Biometri og personvern

Rettslig regulering av biometriske systemer

Kandidatnr: 285
Veileder: Lee A. Bygrave
Leveringsfrist: 25. april 2005

Til sammen 3097 ord

25.04.2005

Innholdsfortegnelse

1. Innledning

1.1 Bakgrunn

I oldtidens Egypt registrerte intendantene opplysninger om arbeidernes fysiske fremtoning og kjennetegn for å kunne skille dem fra hverandre når det var tid for utbetaling av lønn. Dette er sannsynligvis det første eksempelet på biometri satt i system.

Denne oppgaven tar for seg biometri og anvendelse av biometri i elektroniske systemer og rettslig regulering av disse. Temaet er svært aktuelt fordi teknologi til bruk av automatiserte systemer for anvendelse av biometri er i sterk utvikling. Samtidig har et økt behov for sikkerhetssystemer, inkludert adgangskontroll, overvåkning, automatisk gjenkjenning av kriminelle, ført til økt etterspørsel og bruk av slike systemer.

Oppgavens problemstilling er om dagens lovgivning i tilstrekkelig grad ivaretar personvernhensyn i forbindelse med bruk av biometri. Utgangspunktet for vurderingen er Lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven). Oppgaven vil også ta for seg behovet for særregulering av biometriske systemer, og i hvilken form en slik særregulering kan gjennomføres. I avslutningen av oppgaven vil det bli knyttet noen betraktninger til disse spørsmålene.

Av hensyn til oppgavens omfang er det nødvendig med noen avgrensninger. Det er omstridt om biologisk materiale ligger under lovens definisjon av personopplysninger, og debatten om dette vil ikke bli behandlet i herværende oppgave (se også kapittel 1.4). Anvendelsen av biometri er i mange former knyttet til utenlandske og internasjonale forhold, og i den forbindelse vil regelverk i andre land ikke behandles utover det som er nødvendig for forståelsen av norske regler.

1.2 Begrepsavklaring

Biometri kan kort defineres som måling av biologiske mønstre. Det gis en grundigere begrepsforklaring nedenfor. Biometriske systemer defineres som elektroniske systemer for anvendelse av biometri. De tok viktigste anvendelsesområdene for biometri er *identifikasjon* – det å fastslå hvem en person er – og *verifikasjon* – det å fastslå om en person er den han utgir seg for å være. Andre begreper vil bli forklart i teksten.

1.3 Rettskildesituasjonen

I dette kapittelet gis en oversikt over rettskildene på oppgavens rettsområde.

1.3.1 Lov og forskrift

Utgangspunktet for oppgavens drøftelse er personopplysningsloven. Med hjemmel i loven er det gitt forskrift til personopplysningsloven av 15. desember 2000 (personopplysningsforskriften).

1.3.2 Forarbeider

Forarbeidene som er relevante for fortolkningen av lovteksten er NOU 1997: 19, Odelstingsproposisjon nr. 92 (1998–1999), Innst. O. nr. 51 (1999–2000) og Besl. O. nr. 58 (1999–2000)

1.3.3 Rettspraksis og forvaltningspraksis

Jeg har ikke vært i stand til å finne relevant praksis fra norske domstoler og Personvernnemnda for de problemstillingene oppgaven reiser.

1.3.4 Utenlandske og internasjonale rettskilder

Blant utenlandske og internasjonale rettskilder er EUs direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av sådanne opplysninger (heretter *personverndirektivet*) av vesentlig betydning. Med hjemmel i personverndirektivet har Europakommisjonen nedsatt en arbeidsgruppe, ofte kalt artikkel 29-gruppen, som et uavhengig rådgivende organ som skal undersøke hvordan personvernreglene etterleves i EU og EØS-området. Artikkel 29-gruppen har utgitt et arbeidsdokument – *Working document on biometrics*, 1. august 2003 – som ser på personvernhensyn i forhold til bruk av biometri.

Blant andre internasjonale rettskilder er Europarådets konvensjon av 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger og OECDs retningslinjer av 1980 for beskyttelse og utveksling av personopplysninger over landegrenser.

2. Hva er biometri?

Biometri – av gresk *bios*, liv, og *metri*, måling – er måling av biologiske mønstre. Biologiske mønstre – heretter også kalt biometriske data eller opplysninger – kan deles i to hovedgrupper: fysiologiske og adferdsmessige særtrekk. Fysiologiske særtrekk vil typisk være fingeravtrykk, øyets regnbuehinne (iris) og netthinne (retina), ansiktsform og lignende. Adferdsmessige særtrekk kan for eksempel være ganglag eller signaturdynamikk.

