

BIOMETRI

– brug af biometriske teknologier i det danske samfund

Anbefalinger fra en arbejdsgruppe under Teknologirådet



Biometri – brug af biometriske teknologier i det danske samfund

Projektledelse i Teknologirådets sekretariat:
Jacob Skjødt Nielsen

Projektmedarbejder:
Peter Lemcke Frederiksen

Projektsekretær:
Jannie Poulsen

Omslag og tryk:
Vester Kopi

ISBN: 978-87-91614-55-2

Rapporten kan bestilles hos:

Teknologirådet
Antonigade 4
1106 København K
Telefon: 33 32 05 03
Fax: 33 91 05 09
E-Mail: tekno@tekno.dk

Rapporten kan desuden hentes på projektets hjemmeside: www.biometri.info

Samt Teknologirådets hjemmeside:
www.tekno.dk

Teknologirådets rapporter 2010/2

Indholdsfortegnelse

Forord	5
Anbefalinger	6
Introduktion til biometriske teknologier	12
Temaer	
Fremtidig anvendelse af biometri	16
Etik	19
Lovgivning	21
Privacy	23
Sikkerhed	25
Interviewartikler	
Biometriske teknologier vinder frem overalt	27
Biometriske pas – redskab mod terror og illegal indvandring	31
Biometri kan ikke løse alle sikkerhedsproblemer	33
Etik i det biometriske design	37
Biometri udfordrer demokratiske rettigheder	40
Stop glidebanen mod overvågnings- og kontrolsamfundet	43
Scenarier	
Biometriens velsignelser	46
Identitetstyveri med livstruende konsekvenser	48
Ingen skjulesteder i overvågningssamfundet	50
Teknologierne	
Ansigtsgenkendelse	52
Dna-analyse	54
Fingeraftrykslæsning	55
Ganganalyse	57
Håndscanning	58
Irisgenkendelse	60
Signaturanalyse	62
Stemme genkendelse	64
Tastedyamik	65
Venescanning	66
Deltagerliste	67

Forord

Der er et stort potentiale i biometriske teknologier. Men udviklingen på området går hurtigt, og det kan være svært at finde ud af, hvilke reelle fordele og ulemper, der er knyttet til brugen af biometri. På europæisk niveau anvendes biometri i blandt andet pas, id-kort og visumansøgninger. Også i Danmark bliver biometri, som det fremgår af rapportens case-eksempler, anvendt og forsøgt anvendt til en række forskellige formål.

Blandt ulemperne er, at biometri aldrig vil kunne skabe 100 procent sikkerhed, og at ikke alle personer vil kunne registreres i biometriske systemer. Brug af biometriske teknologier kan endvidere medføre risiko for diskrimination og krænkelse af personers privatliv. Denne rapport behandler en række temaer, der er relevante for en samlet vurdering af biometriske teknologier. Rapporten indeholder:

- Et sæt anbefalinger til lovgivere, myndigheder, virksomheder og privatpersoner om hensigtsmæssig brug af biometriske teknologier.
- En debatterende del, hvor muligheder og problemstillinger tematiseres og perspektiveres.
- En beskrivende del, hvor karakteristika ved de forskellige teknologier bliver gennemgået.

Om projektet

Teknologirådet gennemfører hvert år et debatskabende it-sikkerhedsprojekt for Ministeriet for Teknologi og Udvikling. Teknologirådets bestyrelse har i samråd med IT- og Telestyrelsen valgt at gennemføre en teknologivurdering af biometri.

Projektets formål er at vurdere, hvilke fordele og problemer udbredelsen af biometriske teknologier fører med sig. For at belyse dette har Teknologirådet nedsat en tværfaglig arbejdsgruppe bestående af:

- Anette Høyrup, Forbrugerrådet
- Charlotte Bagger Tranberg, Aalborg Universitet
- Henning Mortensen, DI, ITEK
- Lars Kornbek, Vitani A/S
- Niels Christian Juul, Roskilde Universitet

Desuden har Thomas Laursen fra Etisk Råds Sekretariat bidraget i planlægningen. Den 30. september 2009 afholdt Teknologirådet en workshop, hvor en række bredt udvalgte interessenter debatterede et debatoplæg fra arbejdsgruppen og kom med input til projektet.

Rapportens indhold er endvidere præsenteret på hjemmesiden www.biometri.info. Her er der mulighed for at søge information om biometri og for at give sin mening til kende i en holdningsundersøgelse.

Teknologirådet takker alle, der har bidraget til udarbejdelsen af denne rapport – i særdeleshed medlemmerne af arbejdsgruppen –, for at have stillet deres viden og ekspertise til rådighed for projektet.

Teknologirådet, marts 2010

Jacob Skjødt Nielsen, projektleder
Peter Lemcke Frederiksen, projektmedarbejder

Anbefalinger

1. Der skal udformes et sæt retningslinjer for anvendelse af biometri

I lyset af den teknologiske udvikling og digitaliseringen i almindelighed er de nuværende procedurer for vurdering og kontrol af biometriske systemer ikke tilstrækkelige. Den hastige udvikling af nye teknologier bevirker, at det ikke alene er nødvendigt med juridisk ekspertviden men også teknologisk ekspertise for at kunne vurdere, om et biometrisk system er hensigtsmæssigt konstrueret eller ej. For det første anbefaler arbejdsgruppen, at personer med teknologisk indsigt bliver inddraget i vurderingen af systemerne, og at der løbende bliver ført kontrol med, at systemerne anvendes efter forskrifterne. For det andet anbefaler arbejdsgruppen, at personer og virksomheder, der ønsker at anvende systemer, hvor biometri indgår, får langt bedre adgang til både offentlig rådgivning og forhåndsgodkendelse i opstartsfasen, end de har i dag. For det tredje mener arbejdsgruppen, at fortolkningen af Persondataloven skal præciseres i lyset af den omfattende udvikling af biometriske teknologier og andre teknologier, der har fundet sted. I den forbindelse anbefaler arbejdsgruppen, at:

1.1 Datatilsynet tildeles flere ressourcer til kontrol og inddrager flere personer med teknologisk ekspertise i vurdering og godkendelse af biometriske systemer

Vurdering af nye teknologiske løsninger kræver stadig større teknisk ekspertise. Arbejdsgruppen anbefaler, at procedurerne for lovgivning om brugen af biometriske løsninger ændres, så personer med teknologisk indsigt bliver inddraget i vurderingen. Arbejdsgruppen anbefaler videre, at man i den forbindelse lader sig inspirere af den praksis, der er i Norge. En ændret praksis i Danmark vil kræve tilførsel af flere ressourcer, men arbejdsgruppen vurderer, at det er et helt nødvendigt tiltag, da man herved vil kunne sikre en mere kvalificeret vurdering af de enkelte sager.

1.2 Opstillere af biometri tilbydes rådgivning og mulighed for forhåndsgodkendelse

Et stigende antal virksomheder og organisationer ønsker at opstille biometriske systemer. De kan på nuværende tidspunkt ikke få forhåndsgodkendt et system eller få teknisk rådgivning i opstartsfasen. På grund af de biometriske systemers kompleksitet kan det være vanskeligt at gennemskue, hvordan man mest hensigtsmæssigt konstruerer en løsning, der lever op til kravene om effektivitet og privatlivsbeskyttelse. Muligheden for rådgivning og for at få forhåndsgodkendt et system vil for det første skabe større sikkerhed for, at opstillere af et biometrisk system ikke senere i processen får påbud om at ændre i systemet. For det andet vil det medvirke til at sikre, at løsningerne opnår en højere kvalitet.

