Personvernhensyn og biometri i arbeidslivet

Bruk av biometriske adgangskontrollsystemer

Kandidatnummer: 609

Leveringsfrist: 25.11.08

Til sammen 16 001 ord

23.11.2008

Innholdsfortegnelse

1 Innledning

1.1 Tema

Biometri og forholdet til personvern er aktuelle tema som har blitt tatt opp i media og juridisk litteratur mv. i de siste par år. Fokuset på de potensielle farene ved denne registreringen av individers handlinger og bevegelser øker. Det er nettopp kommet en ny utredning[1] vedrørende behovet for nærmere regulering av bruk av biometri. Utviklingen virker tilsynelatende å gå i retning av utstrakt bruk av biometrisk kontroll fordi man søker gode, nøyaktige og enkle måter å identifisere eller autentisere folk på. Jeg ønsker å skrive om noe aktuelt, og da er dette et godt tema som vil bli mer og mer aktuelt ettersom bruksområdene for biometri øker. Innføringen av pass som inneholder biometriske data har resultert i en offentlig debatt rundt nettopp personvernhensyn. Denne fremstillingen har som hovedfokus de biometriske adgangskontrollsystemene som er tilgjengelige for bruk i bedrifter, og konsekvensene av utstrakt bruk, supplert av en mer generell vurdering av forholdet mellom personvernhensyn og den økende aksept for biometriske løsninger.

I USA brukes slike kontrollsystemer i svært stor grad, og norske bedrifter følger etter. Derimot har vi strengere regelverk i Norge, og jeg vil i denne oppgaven søke å belyse de viktigste rettsspørsmålene som oppstår i kraft av dette regelverket.

1.2 Problemstilling og oversikt over oppgavens struktur

Hovedproblemstillingen for denne oppgaven er:
Hva er de personvernmessige konsekvensene av en generell aksept av biometriske adgangskontrollsystemer i arbeidslivet?

[1] Schartum & Bygrave (2008).

Videre er de viktigste underproblemstillingene i fremstillingen:
Faller biometri inn under personopplysningsloven §12?

Hva er forskjellen på, og sammenhengen mellom, identifisering og autentisering og hva betyr det for lovanvendelsen?

Hvilke konsekvenser fører en eskalering av bruken av biometri til? Herunder faren for misbruk av elektroniske spor.

Først (i avsnitt 2), gir jeg en innledende fremstilling av biometri og bruken av slike kjennetegn. Så (i avsnitt 3) skriver jeg noe innledende om personvern på arbeidsplassen. Deretter (avsnitt 4) følger en redegjørelse for biometri brukt som kontrolltiltak i arbeidslivet, fulgt av avsluttende betraktninger (i avsnitt 5).

Begrepene ”personvern”, ”personvernhensyn” mv. vil bli brukt i relativt stor grad i denne oppgaven. Det kan derfor være hensiktsmessig å beskrive kort hva begrepet ”personvern” omfatter. Begrepet brukes i denne fremstillingen slik det er definert i NOU 1997: 19 på side 21 (punkt 3.3): ”På et helt generelt plan kan personvernet sies å gjelde krav til behandling av personopplysninger når kravene er begrunnet ut ifra visse ideelle (ikke-økonomiske) interesser som en tillegger fysiske (og eventuelt juridiske) personer”.

Svært sentralt i oppgaven er også forskjellen på identifisering og autentisering. Jeg behandler begrepene ytterligere i avsnitt 2.3, men det er viktig for forståelsen av den første delen av drøftelsen at jeg innledende skissere skillelinjene.

Begrepet identifisering brukes i situasjoner hvor man ønsker å skille ut én fra en gruppe av mange. Begrepet kan imidlertid også betegne det å etablere en entydig binding mellom et individ og et identifikasjonsmerke/-middel, for eksempel tildele fødselsnummer til en person (navnefunksjonen).[2] Denne betydningen vil derimot ikke bli særlig fremtredende i den

[2] Schartum & Bygrave (2008) s. 8.

videre fremstillingen. Én-til-mange forhold er den sentrale betydningen av begrepet identifisering. Autentisering brukes i én til én situasjoner hvor den som er gjenstand for kontrollen aktivt har fremsatt en påstand om sin egen identitet. Autentisering innebærer altså ikke at man sjekker hvem den aktuelle personen er, men derimot at han eller hun er berettiget til å få tilgang til det kontrollerte miljø (enten det er fysisk tilgang til en bygning eller aksess til filer på en datamaskin).

Tematikken rundt "elektroniske spor" har sitt utspring i teknologisk utvikling. Overgangen til "IT alderen" hvor dagliglivet i stor utstrekning innebærer bruk av teknologiske nyvinninger som potensielt kan medføre en fare for personvernet. Et spor kan være et objekt (for eksempel et dokument) eller dokumentasjon av en hendelse (eksempelvis signatur på at en pakke har blitt mottatt).[3] De elektroniske spor som er særlig relevante for denne fremstillingen er de som kan knyttes til enkeltpersoner. Spor som forteller om en persons handlinger, oppholdssted og lignende. Personopplysningsloven § 2 nr. 1 definerer personopplysninger som "opplysninger og vurderinger som kan knyttes til en enkeltperson." De elektroniske sporene som kan knyttes til enkeltindivid reguleres dermed av personopplysningsloven. Jeg kommer nærmere inn på de rettslige aspekter av elektroniske spor i et senere avsnitt.

1.3 Aktuelle rettskilder og spesielle metodiske problemstillinger

Personvern er et omfattende rettsområde og det er vanskelig å gi en kortfattet og klar definisjon av begrepet. Kort kan man si at det dreier seg om et knippe rettigheter knyttet til vernet av ens integritet, vernet av retten til å være privat og vernet av opplysninger om ens person. I teorien har man ofte sett personvernet fra tre forskjellige perspektiv:

- integritetsperspektivet,
- beslutningsperspektivet og
- maktperspektivet.

[3] Norsk Regnesentral (2005) s. 13.

De utgjør forskjellige tilnærminger til personvernet, men overlapper og utfyller hverandre, og forsøker å klargjøre omfanget av rettsområdet.

Det vil føre for langt i forhold til denne oppgavens rammer å gå i detalj rundt perspektivene. Mens personverninteressene i en viss grad er juridisk-faglige, er personvernperspektivene utpreget verdiorienterte og politiske.[4] Kort sagt tar integritetsperspektivet utgangspunkt i ideen om at den enkelte "eier" opplysningene om seg selv, beslutningsperspektivet ser hen til at personopplysninger ofte danner grunnlag for beslutninger som får betydning for den registrerte, mens maktperspektivet legger til grunn at kunnskap er makt og at det at man vet noe om en person kan påvirke maktbalansen.[5] Alle perspektivene vil være relevante og kunne legges til grunn i et arbeidsforhold. For mer om perspektivene, se NOU 1997: 19, s 21.

Som tittelen indikerer er fokus for oppgaven biometriske kontrolltiltak på arbeidsplassen, derfor må utgangspunktet for fastsettelse av hjemmel tas i Arbeidsmiljøloven,17. juni 2005 nr. 62. I denne loven fikk man et nytt kapittel, nemlig kapittel 9 om kontrolltiltak i virksomheten. Dette vil også omfatte kontrolltiltak hvor arbeidsgiver behandler personopplysninger, og reglene vil derfor være sentrale i denne fremstillingen. Hjemmelen for kontrolltiltak overfor arbeidstaker finnes i § 9-1 første ledd. Drøftelsen av denne problemstillingen foretas i punkt 3 flg.

Personopplysningsloven, 14. april 2000 nr. 31, er den sentrale lov på området. Ovennevnte lov avløste Personregisterloven av 9. juni 1978 nr. 48, og har som et overordnet formål "å beskytte enkeltindivider mot at deres personvern blir krenket som ledd i behandlingen av personopplysninger", jf. formålsbestemmelsen i § 1 (1). Loven ble vedtatt som ledd i implementeringen av EFs personverndirektiv. En kort presentasjon følger ne-

---

[4] Schartum & Bygrave - Personvern i informasjonssamfunnet. s. 23.

[5] Rønholt, Hege Haneborg *Personvern i arbeidsforhold - arbeidsgivers innsynsrett i e-post m.m.* (2006).

denfor. Personopplysningsloven gjelder så lenge emnet ikke er regulert av særlovgivning, jf. *lex specialis-prinsippet*, men i tillegg inneholder loven en såkalt "konfliktbestemmelse" i § 5 som direkte uttaler at særlovgivningen går foran ved konflikt.

I pol § 1 (2) slås det fast at loven skal etablere regler som bidrar til "at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger". Bestemmelsen har to hovedfunksjoner. Den skal for det første gi uttrykk for lovens overordnede målsetning. For det annet vil bestemmelsen i seg selv være en sentral tolkningsfaktor ved anvendelsen av lovens øvrige regler, jf. Ot.prp. nr. 92 (1998-99) side 101. Pol § 1 (2) viser til "grunnleggende personvernhensyn", hvilket innebærer at fastlagte oppfatninger om personvern vil være sentrale i fortolkningen av lovens skjønnsmessige kriterier. Alminnelige arbeidsrettsrettslige prinsipper som beskytter arbeidstakernes personverninteresser vil derfor medføre begrensninger i adgangen til å behandle personopplysninger gjennom denne bestemmelsen, jf. NOU 1997: 19 side 130.

Direktiv 95/46/EF "Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger" (heretter omtalt som Personverndirektivet) har som oppgave å samkjøre lovverkene i medlemslandene i forhold til deres regler vedrørende personopplysninger. Målet er at de forskjellige lands lovverk ikke skal være til hinder for den frie flyt og økonomiske samhandling. Et ytterligere formål er å bidra til å gi den enkelte et sterkere vern. Direktivet er derimot ikke til hinder for at den enkelte stat kan vedta strengere regler, med det krav at disse ikke må medføre begrensninger i den frie flyt. I norsk lov er direktivet søkt gjennomført gjennom Personopplysningsloven. Det kan derfor være hensiktsmessig å se hen til direktivet ved tolkingen av denne loven. Da Personopplysningsloven er antatt å være i overensstemmelse med Personverndirektivet, kommer jeg likevel i liten grad til å gå inn på de enkelte bestemmelsene i direktivet.

Både Den europeiske menneskerettskonvensjonen 4.11.1950 (EMK) artikkel 8 og Den internasjonale konvensjon om sivile og politiske rettigheter 16.12.1966 (SP) artikkel 17 verner om privatlivets fred mv. Det vil føre for langt i forhold til rammene for denne fremstillingen å gå inngående inn på disse reglene. Men jeg vil kort bemerke at det er klart at man også på arbeidsplassen har en viss rett til privatliv, og at denne vernes av EMK artikkel 8 og SP artikkel 17.

Begge de ovennevnte bestemmelsene gjelder som norsk lov, se lov 21. mai nr. 30 1999, Menneskerettsloven, § 2. Norge har også ratifisert Europarådskonvensjon 28.1.1981 (ETS nr. 108) om persondatabeskyttelse, og personopplysningsloven antas å være i overensstemmelse med denne, jf. Ot.prp. nr. 92 (1998–1999), s. 11.

Termen ”sikkerhet” byr på endel utfordringer. Det ligger ikke innenfor rammene til denne oppgaven å definere og drøfte datasikkerhetsspørsmål generelt. Jeg velger derfor å konsentrere meg om skillet mellom identifisering og autentisering og de personvernmessige problemene som oppstår i forbindelse med det. Uttrykk som eksempelvis ”sikker identifikasjon” er ofte brukt i forbindelse med behandling av spørsmål om biometriske adgangskontrollsystemer. Det opptrer i de fleste av avgjørelsene fra Personvernnemnda, men jeg velger her å ikke bruke uttrykket og dermed ei heller gå inn på drøftelsen av uttrykket sikkerhet og dets multiple betydninger og bruksområder.

2 Biometri og biometriske kjennetegn – innledende oversikt

2.1 Biometri

Ordet biometri stammer fra de greske ordene *bios* som betyr liv, og *metron* som betyr mål. Biometri betyr med andre ord ”mål av liv”. I den norske versjonen av Wikipedia er biometri definert som " ... måling av biologiske mønstre. Biologiske mønstre kan være fysiologiske karaktertrekk (for eksempel fingeravtrykk) eller adferdsmønstre (for eksempel ganglag)." I denne definisjonen har en med andre ord valgt en generell beskrivelse, kombinert med en forklaring som peker i retning av identifisering av mennesker og verifisering av

menneskers identiteter.[6] Begrepet biometri har vært brukt lenge innen biologien og i biologisk og plantefysiologisk leksikon[7] er biometri således definert som "Vitenskapen som omhandler bruk av statistiske og matematiske metoder anvendt på biologiske systemer. Statistisk undersøkelse og studium av likheter og forskjeller mellom grupper av arter."[8]

Biometri kan altså 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"[9] eller som *målbar* fysisk karakteristikk av en personlig egenskap, brukt for å gjenkjenne en personidentitet eller bekrefte en påstått personidentitet.[10] Metoden er særlig anvendelig til identifisering, da den er *universell*, det vil si anvendelig på alle fysiske personer, er *entydig* fordi den er særegen for hver enkelt person og er *varig* fordi egenskapene ikke endrer seg over tid.[11] Den teknologiske utviklingen har åpenbart skapt behov for rettslig regulering av adgangen til å foreta denne typen inngrep overfor personer, generelt, og arbeidstakerne, spesielt[12].

Som nevnt over er det helt klart et matematisk aspekt ved biometri. Når jeg tar i betraktning den tiden vi lever i, med det nivået datateknologien har nådd og fortsetter å utvikle seg fra, er det ikke ulogisk at biometri anses av mange som et nødvendig neste steg i utviklingen av

---

[6] Se http://en.wikipedia.org/wiki/Biometrics. Oppslag gjort 21.10.08.

[7] Se http://www.bio.uio.no/plfys/haa/leks/index.htm. Oppslag gjort 25.09.08.

[8] Schartum & Bygrave (2008) s. 13.

[9] Kunnskapsforlagets fremmedord og synonymer blå ordbok 5. utgave, Kunnskapsforlaget 2004.

[10] Datatilsynets revisjonsnotat pol §12, s. 2.

[11] Charlotte Bagger Tranberg, "Persondata og biometri i Skandinavien" publisert i Lov&Data nr. 90, juni 2007.

[12] Ettersom denne oppgaven dreier seg om adgangskontrollsystemer i arbeidslivet er følgene for arbeidstakerne ved biometrisk kontroll spesielt i fokus.

kontrollsystemer. For flere år siden ble det laget film om en fantasiverden hvor ens digitale selv levde i en digital verden. Vår virkelighet er så absolutt ikke i nærheten av "The Matrix"[13], men fokuset skifter mer og mer over på de digitaliserbare kjennetegnene ved hver enkelt, i kontrast til de naturlige kjennetegnene. M. H. Barrera og J. M. Okai beskrev endringene i handlingers sporbarhet i datateknologiverden i sin artikkel (Digital Correspondence: Recreating Privacy Paradigms, International Journal of Communications Law and Policy, nr. 3 1999.) slik:

"Å eksistere i cyberspace[14] er å bli registrert. Digitale handlinger ... er ikke noe annet enn en samling spor og registre. Hver eneste elektroniske handling i cyberspace medfører at det skapes sportråder. ... Disse digitale "fotavtrykkene" kan, av natur, rekonstrueres, gjengis og lagres på ubestemt tid. Der et stort antall handlinger i det tradisjonelle rom er umulige å spore, er handlingene i cyberspace spor i seg selv."[15]

Jeg vil i det følgende forsøke å vise skillet mellom ulike typer biometriske kjennetegn, og hvilke fordeler og ulemper det er ved de enkelte.