Den eldste, og mest brukte, formen for biometri er måling av ansikter. Slik biometri anvendes naturlig av mennesker når vi gjenkjenner personer. Også som teknologi har biometri en lang historie. Det sies at man allerede i oldtidens Egypt registrerte opplysninger om fysiologiske kjennetegn ved personer for senere å kunne benytte opplysningene til å bekrefte at personen var den han utgav seg for å være (*The Economist* 7. sept. 2000). Moderne biometri forbindes ofte med fingeravtrykk. Fingeravtrykk ble første gang tatt i bruk til identifikasjon på siste halvdel av 1800-tallet av en politimann i Buenos Aires (Ashbourn 2000). Scotland Yard tok i bruk fingeravtrykk til registrering og identifikasjon av kriminelle i juni 1900. Siden den gang har sammenligning av fingeravtrykk blitt automatisert.

Ved hjelp av elektronikk (elektroniske systemer, biometrisystemer) kan biometri benyttes til to hovedformål: **identifikasjon** (*hvem er denne personen?*) og **verifikasjon** (*er denne personen den han hevder å være?*). Tradisjonelt har verifikasjon og identifikasjon av brukere vært basert på:

- noe brukeren vet (et passord eller en kode)
- noe brukeren har (en nøkkel, et pass, et identifikasjonskort)

Men slike metoder ikke identifiserer brukeren som sådan, fordi de er basert på egenskaper som kan glemmes, oppdages, mistes eller stjeles eller på annen måte overføres eller gå tapt, vil metoder basert på biometri identifisere mennesker som sådan.

Fordelene er mange. I motsetning til andre former for sikkerhetssystemer kan biometri ikke gå tapt, bli glemt eller overføres fra en person til en annen. Biologiske mønstre kan ikke mistes eller stjeles, som en nøkkel eller et identitetskort. Biologiske mønstre kan ikke glemmes, som et passord.

1.3.5 Identifikasjon

Identifikasjon kan i denne sammenheng defineres som å fastslå en persons identitet. Ved hjelp av biometri kan en persons identitet fastslås ved å måle personens biologiske mønstre og sammenligne disse mønstrene mot mønstre som på forhånd er lagret i en database – en én-til-flere-sammenligning. Eksempler kan være avlesning av fingeravtrykk og påfølgende sammenligning med lagrede avtrykk i en database, for å undersøke om personen er straffedømt, eller observasjon av ansikter med påfølgende sammenligning med lagrede bilder av kjente terrorister.

1.3.6 Verifikasjon

Verifikasjon går ut på å fastslå om en person er den han eller hun hevder å være – en én-til-én-sammenligning. Personens biologiske mønstre sammenlignes da med mønstre som på forhånd er lagret og som er bekreftet å tilhøre den aktuelle personen. Et eksempel kan være scanning av netthinne for å sammenligne med et allerede lagret bilde av personens netthinne, for å gi tilgang til en bank.

1.3.7 Biometriske metoder

I biometriske systemer er følgende biometriske metoder mest anvendt:

- Sammenligning av fingeravtrykk: et unikt mønster på innsiden av fingertuppene avleses og sammenlignes med registrerte fingeravtrykk.
- Sammenligning av håndavtrykk: tilsvarende fingeravtrykk, men med hele håndflaten (krever større systemer).

- Sammenligning av håndgeometri: det tas et tredimensjonalt bilde av en hånd, og dette sammenlignes med et registrert bilde der egenskaper som fingerlengde og fingertykkelse sammenlignes.
- Sammenligning av signaturdynamikk: det gjøres en underskrift (signatur) mot en sensorplate, som registrerer bevegelsen som brukes til å skrive underskriften, inkludert trykk, retning, hastighet, akselerasjon samt strøkenes antall, lengde og varighet, og sammenligner disse med et lagret mønster.
- Sammenligning av stemme: det leses inn et forhåndsbestemt ord eller setning og dette sammenlignes med et lagret stemmemønster.
- Sammenligning av netthinne (retina): blodkar i netthinnen sammenlignes med et lagret bilde.
- Sammenligning av regnbuehinne (iris): den fargede ringen rundt pupillen sammenlignes med et lagret bilde.
- Sammenligning av kroppslukt: en persons unike kroppslukt sammenlignes med et lagret kjemikaliemønster.
- Sammenligning av ganglag: en persons ganglang sammenlignes med et opptak av ganglag.
- Sammenligning av ansikt: et ansikt sammenlignes enten ved å måle kjennetegn i et ansikt, f.eks. nesens posisjon, eller å sammenligne et ansikt med bilder basert på egenvektorer.