1.3 Præcisering af fortolkning af Persondataloven

En række teknologier udvikles i disse år markant og står overfor et massivt gennembrud. Biometri er en af disse teknologier, men også Radio Frequency Identification (RFID) og videoovervågning kan fremhæves. Der er behov for at præcisere, hvordan Persondataloven skal fortolkes i forhold til aktuelle teknologier og disses indflydelse på privatlivets fred. Arbejdsgruppen foreslår, at der bliver udarbejdet en vejledning, som med autoritet fortolker persondataloven og anviser, hvordan teknologier skal anvendes i praksis, og hvilke privatlivsfremmende hensyn såsom Privacy Impact Assessment (PIA), Privacy Enhancing Technologies (PET) og Privacy by Design, der bør tages med i overvejelserne ved implementering af ny teknologi.

2 Biometri skal bruges til at opnå øget privatlivsbeskyttelse og til at sikre, at brugerne har kontrol med egne data

Biometri åbner for at styrke privatlivsbeskyttelsen, da teknologierne giver mulighed for sikker autentifikation (bekræftelse af adgangsrettigheder), uden at ens fulde identitet bliver afsløret. Man kan beskytte en række personfølsomme oplysninger ved hjælp af forskellige former for biometri kombineret med passwords.

Arbejdsgruppen anbefaler, at man undgår at skabe biometriske systemer, hvor for eksempel et fingeraftryk og intet andet giver adgang til en lang række forskelligartede personfølsomme oplysninger.

Arbejdsgruppen anbefaler videre, at der i relation til alle nye biometriske systemer bliver udarbejdet en privatlivsimplicationsanalyse (PIA), der sikrer en fornuftig balance mellem formålet med systemet, detaljeringsgraden af identifikation, de lagrede persondata og risikoen for datamisbrug og -tyveri. Privatlivsbeskyttelse og gennemsigtighed skal medtænkes, når systemerne bliver designet, og man bør udarbejde en plan for anvendelse af "Privacy Enhancing Technologies" (PET) – det er teknologier, som understøtter beskyttelse af borgernes privatliv. Samtidig bør etiske overvejelser om risici for social stigmatisering, social inklusion og social eksklusion medtænkes helt fra start. Arbejdsgruppen peger endvidere på, at jo mere der fra politisk hold bliver lagt vægt på at benytte biometri til at styrke privatlivsbeskyttelsen, jo mere accepteret vil biometri på sigt blive i offentligheden, da risikoen for misbrug herved minimeres.

2.1 Biometriske systemer skal konstrueres på en sådan måde, at de tager mest muligt hensyn til privatlivets beskyttelse

Man bør altid sikre, at målet med den biometriske løsning nås med mindst mulig indgriben i brugernes privatliv. En indledende vurdering med dette formål kan tage udgangspunkt i følgende spørgsmål:

1. Er systemet konstrueret på en sådan måde, at man i videst mulig omfang undgår at lagre personfølsomme oplysninger?
2. Er det muligt, for derved at undgå central lagring af personfølsomme oplysninger, at lagre data decentralt og sikre, at brugerne har kontrol over egne data – for eksempel ved brug af en såkaldt "system on card-løsning" eller en "match on card-løsning"?
3. Er det muligt at opfylde formålet med systemet, uden at brugerens identitet – for eksempel brugerens navn – bliver knyttet til biometriske data?
4. Er der alternative muligheder for brugere, som ikke kan eller ønsker at anvende biometri?
5. Er det muligt at anvende en pseudonymiseret, central database – det vil sige en database, hvor borgernes rigtige navne er erstattet af pseudonymer?
6. Er det biometriske system afsondret fra netværk?
7. Er der anvendt kryptering?
8. Er der fastlagt procedurer for, hvem der har adgang til de biometriske templates eller data knyttet til templates?¹
9. Slettes templates og tilknyttede data, som ikke længere anvendes?

¹ En biometrisk template er en sekvens af 0- og 1-taller, som det biometriske system danner hver gang, det præsenteres for eksempelvis en persons pegefinger, hånd eller ansigt.

2.2 Registrering af borgere og kunder skal ske på en sådan måde, at der bliver taget mest mulig hensyn til privatlivets beskyttelse

De seneste år har en række diskoteker, fitnesscentre og andre søgt Datatilsynet om tilladelse til at anvende biometri. Disse henvendelser har ført til forskelligartede svar, som arbejdsgruppen ønsker at knytte følgende kommentarer til:

Restaurationsbranchen bør anvende ”match on card-teknologi”

Arbejdsgruppen vurderer, at restaurationsbranchens ønsker til brug af biometri er uhensigtsmæssige. Branchens mål vil kunne opnås på mindre privatlivsindgribende vis, hvor restaurantgæster selv beholder deres biometri. Det kan for eksempel ske ved at udstede chipkort til gæsterne, hvorpå deres biometri lagres. På den måde vil man undgå den nuværende sammenknytning af navn, billede og biometri. Arbejdsgruppen vurderer, at lagring af såvel biometriske data som personens navn og billede i en central database repræsenterer et unødigt indgreb i den enkeltes privatliv. Målet kan i stedet nås ved brug af såkaldt ”match on card-teknologi” – det vil sige en løsning, hvor de biometriske data i krypteret form er lagret på et plastikkort med chip. Ved adgang matches informationerne på chippen med resultatet af en aktuel scanning af gæstens fingeraftryk.

Et alternativ kunne være brug af negativlister, hvor kun de uønskede gæster er registrerede. Udfordringen i den sammenhæng er, at uønskede personer vil kunne snyde nogle scannertyper ved fx at placere fingeren skævt på scannerenheden og derved opnå adgang alligevel. Derfor stiller både negativlister og selvbetjeningsløsninger større krav til scannerenhedernes beskaffenhed, så der kan tages højde for fejl. Generelt er det nødvendigt at etablere robuste systemer med læsere, der ikke kan snydes, og løbende følge den teknologiske udvikling og løbende opgradere sikkerheden.

Fitnesscentre bør anvende ”match on card-teknologi”

Flere fitnesscentre har ansøgt om at måtte bruge biometri med det formål at undgå snyd og samtidig skabe nemmere adgang til centrene for medlemmerne. Datatilsynet har afvist at give disse fitnesscentre mulighed for at benytte et system med en tilhørende database, hvor medlemmernes biometri bliver lagret i krypteret form. Arbejdsgruppen vurderer, at de pågældende fitnesscentre bør have mulighed for at udstede medlemskort baseret på ”match on card-teknologi” – en løsning, hvor de biometriske data i krypteret form er lagret på medlemskortets chip og ved adgang til fitnesscentret bliver matchet med resultatet af en aktuel scanning af brugerens fingeraftryk. Denne løsning vil betyde en merudgift for fitnesscentret, men systemet vil formentlig også mindske omfanget af snyd med medlemskort. Arbejdsgruppen anbefaler, at et sådant system skal være frivilligt og baseret på samtykke fra brugerne, ligesom det skal være muligt at vælge et alternativ, som ikke stiller brugerne dårligere, end hvis de benytter den biometriske løsning.

Erhvervslivet bør gå sammen om en fælles løsning, hvor brugerne bevarer kontrollen med egne data

I lyset af de ovenfor nævnte ønsker fra private virksomheder bør man undersøge mulighederne for, at private virksomheder i fællesskab designer et system, som både øger sikkerheden, gør brugen af serviceydelser mere bekvem og lader brugerne bevare kontrollen med egne data. En mulig egnet business case i denne sammenhæng, som bør undersøges nærmere, er biometrisk ”match on card-teknologi” – eventuelt i kombination med en pinkode – som mulig erstatning for adgangskort, medlemskort, betalingskort mv.