2.2 Biometriske kjennetegn

2.2.1 Oversikt

Biometriske kjennetegn kan beskrives som kjennetegn som utgår fra kroppen, er unike for den registrerte og samtidig er permanente eller stabile over tid. Ved å måle disse kjennetegnene kan de benyttes til å gjenkjenne en person (identifisering), eller bekrefte en persons påståtte identitet (autentisering). Skillet mellom identifisering og autentisering blir behandlet i avsnitt 2.3 nedenfor.

---

[13] Se http://no.wikipedia.org/wiki/The_Matrix Oppslag gjort 21.10.08

[14] Se http://en.wikipedia.org/wiki/Cyberspace Oppslag gjort 23.10.08.

[15] Egen, til dels fri, oversettelse fra engelsk sitat. For opprinnelig sitat se Norsk Regnesentral (2005) s. 13.

Biometri er ikke et uproblematisk begrep å definere. Jeg kommer tilbake til den rettslige reguleringen av begrepet et senere avsnitt. I dette avsnittet presenterer jeg den språklige og begrepsmessige definisjonen av biometri.

De mest kjente formene for biometriske kjennetegn er fingeravtrykk, håndavtrykk og ansiktsform, samt de to øyenteknologiene netthinne- og irisavlesning. I utgangspunktet kan alle målbare og unike egenskaper ved mennesker benyttes. Dette kan for eksempel være i form av stemmegjenkjenning, DNA, eller hvilken tastefrekvens vi benytter når vi skriver på et tastatur. Distinktive adferdsmønstre eller ganglag kan også være basis for biometrisk kontroll.

Biometri beskrives ofte som ”noe vi er” når det sammenlignes med de tradisjonelle metodene for å gjenkjenne eller bekrefte en persons identitet. De tradisjonelle metodene omfatter ”noe du vet”, for eksempel et passord, og ”noe du har”, for eksempel en kodebrikke. Biometri har sin egenart, det er uløselig knyttet til kroppen vår, på godt og vondt.”[16] Spørsmålet blir da hvorvidt det gode ved biometri er viktigere enn de negative konsekvensene som kan medføres ved utstrakt bruk.

2.2.2 Ulike typer biometriske kjennetegn

2.2.2.1 Innledning

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.[17] Moderne biometri forbindes ofte med finger-

[16] Datatilsynet, artikkel av Helge Veum og Astrid Flesland, 2007.

[17] The Economist 7. Sept 2000.

avtrykk. Fingeravtrykk ble første gang tatt i bruk til identifikasjon på siste halvdel av 1800-tallet av en politimann i Buenos Aires.[18] Scotland Yard tok i bruk fingeravtrykk til registrering og identifikasjon av kriminelle i juni 1900. Siden den gang har sammenligning av fingeravtrykk blitt automatisert.[19]

En rekke biometriske kjennetegn kan i dag brukes til identifisering eller bekreftelse av identitet, eller begge deler. Disse behandles i de følgende avsnitt.

Ulike typer biometriske kjennetegn har også gjerne forskjellig bruksområde hva gjelder kontroll. De systemer som fungerer for kontroll av idrettsutøvere vil nok oppleves for inngripende dersom brukt mot ansatte i en it-bedrift.

2.2.2.2 Fingeravtrykk og håndflateavtrykk

Et fingeravtrykk er et avtrykk av furer som finnes på menneskefingre. Disse mønstrene skal være unike for hver enkelt person, og også for hver enkelt finger. Mønstrene er del av huden og dermed uløselig knyttet til fingeren det kommer fra.

Denne gruppen biometriske kjennetegn er den mest brukte til identifisering av individer, og da særlig fingeravtrykk. Politiet og rettsvesenet har lenge brukt fingeravtrykk i etterforskning og avgjørelser, og aksepten for slik bruk er relativt høy. Fingeravtrykk er et viktig hjelpemiddel i politiets etterforskning, for å fastslå identitet og knytte gjerningspersoner til et åsted.[20] Ny teknologi bidrar stadig til at systemer for registrering og bruk av fingeravtrykk til ulike formål blir lettere tilgjengelige og mer nøyaktige i gjennomføringen av kontrollen. Det er et tveegget sverd; på den ene siden er det svært bra at unøyaktigheten i systemene reduseres slik at risikoen for feil minimeres. På den andre siden vil økt tilgjengelig-

[18] Ashbourn (2000).

[19] Kongsgaard, Erik Magnus *Biometri og personvern* (2005).

[20] Veum & Flesland (2007).

het medføre større press fra bedriftenes side til å få adgang til å bruke systemene, som igjen da vil medføre større press på personvernet.

I oppgavens avsnitt 4 flg vil jeg hovedsakelig benytte fingeravtrykk som eksempel på biometriske kjennetegn. Bakgrunnen for fokuset er at sakene som er avgjort i Personvernnemnda hovedsakelig gjelder bruk av fingeravtrykklesere av ulik utforming og med ulike formål.

2.2.2.3 Ansiktsgjenkjenning og irisskanning

Som nevnt over er ansiktsgjenkjenning å regne som en av de eldste formene for biometrisk registrering. Men i tillegg er det å kjenne igjen et ansikt en egenskap vi alle har i kraft av å kunne se, huske og resonnere. Bruk av bilde på identifikasjonsbevis (eksempelvis førerkort eller pass) er en form for ansiktsgjenkjenningskontroll. Et bilde på et pass er et analogt kjennetegn, men det er uansett biometrisk. I denne fremstillingen er det de digitale systemene som er i fokus, fordi de bringer med seg vesentlig større mulighet for sporing av biometriske mønstre, jf. avsnitt om elektroniske spor nedenfor.

Skanning av iris er det biometriske kjennetegnet som er mest på linje med fingeravtrykk i forhold til tilgjengelige systemer i markedet i dag. Jeg velger å ikke gå inn på de konkrete eksemplene på systemer som bruker irisskanning til biometrisk adgangskontroll da det ikke er slike saker som hovedsakelig har blitt behandlet av Personvernnemnda.

2.2.2.4 Kroppssekreter og liknende biologiske spor

Kroppssekreter og liknende biologiske spor gir svært detaljerte opplysninger om en persons biometriske data. Analyse av kroppssekreter (spytt, blod, urin etc.), hud og hår har potensiale til å gi langt flere opplysninger om en persons genetiske sammensetning enn det vil være behov for i de aller fleste brukssituasjoner. Denne typen kontroll er svært sjeldent brukt, da den av de fleste vil bli betraktet som altfor inngripende. Som oftest vil eksempel-

vis et fingeravtrykk være tilstrekkelig og da er det lite formålstjenlig å søke slik overskuddsinformasjon.

Denne typen biometrisk kontroll er å anse som svært vanlig innen konkurranseidrett, eksempelvis sykling, langrenn og friidrett. Da det heller ikke er behandlet denne typen saker for Personvernnemnda velger jeg å ikke gå videre inn på anvendelse av slike biometriske mønstre.

2.2.2.5 Adferdsbiometri etc.

Eksempler på biometriske mønstre som faller i kategorien adferdsbiometri er ganglag, skrivemåte på tastatur, stemmeleie og signatur. Digital signatur har vært brukt av banker en god stund, men påliteligheten i forhold til andre former for biometrisk kontroll er svak. En signatur er relativt enkel å etterligne, og feilmarginen på systemet blir for stor til at det kan kategoriseres på linje med irisskanning eller fingeravtrykksleser. Men systemene for registrering av adferdsbiometri er i stor utvikling, og har tildels blitt benyttet av politi og rettsvesen (for identifisering av et par av NOKAS[21]-ranerne), men inntil videre har i alle fall de fysiologiske metodene minst feilmargin.

2.3 Behovet for entydig identifisering eller autentisering – hvorfor biometri

2.3.1 Innledning

Bruken av biometri baseres i voksende grad på effektivitets- og rasjonaliseringshensyn.

Det er grunn til å anta at det ikke bare er identifiserings- og autentiseringsbehov som vil drive den videre teknologiske og samfunnsmessige utviklingen på området fremover. Disse begrunnelsene kan riktignok være "døråpneren"[22] for slik teknologi, men behovet for

[21] Se LG-2006-64391-1 samt Rt-2007-1056. (NOKAS-dommen)

[22] Schartum & Bygrave (2008) s. 22.

praktiske og kostnadseffektive løsninger kan være vel så utslagsgivende på sikt. Det er vanskelig å generalisere om hvorvidt slike praktiske begrunnelser kan anses å være ønsket eller uønsket, og det kan heller ikke sies at løsningene generelt sett er positive eller negative for personvernet.

Det er to spørsmål man må svare på ved avveining om hvorvidt biometrisk kontroll er riktig for arbeidsplassen.

1) Hvorfor bruke biometri i stedet for tradisjonelle kontrollmidler? og
2) Hvor nøyaktige er de biometriske løsningene?

2.3.2 Tradisjonell bekreftelse av identitet og tradisjonell autentisering

Identifisering og autentisering skjer dels ved hjelp av naturlige identitetsmerker (noe du er; irismønster, oppførsel; ganglag) og dels ved hjelp av tildelte identitetsmidler (noe du har eller vet; fødselsnummer, PIN-kode, kundenummer mv). Identifisering og autentisering innebærer med andre ord å kjenne igjen et bestemt individ ved hjelp av identitetsmerker og/eller -midler.[23]

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”, ”det du er” eller en kombinasjon av disse.

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

[23] Schartum & Bygrave (2008) s. 10.

”Det du vet” er kunnskap brukeren besitter, eksempelvis et passord. Problemet her er at noe du ”vet” kan gis bort eller falle i gale hender dersom det skrives ned.

”Det du er” er parametre som er knyttet fysisk til brukerens person, typisk biometriske data. Det vil for eksempel være utseende og andre fysiske karakteristika. Et annet eksempel kan være tradisjonelle ”har”-parametre som er fysisk sikret til den fysiske personen, eksempelvis adgangskort i et håndjern eller RFID-brikke[24] som er operert inn i kroppen.

Hvilke parametre som bør benyttes avhenger av den konkrete situasjonen. Lave autentiseringsbehov tilsier at kun ett parameter kan være tilstrekkelig, eksempelvis nøkkel. Dersom kravene til autentisering på vedkommende arbeidsplass er høyere, kan man med fordel kombinere flere parametre, eksempelvis adgangskort og kode i en fysisk adgangskontroll.[25]

Det er et faktum at man på de aller fleste arbeidsplasser trenger å implementere anordninger som sørger for at kun de som skal ha tilgang får tilgang til bedriftens lokaler og liknende. Årsakene til behovet for kontroll vil variere, men behovet må møtes uansett.

Det er i løpet av de siste årene utviklet svært mange ulike systemer for kontroll av ansatte. De fleste som jobber i kontorlokaler må dra et adgangskort for å komme inn, nøkler blir mindre og mindre brukt. Årsaken er nok at teknologien bringer med seg en større grad av nøyaktighet i kontrollen av hvem som beveger seg hvor. Dersom bedriften ønsker det kan systemer installeres som overvåker og lager lister over bevegelser slik at man kan angi hvilken ansatt man vil følge kortet til og få opp oversikt over dets bruk i den gitte perioden. Slik kontroll er ikke mulig dersom de ansatte bruker nøkler.

---

[24] Det vil si *radiofrekvensidentifikasjon* som innebærer at data kan lagres og innhentes ved hjelp av små enheter, kalt RFID-brikker. Brikkene kan festes til, eller plasseres inn i et produkt, et dyr eller en person.

[25] Datatilsynets revisjonsnotat pol §12, s. 3.

2.3.2.1 Rettslig definisjon av personopplysninger, herunder biometri

Personopplysningsloven definerer personopplysninger som ”opplysninger og vurderinger som kan knyttes til en enkeltperson” (§ 2 nr. 1.) Loven inneholder regler for ulike situasjoner og tidspunkt hvor personvernet er truet, regler om adgangen til å sette i verk behandling av personopplysninger, regler som skal ivareta personvernhensyn under behandlingen og regler som skal sikre ivaretakelsen av de samme hensyn ved å avslutte en behandling.

Håndtering av personopplysninger har altså tre sentrale reguleringspunkt: regler for *innsamling* og registrering av opplysningene, *bruk* av de innsamlede opplysningene og *videre-spredning* av opplysningene til andre, jf. Personopplysningsloven § 2, nr. 2.

Spørsmålet blir så om biometriske opplysninger og bruken av dem faller inn under definisjonene i pol § 2 nr. 1 og 2. For å komme frem til hvorvidt biologiske mønstre faller inn under denne definisjonen, er det naturlig å ta utgangspunkt i en generell definisjonen av biometri. Biometriske data er som tidligere nevnt fysiologiske karaktertrekk eller adferdsmønstre.

I forbindelse med høring av forslag til endring av passloven i mars 2005, ble "biometri" definert som "biometriske kontrollelementer (eng; biometric identifier), (unike) fysiske karakteristika knyttet til en person (ansiktstrekk, fingeravtrykk, irismønster, DNA-profil) eller som beskriver en persons opptreden eller handlemåte (stemme, signatur), og som kan benyttes til å identifisere person eller verifisere at innehaveren av et identitetskort er samme person som kortet opprinnelig ble utstedt til."[26] Biometri er språklig og prinsipielt ikke unikt knyttet til mennesker, men i forbindelse med adgangskontrollsystemer fører *formålet* med bruken av biometri med seg en avgrensning mot andre biologiske mønstre.[27] Formålet med registrering av biologiske mønstre til slik bruk er enten å identifisere eller autentisere

[26] Se http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2005/Hoering-forslag-til-endringer-av-passloven-mm/3.html?id=98152 Oppslag gjort 07.11.08.

[27] Schartum & Bygrave (2008) s. 14.

en person. Å avgrense begrepet biometri ved å angi formålet innebærer ikke at det er klart hvilket innhold det rommer. Delvis er dette fordi de biologiske mønstrene er delt opp i underkategorier og det er usikkert hvilke mønstre som skal trekkes frem i en fortolkning. Det ser ut til å være enighet om at biometriske mønstre kan deles inn i i) de som gjelder fysiologiske karakteristika og ii) adferdsmessige karakteristika ved individer. Innen hver av disse gruppene er det imidlertid ulike mønstre som kan benyttes.[28]

Biologiske mønstre kan registreres maskinelt(digitalt) ved bruk av biometriske systemer. En persons ganglag kan observeres av et kamera, et hårstrå kan analyseres og en stemme kan registreres av en sensor. Når disse mønstrene manifesteres ved at det fysisk dannes et digitalt 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 så tolkes, for eksempel ved at et digitalt 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.