DNA regnes per idag ikke som automatisk nok til å kunne betraktes som en biometrisk teknologi (Jerman-Blažič 2004).

Alle biologiske mønstre kan benyttes til *verifikasjon*, men bare de mønstre som er helt unike kan benyttes for *identifikasjon*.

3. Rettslig regulering av biometriske systemer

1.4 Er biologiske mønstre personopplysninger?

Personopplysningsloven definerer personopplysninger som ”opplysninger og vurderinger som kan knyttes til en enkeltperson” (§ 2 nr. 1). Spørsmålet blir så om biometriske opplysninger kommer inn under denne definisjonen. For å undersøke om biologiske mønstre faller inn under denne definisjonen, er det anvendelig å benytte begrepene ”personobjekt”, ”persondata” og ”personinformasjon” (Schartum og Bygrave 2004). Biometriske data er som tidligere nevnt fysiologiske karaktertrekk eller adferdsmønstre. Hvorvidt biologisk materiale, herunder DNA, kan regnes som personopplysninger, er omstridt. Personvernnemnda har i klagesak 2002/08 uttalt at det må skilles mellom personopplysning og biologisk materiale. Det var imidlertid dissens i vedtaket, og det er også uenighet i juridisk teori. Av plasshensyn vil biologisk materiale holdes utenfor definisjonen av biometriske data i det følgende.

Biologiske mønstre kan ved bruk av biometriske systemer registreres maskinelt. En persons ganglag kan observeres av et kamera, et hårstrå kan analyseres og en stemme kan registreres av en sensor. Disse mønstrene kan sammenfattes som *personobjekter*. Når disse personobjektene manifesteres ved at det fysisk dannes et bilde, et resultat av en DNA-prøve, et opptak av en stemme eller lignende, får man *persondata*, det vil si data som kan knyttes til en person. Når persondata tolkes, for eksempel ved at et bilde tolkes til å være et bilde av et menneske, får man *personinformasjon*. Når personinformasjon, f.eks. bildet av mennesket, kan knyttes til en enkeltperson får man *personopplysning*. Konklusjonen blir således at biologiske mønstre, som kan knyttes til enkeltpersoner, kan regnes som personopplysninger.

1.5 Behøves særregulering av biometriske systemer?

Som allerede fastslått reguleres anvendelse av biometriske systemer av personopplysningsloven. Personopplysningsloven setter opp noen grunnkrav til behandling av personopplysninger i § 11, men loven er svært generell, og det kan hevdes at behandling av biometriske personopplysninger skiller seg fra behandling av andre personopplysninger i så stor grad at det bør særreguleres. Årsakene til dette kan være flere.

Måling av biologiske mønstre kan være mer personlig påtrengende enn andre former for verifikasjon og identifikasjon. Til forskjell fra det å skru om en nøkkel eller taste inn et nummer, er biometri knyttet til en persons kropp og fysiske egenskaper. Fordelene er mange – biometriske data kan ikke glemmes, mistes, stjeles eller på annen måte gå tapt slik en nøkkel eller et passord kan. På den annen side er bruk av personlige egenskaper mer påtrengende i den personlige sfære fordi det er brukeren som sådan som identifiseres, og ikke en ting som en nøkkel eller et smartkort. Brukeren taper på denne måten en anonymitet, da alle handlinger kan spores til personen fremfor til nøkkelen. Tilsvarende taper man muligheten til å opprette flere identiteter – for eksempel flere brukernavn og passord – fordi "nøkkelen" alltid vil være den samme, nemlig brukeren selv.

Biometriske data kan i tillegg inneholde sensitive, personlige opplysninger. En persons DNA kan fortelle om personen er disponert for noen sykdommer. Kroppslukt kan røpe noe om hva slags aktiviteter personen har bedrevet i en tid forut, blant annet om seksuell aktivitet. Observasjon av en persons pupiller i forbindelse med scanning av øyne kan fortelle om bruk av narkotika.