3. Et fremtidigt biometrisk borgerservicekort skal baseres på "system on card-teknologi" eller lignende teknologier

Arbejdsgruppen mener, at et borgerkort med krypterede biometriske data, som er baseret på "system on card-teknologi" eller lignende teknologier, ud fra en sikkerhedsmæssig betragtning er en ønskelig løsning. "System on card" betyder, at brugeren ved hjælp af biometrisk identifikation har adgang til sit eget kort, som rummer en række koder/elektroniske nøgler til forskellige formål – blandt andet udveksling af informationer med det offentlige. Brugeren vil med denne teknologi have fuld kontrol over egne data, og systemet vil være mere privatlivsbeskyttende end for eksempel den nuværende digitale signatur. Arbejdsgruppen anbefaler, at et borgerservicekort baseres på decentral datalagring, og at borgeren via kortet kan aktivere en række forskellige koder/nøgler. Ved tyveri eller tab af kortet skal det være muligt at blokere det og oprette et nyt uden væsentlige omkostninger for hverken det offentlige eller brugeren.

Prisen for et sådant system er dog på nuværende tidspunkt relativ høj, og det er blandt andet derfor værd at overveje alternativer til et borgerkortservicekort, som er udstedt og finansieret af staten. Arbejdsgruppen vurderer, at der på lidt længere sigt er potentiale i at anvende biometri i mobiltelefoner, PDA'er eller lignende, hvor adgang til de lagrede oplysninger, koder og nøgler kontrolleres af brugerne selv. Arbejdsgruppen peger på, at brug af mobiltelefon frem for et borgerservicekort vil have en række fordele:

- Brugere er vant til at benytte mobiltelefonen
- Brugere har (altid) mobiltelefonen med
- Brugere betaler selv for den
- Mobiltelefonen har indbygget processor og kan derfor generere koder og nøgler
- Et stigende antal mobiltelefoner har både kamera, mikrofon og trykfølsomt display, hvilket potentielt giver mulighed for brug af følgende biometriske teknologier: Tastedynamik, iris-scanning, ansigtsgenkendelse, signaturanalyse og stemmegenkendelse. Flere vil komme til i de kommende år.

4. Start med at definere formålet med den biometriske løsning

Hvis formålet med den biometriske løsning er tydeligt defineret på forhånd, kan man undgå urealistiske forventninger til løsningens formåen. Erfaringer fra udlandet viser, at manglende formålsspecifikationer har resulteret i biometriske løsninger, der ikke lever op til forventningerne hos hverken opstillerne eller brugerne.

Arbejdsgruppen anbefaler derfor, at man allerede i udviklingsfasen skaber maksimal klarhed om den biometriske løsnings reelle formål og performance. Dette vil endvidere sætte fokus på potentielle faldgruber – for eksempel risikoen for såkaldt "function creep", hvilket vil sige, at data bruges til andet end det oprindelige formål.

Arbejdsgruppen anbefaler, at man i en personalehåndbog eller lignende fastslår formålet med den biometriske system og samtidig formulerer præcist, hvad de opsamlede data bliver brugt til. Det vil give medarbejderne sikkerhed for, at data ikke bruges til andre formål end de tilsigtede. Det er arbejdsgruppens holdning, at en klar og tydelig formålsspecifikation vil skabe tryghed om den biometriske løsning hos medarbejdere/brugere. Samtidig vil det mindste risikoen for misbrug af data.

Arbejdsgruppen fremhæver, at de mulige konsekvenser ved misbrug af data, som er opsamlet i en biometrisk løsning, afhænger af løsningens størrelse og omfang. De følgende anbefalinger er primært rettet mod større biometriske installationer:

5. Et biometrisk systems sikkerhed er betinget af sikkerheden i hele systemet

Et biometrisk systems sikkerhed er altid betinget af sikkerheden i hele den it-løsning, som biometrien er ét af mange elementer i. Arbejdsgruppen fremhæver derfor, at man altid skal se på helheden, når man vurderer et systems sikkerhed. Risikoen i et givet system for blandt andet "hacking" og "spoofing" – "spoofing" er, når en person udgiver sig for at være en anden ved for eksempel at anvende et falsk fingeraftryk – skal vurderes i alle de faser, en bruger skal gennemgå i forhold til registrering og øvrig brug af systemet. Arbejdsgruppen påpeger, at selve registreringsprocessen i et biometrisk system er en særligt sårbar fase. For eksempel skal der kun én uopmærksom medarbejder i kommunen til at skabe et lovligt udstedt pas, hvor de anvendte biometriske data passer sammen med en andens identitet.

6. Procedurerne for registrering af biometriske data skal standardiseres

For at sikre interoperabilitet på tværs af grænserne – interoperabilitet er produkters, systemers og forretningsprocessers evne til at arbejde sammen om løsningen af en fælles opgave – anbefaler arbejdsgruppen, at registrering af biometriske oplysninger standardiseres. Dette skal helst ske globalt, men i det mindste i EU. Arbejdsgruppen anbefaler, at en person, der skal registreres i en biometrisk løsning, skal oplyses om formålet med og omfanget af registreringen. Det skal endvidere være muligt for brugeren at se og kontrollere, om de registrerede oplysninger er korrekte. Registreringsproceduren skal derudover indeholde nogle klare, standardiserede procedurer for, hvordan man fjerner data om en bruger fra systemet. Veluddannet personale og transparente procedurer skal i det hele taget sikre fuld gennemskuelig-
hed for de registrerede brugere. Der skal desuden udformes standardiserede procedurer for sletning af data.

7. Procedurerne for lagring og matchning af biometriske data skal standardiseres

Arbejdsgruppen anbefaler, at man, når det er muligt, undgår at anvende centrale databaser i forbindelse med biometriske løsninger. Hvis en biometrisk løsning alligevel baseres på en central database, skal datakvaliteten i denne være af højst mulig kvalitet og behandles af certificeret personale. Samtidig skal det være muligt for brugere at trække egne data tilbage eller rette i egne data, hvis brugerne finder, at der er fejl eller mangler i de registrerede data. Der skal ligeledes være en standardiseret klagemulighed, som fuldt ud respekterer individets suverænitet, og som understøtter procedurerne i et demokratisk samfund. Arbejdsgruppen anbefaler videre, at biometriske data aldrig lagres i råformat, hvilket for eksempel kan være et digitalt billede af et fingeraftryk. I stedet lagres data som krypterede templates. Dette vil reducere risikoen for identitetstyveri og misbrug af persondata betydeligt. Samtidig anbefaler arbejdsgruppen, at man undgår at udlicite databehandling til tredjepart, da man derved forringer adgangen til at praktisere sikker kontrol med de lagrede oplysninger. Endelig anbefaler arbejdsgruppen øget standardisering på teknisk niveau i form af fælles algoritmer, kalibrering og interface og i forhold til uddannelse af certificeret personale. Standardiseringen på disse områder bør ske globalt og i det mindste på EU-niveau. Arbejdsgruppen anbefaler, at biometrisk matchning kun matcher de biometriske data og ikke forespørger de persondata, der er knyttet til de biometriske data. Det vil mindske risikoen betydeligt for, at personfølsomme oplysninger falder i forkerte hænder.

8. Der skal altid være sikre alternativer og "fall-back-procedurer"

Arbejdsgruppen peger på, at der især knytter sig to svagheder til biometrisk identifikation: Biometri kan aldrig blive 100 procent nøjagtigt, og biometriske systemer vil altid både afvise og acceptere en andel "forkerte" personer. Ikke alle har brugbare biometriske karakteristika – for eksempel kan et fingeraftryk være beskadiget, hvorfor det ikke kan registreres korrekt. Disse forhold gør, at det er umuligt at skabe et sikkert system, som udelukkende er baseret på biometri. Der vil derfor altid være behov for et eller flere klart definerede alternativer – såkaldte "fall-back-procedurer". Der bør endvidere i forbindelse

med blandt andet automatiseret grænsekontrol uddannes operatører, der forstår at behandle både korrekt og forkert afviste personer på en anstændig måde, så der ikke foregår social stigmatisering og lignende.