Et svært sentralt moment i definisjonen av biometri at det dreier seg om informasjon i digitalisert form. Det er omstridt hvorvidt et analogt bilde av en person er å regne som en personopplysning. ”Analog identifisering” dreier seg om bruk av tradisjonelle identifiseringsmetoder (fremstilt i avsnitt 2.3.2) og vil ikke være sporbar på samme måte som digital informasjon. Etter hvert som samfunnet blir mer og mer digitalisert gjennom dataverdenen, blir den beskyttende sfære rundt hver enkelt persons privatliv mindre og mindre. Nye bruksområder for teknologi (og dermed også elektroniske spor) er i stadig utvikling. Jeg kommer tilbake til dette spørsmålet i avsnitt 5.

Hva skiller den vanlige identifiseringen fra biometrisk identifisering i lovens forstand?

---

[28] Schartum & Bygrave (2008) s. 15.

Den rettslige reguleringen vedrørende identifisering kan i hovedsak deles i tre deler.[29] For de første har vi regulering vedrørende hjemmel for og kompetanse til å registrere opplysninger om identitet. I denne kategorien faller bruk innen kriminalområdet, folkeregistrering og utlendingsforvaltningen, helseområdet og alminnelig personvernrett. For det annet har vi regulering om bruk av ID-kort og plikt til å identifisere seg, eksempelvis brukt i transportsektoren og på arbeidsplasser, overfor politi- og fengselsmyndigheter og i saker om pass og statsborgerskap. For det tredje har vi regler som gjelder beskyttelse av identitet og rett til å opptre anonymt. Disse regulerer eksempelvis saker vedrørende vitner og vitneførsel, slektskap og humant materiale, samt tiltak mot menneskehandel, prostitusjon etc.

Vanlig identifisering er, som nevnt over, nødvendig for at store deler av samfunnet skal fungere. Forskjellen på vanlig identifisering og biometrisk identifisering er at ved bruk av biometri krysser man en grense i forhold til den enkeltes rett til privatliv. Skillet i lovens forstand innebærer et krav til strengere vilkår for bruk av biometri enn for bruk av tradisjonelle midler for identifisering.

Personopplysningsloven skal beskytte individet mot personvernmessige krenkelser, jf. lovens formål. Det er mange særregler i mange lover som regulerer kontroll innenfor ulike rettsområder. Antallet regler forteller muligens også noe om spredningspotensialet som biometriske metoder med identifiseringsformål kan ha.[30] Det kan være grunn til å forvente at det i tilknytning til de deler av særlovgivningen som i dag inneholder krav til identifisering og autentisering, kan oppstå krav om å få adgang til å anvende biometriske teknikker. I så tilfelle vil ikke de generelle reglene i Personopplysningsloven være toneangivende i forhold til vilkårene for bruk av biometri og beskyttelse av personvernet. På områdene der vernebehovet er størst, for eksempel innen helsesektoren, strafferettspleien, kriminalomsorgen, ved sikring av transportmidler, utlendingsadministrasjonen og i spørsmål om pass og statsborgerskap kan særreguleringer komme til å dominere rettstilstanden.

---

[29] Dag Wiese Schartum *Rettslig regulering av identitet og identifisering i Norge.*

[30] Schartum & Bygrave (2008) avsnitt 3.2.5.

Listen over områder illustrerer mulighetene for særlovgivning på svært bred basis. Personopplysningslovens regulering vil få betydning for annen spredt anvendelse av biometriske teknikker (som adgangskontroll, pålogging på datamaskiner etc), men det kan neppe utelukkes en eksplosiv økning i antall lover og forskrifter vedrørende identifisering og biometri.

2.3.2.2 Grunnkrav til behandling av personopplysninger

Personopplysningsloven § 11 første ledd bokstav a, jf § 8, angir vilkår for behandling av personopplysninger. Det må foreligge behandlingsgrunnlag før personopplysninger kan behandles. Et av behandlingsgrunnlagene som § 8 gir anvisning på er samtykke.[31] Det kan hevdes at samtykke er innhentet ved at påloggingsteknologien er frivillig[32]. De ansatte avgir fingeravtrykket frivillig, de gjør dette selv ved førstegangs pålogging på maskinen og det er mulig å velge teknologien vekk. Vilkåret i Personopplysningsloven § 8 første ledd er dermed oppfylt. Jeg kommer tilbake til samtykke som behandlingsgrunnlag for personopplysninger i avsnitt 4.3.1.2.

Det er videre vesentlig, i den enkelte sak, hvorvidt de øvrige kravene i personopplysningsloven § 11 er oppfylt. Det gjelder særlig pol § 11 bokstav b og c, om at opplysningene bare brukes til formål som er saklig begrunnet i den behandlingsansvarliges virksomhet og at de ikke brukes senere til formål som er uforenelig med det opprinnelige formålet.[33]

---

[31] jf. Pol § 2 nr. 7.

[32] Jeg forutsetter her at det er snakk om faktisk frivillighet, ikke frivillig tvang, jf. drøftelsen i avsnitt 4.3.1.2.

[33] PVN-2006-7 avsnitt 7.2.

2.3.3 Hva er forskjellen mellom identifisering og autentisering?

Sentral problemstilling:
Hva er forskjellen på, og sammenhengen mellom, identifisering og autentisering og hva betyr det for lovanvendelsen?

For oppgavens videre utvikling er det viktig å uttrykke forskjellen mellom identifisering og autentisering. De ulike begrepene medfører ulike krav og konsekvenser og en distinksjon dem imellom er sentral for oppgaven. Betydningen av sondringen for lovanvendelsen vil jeg komme tilbake til i avsnitt 4.2.

Banalt kan det sies at *identifisering* er svaret på spørsmålet: Hvem er jeg? *Autentisering* er derimot svaret på spørsmålet: Er jeg den jeg sier jeg er?

Identifisering innebærer at den som kontrolleres knyttes opp til data som viser hvem personen er. Autentisering er en kontroll av at den som søker tilgang til det kontrollerte miljø faktisk har lov til å være der, at man er den man hevder å være. Det innebærer krav til at den som kontrolleres aktivt fremsetter en påstand om sin identitet. Som nevnt over er biometri egnet til å identifisere individer og derfor også til å autentisere dem. En sentral problemstilling er dermed hvorvidt autentisering faller inn under uttrykket ”entydig identifikasjonsmiddel” i pol §12. Dette tema drøftes videre i avsnitt 4.

På en gjennomsnittsarbeidsplass er de ansatte vant til å både identifisere seg og autentisere seg opptil flere ganger om dagen. Man har gjerne et nøkkelkort som må dras i en leser for å åpne dører eller for å registrere tilstedeværelse (og fravær) osv. Deretter skriver man inn brukernavn og passord på bedriftens datamaskin, kanskje flere forskjellige for å få tilgang til forskjellige programmer. I vanlig språklig forståelse innebærer brukernavnet en identifisering av brukeren. Det er derimot ikke tilfellet i denne situasjonen. Brukernavnet (brukeridentiteten) er en autentiseringsopplysning som kan ”lånes” bort til hvem som helst og dermed gi tilgang for uautoriserte personer. Likeledes er også passordet en autentiseringsopplysning. Ved kortbruk oppstår en lignende situasjon. Dersom man må slå kode etter å

ha dratt kortet over leseren er koden autentisering og kortet identifiseringen, i teorien. Men slik som med brukernavn kan også kort og koder ”lånes” bort, mistes eller fratas rette eier og medføre en autentisering av uautorisert personell.

Hva gjelder biometri, vil identifisering og autentisering falle sammen på en annen måte enn nevnt over. Fingeravtrykket opptrer som identifikasjonsmiddel ved første gangs registrering, men blir så autentiseringsmiddel ved videre bruk (i et system som baserer seg på kun fingeravtrykk). Et eksempel er åpning av dører med fingeravtrykk, ingen kode, kun registrert fingeravtrykk som autentisering av personen.

Dersom man derimot installerer et system som baserer seg på fingeravtrykk template som identifiseringsmiddel for så å autentisere brukeren gjennom passord eller kode vil skillet mellom identifisering og autentisering være klarere.

2.3.4 Hvor nøyaktige er biometriske sikkerhetsløsninger?

Biometri anses for å være en teknikk som gir identifisering og autentisering med svært høy grad av nøyaktighet.

Bruk av biometriske data i identifisering og bekreftelse av identitet er derimot ikke en eksakt vitenskap, men brutal sannsynlighetsberegning, og man må velge hvilken feilrate man godtar.[34] Feilfunksjonen for biometrisk id-teknologi kan måles i Failure Acceptance Rate (FAR) og Failure Rejection Rate (FRR), dvs andelen uriktig akseptans og avvisning. For begge mål er det ikke uvanlig å sette en grense på 1%. Det er imidlertid grunn til å tro at den teknologiske utviklingen vil gi økt prosesseringskraft i de biometriske systemene og lavere feilrater. [35]

[34] Datatilsynets revisjonsnotat pol §12, s. 4.

[35] Schartum & Bygrave (2008) s. 16.

Grunnleggende for biometriske systemer er at de utfører mønstergjenkjenning som både forutsetter at det allerede er registrert mønstre som skal være sammenligningsgrunnlag, og at det ved bruk registreres mønstre som skal sammenholdes med dette grunnlaget for å avgjøre om mønstrene er tilstrekkelig like til at det kan sies å foreligge likhet.[36] Registreringen av mønstrene kan kalles innrullering av biologiske mønstre (eng.: "templates"), mens den siste delen gjelder bruk i form av identifisering og/eller autentisering. Jeg vil komme tilbake til hvordan registrering og bruk foregår i praksis i senere avsnitt.

Egenskap **Type**	Allment fore-kommen-de	Entydighet	Holdbarhet	Tilgjengelighet	Gjennomføring	Grad av aksept	Omgåelses-fare
Ansikt	H	L	M	H	L	H	L
Hånd	M	M	M	H	M	M	M
Fingeravtrykk	M	H	H	M	H	M	H
Iris	H	H	H	M	H	L	H
DNA	H	H	H	L	H	L	L
Tastemønster	L	L	L	M	L	M	M
Signatur	L	L	L	H	L	H	L
Stemme	M	L	L	M	L	H	L
Ganglag	M	L	L	H	L	H	M

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

Figur 1. Vurderingskriterier for kvaliteten av biometrisk id-håndtering.
Kilde: Schartum & Bygrave (2008) s. 18.

Tabellen ovenfor gjengir de viktigste vurderingskriteriene for kvaliteten av biometrisk id-håndtering, men må brukes med en viss skepsis og varsomhet all den tid den kun indikerer visse forskjeller mellom kjennetegnene. Det er klart at teknologiutvikling, brukssituasjoner og kulturelle forskjeller kan virke inn på vurderingene og endre klassifiseringen og dermed forskjellene mellom teknikkene. Det mest vesentlige å merke seg er imidlertid at det finnes

[36] Schartum & Bygrave (2008) s. 15.

vurderingssystemer for bioteknologi som kan og vil bli videreutviklet, og som kan være til hjelp ved fremtidig vurdering om bestemte teknikker bør tillates brukt.[37] Schartum og Bygrave har spesifisert betydningen av de ulike vurderingskriteriene som følger[38]: *Allment forekommende* gjelder spørsmålet om de biologiske/fysiologiske trekk som måles, er allment forekommende i befolkningen eller ikke. Noen mennesker vil for eksempel mangle hender og kan således ikke benytte teknologien. *Entydighet* gjelder i hvilken grad hvert menneske har de egenskapene som måles på måter de er alene om. Irisgjenkjenning har meget høy entydighet, mens for eksempel stemme kan ligne så mye at den ikke kan brukes til å skjelne enhver person fra andre. *Holdbarhet* sier noe om hvor holdbar over tid biometriske kjennetegn er, herunder hvor sårbare de er for skade, aldring mv. Ansiktsgjenkjenning er for eksempel lett påvirket av skade og forandringer som skyldes sykdom og aldring mv, mens fingeravtrykk er klart mer stabile og robuste. *Tilgjengelighet* gjelder hvor enkelt eller vanskelig det er å samle inn de biologiske egenskapene som skal brukes. Ganglag er lett å samle inn informasjon om fordi det gjelder en handling som normalt lett lar seg observere, mens kroppslukt er vanskeligere tilgjengelig fordi det hører til den intime sfæren. Gjennomføringskriteriet gjelder hvor lett eller vanskelig det er å bruke vedkommende biometriske teknikk. I praksis er det for eksempel vanskelig å gjennomføre ansiktsgjenkjenning, og forholdsvis lett å gjennomføre fingeravtrykkavlesning. *Grad av aksept* gjelder i hvilken grad folk er villig til å la den biometriske teknikken bli brukt på seg selv, noe som igjen kan være et bilde på hvor integritetskrenkende folk mener bruken av teknikken er. Tabellen viser at ansiktsgjenkjenning er mer akseptabelt enn for eksempel skanning av iris, men slike oppfatninger vil trolig være kulturavhengige og i tillegg variere over tid. Til slutt kan biometriske teknikker vurderes ut i fra hvor stor *omgåelsesfare* det er. Ansiktsgjenkjenning er i tabellen klassifisert som lite utsatt, mens fingeravtrykk er relativt mye utsatt for omgåelse, for eksempel fordi det kan være mulig å benytte avtrykk av andres fingeravtrykk.

---

[37] Schartum & Bygrave (2008) s. 17.

[38] Jeg har her valgt å gjengi store deler av tabellforklaringen til Schartum & Bygrave, da den er konsis og godt forklart som den er.

I lys av disse vurderingskriteriene er det naturlig å ta med en bemerkning om at det er helt riktig at det er mange forskjellige former for biometriske kjennetegn som kan digitaliseres. Det er således viktig å poengtere at det er svært ulik grad av nøyaktighet knyttet til bruk av de ulike kjennetegnene. At et kontrollsystem baserer seg på biometri innebærer ikke automatisk en tilnærmet feilfri identifiserings- eller autentiseringsprosess. Selv om fingeravtrykket er unikt, er ikke dermed bruken av teknikken feilfri. Det er alltid en fare for at systemet kan manipuleres til å produsere gale resultater. I tillegg er det viktig å hindre mangelfull identitetskontroll ved innregistrering i systemet. Dersom feil person blir registrert i utgangspunktet vil ikke bruk av biometri medføre riktigere autentifisering ved videre bruk.

Problemet med all form for identifisering og autentisering er at man aldri kan oppnå 100 % nøyaktighet. Dersom man bruker naturlige kjennetegn og legitimasjonspapirer i en manuell sjekk er det alltid en viss sannsynlighet for at det begås feil av kontrolløren. Enten bevisst eller ubevisst. Det er en sjanse for at dørvakten på et utested vil se gjennom fingrene med alderen på to pene jenter som vil inn. De er ikke 23, men 21 år gamle, og således bør de ikke slippes inn på 23 års aldersgrense (autentisering). I motsatte tilfelle kan det hende at man ikke slipper inn selv om man er gammel nok, men eksempelvis ikke har ”riktig utseende” for utestedet. Dette er et eksempel på en situasjon der autentiseringsbehovet ikke er særlig sterkt, og hvor feilraten rent objektivt sett er høy. Foregående eksempel på ”kontrollsystem” illustrerer et scenario hvor bedriften ikke har behov for mer nøyaktig autentisering enn de kan få av mennesker som fysiske kontrollører.
I det følgende vil jeg søke å belyse forskjellen mellom ulike behov for ulike bedrifter, samt hvilke rettsregler som regulerer bruk av biometrisk kontroll i arbeidsforhold.