Etter terrorangrepet mot USA 11. september 2001 og det påfølgende bevisstheten og kampen mot terrorisme har bruken av biometri for identifikasjon og verifikasjon vært økende (*The Economist* 4. des. 2003). Flere land har innført krav om pass som inneholder lagret biometrisk data, og det benyttes fingeravtrykk til identifikasjon og verifikasjon ved ankomst på flyplasser i USA. På flyplassene og mange andre offentlige steder er det blitt vanlig å installere kameraer tilknyttet programvare som kan sammenligne ansikter og identifisere kriminelle basert på databaser med bilder (Jerman-Blažič et al. 2004). I Storbritannia har regjeringen foreslått å innføre nasjonale

identitetskort med biometriske data lagret på kortet, mens i Norge jobber myndighetene med å innarbeide biometri i pass.

I den private sektor er salg av datamaskintastatur og -skjermer med mulighet for avlesing av fingeravtrykk nå i ferd med å komme i gang i stort omfang. Noen spår at avlesing av fingeravtrykk vil kunne brukes som erstatning for passord ved for eksempel innlogging i nettbank om ikke lang tid (*The Economist* 7. sept. 2000).

På grunn av rask teknologisk utvikling, er også mulighetene for anvendelse av biometri sterkt økende. Et av de tradisjonelle problemene med biometriske systemer har vært nøyaktigheten. Tidligere var biometriske systemer mindre pålitelige, men etterhvert som teknologien utvikles, vil påliteligheten øke, og dermed også anvendelsen av slike systemer. Når teknologien blir bedre og anvendelsen av biometri brer om seg, kan man heller ikke se bort fra at prisen på biometrisystemer vil falle, og omfanget vil dermed også øke.

1.6 Krever noen former for biometriske systemer mer oppmerksomhet?

Det kan stilles spørsmål om noen former for biometriske systemer krever mer oppmerksomhet fra lovgiver enn andre. Noen metoder kan føles som mer integritetskrenkende enn andre.

Avlesing og sammenligning av fingeravtrykk har vært benyttet i over 100 år, lenge før vedtakelsen av personvernlovgivningen. Bruk av fingeravtrykk i rettsvesenet er imidlertid svært begrenset, og det kan være et argument for å gi en egen bestemmelse om fingeravtrykk i en lov om biometri. Avlesning av fingeravtrykk og håndflater kan også være integritetskrenkende for de som har motforestillinger mot å berøre en plate som mange har tatt på. Avlesning av ansikt kan ansees som inntrengende for personer som normalt dekker til ansiktet, for eksempel av religiøse grunner. Som tidligere nevnt kan sammenligning av kroppslukt innebære at intime opplysninger om helse og adferd kan komme på avveie. Mye taler derfor for at biometriske metoder som fingeravtrykkavlesning, avlesning av ansikt og øyne, og registrering av lukt, kan være såvidt integritetskrenkende at det behøves nærmere regulering enn andre systemer.

1.7 Former for regulering

Regulering av biometri kan ta flere former. Man kan tenke seg at det gis en ny lov om biometri. Det kan også gis en egen forskrift om biometri med hjemmel i personopplysningsloven § 3 fjerde ledd. Regulering kan også skje i form av selvregulering, gjennom adferdskodeks, retningslinjer, standardisering og lignende.

1.7.1 Adferdskodeks

Jfr. betraktning nr. 61 i innledningen til personverndirektivet skal myndighetene oppfordre berørte yrkesmiljøer til å utarbeide regler for hvordan direktivet skal anvendes. Direktivet sier videre i art. 27 at myndighetene skal oppmuntre til utarbeidelse av adferdsregler som skal bidra til en riktig anvendelse av nasjonale bestemmelser.
Datatilsynet har utarbeidet retningslinjer om informasjonssikkerhet ved behandling av personopplysninger. Man kan tenke seg at det utarbeides tilsvarende retningslinjer – en adferdskodeks – for bruk av biometriske systemer. Biometrics Institute i Australia har allerede utarbeidet en adferdskodeks, som er oversendt det australske datatilsynet for offentlig godkjenning. Med utgangspunkt i denne kan en tilsvarende kodeks for Norge formuleres:

1. Beskyttelse
    a. Forsåvidt mulig skal en organisasjon sørge for at biometrisk informasjon krypteres rett etter innsamling, at den originale biometriske informasjonen ødelegges etter kryptering og at biometrisk informasjon kun lagres i kryptert form.
    b. Biometrisk informasjon skal oppbevares separat fra andre personopplysninger som organisasjonen besitter. Der hvor det er praktisk mulig skal personopplysninger avidentifiseres og oppbevares på slik måte at de ikke kan kobles til identifiserende informasjon.