9. Der er brug for flere test af biometriske systemer

Det er på nuværende tidspunkt meget vanskeligt at sammenligne forskellige biometriske systemers performance. De fleste af de tilgængelige test er fortaget af producenterne selv i laboratorier uden de fejlkilder, som findes i de miljøer, hvor systemerne bliver anvendt. En omfattende test af biometriske systemer fortaget af den britiske regering har vist en meget stor reel fejlrate for systemer, som er baseret på fingeraftryksscanning, irisgenkendelse eller ansigtsgenkendelse. Arbejdsgruppen anbefaler, at man indfører flere standardiserede test, og at der derigennem bliver skabt større åbenhed om de biometriske systemers reelle formåen.

10. Berøringsfrie enheder bør benyttes i miljøer, hvor hensynet til hygiejne er vigtigt

Arbejdsgruppen anbefaler, at man benytter berøringsfrie scannere – hvor man for eksempel holder hånden i nogle centimeters afstand fra scanningspladen – på steder, hvor en høj grad af hygiejne er påkrævet. Det gælder eksempelvis på hospitaler. Arbejdsgruppen peger på, at iris- og venescanning i denne sammenhæng bør overvejes som gode alternativer til scanning af fingeraftryk.



Introduktion til biometriske teknologier

Biometri kan defineres som biologiske egenskaber, fysiologiske karakteristika, særlige træk eller gentagne handlinger, hvor karakteristika eller handlinger entydigt vedrører en specifik person og samtidig er målelige. Biometri forbindes i dag typisk med enten semi- eller fuldautomatiske processer, hvor der anvendes digitale scannerenheder og computerprocessorer, som i løbet af en brøkdel af et sekund kan be- eller afkræfte en persons identitet.

I denne rapport vil biometri primært blive behandlet som identifikation eller verifikation baseret på automatiske processer, men vil også blive brugt i en bredere forstand, hvor den primære funktion ikke direkte er identifikation eller verifikation. For eksempel vil registrering af personers fysiske eller psykiske tilstand ud fra adfærd eller fysiologiske faktorer i det følgende også blive omtalt som biometri.

Det er muligt at opdele de biometriske teknologier i to hovedkategorier: teknologier baseret på henholdsvis fysiologiske karakteristika og adfærd.²

Teknologier baseret på fysiologiske karakteristika:

- Fingeraftryksgenkendelse
- Ansigtsgenkendelse
- Håndscanning
- Irisgenkendelse
- Retinascaning (nethinden)
- Venescanning
- Øreformsanalyse
- Hjernebølgeanalyse
- Lugtanalyse
- Dna

Teknologier baseret på adfærd:

- Signaturanalyse
- Tastedynamik
- Stemmeanalyse
- Ganganalyse



Verifikation eller identifikation?

Man skelner typisk mellem verifikation og identifikation. Verifikation er karakteriseret ved, at ens data kun bliver matchet med én bestemt profil. Et konkret eksempel på verifikation kunne for eksempel være biometrisk adgangskontrol på en arbejdsplads, hvor man kører sit ID-kort igennem en kortlæser. Systemet vil herefter hente de informationer, som er tilknyttet det specifikke ID-kort, i en database og derefter matche informationerne med de data, som kræves for at få adgang med det specifikke kort. På denne måde bliver det fingeraftryk, man afgiver, kun forsøgt matchet med det ene fingeraftryk, som indehave-

² Distinktionen mellem biometriske teknologier baseret på enten fysiologiske eller adfærdsmæssige karakteristika er i virkeligheden ikke helt korrekt, da der for eksempel i forbindelse med en fingeraftryksscanning også registreres rent adfærdsmæssige forhold, såsom måden fingeren bliver placeret på for at forhindre "spoofing".

ren af ID-kortet tidligere har registreret. I fagsprog omtales verifikation også som 1:1 (én til én), da man kun sammenligner de præsenterede data med data fra én bestemt lagret profil.

Når man taler om identifikation, kan det derimod være ens afgivne biometriske data, der bliver sammenlignet med et stort antal lagrede data. Hvis vi igen anvender adgangskontrol med fingeraftryk som eksempel, vil man for at få adgang blot skulle scanne sin finger³. De data, der genereres af det aflæste fingeraftryk, sammenlignes herefter med en mængde lagrede data. Dette kan forgå på to forskellige måder. Enten ved at et positivt match giver adgang, eller ved at det er et negativt match, der giver adgang. Er målet med det biometriske system for eksempel at identificere nogle få uønskede personer med henblik på at nægte dem adgang, vil det være mest hensigtsmæssigt at operere med en negativ match-liste, hvor kun de personer, hvis data ikke findes i databasen, får adgang. En positiv match-liste vil modsat være mest hensigtsmæssig i en situation, hvor der er en stor gruppe, som ikke skal have adgang, mens der er en relativt lille gruppe, der skal have adgang. Om et biometrisk system opererer på den ene eller anden måde er vigtigt, da det kan have stor betydning for, hvor mange personers data, der skal registreres i den pågældende database.

Identifikation bliver også kaldt for 1:N (én til mange), da man netop kan sammenligne én profil med mange registrerede profiler.⁴

Hvad er en template?

Når et biometrisk system skal be- eller afkræfte en persons identitet, sammenligner systemet ikke de komplette biometriske data, men derimod såkaldte templates baseret på biometriske data. Templates er små filer (typisk mindre end 1 kilobyte) skabt på baggrund af specifikke karakteristika ved den enkelte brugers biometriske data. En template kan dermed siges at være et koncentrat af en persons karakteristika, som dog stadig er unikt for den pågældende person.

På grund af filernes relativt lille størrelse kan selve matchningen af templates foregå i et meget højt tempo. En anden fordel, der opnås ved at lagre templates som små filer, er, at de desuden kan lagres på et såkaldt "smartcard"⁵.

Der er ikke ét fælles format for templates baseret på biometriske data. Det betyder i praksis, at en template skabt af et biometrisk system fra producent A ikke nødvendigvis kan bruges af producent B eller omvendt. Komplette biometriske data, som for eksempel et helt fingeraftryk eller vellignende billeder fra en ansigtsscanning, kan ikke genskabes på baggrund af biometriske templates, da der netop er tale om filer skabt ud fra specifikt udvalgte karakteristika. På samme måde som hvis man udvalgte det tiende, tyvende, tredivte, etc. bogstav på denne side, ville det være muligt at skelne denne side fra andre sider med skrevet tekst, uden at det dog ville være muligt at genskabe hele siden ud fra de registrerede bogstaver. Her er det vigtigt at påpege, at et biometrisk system netop kun vil fokusere på de dele, som kan rekonstrueres, og at man derfor i princippet godt ville kunne snyde sig til uberettiget adgang ud fra en kunstig finger, der for eksempel kun indeholdt de 10 afgørende karakteristika.

Unikke templates bliver genereret hver eneste gang, en bruger præsenterer biometriske data. Dette betyder, at to fingeraftryksscanninger taget fra den samme finger blot sekunder efter hinanden ikke vil resultere i identiske templates. Grunden hertil er, at selv minimale forskelle i position og tryk vil afføde små forskellige i den algoritme, som den enkelte template dannes på baggrund af.