3 Personvern på arbeidsplassen

3.1 Innledning

Som tidligere nevnt må utgangspunktet tas i Arbeidsmiljøloven. Det er personvernet på arbeidsplassen som utfordres. Arbeidsmiljøloven gir i kapittel 9 hjemmel for beskyttelse av personvernet ved kontrolltiltak i virksomheten. Aml § 9-1 er den relevante hjemmel for slike biometriske adgangskontrollsystemer som omhandles i denne oppgave. Hjemmelen er vag og viser selv til Personopplysningsloven for supplerende regelverk.

Personvernretten som sådan har et meget vidt nedslagsfelt. Dette er også et av hovedproblemene med personopplysningsloven – den kan tenkes å være litt for generell til å fungere tilstrekkelig i reguleringen av forholdet mellom partene i arbeidslivet. Arbeidsretten har på sin side et forholdsvis snevert og klart avgrenset virkeområde, og reglene er utformet deretter. Den regulerer alene forholdet mellom arbeidsgivere og arbeidstakere, samt forholdet mellom arbeidsgiver- og arbeidstakerorganisasjonene. Forarbeidene[39] uttaler at regelbildet er fragmentarisk og gir en uoversiktlig og vanskelig tilgjengelig rettstilstand hva gjelder kontroll og overvåkning av arbeidstakere. Personopplysningsloven er som nevnt svært generell og ikke tilpasset arbeidslivet. I tillegg gjelder en del generelle ulovfestede prinsipper i forholdet mellom arbeidsgiver og arbeidstaker, samt en rekke særregler i forskjellige lover. Den faktiske tilstand er i konstant bevegelse, preget av en teknologisk utvikling som raskt øker arbeidsgivers mulighet til å kontrollere og samle informasjon om arbeidstakere.

Arbeidsgiverne må dermed forholde seg til både personvernretten og arbeidsretten i forbindelse med kontrolltiltak på arbeidsplassen. De rettslige grunnlagene for slike kontrolltiltak er imidlertid noe forskjellig utformet på de ulike rettsområdene. Etter de arbeidsrettslige reglene utgjør styringsretten det mest sentrale hjemmelsgrunnlaget. Med de begrensninger som følger av ovennevnte lovfestede og ulovfestede regler og prinsipper, gir styringsretten arbeidsgiver en viss rett til å foreta kontrolltiltak overfor sine ansatte. I personopplysningsloven er utgangspunktet i stedet at enhver behandling av personopplysninger

[39] Ot.prp.nr. 49 (2004-2005) s. 143.

er forbudt – med mindre det finnes et konkret rettslig grunnlag. Personopplysningsloven fremtrer dermed som en sentral begrensning i styringsretten.[40]

3.2 Arbeidstakers forventninger til personvern

Aml § 9-1 hjemler en rett for arbeidstakeren til ikke å bli "uforholdsmessig belastet" av kontrolltiltak på arbeidsplassen. Tolkningsmessig angir første ledd vilkår for oppfyllelse av hjemmelen. I det enkelte tilfelle må man veie bedriftens "saklig(e) grunn" for å implementere kontrolltiltaket mot arbeidstakers rett til at tiltaket "...ikke innebærer en uforholdsmessig belastning for arbeidstakeren." Forarbeidene uttaler at "bestemmelsen angir de generelle vilkår for arbeidsgivers kontrolladgang og er ment å kodifisere gjeldende ulovfestet rett. Saklighetskravet innebærer at det må foreligge et formål som er forankret i virksomheten og som i seg selv er saklig."[41]

Bruk av ordet "kan" viser til at arbeidstakers rettigheter kommer foran virksomhetens dersom ikke arbeidsgiver kan vise til tunge relevante årsaker til bruk av belastende kontrolltiltak. Det må her foretas en skjønnsmessig avveiing av partenes hensyn. Et tiltak som er saklig for én arbeidsgruppe eller arbeidstaker kan likevel være for lite saklig for en annen. Ot.prp.nr. 49 (2004-2005) viser til praksis rundt anvendelse av saklighetskriteriet ved oppsigelser etter arbeidsmiljøloven § 60 for å illustrere rekkevidden av kravet om tilstrekkelig saklig grunn.

Jo større behov for å kontrollere aksess til virksomhetens lokaler og sensitive opplysninger, desto større belastning må kontrollen innebære for å bli stanset etter aml § 9-1. Hvilke tiltak som medfører uforholdsmessig belastning på arbeidstakeren vil variere fra arbeidsplass til arbeidsplass. Det er naturlig at en pilot må tåle flere tiltak mot sin person for å verifisere ens identitet enn en medarbeider i en klesforretning. Hvor grensen går beror på en

---

[40] Stefan Jørstad *Arbeidsgivers adgang til å kontrollere og overvåke sine ansatte*, side 6.

[41] Ot.prp.nr. 49 (2004-2005) kommentar til § 9-1.

skjønnsmessig vurdering ut fra visse gitte parametre. Forarbeidene[42] har uttalt at ved forholdsmessighetsvurderingen vil det "ikke være tilstrekkelig å vurdere det enkelte tiltak for seg; også summen av kontrolltiltak vil være relevant. Et kontrolltiltak som isolert sett er saklig og forholdsmessig, vil likevel kunne bli ansett som ulovlig dersom tiltaket medfører at den forsvarlige tålegrense for arbeidstakerne eller arbeidsmiljøet som sådan blir overskredet."

Arbeidsgivers rettigheter vil naturlig nok møtes av en plikt på arbeidstakers side. I Ot.prp.nr. 49 uttaler departementet at "dersom vilkårene for å gjennomføre kontrolltiltaket er oppfylt, vil arbeidstakerne med andre ord ha plikt til å etterkomme arbeidsgivers pålegg om kontroll."[43] Konsekvensene av disse vilkårene blir at dersom arbeidstakerne unnlater å medvirke til gjennomføring av et kontrolltiltak som ligger innenfor rammene for saklighet og forholdsmessighet, vil det formelt sett foreligge et brudd på eller mislighold av arbeidsforholdet. Dette forholdet må således bedømmes på basis av de alminnelige regler om mislighold av plikter i arbeidsforhold.

Graden av uforholdsmessighet er altså blant annet avhengig av forutberegneligheten for de ansatte. Dersom man var klar over bedriftens kontrollsystemer før man ble ansatt er det liten sannsynlighet for at man forventer at man selv ikke må irettesette seg etter det. Noen arbeidsområder har høyere krav til kontroll av sine ansatte kun i kraft av hva man arbeider med, eksempelvis logistikkmedarbeidere i Forsvaret og medarbeidere hos NOKAS (Den Norske Bank). Arbeidsplasser som krever vandelsattest i søkeprosessen er andre eksempler på tilfeller hvor de ansatte ikke bør være overrasket over eventuell høy grad av kontroll i det daglige.

---

[42] Ot.prp.nr. 49 (2004-2005) kommentar til § 9-1.

[43] Ot.prp.nr.49 (2004-2005) s. 144.

3.3 Problematikken rundt innføring av biometrisk adgangskontroll i arbeidslivet – personvernhensyn

3.3.1 Oversikt

Hovedproblemstillingen for oppgaven omhandler biometrisk adgangskontroll i arbeidslivet. Dette avsnittet tar sikte på å gjennomgå de viktigste personvernmessige bekymringene i forhold til slik kontroll.

3.3.2 Misbruk av biometrisk informasjon – elektroniske spor

Den potensielle personverntrusselen ved bruk av biometriske adgangskontrollsystemer i arbeidslivet er at arbeidsgiver misbruker informasjonen til andre formål enn det opprinnelige (autentisering). Verdien av opplysninger som kan knyttes entydig til individer har en egenverdi som kan virke forlokkende og lede til misbruk. Som tidligere nevnt er det et sentralt aspekt ved biometriske persondata at de er digitale, altså maskinlesbare. De er dermed svært omsettelige og enkle å sette i system.

Et eksempel på mulig misbruk av biometriske personopplysninger er at dersom arbeidsgiver har de ansattes fingeravtrykk, kan disse overlates til politiet dersom det har vært innbrudd på bedriften, og mistanken er rettet mot egne ansatte?[44] Spørsmålet er om slik bruk av biometriske personopplysninger bør godtas, da det er snakk om en klar formålsendring fra det opprinnelige autentiseringsformålet.[45] Jeg går nærmere inn på denne problemstillingen i avsnitt 5 flg.

---

[44] Eksemplet er kanskje litt søkt, for et adgangskontrollsystem vil sjelden ha lagret fingeravtrykk av mer enn en finger, og det hjelper ofte ikke i forbindelse med etterforskning av innbrudd, men en kombinasjon av ulik informasjon i et slikt system vil kunne være til nytte (bevegelsesmønstre etc.)

[45] Jens Petter Berg, mail 19.11.08.

3.3.3 Adgangskontrollsystemers frihetsinnskrenking

En økning av adgangskontroll på arbeidsplassen innebærer en begrensning av de ansattes "frihet". Som tidligere nevnt er det en fare for at informasjonen som høstes til bruk til identifisering og autentisering ikke utelukkende blir brukt til det opprinnelige formål. En registrering av fingeravtrykk hver gang noen går inn og ut av arbeidsområdet er egnet til å overvåke bevegelsene til de ansatte, ikke bare til å sørge for at kun autorisert personell har tilgang til området. Jeg må her bemerke at dette argumentet ikke er begrenset til kun å ramme biometrisk adgangskontrollsystemer. All form for kontroll, også analog, er frihetsinnskrenkende.

Her må man derimot være nyansert. En viss form for kontroll er nødvendig for å møte bedriftenes autentiseringsbehov, og som nevnt er forutberegneligheten for de ansatte av betydning for tolkningen av hva som må anses uforholdsmessig. De tradisjonelle, analoge, formene for adgangskontroll (adgangskort, resepsjonisten som må passeres og eventuelle koder for dørlås etc.) gir også arbeidsgiver anledning til å etterspore ansattes bevegelser på jobb. Den vesentlige forskjellen mellom analog og biometrisk adgangskontroll er at biometri innebærer en uløselig tilknytning til vedkommende. Opplysninger med høy nøyaktighetsgrad, som indikerer at bestemte personer har vært på et bestemt sted, til en bestemt tid, samt opplysninger om personen som er knyttet til selve fingeravtrykkleseren (for eksempel et kjøp, omfang og innhold av forbrukte tjenester mv) kan innebære en selvstendig merverdi for den som har disposisjonsrett over opplysningene.[46] Konsekvensene av at slik informasjon om hver enkelt blir lagret og brukt i bedriften er at det til enhver tid vil være risiko for misbruk av dataene (jf. drøftelsen i avsnitt 3.3.2).

[46] Schartum & Bygrave (2008) s. 20.

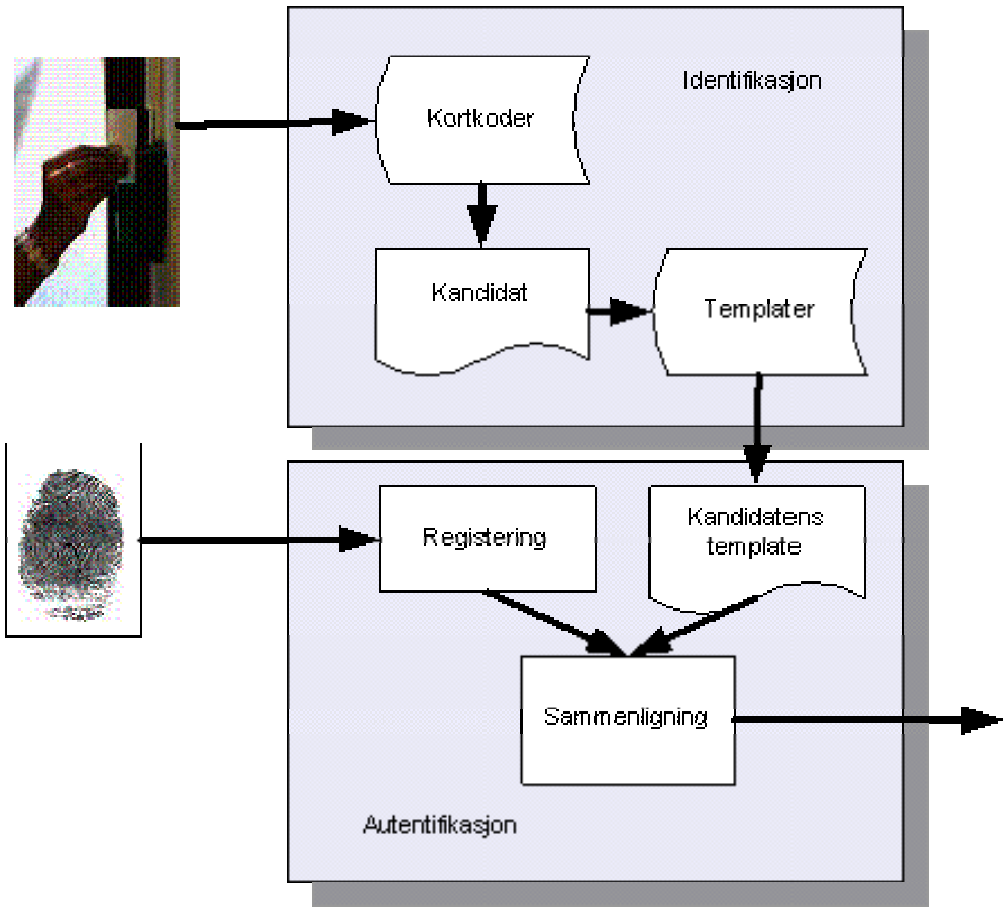
4 Nærmere om praktiseringen av gjeldende bestemmelser

4.1 Oversikt

I denne del av avhandlingen vil jeg ta for meg de sentrale avgjørelsene vedrørende bruk av biometriske adgangskontrollsystemer og de sentrale problemstillinger som oppstår som følge av avgjørelsene. I avsnitt 4.2 behandles kort begrepet template og hvordan systemet fungerer. I avsnitt 4.3 drøftes personvernnemndas avgjørelser med fokus på anvendelse av pol § 12.

To sentrale problemstillinger for denne delen av fremstillingen er
1)Hvilke slutninger kan dras fra avgjørelsene vedrørende vilkår for bruk av biometriske adgangskontrollsystemer? og
2)Hva betyr avgjørelsene for arbeidstakere?

4.2 ”Fra kodekort til fingeravtrykk” - En forenklet og prinsipiell fremstilling av bruken av template



Figur 2. Illustrasjon av bruk av kort og biometri

Kilde: PVN-2006-10 punkt 6.2

Illustrasjonen over viser hvordan prosessen foregår dersom man bruker et kort med magnetstripe eller mikroprosessor i tillegg til template. En template er, som jeg vil redegjøre nærmere for senere i avsnittet, et antall punkter tatt fra et fingeravtrykk og regnet om til en verdi som lagres i en enhet for kontroll. Personen identifiseres ved hjelp av kortet. Koden i kortet sammenlignes med en database, og kandidaten for autentisering velges ut. På det grunnlaget kan systemet slå opp i en database med templater.

