ny § 12 a og andre entydige identifikasjonsmidler som skal følge § 12. Endringen er ikke ment å begrense omfanget av § 12 i forhold til andre typer entydige identifikasjonsmidler som per i dag faller inn under paragrafen.

Til § 12 a

Paragrafen er ikke ment å skulle begrense muligheten for forskning på biometriske data eller annen forskning hvor biometriske data inngår i forskningsmaterialet.

Med identifisering menes bruk av biometriske kjennetegn der bruken knyttets opp mot tradisjonelt identifiserende opplysninger, for eksempel der fingeravtrykk kontrolleres opp mot fingeravtrykk lagret i et adgangskort med navn. I tillegg er det hensikten at identifisering skal omfatte bruk av biometriske kjennetegn i såkalte ”anonyme løsninger”, for eksempel brukt som alternativ til garderobelapp uten at det skjer noen registrering av andre tradisjonelt identifiserende opplysninger. Det er Datatilsynets oppfatning at begge typene bruk bør omfattes fordi bruk av biometriske kjennetegn uten tilknytning til andre identifiserende opplysninger kan sammenlignes med behandling av avidentifiserte personopplysninger, og at det i såkalte anonyme løsninger vil foreligge en mulighet for bakveisidentifisering fordi man forholder seg til opplysninger som er unike for individet.

Sammenlignet med § 12 er det i den nye § 12 a ikke stilt opp noe krav til nødvendighet. Det er Datatilsynets oppfatning at det ikke er grunnlag for et slikt tilleggskrav dersom den behandlingsansvarlige oppfyller lovens øvrige vilkår, som vilkårene i §§ 11 og 8. Dette har særlig betydning for situasjoner hvor den registrerte samtykker til behandlingen eller behandling som medfører svært liten personvernrisiko. Det er lite hensiktsmessig at loven skal forhindre slik bruk, selv om bruken strengt tatt ikke er nødvendig. Kravet til saklig behov utgjør likevel en nedre grense for hva som tillates.

Det anses viktig at reglene om konsesjonsplikt og meldeplikt klargjøres. Reglen om konsesjonsplikt der bruken medfører behandling av sensitive opplysninger er forsøksvis tatt inn i paragrafen. Alternativt kan det gjøres endring i personopplysningsforskriften slik at det innledningsvis i kapittel 7 slås fast at bruk av biometriske kjennetegn uten unntak medfører enten melde- eller konsesjonsplikt. Det er ikke tatt med noen henvisning til §§ 31 og 33 i forslaget, da en slik henvisning kan medføre uklarhet i forhold til om unntakene likevel skal komme til anvendelse.

Lagring av biometriske data på smartkort eller lignende som den registrerte bærer med seg kan skje så snart vilkårene i første ledd er oppfylt. Det er bare dersom man skal ha sentral eller lokal lagring hos andre at tilleggsvilkårene i tredje ledd må oppfylles.

I forslaget er det ikke skilt mellom lagring i sentral database og lokal database fordi dette medfører behov for definering av disse begrepene. Sentral database kan for eksempel være en base på nasjonalt nivå, men også en base hos arbeidsgiver. Lagring i utstyret eller systemer uten nettverkstilkobling vil kunne anses som lokal lagring. Det vil imidlertid lett oppstå grensetilfeller hvor lagringen vanskelig kan kategoriseres inn under en eventuell definisjon av sentral eller lokal database. Det er Datatilsynets oppfatning at lagring hos den behandlingsansvarlige i seg selv er uheldig, og bør unngås. Det er derfor ikke nødvendig å skille på lokal og sentral lagring.

Samtykke har særlig verdi som behandlingsgrunnlag for personopplysninger, herunder biometriske kjennetegn. Vi står imidlertid overfor ny teknologi hvor personverntrusler og farer er vanskelige å overskue, og hvor teknologiens utforming i stor grad legger premissene for den behandlingsansvarliges valg av type biometriske data, metode for innsamling, lagringstid, sikring osv. Det er derfor viktig at Datatilsynet i en innledende fase fører kontroll med behandling som skjer på grunnlag av den registrertes samtykke.

Bokstav c. er tatt inn som en sikkerhetsventil. Det er ikke ønskelig at Datatilsynet skal bli oversvømt av konsesjonssøknader. Det bør derfor være anledning for tilsynet til å forskriftsregulere at lagring av biometriske data for konkrete formål og på bestemte vilkår kan aksepteres. Man kan for eksempel se for seg en regulering av biometriske data brukt i tilknytning til adgangskontroll til datasystemer i offentlig forvaltning eller helsevesenet eller for obligatorisk kontroll av biometriske data ved bagasjeinnsjekking på fly.

Med ”sikkerhetshensyn” siktes det til både krav til datasikkerhet, sikkerhet mot terror og for eksempel sikkerhet mot ran. Det er viktig at Datatilsynet gis denne skjønnsmessige adgangen til å pålegge bruk av biometriske kjennetegn i sammenhenger hvor dette er av viktighet for personvernet.

Paragrafen inneholder ikke krav til datasikkerhet, som for eksempel krav til kryptering av data. Slike krav vil følge av personopplysningsloven og personopplysningsforskriften for øvrig. Det er åpnet for at det lages særlige forskrifter for bruk av biometriske kjennetegn.

4.2 Dagens ordlyd

§ 12 Bruk av fødselsnummer m.v.

Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.

Datatilsynet kan pålegge en behandlingsansvarlig å bruke identifikasjonsmidler som nevnt i første ledd for å sikre at personopplysningene har tilstrekkelig kvalitet.

Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer og andre entydige identifikasjonsmidler.

4.3 Forslag til ny ordlyd

§ 2 Definisjoner

I denne lov forstås med:…

Alternativ 1:
9) biometri: målbar fysisk karakteristikk av en personlig egenskap, brukt for å gjenkjenne en personidentitet eller bekrefte en påstått personidentitet.

Alternativ 2:
9) *biometriske kjennetegn: kjennetegn som utgår fra kroppen og som er unike for den registrerte og samtidig er permanente eller stabile over tid og er egnet for identifisering eller bekreftelse av en påstått identitet.*

§ 12 Bruk av fødselsnummer *og lignende entydige identifikasjonsmidler*

Fødselsnummer og *lignende* entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.

Datatilsynet kan pålegge en behandlingsansvarlig å bruke identifikasjonsmidler som nevnt i første ledd for å sikre at personopplysningene har tilstrekkelig kvalitet.

Kongen kan gi forskrift med nærmere regler om bruk av fødselsnummer og *lignende* entydige identifikasjonsmidler.

§ 12a Biometriske kjennetegn/biometri (Ny paragraf)

Biometriske kjennetegn/biometri kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering eller bekreftelse av en påstått identitet og behandlingen er tillatt etter § 11.

Behandling av biometriske kjennetegn/biometri som innebærer behandling av sensitive personopplysninger krever uten unntak konsesjon fra Datatilsynet. Øvrig behandling av biometriske kjennetegn skal meldes til Datatilsynet.

Lagring av biometriske kjennetegn/biometri hos den behandlingsansvarlige eller databehandlere kan bare skje

a. med hjemmel i lov,
b. med den registrertes samtykke og konsesjon fra Datatilsynet eller
c. når det følger av personopplysningsforskriften

Datatilsynet kan pålegge en behandlingsansvarlig å bruke biometriske kjennetegn/biometri som nevnt i første ledd der dette anses nødvendig for sikker identifisering eller bekreftelse av en påstått identitet og bruken er nødvendig av sikkerhetshensyn.

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