En måde at kryptere de biometriske templates, så de bliver umulige⁶ at rekonstruere, er ved at konvertere de biometriske templates til såkaldte hash-værdier. Dette kan gøres via en hash-funktion, der er en en-

³ Biometrisk identifikation kan evt. kombineres med efterfølgende indtastning af PIN eller password, hvis der ønskes et højere sikkerhedsniveau.

⁴ I princippet kan der sagtens kun være én registreret profil i et biometrisk system baseret på identifikation. Dette ville for eksempel være tilfældet i et biometrisk overvågningssystem, hvor man kun eftersøger én bestemt person.

⁵ Et plastikkort, der indeholder en computerchip.

vejsfunktion, som er kendetegnet ved, at man kan gå fra en talværdi til en anden og kortere talværdi uden mulighed for at komme tilbage igen. Som tidligere nævnt er det næsten umuligt at generere to ens templates, så hvis der skal anvendes en hash-funktion til krypteringen af biometriske templates, skal værdierne fra de templates, der ligger inden for de acceptable grænseværdier, først konverteres til én og samme talkode.

Biometrisk matchning:

For at forstå, hvorledes de biometriske systemer afgør, om et match er gyldigt eller ej, er der en række fagudtryk, som kan være gode at kende til. De vigtigste er: False match rate (FMR), false non-match rate (FNMR) og failure to enroll (FTE).

FMR⁷ angiver sandsynligheden for, at en brugers template fejlagtigt bliver vurderet som værende en anden persons template. I praksis vil et sådant falsk match kunne give en uberettiget person adgang til en facilitet, som vedkommende ikke burde have adgang til – eller omvendt nægte en berettiget person adgang. Grunden til, at falske match finder sted, er, at nogle personer kan have tilstrækkeligt ens biometriske karakteristika, og at der derfor opstår høj korrelation mellem de to personers templates. Det biometriske system vil derfor opfatte de to forskellige personer som værende én og samme person.

FNMR⁸ angiver sandsynligheden for, at en brugers template fejlagtigt bliver vurderet til ikke at matche personens tidligere registrerede template. FNMR finder sted, fordi der ikke er tilstrækkelig høj korrelation mellem den tidligere registrerede template og den aktuelt præsenterede template. Der kan være en række forskellige grunde til dette. For eksempel kan der være sket ændringer i brugerens biometriske data, der kan være afvigelser i forhold til, hvorledes de biometriske data er blevet præsenteret, eller der kan være sket ændringer i det miljø, hvor de biometriske data er blevet præsenteret.

FMR og FNMR skal altid betragtes i fællesskab, da de er gensidigt afhængige på den måde, at hvis FMR reduceres, øges FNMR – og omvendt.

FTE er et mål for, hvor ofte det er umuligt for en person at lade sig registrere i et biometrisk system. "Failure to enroll" er både afhængig af de bagvedliggende algoritmer og det biometriske systems kvalitet, men er også betinget af det omgivende miljø. De biometriske systemers FTE er dermed en størrelse, som er svær at sammenligne, men det er alligevel et område, man bør være opmærksom på, hvis man overvejer at opstille et biometrisk system.

Potentielle fordele ved anvendelsen af biometriske teknologier

De mest benyttede metoder til autentifikation er i dag passwords og PIN-koder. De biometriske teknologier har dog en række fordele:

Bekvemmelighed

En af hovedbegrundelserne for at benytte biometriske teknologier er bekvemmelighed – ofte kaldet "convenience". Koder og passwords kan være vanskelige at huske, og biometriske løsninger vil derfor ofte være en mere bekvemt måde at få adgang til beskyttede data. Det vil især være tilfældet i systemer, hvor der ikke blot kræves én men derimod en hel række forskellige passwords, før man får adgang til de øn-

⁶ At det engang i fremtiden vil blive muligt at rekonstruere dele af de biometriske karakteristika på baggrund af hash-værdier er dog ikke utænkeligt.

⁷ Nogle anvender i stedet termen false acceptance rate (FAR).

⁸ Nogle anvender i stedet termen false rejection rate (FRR).

skede applikationer eller data. Problemet med glemte passwords til sikre systemer er i nogle virksomheder et så stort problem, at det direkte kan registreres på bundlinjen. Med indførelsen af biometriske systemer vil log-in-situationer i mange tilfælde kunne gøres mere effektive. Dette vil især være tilfældet i situationer, hvor det ikke er nødvendigt at anvende password eller PIN-koder, men hvor et biometrisk bruger-ID er tilstrækkeligt.

Øget sikkerhed

Biometri kan desuden anvendes med henblik på at opnå større sikkerhed. Det er dog vigtigt at huske, at de biometriske karakteristika ofte er nogle, som personen bærer til offentlig skue, og som dermed relativt nemt kan aflæses. Kritikere vil derfor hævde, at det er nemmere at stjæle en persons fingeraftryk eller dna, end det er at stjæle vedkommendes brugerkort eller nøgle. Desuden er det, som det for eksempel bliver demonstreret i tv-programmet "MythBusters" på Discovery Channel, muligt at snyde ("spoofe") biometriske systemer⁹.

På trods af dette kan anvendelsen af biometri i kombination med enten smartcards, PIN-koder eller passwords være med til at øge sikkerhedsniveauet.

Øget kontrol

Endelig kan biometriske teknologier sikre større kontrol med hvem, der gør hvad. I det hele taget kan visse biometriske systemer gøre det nødvendigt at følge en række "spilleregler", som ellers bliver brudt. For eksempel vil man i et supermarked med biometri i stedet for nøglesystemer kunne sikre, at den betroede medarbejder ikke uberettiget låner sin nøgle ud til kasseeksponenter, som skal annullere transaktioner. Biometrien er med til at sikre, at den rigtige person rent faktisk er til stede i situationen. Ligeledes vil det på en arbejdsplads med biometrisk tidsregistrering være umuligt at tjekke ind for sin kollega. På den måde kan biometriske systemer være med til at sikre, at folk "spiller efter reglerne".

I udlandet bruges biometriske teknologier desuden af blandt andre FN til at sikre en retfærdig fordeling af nødhjælp. Biometri vil på lignende vis for eksempel kunne være med til at forhindre svindel med sociale ydelser i Danmark. Øget kontrol kan altså både ses som noget positivt og negativt.



⁹ Teknologierne bliver hele tiden forbedret. Dog bliver de personer, som ønsker at omgå de biometriske systemer, samtidig dygtigere og dygtigere.

Fremtidig anvendelse af biometri

Der er utallige anvendelsesmuligheder for biometriske teknologier. Biometri kan både bruges til at skabe øget bekvemmelighed for brugerne og til at skabe højere sikkerhed. For eksempel med hurtig og nem check-in i lufthavne for udvalgte passagergrupper.

Biometri bliver på nuværende tidspunkt blandt andet anvendt til:

- Automatiseret grænsekontrol
- Visumansøgninger
- Fast track i lufthavnen
- Efterforskning
- Overvågning
- Militære formål
- Uddeling af nødhjælp
- Økonomiske transaktioner
- Arbejdstidsregistrering
- Eksamensregistrering
- Udbetaling af sociale ydelser
- Låse på køretøjer, værktøj og boliger
- Sikring af adgang til journaler
- Udlån af bøger på biblioteket

Anvendelse i den offentlige sektor

I det offentlige anvendes biometri i dag af politiet (dna-registre, registrering af fingeraftryk) og af pasmyndighederne (digitale billeder), ligesom det overvejes at integrere biometriske sikkerhedsløsninger i et fremtidigt borgerservicekort. Alle danske pas udstedt efter 1. august 2006 er såkaldte biometriske pas, da de indeholder et digitalt billede lagret på en indbygget chip. Der er desuden planer om at lagre både fingeraftryk og iris i danske pas. Tidspunktet for indførelsen af de nye pas er endnu ikke fastsat. Planerne for et biometrisk borgerkort, hvor en række funktioner (såsom blandt andet sygesikringsbevis, kørekort, dankort og mobil digital signatur) er samlet i ét kort, er indtil videre blevet udskudt med den begrundelse, at det på nuværende tidspunkt er for dyrt. Det må antages, at teknologierne vil falde så meget i pris, at økonomi ikke vil kunne forhindre udbredelsen af et biometrisk borgerkort, som mange eksperter anser for at være den foretrukne løsning.