Ved bruk av fingeravtrykk for å gi tilgang til (eksempelvis) en datamaskin, erstatter lesing (skanning) av fingeravtrykket bruk av passord, eventuelt både brukernavn og passord. Brukeren har på forhånd registrert avtrykk av en eller flere fingrer ved å trekke fingeren over en smal skanner (optisk leser) integrert i maskinen. Ved første gangs registrering trekkes fingeren flere ganger inntil maskinen finner at avtrykket avleses på samme måte hver gang og godkjenner registrering. Dette første steg er bruk av en sensor som gjør datafangst, og registrerer det/de biologiske kjennetegnene en ønsker å gjøre bruk av (fingeravtrykk, iris mv). Denne første registreringen gjelder fingeravtrykket mv slik det i virkeligheten fremstår.[47]

Avtrykket behandles så av registreringsenheten. En sensor vil registrere enkelte data i tillegg til ovennevnte som det ikke er formålstjenlig å behandle videre, dvs "støy" som ikke gjelder det ønskede mønstret. Slik støy fjernes gjennom andre steg som kan kalles "forbehandling". I tredje steg velges de egenskaper ved de registrerte dataene som (i fjerde steg) skal danne grunnlag for registrering av det biologiske mønstret.[48] Et eksempel som ofte brukes er utvelgelse av visse punkter fra mønsteret i fingeravtrykket etter en regel som kan variere fra enhet til enhet. Disse punktene vil ha ulike verdier alt etter utseende til de deler av mønsteret som faller sammen med punktene.

Disse verdiene behandles så etter en regneregel (en algoritme) som danner en ”template” (mal), denne templaten lagres så i en database, et kort eller (som vist på figuren over) enheten for tilgangskontroll. Det er gjerne et lite antall punkter som velges ut ... for få punkter til at det er mulig å regenerere fingeravtrykket ved hjelp av templaten. Om det skal være mulig, må det registreres nok punkter til at det kan regenereres et bilde – en vanlig telefaks har en oppløsning på 9000 punkter per kvadrattomme, som gir et inntrykk av hva som kreves for å lagre avtrykket som et ”bilde”. Men det kreves likevel nok punkter til at det skapes en slags forenklet modell som karakteriserer det virkelige fingeravtrykket.

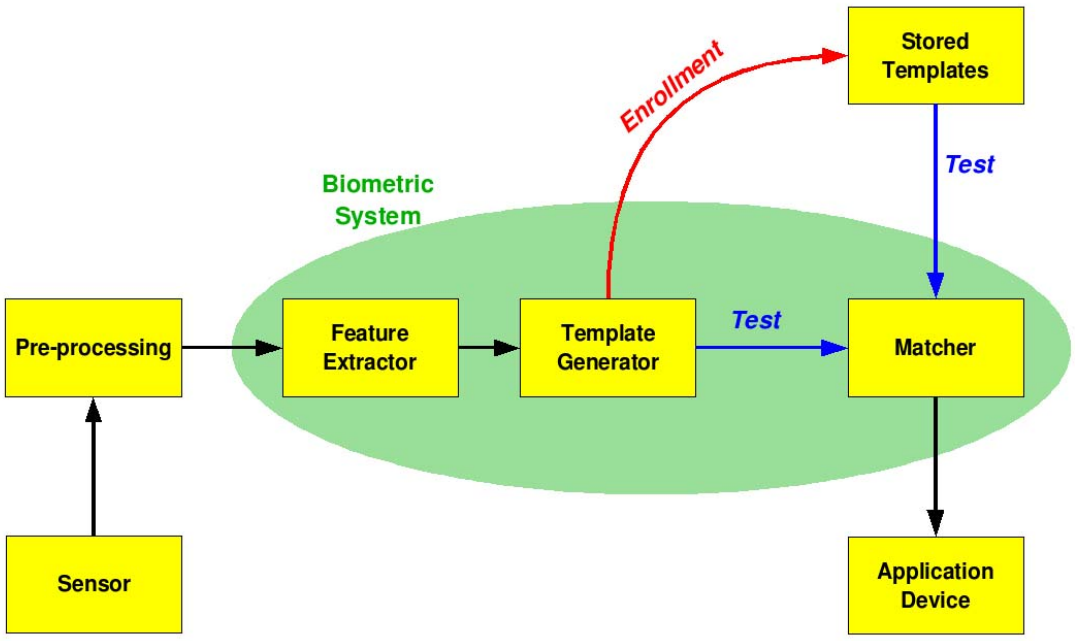
---

[47] Schartum & Bygrave (2008) s. 15.

[48] Schartum & Bygrave (2008) s. 15.

Når brukeren skal benytte maskinen, trekkes fingeren over leseren på ny. Punkter registreres etter regelen, og det beregnes en verdi. Denne sammenlignes med den registrerte verdi, det vil si templaten. For å godkjennes, må den beregnede verdien ligge innenfor en definert grense for avvik, ellers avvises forsøket på å få tilgang. Hvis avlesningen er vellykket, sender enheten for tilgangskontroll en kryptert melding til maskinen, som deretter blir tilgjengelig for brukeren.[49]

I tilfelle som vist på illustrasjonen over skjer identifiseringen ved hjelp av kortet. Den vanlige måten ved tradisjonell autentisering er at personen deretter taster en kode. Ved bruk av biometri erstatter fingeravtrykket (templaten) koden. Det er også andre muligheter, enn ovennevnte, for bruk av fingeravtrykk, enten alene eller sammen med kode eller passord. Wikipedia har lagt opp en mer generell illustrasjon av biometriske systemer.



Figur 3. Modell av biometriske systemer.[50]

Kilde: Wikipedia

[49] Fremgangsmåte jf. PVN-2006-7 punkt 7.3.

[50] se http://en.wikipedia.org/wiki/Biometrics. Oppslag gjort 08.11.08.

4.3 Personvernnemndas avgjørelser

4.3.1 Innledning

Personvernnemnda har behandlet spørsmålet om adgangen til å bruke biometri som autentiseringsmiddel i flere saker. Nedenfor følger en gjennomgang av de rettslige momenter i nemndas klagevedtak, supplert med ytterligere kilder for en bredere drøftelse. Jeg bruker endel momenter fra PVN-2006-7 Tysvær kommune (noe skjevfordelt i forhold til de andre avgjørelsene). Bakgrunnen for dette valget er at avgjørelsen er av særlig interesse i forhold til tolkningsmomenter til pol § 12, i tillegg til at senere avgjørelser refererer til, og bruker den i sin drøftelse.[51] Saken vedrørende Tysvær kommune danner altså grunnlag for etablering av en praksis som har bidratt til å klargjøre anvendelse av pol § 12 i forhold til fingeravtrykk.[52] På bakgrunn av dette ser jeg det naturlig å ta utgangspunkt i dette klagevedtaket.

4.3.2 Pol §12

4.3.2.1 Oversikt

En sentral problemstilling vedrørende tolkning av pol § 12 er:
Hva er forskjellen på, og sammenhengen mellom, identifisering og autentisering og hva betyr det for lovanvendelsen?

Jeg har tidligere behandlet første del av problemstillingen i avsnitt 2.3 foran, og vil her søke å belyse hva resultatet betyr for anvendelsen av pol § 12.

Pol § 12 omhandler bruk av entydige identifikasjonsmidler. Fødselsnummer er det mest typiske, og er også nevnt spesifikt. Spørsmålet her er hvorvidt biometriske data faller inn i

[51] PVN-2006-10, avsnitt 6.3.

[52] Schartum & Bygrave (2008) s. 41.

denne kategorien og hvilke konsekvenser det medfører for adgangen til å bruke biometriske adgangskontrollsystemer.

Personopplysningsloven § 12 første ledd lyder:
”Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.”

Det er tre hovedtolkningsmoment i § 12 første ledd. De er ”entydig identifikasjonsmiddel”, ”saklig behov” og ”nødvendig for å oppnå slik identifisering”. Drøftelse av momentene følger i avsnitt 4.3.2.2 og 4.3.2.3.

Forarbeidene, Ot.prp.nr. 92 (1998-99) s. 114 første spalte legger følgende føringer for tolkningen av § 12:

”Bestemmelsen gir en generell regulering av bruk av fødselsnummer og andre entydige identifikasjonsmidler som for eksempel fingeravtrykk og andre biometriske data. Slike identifikasjonsmidler bør ikke benyttes i utrengsmål.”

Videre sies det at
”Kravet til nødvendighet i første ledd vil bare være oppfylt dersom andre og mindre sikre identifikasjonsmidler, som for eksempel navn, adresse og kundenummer ikke er tilstrekkelig. Det vil også ha betydning hvor viktig sikker identifisering er for den registrerte, det vil si hvilke konsekvenser en forveksling kan føre til.”

I NOU 1997: 19 s. 141 ble det lagt avgjørende vekt på samfunnets behov, samt den *behandlingsansvarliges* behov, i motsetning til lovproposisjonen som bare fremhevet samfunnets behov. Lovproposisjonen viste videre til betydningen av nøyaktighet for den *registrerte*, ikke for den som registrerer. Av det kan man slutte at ved anvendelse på en gitt kon-

flikt vil hensynet til den enkeltes personvern veie tyngre enn den enkelte bedrifts autentiseringsbehov.[53]

Personopplysningsloven gir i § 12 andre ledd Datatilsynet kompetanse til å pålegge bruk av slike entydige identifikasjonsmidler. Datatilsynets kompetanse etter ovennevnte § er også et resultat av lovgivers vilje til å beskytte den som blir registrert. Dersom det er viktig å unngå forveksling mellom ansatte, for de ansattes del, foreligger grunnlag for at Datatilsynet kan pålegge strengere kontroll.

Hensynet til den registrerte medfører at spørsmålet om behov for entydig identifisering trolig må presiseres til et spørsmål om behovet for å unngå muligheten for personforveksling, innenfor området for relativt nøyaktig identifisering. En slik forståelse peker i retning av risikovurdering i samsvar med § 2-4 i personopplysningsforskriften[54]. I så tilfelle vil spørsmålet av hvor nøyaktig identifiseringen bør være avhenge av en vurdering av hvor alvorlige negative følger en forveksling av personer vil kunne medføre for personvernet for den enkelte.[55] Jeg kommer ytterligere inn på tolkningsmomentene ”entydig identifikasjonsmiddel” og ”saklig behov” nedenfor.

I motsetning til behandlingsansvarliges behov som er utelatt i lovproposisjonen, så nevnes hensynet til samfunnets behov spesielt. Dersom den aktuelle bedriftens autentiseringsbehov speiler et større samfunnsmessig behov, vil dette hensynet nok ha betydelig større vekt i en skjønnsmessig avveiing. PVN-2006-7 Tysvær kommune uttrykker nemnda forståelse for kommunens autentiseringsbehov sett i lys av hva de søker å beskytte; opplysninger om tredjepart. Selv om de personvernmessige følgene er små kan det derfor forsvares å anslå autentiseringsbehovet som stort dersom uriktig identifisering kan følge til helseskader eller

---

[53] En alternativ slutning er at lovgiver anser behandlingsansvarliges og samfunnets behov som sammenfallende, og dermed ikke så behov for å skille mellom dem i lovproposisjonen.
[54] Det vil føre for langt i forhold til rammene for denne fremstillingen å gå videre inn på nevnte risikovurdering. Se Schartum & Bygrave (2008) s. 34 flg. for inngående drøftelse.
[55] Schartum & Bygrave (2008) s. 33.

store økonomiske tap i tillegg til de negative personvernmessige følgene.[56] Dette er et eksempel på et samfunnsmessig behov for beskyttelse, ivaretatt av en bedrifts økte adgangskontroll.

Et potensielt problem med dette scenariet er at hysteri i befolkningen, på bakgrunn av eksempelvis terror eller oppblomstring av internasjonal kriminalitet, kan medføre endringer i hva som anses som ”viktig nok” til å kvalifisere for strengere kontroll. Faren er at aksepten for økt kontroll kan eskalere uten at de totale konsekvensene blir tatt i betraktning.

4.3.2.2 Er fingeravtrykk et ”entydig identifikasjonsmiddel”?

Utgangspunktet for drøftelsen er spørsmålet:
Hva ligger i definisjonen av ”entydig identifikasjonsmiddel”?

Datatilsynet og personvernnemnda tolker pol § 12 svært forskjellig. Dette er et hovedpoeng i denne fremstillingen. Personvernnemndas klagevedtak viser en gjennomgående bokstavtro tolkning av pol § 12 fra Datatilsynets side. Det anføres at ” ... Datatilsynet finner at ordet ”identifisering” skal tolkes strengt, slik at bruken av entydige identifikasjonsmidler som legitimasjon eller i tilknytning til verifisering av identitet/autentisering ikke er tillatt.”[57] Denne anførselen er representativ for tilsynets andre anførsler i saker vedrørende pol § 12. Datatilsynet legger videre avgjørende vekt på forarbeidenes uttalelse om at entydige identifikasjonsmidler ikke skal brukes i utrengsmål. Etter tilsynets mening følger det av denne uttalelsen at nøyaktighetsvurderingen bør være streng. Jeg kommer tilbake til nevnte nøyaktighetsvurdering i avsnitt 4.3.2.3.

Personvernnemnda har tatt skritt for å forsøke å manøvrere noe mer pragmatisk gjennom anvendelsen av pol § 12, uten åpenlyst å krenke personopplysningsloven. Reguleringen er

[56] Schartum & Bygrave (2008) s. 34.

[57] PVN-2006-8, avsnitt 5.

helt klart for knapp, hvilket både Datatilsynet og Personvernnemnda har gitt sterkt uttrykk for. En vurdering av revisjonsforslagene følger i avsnitt 5 flg.

Personvernnemnda har tatt stilling til innholdet i "entydig identifikasjonsmiddel" i flere klagevedtak. Deriblant i PVN-2006-7 Tysvær kommune.[58] Dette klagevedtaket er særlig egnet til å illustrere et sentralt moment i tolkningen av pol § 12. Avgjørelsen er avgjort enstemmig, men med en særmerknad fra et mindretall på to av medlemmene vedrørende vektingen av forarbeidsuttalelsen i Ot.prp.nr. 92 (1998-1999) side 114, første spalte (sitert over).

To medlemmer av nemnda uttrykte skepsis til hvorvidt det er ønskelig å regulere fødselsnummer og fingeravtrykk på samme måte, særlig når dette bare har grunnlag i en enkelt setning i forarbeidene uten nærmere utredning av konsekvenser.[59] I særmerknaden ble det uttrykt at mindretallet[60] kom til at forarbeidene ikke bør vektes like tungt som flertallet kom til. De begrunnet sitt avvikende syn på vektlegging med at

"... det er uheldig å låse lovtolkningen på grunnlag av en kort bemerkning i lovforarbeidene, som åpenbart ikke er bygget på en nærmere vurdering av hvilke ulike måter fingeravtrykk kan brukes på og som derfor framstår som svært summarisk og lite nyansert."

Mindretallet antok at meningen bak lovgivers uttalelse i forarbeidene er at likhetstegnet mellom fødselsnummer og fingeravtrykk er situasjonsavhengig. Altså at "... forfatteren ... har siktet til situasjoner hvor fingeravtrykk benyttes på en måte som har likhetstrekk med den måte fødselsnummer benyttes på, og hvor man altså teoretisk kunne velge mellom å bruke det ene eller det andre." Da den foreliggende saken gjaldt autentisering ved pålogg mente mindretallet på bakgrunn av ovennevnte tolkning, at pol § 12 ikke er ment å skulle

---

[58] Se PVN-2006-7 punkt 7.5.1.

[59] PVN-2006-7 avsnitt 7.5.1.