c. Med mindre det kreves etter gjeldende rett, skal biometriske opplysninger oppbevares kun så lenge som det er nødvendig for at det biometriske systemet de ble samlet for, fungerer slik det skal.
d. Etter at personopplysninger ikke lenger behøves, skal de ødelegges eller på annen måte fjernes på sikker måte.
e. Overføring av biometrisk data skal foregå på sikker og forskriftsmessig måte.
f. Tilgang til biometriske opplysninger skal begrenses til de innen organisasjonen som har et spesielt behov for å ha tilgang for å kunne utføre deres arbeidsfunksjoner. Organisasjonene skal holde register over hvilke personer som har adgang til biometrisk data.

2. Kontroll
    a. Deltagelse i biometriske systemer skal være frivillig med mindre det kreves i lov.
    b. Personer som deltar i et biometrisystem skal informeres om enhver endring i systemets utstrekning og formål. Sekundær analyse av biometriske opplysninger innsamlet med formål for verifikasjon eller identifikasjon er ikke tillatt uten uttrykkelig samtykke.
    c. Personer som deltar i et biometrisystem skal, hvor det er mulig, og ved anmodning, få anledning til å få sine biometriske opplysninger fjernet fra systemet.
3. Ansvarlighet
    a. En organisasjon skal oppgi formålene for opprettelse av et biometrisystem.
    b. Revisjon av biometrisystemer av en tredjepart skal implementeres.
    c. En organisasjon skal gjennomføre personvernanalyser som del av planleggingen av opprettelse av biometrisystemer.
    d. En organisasjon skal ikke bevisst villede klienter eller brukere om virkninger og {nature of} biometriske produkter eller systemer som de er ansvarlig for.

En slik adferdskodeks kan gjennomføres ved å gi en fagorganisasjon ansvaret for implementeringen eller ved å gi Datatilsynet ansvar for å utarbeide og følge opp slike retningslinjer.

1.7.2 Standardisering

Gjennom standardisering av biometriske systemer og behandling av biometriske opplysninger kan personvernet styrkes. En kan for eksempel tenke seg standardisering av sensorer for avlesning av fingeravtrykk med innebygget personvernteknologi. En slik standardisering vil dessuten kunne føre til økt nøyaktighet og pålitelighet ved bruk av standardsystemer for biometri.

4. Avsluttende betraktninger

I innledningen av oppgaven ble spørsmålet stilt om dagens lovgivning i tilstrekkelig grad ivaretar personvernhensyn i forbindelse med biometri. Ettersom biometriteknologi er i meget rask utvikling og omfanget av anvendelsen av biometri er økende, er det nærliggende å svare nei på spørsmålet. Personopplysningsloven er imidlertid så omfattende og generalisert at den gjennom rettspraksis og forvaltningspraksis vil kunne fremstå som klart anvendbar på de fleste metoder for biometri. EU-direktivet gir myndighetene i hver medlemsstat i oppgave å oppfordre til utarbeidelse av adferdsregler som skal bidra til en riktig anvendelse av nasjonale bestemmelser. Slike adferdsregler, eller retningslinjer, kan være en god idé, og spesielt frem til det viser seg om gjeldende regler ikke holder mål. Så langt er biometriske systemer ikke utbredt nok i Norge til at man kan trekke noen konklusjon om dagens regelverk ikke er nok.

(Jeg beklager at kapittelnummereringen ikke virker; noe må ha gått galt med bruk av malen, og deler av teksten har gått tapt på grunn av dette.)

5. Litteraturliste

Ashbourn, Julian.
Biometrics: Advanced Identity Verification. New York, 2000.

Hopkins, Richard.
An Introduction to Biometrics and Large Scale Civilian Indentification.
International Review of Law Computers & Technology, vol. 13, nr. 3, 1999.

Kofod Olsen, Birgitte.
Identifikationsteknologi og individbeskyttelse. København, 1998.

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

Security and Privacy in Advanced Networking Technologies.
Redigert av Borka Jerman-Blažič, Wolfgang Schneider og Tomaž Klobučar. 2004.

The Economist:
Prepare to be scanned. 4. desember 2003.
The measure of man. 7. september 2000.
Too flaky to trust. 4. desember 2003.
Watching you. 20. september 2001.
For your eyes only. 12. februar 1998.
Biometric fact and fiction. 24. oktober 2002.

6.

A