Anvendelse i den private sektor

Især den private sektor har taget biometri til sig på flere områder og overfor både ansatte og kunder. Flere arbejdspladser, restauranter, transportsektoren mv. benytter i stigende omfang biometriske data til at sikre identifikation af kunder eller medarbejdere. Her benyttes de biometriske teknologier både i forbin

delse med betaling og til fysisk og logisk adgangskontrol – adgang til for eksempel pc, database eller bestemte applikationer.

Biometri kan anvendes til utallige formål. For eksempel vil man kunne installere ansigtsgenkendelse i biler, som kan udelukke andre end autoriserede personer fra at køre dem. Ligeledes vil teknologien kunne give signal fra sig, hvis føreren gør tegn til at falde i søvn bag rattet. Registrering af det enkelte menneskes fysiske ledningsevne kan implementeres i for eksempel store håndværktøjer, som automatisk detekterer, om man har autorisation til at bruge det pågældende værktøj.

Datatilsynet har givet tilladelse til, at diskoteks-kæden Crazy Daisy kan registrere gæsternes fingeraftryk (med deres samtykke), så deres adgang til diskoteket kan lettes, og i restaurationsbranchen arbejder man på at få indført et landsdækkende bølleregister baseret på biometriske identifikation. Et biometrisk borgerkort ville også potentielt kunne bruges til meget andet end udveksling af oplysninger mellem borgere og det offentlige. For eksempel adgang til netbank, som betalingskort, som adgangskort til arbejdspladsen og til transport.

International anvendelse af biometri

Registrering ved hjælp af biometriske teknologier bliver stadig mere udbredt internationalt. For eksempel har irisscanning i en årrække været brugt i forbindelse med grænsekontrol i De Forenede Arabiske Emirater, af FN til uddeling af nødhjælp og af det amerikanske militær i Irak og Afghanistan til at sikre, at kun de rette personer har fået adgang til bestemte faciliteter. I USA og England kan man i nogle lufthavne springe dele af sikkerhedskontrollen over, hvis man tidligere er blevet registreret som "trusted traveller". Automatiseret biometrisk grænsekontrol baseret på ansigtsgenkendelse bruges i dag i Australien og Kina, og der arbejdes på at udstede biometriske ID-kort til alle borgere i blandt andet Indien, Thailand og Portugal. I Japan anvendes biometrisk ansigtsgenkendelse desuden til registrering af forbrugeres køn og alder og til at kontrollere, om de ansatte smiler tilstrækkeligt på jobbet.

Lånerkort med fingeraftryk

Ringkøbing Bibliotek er det eneste bibliotek i Danmark, hvor man anvender fingeraftryk i stedet for sygesikringskort som identifikation ved bogudlån. Fordelen for brugerne er, at de ikke længere behøver at huske sygesikringskortet. På biblioteket oplever man, at ekspeditionen er blevet hurtigere, og at der er stor sikkerhed for brugerens identitet. Det hele startede som et pilotprojekt i Ringkøbing-Skjern Kommune i 2007, hvor kommunen valgte at implementere biometri på et af sine biblioteker. Det skete for at afmystificere teknologien men også for at vise, at der er fordele for både lånere og bibliotek forbundet med den biometriske løsning.

Bibliotekschef ved Ringkøbing-Skjern bibliotekerne, Per Høgh, fremhæver, at biblioteket valgte det biometriske lånerkort med fingeraftryk, fordi det umiddelbart var den løsning, der på det pågældende tidspunkt var mest ukompliceret: "Vi kunne udmærket have valgt andre løsninger såsom irisscanning eller kropsgenkendelse, men de var – og er vel stadig – mere komplicerede rent teknologisk og mere omkostningstunge," siger han.

Biblioteket har gode erfaringer med udlån via en fingeraftryksscanner. Ifølge Per Høgh var det også et formål med pilotprojektet at afklare, hvordan brugerne ville modtage den biometriske løsning: "Vi havde en forestilling om, at systemet kunne virke skræmmende på en del brugere, men det viste sig ikke at holde stik. Kun ganske få har ikke ønsket at benytte scanneren. Det er klart, at folk har spørgsmål og er kritiske, men de bliver trygge igen, når vi fortæller, at fingeraftrykket kun registreres og kan bruges på biblioteket," siger Per Høgh og fortsætter: "Udover at løsningen giver hurtigere ekspeditionstid, er den oplagt til børn, som har det med at miste deres sygesikringskort. Det er ikke noget problem hos os – her bruger de bare fingeren. Vi skal blot huske at opdatere børnenes fingeraftryk med jævne mellemrum, fordi de er i voksenalderen. Sikkerhedsaspektet er også et plus ved løsningen. Hvis du mister dit sygesikringskort, kan det misbruges af andre – det undgår du her," siger Per Høgh. På negativsiden fremhæver han, at det sker, at scanneren ikke kan aflæse et fingeraftryk. Forklaringen kan være, at fingeren er meget slidt. Det betragter han dog som en teknologisk børnesygdom, og han forsikrer om, at Ringkøbing Bibliotek vil holde fast i biometrisk bogudlån.

Trends

Både store offentlige og militære biometriske systemer vil i de kommende år forsat blive udbygget. Samtidig vil flere og flere billige løsninger til private og firmaer vinde frem. Mobiltelefoner med biometri, automatiseret grænsekontrol, overvågningskameraer med ansigtsgenkendelse og banktransaktioner er allerede udbredt andre steder i verden. Danmark er på nuværende tidspunkt under massivt pres fra udlandet om at anvende biometri i det offentlige. Det gælder for eksempel i forhold til biometriske pas og det europæiske immigrationssystem EURODAC. Men de biometriske teknologier vil, som det fremgår af case-artiklerne i denne rapport, vinde frem over alt: Blandt andet i hjemmet, på arbejdspladsen, på rejsen, på biblioteket, i Forsvaret og i supermarkedet.

Biometri i Afghanistan

Biometri kan være et effektivt redskab i genopbygningen af Afghanistan, og der arbejdes på nuværende tidspunkt på at få implementeret biometri på flere niveauer. Amerikanerne er ikke overraskende dem, der er længst fremme i brugen af biometriske teknologier i Afghanistan.

Biometrisk pilotprojekt i gang

Biometriske teknologier bliver i øjeblikket forsøgt anvendt i et pilotprojekt blandt de danske soldater i Afghanistan. Projektet er sat i verden for at undersøge, om det via moderne biometriske teknologier er muligt at højne sikkerhedsniveauet i de lejre, hvor soldaterne bor.

Bo Wolff, major og sagsbehandler i Hærens Operative Kommando, forklarer, at der på ISAF-baserne jævnlige kommer personer ind udefra for at varetage en række praktiske funktioner som for eksempel tømning af skraldespande mv.: "Indtil nu er disse personer blot blevet registreret på et stykke papir og har fået lavet et simpelt ID-kort med navn og billede, som så har givet adgang til nogle ganske bestemte områder og faciliteter i lejren. Med pilotprojektet undersøger vi mulighederne for at øge sikkerhedsniveauet ved hjælp af biometriske teknologier."