[60] Se PVN-2006-7 avsnitt 7.5.1 siste del.

regulere slike situasjoner. Biometriske metoder til bruk for identifikasjon eller autentisering har vært i sterk utvikling siden loven ble vedtatt. Nye systemer lanseres og nøyaktigheten hevdes økt ved forbedret teknologi. Samme særmerknad er også tatt inn i nemndas klagevedtak PVN-2006-10 Esso Norge, avsnitt 6.3.

Men klager ble altså gitt medhold i begge avgjørelser på tross av ovennevnte særmerknad. Personvernnemnda la også vekt på kravet til saklig behov og nødvendighetskravet i sin endelige avgjørelse av saken. Jeg belyser disse kravene nedenfor.

Forarbeidene[61] sier eksplisitt at fingeravtrykk (og andre biometriske data) er å anse som entydige identifikasjonsmidler på lik linje med fødselsnummer. Personvernnemnda har lagt vekt på forarbeidene i sin behandling av spørsmålet. Derimot er nemnda også av den oppfatning at det er viktig å være klar over de store forskjellene på de to.

Den videre fremstillingen vil veksle mellom vurderingen av situasjonsavhengigheten (altså hvorvidt informasjonen skal brukes til identifisering eller autentisering) og forholdet mellom fødselsnummer og fingeravtrykk (og andre biometriske data, jf. forarbeidene).

Av klagevedtakene for Personvernnemnda fremgår det at slik nemnda ser det, sikter loven til noe mer enn at identifikasjonen er entydig i det enkelte tilfelle, overfor det enkelte system. Det er klart at en identifikasjon må være entydig innenfor systemets rammer, ellers vil den ikke kunne benyttes til å oppnå det ønskede formål. I denne forstand vil for eksempel en kundeidentifikasjon (KID) også være entydig innenfor det aktuelle systemet for de aktuelle kunder. Når loven krever at identifikasjonsmiddelet må være entydig, kreves det altså noe *mer*.

Personvernnemnda har behandlet flere saker av denne typen. Den sentrale problemstillingen er i all hovedsak relativt lik, og går ut på hvorvidt vilkårene i pol § 12 er oppfylt i den

[61] Ot.prp.nr. 92, kommentar til § 12.

enkelte sak. Personvernnemnda har, ved tolkningen av termen ”identifikasjonsmiddel”, i flere avgjørelser[62] gjort det klart at de”... legger til grunn at loven må tolkes slik at identifikasjonsmiddelet må være egnet til bruk som identifikasjon i *flere* systemer.” Nedenfor følger en kort gjennomgang av egenskapene som et fødselsnummer innehar og forskjeller og likheter mellom fødselsnummer og et fingeravtrykk.

Fødselsnummer

Fødselsnummer nevnes spesifikt i § 12. Det er et entydig nummer som tildeles alle som blir norske statsborgere (enten de fødes her eller kommer hit senere). Nummeret kan brukes til oppslag i ett system, men også til samkjøring av flere systemer som bruker fødselsnummeret. Den restriktive bruken av fødselsnummer har nok historisk sett størst tilknytning til den siste bruken, samkjøring av systemer. Fødselsdato og personnummer, som til sammen utgjør fødselsnummer, blir ofte utlevert fra folkeregisteret til personer, private institusjoner og offentlige myndigheter. Et stort antall forvaltningsorganer og private organisasjoner innhenter fødselsnumre. Fødselsnummeret er normalt heller ikke underlagt taushetsplikt i slike situasjoner. Det ligger utenfor denne oppgavens rammer å ytterligere kommentere den generelle historie og regler rundt fødselsnummer.[63]

Fødselsnummeret er svært egnet som ”nøkkel” [64] i et system i kraft av å være unikt for det enkelte individ, og vil i denne forstand være et entydig identifikasjonsmiddel fordi det kan gjenfinne informasjon i flere ulike systemer. Fingeravtrykk vil også være et entydig identifikasjonsmiddel i denne forstand fordi samme avtrykk kan brukes til å få tilgang til flere system.

Det er et sentralt moment at nemnda direkte uttaler at de tolker loven dit hen at det ikke nødvendigvis bare er bruk av selve fødselsnummeret som kvalifiserer det som ”entydig

---

[62] Se eksempelvis PVN-2006-8 avsnitt 6.3 eller PVN-2006-7 avsnitt 7.5.1.

[63] Se Schartum & Bygrave (2008) avsnitt 2.5 flg. for en noe mer inngående fremstilling.

[64] Se videre drøftelse om begrepet ”nøkkel” i et kommende avsnitt.

identifikasjonsmiddel". Fingeravtrykket konverteres i de fleste tilfeller til en template som så brukes i kontroll. Selve bildet av fingeravtrykket er ikke det som systemet lagrer og bruker. Likeledes kan også fødselsnummeret behandles av et system slik at systemet selv bruker (og viser) et kryptert eller pseudonymisert nummer. Dermed kan et fødselsnummer også brukes til kontroll uten av det faktiske nummeret blir lagret eller brukt.

I PVN-2006-10 Esso Norge uttrykker to av nemndas medlemmer i en særmerknad en motforestilling mot å kunne oppfatte biometriske templater som entydige identifikasjonsmidler. Medlemmene legger vekt på at det ikke er"... mulig å etablere noen en-til-en-relasjon mellom en fysisk person og en template."[65] I tillegg bemerkes at fingeravtrykket som sådan verken samles inn eller registreres i prosedyren for å utarbeide en template. Etter mindretallets mening medfører dette at Personopplysningsloven § 2 ikke kommer til anvendelse, da det ikke foretas noen behandling etter lovens definisjon. Selv om dette synspunktet ikke fører frem i forhold til nemndas avgjørende syn på betydningen av at de biometriske mønstrene blir redusert til en template, er innvendingen likevel relevant som moment i forhold til definering av begrepet identifikasjonsmiddel, og bør tas med i en vurdering av behovet for ytterlig regulering av rettsområdet.

Personvernnemnda har gjort det klart at den forstår loven dit hen at den med "identifikasjonsmiddel" sikter til hva brukeren presenterer til systemet. Altså et fingeravtrykk (som så behandles av systemets adgangskontroll) eller et fødselsnummer (som også eksempelvis kan krypteres). Fingeravtrykket vil kunne brukes til å få tilgang til flere systemer, mens de ulike systemene i praksis vil konverterte det avleste avtrykket til ulike templater. Dette forhindrer ikke at fingeravtrykket anses som et "entydig identifikasjonsmiddel" i lovens forstand.[66] En template av biometriske mønstre, eksempelvis iris eller fingeravtrykk, oppfyller dermed lovens krav til entydighet.

---

[65] PVN-2006-10 punkt 6.3, siste avsnitt.

[66] Se PVN-2006-7 punkt 7.5.1.

Termen ”identifikasjonsmiddel” kan lett tolkes dit hen at den innebærer krav til at brukeren identifiseres, jf. definisjon av biometrisk kjennetegn samt kommunens tolkning referert over. Derimot er ikke dette eneste mulige tolkning av begrepet. Personvernnemnda uttaler i PVN-2006-7 at termen identifikasjonsmiddel kan tolkes på to måter:
”...For det første kan et identifikasjonsmiddel være ”noe” som brukes for å gjenfinne opplysninger om én enkelt, på forhånd kjent person i en stor mengde med data, typisk en database.” Dette ”noe” vil i en database være kjent som en ”nøkkel”.
”For det annet kan et identifikasjonsmiddel benyttes til autentisering etter at identifiseringen har funnet sted.”

I en database vil det, som nevnt over, være en ”nøkkel”. Denne nøkkelen vil måtte være entydig, ellers vil opplysninger om flere personer kunne forveksles. Fødselsnummer er en slik entydig identifikasjonsnøkkel, og bruk av denne vil medføre en identifisering av brukeren. Det er klart at slik bruk faller inn under § 12 etter kun tolkning av ordlyden. Basert på drøftelsen over er det også klart at en biometrisk template også er en entydig identifikasjonsnøkkel.

Identifisering og autentisering
Av klagevedtakene fra PVN er det videre naturlig å slutte at termen identifikasjonsmiddel kan brukes om både identifisering og autentisering, jf. drøftelsen over. Pol § 12 er hjemmel for begge former for behandling av personopplysninger. Anførslene hvor det hevdes at pol § 12 ikke er hjemmel for regulering av autentiseringssystemer førte altså ikke frem.

Når det gjelder autentisering er det viktig at man sørger for at sannsynligheten for korrekt identitet er høy, i alle fall høyere enn den man får ved bruk av navn og fødselsdato. Registreres gal person i utgangspunktet, vil ikke autentiseringsprosessen medføre riktighet selv om det brukes biometri.

Som vist i avsnitt 2.2.2.2 er fingeravtrykk en personlig egenskap, en biometrisk egenskap som er unik for hvert individ. Bruk av fingeravtrykk vil først og fremst være nyttig for å

bestemme om en person, ved gjentatt bruk av et system, er den samme personen som i utgangspunktet registrerte seg i systemet med fingeravtrykket sitt.

Datatilsynet er av den oppfatning at ordet ”identifisering” skal tolkes strengt, slik at bruken av entydige identifikasjonsmidler som legitimasjon eller i tilknytning til autentisering ikke er tillatt, i tråd med tilsynets bokstavtro tolkningslinje.

Flertallet i Personvernnemnda uttrykte i sin avgjørelse (PVN-2006-7) sitt standpunkt i forhold til tolkningen av begrepet:

”Et annet hovedformål med personopplysningsloven § 12 er å unngå at fødselsnummer brukes til noe mer enn identifikasjon. I en typisk situasjon hvor en bruker søker tilgang til et system, vil brukeren først *identifisere* seg med et brukernavn, en brukerkonto eller lignende, deretter vil brukeren måtte *autentisere* denne ”påstanden”, noe som typisk gjøres ved et passord, en PIN-kode, et magnetstripekort mv som bekrefter identiteten ved sammenligning med forhåndslagrede opplysninger. Fødselsnummeret vil være velegnet til identifikasjon, men er helt uegnet til autentisering (legitimasjon). Fingeravtrykket kan derimot brukes til begge deler.”

I ovennevnte avgjørelse (PVN-2006-7 Tysvær kommune), anførte kommunen at deres bruk av fingeravtrykk kun var autentisering, ikke identifisering, og at den derfor ikke falt inn under pol §12. Selv om nemnda kom til at kommunens anførsel er gal, så ble klager (kommunen) likevel gitt medhold i bruk av biometriske adgangskontrollsystemer. I etterfølgende avgjørelser, som PVN-2006-10 Esso Norge, har klager gått bort fra dette argumentet, og fokuset er på formålet for bruk av biometri i den enkelte bedrift. I sistnevnte klagevedtak uttalte nemnda at personopplysningsloven § 12 dekker både identifisering og autentisering basert på to momenter. For det første at nemnda selv har kommet til at fingeravtrykk faller inn under pol § 12 for identifiseringsbehov og for det andre fordi autentisering er en bruk

som omfattes av sikker[67] identifisering, jf. saklighetskravet som behandles nedenfor. De to fasene som inngår i etableringen av en høy nøyaktighet for korrekt identitet er deler av et samlet system, og det er derfor nødvendig å se hele systemet samlet i vurderingen av de to siste momentene i pol § 12, saklighetskravet og nøyaktighetsvilkåret.[68]

Personvernnemnda har lagt stor vekt på hvorvidt ønsket identifisering kan oppnås uten bruk av så store inngrep i en persons identitet som midlene regulert av pol § 12 i realiteten er. Derimot er de som tidligere nevnt mer pragmatiske i sin tilnærming til pol § 12 enn Datatilsynet, og dermed også mer nyanserte i sin vurdering av nødvendighetsvilkåret. Jeg kommer nærmere inn på dette tema nedenfor.

Både Datatilsynet og Personvernnemnda har gitt klart uttrykk for at det er et stort behov for lovendring for bedre å kunne regulere bruk av biometriske kontrollsystemer. Det er nødvendig å tilpasse kartet til terrenget, ellers er det svært vanskelig å komme i mål. Personvernnemndas uvanlig klare rettspolitiske uttalelse i PVN-2006-7 Tysvær kommune[69], sammen med Datatilsynets forslag om særlig regulering av biometriske metoder, er blant annet grunnlag for Schartum & Bygraves nye utredning for Justisdepartementet. Jeg kommer tilbake til dette temaet i avsnitt 5.

---

[67] Jeg går, som nevnt, ikke inn på tolkningen av termen ”sikkerhet”, men bruker kun nemndas ordbruk i sitatet.

[68] Behandles i avsnitt 4.3.2.3.

[69] PVN-2006-7 avsnitt 7.5.1: "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."

4.3.2.3 Foreligger det "saklig behov", og er metoden "nødvendig for å oppnå slik identifisering"?

Personopplysningsloven åpner for at man kan bruke entydige identifikasjonsmidler hvis særlige forhold foreligger, jf. § 12 andre ledd. Datatilsynet gis kompetanse til å pålegge slik bruk.

Datatilsynet har uttalt at ved barnehageopptaksprosessen bør barnets fødselsnummer brukes fordi faren for forveksling av barna er spesielt stor og konsekvensene av en forveksling vil kunne være svært uheldige. Identifiseringsbehovet ligger her hos den registrerte. Dette behovet er vektlagt i forarbeidene, jf. NOU 1997: 19 s. 141. I nevnte kommentar til bestemmelsen uttaler lovgiver videre at

"Annet ledd gir Datatilsynet kompetanse til å bestemme at fødselsnummer skal brukes for å sikre tilstrekkelig kvalitet på personopplysninger. Dette bygger på en oppfatning om at personvernet i mange sammenhenger er tjent med at det er sikkerhet mht hvilke personer de aktuelle opplysningene knytter seg til, jf utvalgets vurderinger i 12.5.7[70]. Kravet til tilstrekkelig kvalitet omfatter blant annet oppdaterthet og at personopplysningene er dekkende."

Saklig behov

I saken om Tysvær kommune (PVN-2006-7) skulle identifiseringen skje av gitte brukere for å få tilgang til egne, bærbare datamaskiner. På disse maskinene lagres opplysninger blant annet om tredjeparter, for eksempel klienter for sosial- eller helsetjenesten. Et svært vesentlig tolkningsmoment er det faktum at fingeravtrykkspålogging skulle skje av hensyn til klientenes behov for konfidensialitet, ikke behandlingsansvarliges. Personvernnemnda la vesentlig vekt på dette momentet og kom til at det for dem sto rimelig klart at i slike tilfeller foreligger et saklig autentiseringsbehov.

[70] Omtalte vurderinger blir ikke behandlet i denne fremstillingen.

Av nemndas avgjørelse i denne saken kan man slutte at kravet til ”saklig behov” kan oppfylles flere måter. Hensyn til den registrerte er utgangspunktet, men også hensyn til tredjeparter kan kvalifisere. Forarbeidene støtter denne tolkning, som referert over kan *også samfunnets behov ... tillegges vekt.* Men i alle tolkninger må man foreta en interesseavveiing basert på faktum i den enkelte sak, så noen klar regel for hva som er ”nok” kan ikke utledes fra avgjørelsen. Den gir derimot et bilde av hvordan lignende saker bør løses og dermed også en idé om hvilke situasjoner som nok ikke kvalifiserer. Nemndas uttalelser viser at behovet for ytterligere rettslig regulering av problematikken rundt saklig behov er stort.