I praksis eksperimenterer man med en biometrisk enhed, der både kan anvende ansigtsgenkendelse, irisscanning og fingeraftryksscanning. Bo Wolff forklarer, at amerikanerne allerede i en årrække har brugt biometriske teknologier i Afghanistan, men at det ikke er noget, de danske styrker har været med i: "Vi har slet ikke været med på den teknologivogn – ikke mindst fordi, det koster en formue. Vi er jo, sammenlignet med amerikanerne, en meget lille nation uden så mange penge i ryggen." Ifølge Wolff er tiden endnu ikke moden til at vurdere, om de biometriske teknologier vil blive endegyldigt implementeret: "Der er helt sikkert nogle spændende perspektiver i det her, men vi ønsker ikke at drage forhastede konklusioner, da de registrerede biometriske oplysninger også udgør en sikkerhedsrisiko, hvis data skulle falde i de forkerte hænder. Vi skal for enhver pris undgå, at data siver ud, og vi skal sikre os, at data ikke kan blive brugt mod dem, der er registreret. Hvis sådanne oplysninger lækkes til Taleban, kan det få forfærdelige konsekvenser."

Ifølge Bo Wolff er måden udveksling af data kommer til at foregå på helt centralt for, om forsøget bliver en succes eller ej: "Foreløbig er vi danskere en del af den britiske styrke dernede, og der findes allerede aftaler mellem de store nationer om, hvem der har adgang til de relevante databaser. Der er behov for, at Forsvarskommandoen udarbejder et direktiv, som beskriver, hvordan man skal bruge det biometriske udstyr, og hvad man ikke må bruge det til. På nuværende tidspunkt bliver de biometriske data, som vi danskere opsamler, ikke udvekslet med nogen som helst – heller ikke briterne, som vi ellers arbejder tæt sammen med. Og hvis vi på sigt skal udveksle data med de afghanske sikkerhedsmyndigheder, skal vi være 100 procent sikre på, at de håndterer data korrekt. Vi er i koalition med dem, men man bliver altid nødt til at tage nogle forbehold," siger Bo Wolff.

Etik

Hvad er din holdning – hvornår er brugen af biometri okay? Biometriske teknologier kan både være socialt inkluderende, frihedsskabende og privatlivsbeskyttende, men de kan modsat også være ekskluderende, frihedshæmmende og privatlivskrænkende. Hvornår er en biometrisk løsning etisk acceptabel, og hvornår er den direkte uetisk?

Hvilken vej bør vi gå?

Udviklingen går i øjeblikket i en retning, hvor flere og flere informationer bliver samlet hos myndighederne. Hvis vi åbner for at sammenkøre alle de oplysninger, der på nuværende tidspunkt ligger i separate databaser, kan vi udvikle avancerede og detaljerede profiler over alle borgeres adfærd, vaner, præferencer, økonomi, sociale forhold, sundhed og meget mere. Argumenterne herfor er mange, blandt andet: Øget effektivitet og bedre service hos offentlige myndigheder, sikkerhed mod terrorisme, målrettet service i butikkerne, målrettet markedsføring og bedre indtjening i den private sektor, øget sikkerhed i trafikken og øget sundhed i befolkningen. For blot at nævne nogle få.

Men biometri kan også modsat understøtte en udvikling, hvor al information ligger hos borgeren. Ved at benytte biometri og koble det med kryptering kan vi være tæt på 100 procent sikre på, at de oplysninger, en borger afgiver, rent faktisk stammer fra denne borger.

Individ vs. kollektivet

I en etisk diskussion er det derfor afgørende, om vurderingen af et biometrisk system bliver foretaget ud fra hensyntagen til individets eller kollektivets behov. Kan kollektivets behov for eksempel være af en sådan karakter, at de overstiger hensynet til individet? Og hvornår bør hensynet til det enkelte menneskes frihed og ret til privatliv omvendt vægtes over kollektivets behov? Hvilke private og følsomme oplysninger skal lagres? Hvor skal de lagres, og hvilken kontrol bør det enkelte individ have over oplysningerne? Opretholdelsen af privatlivets fred står dermed i modsætning til kollektivets interesse i øget bekvemmelighed, sikkerhed og kontrol.

I de kommende år vil borgerne og forbrugere i stigende grad blive stillet i situationer, hvor de skal aflevere biometri som følge af lovkrav. Dette gælder blandt andet EU-krav til pas og opholdskort. Hvis borgerne ikke vil medvirke, vil konsekvensen være, at deres personlige frihed – her friheden til at rejse – bliver begrænset.

Social inklusion og eksklusion

Biometri kan være både socialt inkluderende og ekskluderende. For eksempel vil blinde eller mennesker med nedsat syn kunne få adgang til betalingsautomater via sikkerhedssystemer, der bygger på stemmeidentifikation i stedet for en pinkode. Tilsvarende vil en erstatning af foto med irisgenkendelse eller finger- eller håndaftryk i passet have den konsekvens, at muslimske kvinder, der af religiøse årsager bærer tørklæde, ikke tvinges til at blotte ansigtet. Et fingeraftryk eller iris afgiver i sig selv ikke informationer om religiøs baggrund, eller om man har en ren straffeattest eller ej. Dog er det ud fra iris og fingeraftryk men især ud fra ansigtsgenkendelse muligt at lave estimater for personens etniske oprindelse. Biometrisk ansigtsgenkendelse vil, ud over at anslå personens etniske baggrund, også kunne estimere køn og alder. Desuden er det muligt at registrere visse former for sygdomme og handicap. Også social klasse

bliver i Japan forsøgt kortlagt i forbindelse med biometrisk skabte forbrugerstatistikker af handlende i butikker og indkøbscentre.

En ny forståelse af kroppen

Indførslen af biometriske teknologier vil betyde, at spørgsmål om, hvem man er, og hvordan man vil blive behandlet i forskellige situationer, i stigende grad vil blive afgjort på baggrund af informationer, som oprindeligt nedstammer fra din egen krop, men som er behandlet andetsteds gennem netværk, databaser og algoritmer. Dette gør det muligt at analysere og kategorisere personer og personoplysninger på en måde, der ikke var mulig før. En sådan udvikling kan forandre den måde, vi opfatter os selv som mennesker og individer i et fællesskab.

Internationalt perspektiv

Biometriske teknologier skaber en række muligheder i det internationale samfund. Biometri kan for eksempel være med til at sikre en lige fordeling af nødhjælp i ulande eller bruges til at forhindre selvmordsbombere i at få adgang til centrale offentlige faciliteter i Irak og Afghanistan. I fattige lande, hvor der ikke findes sikre identifikationspapirer, kan biometri skabe øget sikkerhed for, at en person er den, som vedkommende giver sig ud for – og for eksempel sikre, at det kun er kvinden i en familie, der har adgang til en bankkonto, hvis manden i stedet ønsker at drikke pengene op. Om en sådan adfærdsregulering vil være etisk korrekt eller ej afhænger dog i høj grad af den konkrete kontekst.

Magt over mennesker

Hvis biometriske data er registreret i et biometrisk system, medfører dette, at nogle mennesker har viden og dermed magt over andre mennesker. Kritikere argumenterer for, at en sådan magt altid vil blive misbrugt, hvis der er mulighed for misbrug. De individuelle frihedsrettigheder vil i så tilfælde blive svækket, hvilket i yderste konsekvens kan være til fare for både det demokratiske system og markedets funktions-evne. Set i dette lys er det derfor helt afgørende, at der udvikles biometriske løsninger, som sikrer, at biometriske data ikke kan misbruges.

Hvorfor overhovedet registrere?