Vilkårene i § 12 er kumulative. Dersom man kommer til at det foreligger saklig behov for sterk grad av nøyaktighet ved autentisering må likevel kravet til nødvendighet oppfylles for at bruk av biometriske adgangskontrollsystemer skal kunne godtas.

Nødvendighetsvilkåret

For å kunne anvende biometriske data for pålogg krever forarbeidene som tidligere nevnt at det ikke kan tas i bruk et kontrollsystem som *ikke* forutsetter bruk av entydig identifikasjonsmiddel, men som gir samme oppfyllelse av bedriftens formål og behov for adgangskontroll.

Etter forarbeidene skal ikke bruk av entydige identifikasjonsmidler tillates dersom *andre og mindre sikre identifikasjonsmidler, som for eksempel navn, adresse og kundenummer* er tilstrekkelig. Datatilsynet har ved flere anledninger, deriblant PVN-2006-7, ment at tilfredstillende nøyaktig registrering kan oppnås ved bruk av andre autentiseringsmidler, eksempelvis (som i nevnte klagevedtak) ved bruk av smartkort kombinert med passord. Utgangspunktet for vurderingen er med andre ord et visst intervall for akseptabel risiko for feil identifisering, sammenholdt med en anslått/beregnet risiko for samme. Dersom den anslåtte risikoen er større enn den akseptable risikoen, oppstår spørsmålet om bruk av fød-

selsnummer eller andre entydige identifikasjonsmidler er nødvendige for å sikre et akseptabelt nøyaktighetsnivå.[71]

En vurdering av samtlige andre tiltak og virkemidler (som ikke innebærer bruk av like inngripende midler som fødselsnummer representerer) må foretas for å slutte hvorvidt nødvendighetsvilkåret er oppfylt eller ikke. Effekten av alle tilgjengelige tekniske, fysiske, organisatoriske, pedagogiske[72] virkemidler må vurderes. Dersom slike andre virkemidler bringer risiko for identitetsforveksling eller liknende ned til et akseptabelt nivå, er de svært inngripende virkemidlene (som fingeravtrykk) ikke nødvendige å bruke, og kravet i § 12 er ikke tilfredsstilt.[73]

Datatilsynet har (som vist tidligere) lagt en svært bokstavelig tolkning av loven og forarbeidene til grunn for sine anførsler i sakene for Personvernnemnda. I PVN-2006-10 anfører tilsynet at tilstrekkelig trygghet i forhold til uvedkommendes adgang til et tankanlegg ville oppnås gjennom andre midler enn biometrisk adgangskontroll. Nemnda sa seg ikke enig i Datatilsynets vurdering og la vekt på hensynet til tredjepersons[74] helse og velferd som en bakgrunn for bedriftens autentiseringsbehov. I avgjørelsene PVN-2006-11 REMA 1000 og PVN-2006-8 har bedriftene et formål med bruk av biometriske systemer som innebærer en overvåkning av de ansatte og besøkende. Et slikt formål kvalifiserer ikke til å oppfylle kravene i pol § 12 etter gjeldende rett.

Personvernnemnda har derimot (som i avgjørelsen over) gitt klart uttrykk for at eksempelvis hensynet til tredjepart veier tilstrekkelig tungt til at det i slike tilfeller ikke vil være tilstrekkelig med bruk av for eksempel et brukernavn kombinert med et passord. Selv om

---

[71] Schartum & Bygrave (2008) s. 36.

[72] Listen er ikke uttømmende.

[73] Schartum & Bygrave (2008) s. 36.

[74] PVN-2006-10 avsnitt 6.4: ”Dette er både i sjåførenes, de ansattes, arbeidsgivers og samfunnets interesse.”

disse midlene rent teoretisk har en tilfredstillende sikkerhet, bygger dette på en forutsetning om at ikke andre enn den autoriserte blir kjent med passordet. Brukernavn vil ofte være kjent, det maskeres ikke ved inntasting, og vil ofte være identisk med en persons navn, initialer eller andre vanlige forkortelser. Erfaring viser at brukere ikke stoler på sin egen evne til å huske passord, og derfor ofte gjør notater hvor passordet angis.[75] Nemnda viser videre til praksis fra blant annet Bankklagenemnda som gir et rikt materiale med eksempler på hvordan brukere har oppbevart PIN-koden for bankkort slik at uvedkommende har fått tilgang til passord. Et ytterligere moment i vurderingen av hvorvidt passord er tilstrekkelig som kontrollmiddel er at passord har den egenskap at hvis de først er kompromittert, vil de gi en ikke-autorisert tilgang inntil passord endres. I nevnte klagevedtak viser nemnda til at ved bruk av bærbare maskiner er det nærliggende at en bruker vil falle for fristelsen til for eksempel å gi en annen i familien tilgang til maskinen for eget bruk i en situasjon hvor dette fremstår som viktig. Da vil det foreligge en kompromittering av sikkerheten inntil en autorisert bruker tar initiativ til å endre passordet.[76]

Hensynet til brukers personvern veier tungt i norsk rett og forarbeidene til pol viser nettopp dette. Nødvendighetskravet er strengt i pol § 12, jfr forarbeidene, og det er nok av eksempler på avgjørelser hvor Personvernnemnda ikke anser biometri som nødvendig for å oppfylle bedrifters behov for kontroll, eksempelvis PVN-2006-9. Etter forarbeidene kreves det mer enn at den biometriske løsningen vil være en god løsning på bedriftens kontrollbehov. Det må i tillegg ikke kunne tas i bruk en løsning som *ikke* forutsetter bruk av et entydig identifikasjonsmiddel, og som gir samme grad av nøyaktighet ved autentisering.[77]

Et problem med bruk av kort, eksempelvis slikt smartkort som Datatilsynet har anført at ville *medføre tilstrekkelig grad av sikkerhet* er at smartkortet er et påloggingsmiddel som kan gjenglemmes eller fratas den autoriserte brukeren. Selv om smartkortet også kan, etter

---

[75] Se PVN-2006-7 avsnitt 7.5.2.

[76] Se PVN-2006-7 avsnitt 7.5.2.

[77] PVN-2006-9, avsnitt 6.4.

Personvernnemndas mening, kvalifisere til entydig identifikasjonsmiddel hvis det benyttes for å få tilgang til mer enn ett system, er det i tilfeller hvor området for pålogg ikke er et kontrollert område for stor fare for å glemme kortet, miste det eller bli fratatt det av uvedkommende. Pålogg på eksempelvis bærbare maskiner innebærer slik flytting av område også utenfor arbeidsplassen.

De momentene som er behandlet over er sentrale i Personvernnemndas vurderinger av alternative løsninger for adgangskontroll. I tillegg behandler nemnda spørsmålet om samtykke og frivillighet i endel av sine klagevedtak. Jeg kommer tilbake til denne problematikken i avsnitt 4.3.2.4.

Kort oppsummert er nødvendighetsvilkåret i utgangspunktet avhengig av en vurdering av personvernmessige konsekvenser i forhold til risikonivået til bedriften. Forutsetningen for å kunne benytte entydige identifikasjonsmidler er da at disse er nødvendige for å oppnå et akseptabelt risikonivå, dvs en akseptabel risiko for personforveksling eller liknende. Hensynet til samfunnets behov kan også tillegges vekt, jf. forarbeidene. Dersom (nesten) enhver risiko for slik forveksling er uakseptabel (ut i fra en personvernmessig, eventuelt samfunnsmessig vurdering), vil det være nødvendig å benytte entydige identifikasjonsmidler, og slik bruk vil også være tillatt - og kanskje også påbudt.[78] Kravet til saklig behov for sikker identifisering byr ikke på tvil i noen av sakene, og alle saker er derfor avgjort ut i fra nødvendighetskriteriet i pol § 12. Det er vanskelig å konkludere med at Personvernnemnda har lagt klare generelle retningslinjer for hvorledes spørsmålet om nødvendighet skal vurderes, da klagevedtakene ikke kan sies å legge opp til en generell vurdering. Nødvendighetsvurderingen må derfor fremdeles - generelt sett - sies å være svært åpen og skjønnsmessig, og utenfor de sakstyper som er behandlet, kan det ikke sies å være stor forutberegnelighet. Likevel er flere av de avgjorte sakene svært like hverandre, og innen sakstypen er det lett å identifisere en konsekvent praksis.[79]

---

[78] Schartum & Bygrave (2008) s. 36.

[79] Schartum & Bygrave (2008) s. 43.

4.3.2.4 Hva betyr PVN-praksis for arbeidstakere?

For å kunne behandle personopplysninger, uansett type, må grunnkravene i Pol § 11 første ledd bokstav a jf. § 8, oppfylles, som jeg tidligere har nevnt. I tilfellet hvor biometri brukes for å kontrollere ansatte kan det hevdes at samtykke er innhentet ved at påloggingsteknologien er frivillig. De ansatte avgir fingeravtrykket frivillig, de gjør dette selv ved førstegangs pålogging på maskinen og det er mulig å velge teknologien vekk. Vilkåret i Pol § 8 første ledd vil dermed være oppfylt. Dette er et fint resonnement i teorien, men i praksis vil nok begrepet ”frivillig” har et noe annet innhold enn det rent språklige. På en arbeidsplass er det stor sjanse for at det benyttes såkalt ”frivillig tvang” for å gjennomføre tiltak som eksempelvis biometriske adgangskontrollsystemer. Det er ikke gitt at man, kanskje som eneste ansatte, står imot bedriftens krav om biometrisk registrering uten å bli stemplet som vanskelig. Selv om det i teorien er presentert et alternativ til biometri så betyr ikke det at det alternativet faktisk representerer et reelt valg for den ansatte. Jeg forutsetter i den videre bruk av termen ”frivillig” at det er snakk om faktisk frivillighet, ikke frivillig tvang.

Det er, som nevnt tidligere, slått fast i forarbeidene at dersom det er mulig å unngå bruk av biometriske adgangskontrollsystemer (entydige identifikasjonsmidler) så skal de unngås i all hovedsak. Eventuelt manglende samtykke vil kunne medføre at nødvendighetskravet ikke anses oppfylt. Dersom det er et alternativ som ikke innebærer bruk av biometri, og det er et reelt alternativ, vil man kunne argumentere med at det jo ikke kan være *nødvendig* med biometrisk adgangskontroll for å oppnå autentiseringsformålet til bedriften. Dette synspunktet deles av (i alle fall) ett medlem i Personvernnemnda, som uttalte i en særmerknad i PVN-2006-10 avsnitt 6.4 at ”så lenge det er mulig for ... ansatte å la være å samtykke til bruk av fingeravtrykkleser, jf. Personopplysningsloven § 2 nr 7, kan det ikke logisk sies å være nødvendig med bruk av denne metoden (les: biometrisk adgangskontrollsystem) for å oppnå sikker[80] identifisering, jf. Personopplysningsloven § 12.”

[80] Jeg siterer medlemmet i Personvernnemnda, og går fortsatt ikke inn på en drøftelse av begrepet sikkerhet, jf. note 65.

Uttalelsene fra forarbeidene korresponderer ikke med uttalelser i avgjørelser av Personvernnemnda. Nemnda har uttalt at det i spesielle tilfeller vil være tilstrekkelig å bygge på samtykke. I PVN-2005-6 har den uttalt seg generelt om samtykke fra arbeidstaker som behandlingsgrunn. Nemnda legger der til grunn at hovedregelen vil være at samtykke ikke kan være en tilfredsstillende behandlingsgrunn etter personopplysningsloven § 8 første alternativ. Imidlertid utelukket den ikke at det kan være spesielle situasjoner der man kan bygge på samtykke. Eksempelvis i ansettelsesforhold hvor det er mulig å velge bort teknologien uten at det vil få negative følger for arbeidsforholdet.[81] Altså gjør nemnda et stort poeng av at kontrollen kan utføres tilfredstillende *uten* bruk av biometri, og at det faktum innebærer at bedriften får adgang til å benytte en strengere form for kontroll *med* bruk av biometri. Dette er lite logisk, jf. omtalte særmerknad i PVN-2006-10 Esso Norge.

Problematikken rundt samtykke og nødvendighetskravet er vanskelig regulert og er, som vist over, hovedkilden til dagens "floker" i Datatilsynets og Personvernnemndas praksis. Kort oppsummert kan problemet belyses som følger:
Dersom det foreligger samtykke, er forholdet greit i forhold til pol § 8. Men samtykke medfører ikke at vilkårene i pol § 12 er oppfylt. Bestemmelsen kommer inn som et tilleggshinder for anvendelsen av pol § 8; samtykke er ikke nok; det kreves nødvendighet uansett. Dersom det derimot ikke foreligger samtykke må nødvendighetskravet også oppfylles for at bruk av biometri skal være lovlig etter pol § 8.

I tillegg til den ufullstendige reguleringen av pol §§ 12 og 8 bemerker jeg kort at Datatilsynet har presentert ennå ett regelsett som krever revisjon. Tilsynet har uttalt i sitt revisjonsnotat til pol § 12 at det råder stor usikkerhet blant de behandlingsansvarlige med hensyn til hvorvidt 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

[81] Se PVN-2006-7 avsnitt 7.2.

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 som det er fare for at Datatilsynet går glipp av viktige opplysninger om bruk av biometriske løsninger. Bakgrunnen for den siste uttalelsen er at de behandlingsansvarlige i de andre tilfellene (enn de som ønsker å være på sikre siden) ikke er kjent med at bruken er meldepliktig, eller fordi bruken er omfattet av et av de mange unntakene i forskriften.[82]

Betydningen av dagens regelverk for arbeidstakerer kan oppsummeres som forvirrende og lite oversiktlig med stor margin for at det benyttes strengere kontroll enn bedriften har konsesjon for. Det er liten sjanse for at de berørte arbeidstakere kan klare å skaffe seg nok oversikt over rettighetene sine til å kunne protestere mot bedriftens kontrolltiltak. Bruksområdene for biometriske adgangskontrollsystemer er som nevnt i stor vekst, og det er viktig at lovgiver tar stilling til de problemstillingene som har presentert seg gjennom praksis og undersøkelser slik at den rettslige reguleringen er tilpasset de ulike scenariene i samfunnet.

4.3.2.5 Undersøkelser vedrørende bruk av kontrollsystemer.

Det er gjort flere undersøkelser vedrørende bruk av biometriske adgangskontrollsystemer, og de ulike aspektene av slik kontroll. Deriblant en undersøkelse utført som en del av Hitachi Data Systems Storage Index. Den ble basert på 840 anonyme intervju i en rekke land, deriblant Norge. De fleste bedriftene holdt til i Europa. Det kom frem at de fleste bedrifter vurderer å implementere biometrisk teknologi for å øke det interne sikkerhetsnivået.

Omtrent 55 % av bedriftene vurderer å innføre systemer som kan gjenkjenne en ansatt basert på skanning av iris eller fingeravtrykk. Holdningen til biometrisk teknologi ser ut til å

[82] Datatilsynets revisjonsnotat (2006) s. 13.

bli stadig mer åpen ettersom både ledelse og de ansette innser fordelene med økt sikkerhet.[83]

Den samme undersøkelsen indikerer også at færre enn en av fem biometriske kontrollanordninger er forventet å være operative i løpet av de neste tolv månedene. Bekymringer vedrørende feil i det tekniske og sikkerhetsbrudd medfører at de fleste planlagte implementeringer av denne teknologien blir forsinket i påvente av ny teknologi og nye systemer som beskytter mot slike feil og risiki. Omtrent halvparten av de spurte (51 prosent) indikerte at risikoen for kriminelle handlinger, eksempelvis elektronisk ID-tyveri, er et stort problemfelt for bedrifter som bruker og lagrer biometriske data. Et tilsvarende antall (47 prosent) følte at faren for tekniske problemer, som at ansatte ved feil blir stengt ute av bygninger grunnet feilaktig avvisning (som nevnt tidligere er en risiko) nok er et potensielt stort problemområde.

Personvernundersøkelsen 2008 er viktig i forhold til å etablere en oversikt over hvilke momenter ved kontroll som anses som viktige av befolkningen. Derimot omtales ikke biometriske adgangskontrollsystemer eksplisitt, og jeg velger derfor å ikke gå ytterligere inn i en drøftelse av funnene i undersøkelsen.

[83] Etter artikkel på http://www.hds.com/corporate/press-analyst-center/press-releases/2004/gl040927.html jfr artikkel av Jan Aril Sigvartsen på Hardware.no, publisert 13.10.04.

5 Biometri og personvern – avsluttende rettspolitiske betraktninger

5.1 Hvorfor øker bruken av biometri?

Jeg har i denne oppgaven søkt å belyse de ulike former for biometrisk kontroll og hvilke rettslige vilkår og konsekvenser som finnes på området. I dette avsnittet er fokuset ikke utelukkende på det rettslige, men også på det menneskelige plan.

Det er foretatt flere undersøkelser vedrørende innføring av biometri, både i forhold til bedrifter (som vist i avsnitt 4.3.2.5) og i forhold til personer generelt. Personvernundersøkelsen 2008 gav klart uttrykk for den voksende aksept for biometri i befolkningen. Undersøkelsen viser at 7 av 10 nordmenn støtter innføringen av biometrisk teknologi. Bakgrunnen for aksepten for såpass inngripende kontroll av privatlivet er i følge Steria (en stor aktør innen biometriske løsninger) at oppfatningen i befolkningen er at de tradisjonelle metodene for identifisering og autentisering er for lette å lure (av de med kriminelle hensikter). Terrortruslene de siste årene har økt bevisstheten omkring kontrollsystemers feil og mangler. Samfunnsbildet har endret seg dramatisk, og kunnskapen om teknologien i befolkningen er sterkt voksende. Biometriske kontrollsystemer presenteres imidlertid for befolkningen *uten* fremheving av den eventuelle faren for misbruk av de registrerte data[84], og da er det vanskeligere for folk å foreta en nyansert vurdering av innvirkningen på eget personvern. Behovet for at lovgiver holder personvernhensyn i høysetet ved revisjon av rettsreglene er av denne grunn stort.

5.2 Må personvernet vike for kravene til identifisering og autentisering?

Den beskyttende sfæren rundt de opplysninger hver av oss ønsker å beskytte blir stadig snevrere. I dagens samfunn er det en stor grad av selveksponering. Mange har behov for å dokumentere livet sitt for andre. Når andre tar dette valget for oss, og offentliggjør sider av vårt privatliv som vi ønsker å ha for oss selv, blir situasjonen imidlertid en annen. Det kan

[84] jf. artikkel *Fingeravtrykket – ditt neste bankkort* Pdf publisert på http://www.steria.no/asset/4178/1/4178_1.pdf Oppslag gjort 19.09.08.

være svært ødeleggende når informasjon som legges ut på Internett, misbrukes og benyttes til helt andre formål enn de opprinnelige.[85] Fenomener som Facebook[86], MySpace[87] og YouTube[88] er eksempler på folks eksponeringsbehov, og mangel på nyanserte vurderinger rundt eierforholdet til egne biometriske data. Når noen stjeler en annens identitet og sprer krenkende uttalelser i vedkommendes navn, råder maktesløshet og sinne. Denne formen for identitetstyveri er riktignok viktig å forsøke å stoppe, men poenget er hva man må gi avkall på for å oppnå det.

Bør man være bekymret for utviklingen? Det kan hevdes at dersom man ikke har noe å skjule, så bør man ikke bekymre seg for hvor og hvor ofte man blir registrert. Synspunktet er, slik jeg ser det, for snevert og lite reflektert. Ved bruk av biometri i samfunnet vil potensialet for misbruk stige i tråd med antall bruksmetoder. Det forekommer meg åpenbart at dersom behandlingsansvarlig (eller andre med tilgang til personopplysningene) med enkle grep kan skaffe seg oversikt over ansattes bevegelses- og handlingsmønstre, er faren for misbruk svært nærliggende.

Hvem har tilgang til de biometriske dataene om arbeidstakerne?
Det er viktig at de rettslige reguleringene av lagringsenheter gjenspeiler prinsippet om at enhver eier sine egne personopplysninger i Norge, jf. integritetsprinsippet omtalt i avsnitt 1.3. Dersom adgangen til bruk av sentrale lagringsenheter er kraftig skjerpet vil det være et steg i riktig retning i forhold til å begrense risikoen for misbruk som nevnt over. Videre er det også viktig å skjerpe kravene til behandlingsansvarliges formål for registreringen og å eksplisitt behandle adgangen til sammenlikning av ulike systemer. En særregulering av rettsaparatets adgang til å benytte bedrifters innsamlede personopplysninger kan være fordelaktig både for rettsanvendelsen og for den allmene rettsoppfatning.

---

[85] Datatilsynet *Personvern – hva er det?* Publisert 12.11.06.

[86] Se http://www.facebook.com/

[87] Se http://www.myspace.com/

[88] Se http://www.youtube.com/

Brukt riktig kan biometri være et godt og effektivt verktøy for nøyaktig kontroll. Løsninger som baserer seg på biometri nyter generelt høy tillit i befolkningen, som Personvernundersøkelsen 2008 viser, med hensyn til presisjon og pålitelighet. Det er derfor viktig å forhindre uriktig bruk av slike verktøy. Når tilliten til metoden er høy, kan et eventuelt misbruk få store konsekvenser.[89]

Som en avsluttende kommentar til innføring av biometrisk adgangskontroll, eksempelvis for å komme inn i kontorfellesskapet, vil jeg bemerke at uavhengig av regelverket bør bedriftslederen (behandlingsansvarlige) gjøre de ansatte oppmerksom på at persondataene ikke vil bli brukt til å overvåke antall timer arbeidstakeren sitter på sin kontorstol. Man bør la adgangskontroll være adgangskontroll og ikke bruke en slik løsning til å føre statistikk over de ansatte.[90]

5.3 Behovet for ny rettslig regulering

Den rettslige reguleringen av biometriske kontrollsystemer er som vist i denne fremstillingen lite oversiktlig og har stort behov for revisjon og ytterlige bestemmelser. Personvernnemnda og Datatilsynet har gitt klart uttrykk for at gjeldende rett er utilfredstillende. Justisdepartementet har nettopp publisert en utredning vedrørende revisjon av pol § 12, så utviklingen av den rettslige reguleringen på dette området er absolutt spennende å følge videre.

Datatilsynet har uttrykt i sitt revisjonsnotat at lovreguleringen på den ene siden 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.”[91] Tilsynet har også fremhevet

[89] Veum & Flesland (2007).

[90] Artikkel av Jan Aril Sigvartsen på Hardware.no, publisert 13.10.04.

[91] Datatilsynets revisjonsnotat (2006) s. 12.

at konsesjons- og meldeplikt for bruk av biometriske personopplysninger bør reguleres særskilt for bedre å fange opp bruken av disse, jf. avsnitt 4.3.2.4.

Datatilsynet har foreslått endring av personopplysningslovens § 12, forslag til ny § 12 a, samt endring av § 2 ved at det inntas en ny definisjon. Jeg går ikke inngående inn på drøftelse av endringsforslagene da de anses å være inntatt i vurderingen av forslag i den nye utredningen for Justisdepartementet.

Nedenfor følger en kort gjennomgang av forslagene til endringer i Personopplysningslovens regler om biometriske personopplysninger i Schartum og Bygraves *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12* utført på oppdrag av Justisdepartementet.

Er forslagene i den nye utredningen svaret på problemene?
Forslaget til ny regulering av fødselsnummer i personopplysningsloven har dagens § 12 som påbygningsgrunnlag. I hovedtrekk innebærer forslagene følgende:

Den behandlingsansvarlige må ha gjennomført en risikovurdering som klart viser at fødselsnummer er nødvendig for å oppnå sikker[92] identifisering. Videre anbefales det at det innføres et forbud mot bare å benytte fødselsnummer for å autentisere personers identitet. Forslaget til ny regulering 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

[92] Jeg refererer utredningens språkbruk, jf. tidligere noter 65 og 80 vedrørende termen ”sikkerhet”.

tilbys alternative fremgangsmåter for personer som ikke ønsker å bli autentisert ved hjelp av biometri.[93]

I tillegg foreslås det mindre, supplerende endringer i andre deler av personopplysningsloven, blant annet når det gjelder plikt til å vurdere nødvendigheten av å behandle personidentifiserbare opplysninger, sletting, straff og erstatning.[94]

I all hovedsak ser forslagene til ny regulering[95] ut til å imøtekomme store deler av kravene til klargjøring som drøftelsen over har belyst. Utredningen er bredspektret og synes å ta stilling til de relevante bakgrunnsspørsmål for utformingen av rettsregler på området for biometri, fødselsnummer og andre entydige identifikasjonsmidler. Særlig fremstillingen av autentisering av *roller* og mulighetene for bruk av systemer som minimerer behovet for biometrisk registrering er viktig å ha med i en regulering av vilkår for adgang til anvendelse av mer inngripende midler jf. pol § 12.[96] Som nevnt er teknologien for anvendelse av biometriske adgangskontrollsystemer vidt tilgjengelig, både i kraft av ulike typer systemer og lavere pris, og det er stor sannsynlighet for at bruken kun vil øke i omfang. Ovennevnte utredning og lovendringsforslag er forhåpentligvis et steg i riktig retning for å gi Datatilsynet, Personvernnemnda, bedrifter og befolkningen generelt en større grad av forutberegnelighet i forhold til en teknologi som har potensiale til både å gjøre samfunnet bedre og verre på samme tid. Selv om teknologien kan gjøre hverdagen (betaling etc) enklere, så er det lovgivers oppgave å minne om konsekvensene som folk ikke tenker på og sette på bremsene av hensyn til personvernet.

---

[93] Oppsummering av Schartum & Bygrave (2008) publisert 05.11.08 på http://www.regjeringen.no/nb/dep/jd/dok/rapporter_planer/rapporter/2008/utredning-om-fodselsnummer-fingeravtrykk.html?id=534749&epslanguage=NO

[94] Se note 92.

[95] Se Schartum & Bygrave (2008) s. 58 flg.

[96] Se Schartum & Bygrave (2008) s. 10 flg og s. 59 flg.

6 Henvisninger

6.1 Litteratur

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

Arbeidsgivers innsynsrett

publisert på

http://www.npt.no/portal/page/portal/PG_NETTVETT/PAG_HOME/PAG_EMNER_HOVED/PAG_NETTRETT_INTRO/PAG_HVASIERLOVEN/PAG_INNSYN_

Datatilsynet

Personvern – hva er det?

Publisert 12.11.06 på

http://www.datatilsynet.no/templates/article____396.aspx

Datatilsynet

Personvernrapporten 2008

Pdf versjon publisert 18.04.08 på

http://www.datatilsynet.no/upload/Dokumenter/publikasjoner/Personvernrapporten/Personvernrapporten%202008.pdf

Datatilsynet

Personvernundersøkelsen 2008

Pdf versjon publisert 18.04.08 på

http://www.datatilsynet.no/upload/Dokumenter/saker/2008/personvernundersøkelsen%202008%20til%20web.pdf

Datatilsynet

Revisjonsnotat pol §12

Oslo, 04.04.2006

Publisert som pdf fil under ”Dokumenter” på
http://www.datatilsynet.no/templates/Search____53.aspx?quicksearchquery=biometri

Flesland, Astrid
Innsyn i e-post
Arbeidsrett, Årgang 2006 nr. 1
publisert på http://www.idunn.no/?siteNodeId=2044825

Jørstad, Stefan
Arbeidsgivers adgang til å kontrollere og overvåke sine ansatte
Oslo, UiO, Juridisk fakultet (2003) spesialoppgave ved embetsstudie
Publisert i DUO

Kongsgaard, Erik Magnus
Biometri og personvern
Oslo, UiO, Juridisk fakultet (2005) spesialoppgave ved embetsstudie
Publisert i DUO

Kunnskapsforlaget
Fremmedord og synonymer
blå ordbok 5. Utgave, Kunnskapsforlaget 2004

Norsk Regnesentral
Elektroniske spor
rapport nr 1008, 6.juni 2005

Rønholt, Hege Haneborg
Personvern i arbeidsforhold - arbeidsgivers innsynsrett i e-post m.m.
Oslo, UiO, Juridisk fakultet (2006) spesialoppgave ved embetsstudie
Publisert i DUO

Schartum, Dag Wiese, AFIN

Rettslig regulering av identitet og identifisering i Norge

Publisert som PowerPoint presentasjon på

http://www.uio.no/studier/emner/jus/afin/FINF4001/h08/Rettslig%20regulering%20av%20identitet%20og%20identifiserng%20i%20Norge.ppt.

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

Schartum, Dag Wiese og Bygrave, Lee A.

Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i

Forbindelse med lov om behandling av personopplysninger § 12

Oslo, Justisdepartementet 2008.

Publisert 05.11.08 på

http://www.regjeringen.no/nb/dep/jd/dok/rapporter_planer/rapporter/2008/utredning-om-fodselsnummer-fingeravtrykk.html?id=534749&epslanguage=NO

Sigvartsen, Jan Arild

Biometrisk teknologi hever sikkerheten

publisert 13.10.04 på

http://www.hardware.no/artikler/biometrisk_teknologi_hever_sikkerheten/11026

The Economist:

The measure of man

7. september 2000.

Tranberg, Charlotte Bagger

Persondata og biometri i Skandinavien

publisert i Lov&Data nr. 90, juni 2007.

Veum, Helge og Flesland, Astrid
Biometri - fordeler og ulemper
publisert på Datatilsynets hjemmesider 02.03.2007.
http://www.datatilsynet.no/templates/article____1729.aspx

6.2 Forskrifter og NOUer

FOR 2000-12-15 nr 1265:
Forskrift om behandling av personopplysninger (personopplysningsforskriften)

Innst.O.nr.51 (1999-2000)

NOU-1997-19. *Et bedre personvern*

Ot.prp.nr.49 (2004-2005)
Arbeidsmiljø, arbeidstid og stillingsvern mv. (Arbeidsmiljøloven)

6.3 Avgjørelser fra Personvernnemnda

PVN-2002-7
Norskespill.no AS

PVN-2003-6
Norsk Rikstoto AS

PVN-2006-7
Tysvær kommune

PVN-2006-8
Oxigeno Fitness

PVN-2006-9
Oslo trimsenter

PVN-2006-10
Esso Norge

PVN-2006-11
REMA 1000

PVN-2007-7
Ung1881.no