Spørgsmålet er, om der overhovedet skal registreres biometriske data. Hvad er det, vi gerne vil opnå med registreringen – og kan dette opnås på andre måder, som ikke har en nær så indgribende karakter? Er al denne registrering og identifikation overhovedet ønskelig eller nødvendig? Får vi løst de problemer, som vi gerne vil have løst, eller er det udtryk for, at politikerne har behov for at udtrykke handlekraft i situationer, hvor de føler sig afmægtige?

Lovgivning

Er eksisterende lovgivning tilstrækkelig? Beskytter lovgivningen borgeren mod misbrug, og giver den mulighed for at udnytte teknologiens potentiale?

Persondataretlige implikationer

Biometriske personoplysningers varige karakter gør dem principielt egnede til at identificere en person gennem et helt liv. Når det offentlige eller en privat virksomhed vil behandle en persons biometriske oplysninger, kan det ske på baggrund af et samtykke eller en interesseafvejning. Når en offentlig myndighed eller en privat virksomhed behandler biometriske personoplysninger på baggrund af et samtykke, er der altid mulighed for, at den person, som er indehaver af f.eks. et fingeraftryk, kan tilbagekalde samtykket med den konsekvens, at den biometriske personoplysning skal slettes.

Når man skal behandle biometriske personoplysninger, er det også væsentligt at vurdere, om anvendelse af biometri er den nødvendige løsning. Man skal således spørge sig selv, om der findes andre mindre indgribende metoder, som kan identificere/verificere den pågældende person. Hvis eksempelvis et sygesikringsbevis og et foto i en database kan identificere en diskoteksgæst, er det ikke nødvendigt at etablere en central database med fingeraftryk.

Vurderingen af, om det er nødvendigt at anvende en konkret biometrisk løsning, skal også indeholde en vurdering af, om det enkelte menneske selv er i besiddelse af sine biometriske personoplysninger på eksempelvis et smart card, eller om oplysningerne opbevares i en central database. En central database indebærer en større risiko for, at den menneskelige integritet kompromitteres.

Samtykkets betydning

Uanset om en dataansvarlig behandler almindelige eller følsomme personoplysninger, kan et samtykke fra den registrerede altid danne det retlige grundlag for behandlingen. Forudsætningen er dog, at selve samtykket opfylder de krav, som lovgivningen stiller til det, og at behandlingen også opfylder de regler, der ligger i kravet om god databehandlingskik.

Muligheden for at tilbagekalde et samtykke, kan også ses som en ulempe, fordi den iværksatte behandling skal stoppe, og der skal udtænkes alternative identifikations/verifikationsmetoder. Her er det spørgsmålet, om det reelt er muligt at basere en teknologisk behandling af personoplysninger på den registreredes samtykke. Det er muligt at basere behandling af biometriske personoplysninger på en afvejning af interesser, hvor hensynet til den virksomhed eller offentlige myndighed, som anvender en biometrisk løsning vejer tungere end hensyn til den person, hvis biometriske personoplysninger behandles. Denne løsning har den fordel, at det ikke er muligt for den registrerede at stoppe behandlingen, fordi samtykket tilbagekaldes.

Behandling af biometriske oplysninger er ikke genstand for nogen form for specialregulering fra hverken national eller europæisk side. Persondataretten har allerede vist sig vanskelig at anvende i praksis, når nye teknologiers lovlighed skal vurderes. Den praktiske anvendelse bliver nok ikke mindre besværlig af, at den dataansvarlige også skal vurdere, om en behandling af personoplysninger ved hjælp af ny teknologi er i overensstemmelse med ikke altid lige gennemsigtige regler.

Stadig mere registrering og overvågning

I fremtiden vil politikere sandsynligvis også skulle forholde sig til befolkningens ændrede holdning til registrering og overvågning. Hvis befolkningen først og fremmest er styret af "convenience"- og "I've got nothing to hide"-argumenter, kan politikerne indskrænke det enkelte individs privatsfære med deraf øget adgang til behandling af personoplysninger.

Der opsættes i disse år stadig flere kameraer, som overvåger trafikken på motorvejene, passagerer i toge, kunder på posthuse, i banker, på benzinstationer, i butikker, i indkøbscentre og tilskuere til fodboldkampe. På mange arbejdspladser registreres de ansattes aktivitet på internettet, på mailen og telefonen. På biblioteket registreres alle udlån med cpr-nummer som reference. I virksomheder og i detailhandlen registreres kunderne og deres indkøb. Teleselskaberne registrerer al teletrafik og opbevarer oplysningerne, så politiet kan få adgang til dem i en sag. På samme måde kan alle med en mobiltelefon i dag spores døgnet rundt på grund af registrering og opbevaring af oplysninger fra sendemasterne. Flyselskaberne indsamler passageroplysninger om destinationer og madpræferencer, som politiet har direkte adgang til uden dommerkendelse. Der er således åbnet op for, at man i princippet vil kunne udvikle mere og mere detaljerede profiler over alle borgeres adfærd, vaner, præferencer, økonomi, sociale forhold, sundhed og meget mere.

Dna-analyse i politikorpset i Afghanistan

Der er planer om at bruge biometri – i form af dna-analyse – i arbejdet med at opbygge et selvstændigt Afghansk politikorps. Der er dog ifølge Kai Vittrup, der er ansvarlig for opbygning af politiet i Afghanistan, langt igen, før det afghanske politikorps kan operere med dna-prøver eller andre biometriske løsninger. "Selvfølgelig er biometri også en del af fremtiden i Afghanistan, men det afghanske politikorps befinder sig på mange områder på et meget lavt niveau lige nu – vi slås blandt andet med analfabetisme –, så der er lang vej igen," siger Kai Vittrup og understreger, at det er målet, at det afghanske politikorps på et tidspunkt skal kunne lave dna-prøver. Men der er brug for flere ressourcer, og politikorpset skal blandt andet lære, hvordan man sikrer dna-prøverne på varme, støvede gerningssteder. "Vi kan ikke komme hurtigt nok i gang, men vi ved også, at det kommer til at tage tid før dna bliver en del af hverdagen. Første skridt er at implementere tankegangen og målene på højt niveau i politiet," siger han.

Kai Vittrup forklarer videre, at man også i det afghanske indenrigsministerium arbejder på at indføre biometri, men at man indtil videre kun er nået til de indledende overvejelser: "Amerikanerne er de eneste blandt de internationale styrker, som virkelig har fået de biometriske teknologier implementeret i deres arbejde i Afghanistan. Men da sikker personidentifikation er et afgørende vigtigt element i en effektiv genopbygningsproces, er det helt sikkert noget, vi alle fremover vil have fokus på".

Privacy

Biometri kan alt efter det teknologiske design være både privatlivsbeskyttende og -krænkende. På den ene side kan biometri understøtte en udvikling, hvor al information ligger hos borgeren. Modsat kan biometri også forstærke den nuværende udvikling, hvor der samles flere og flere informationer hos myndighederne.

Privatlivsbeskyttelse er en grundlæggende rettighed

Privatlivsbeskyttelsen er en grundlæggende rettighed i den Europæiske Menneskerettighedskonvention. Af artikel 8 fremgår det, at både personen selv, herunder krop og udseende, og hans eller hendes adfærd i forhold til for eksempel familie, seksualitet og kommunikation er omfattet af beskyttelsen. Det samme er de materielle ting, der tilhører vedkommende, og de oplysninger, der er knyttet til ham eller hende.

Biometri og personfølsomme oplysninger

Biometriske systemer åbner for identifikation af en person, der enten har eller ikke har nogle bestemte rettigheder. Det betyder, at information om køn, alder, etnicitet mv. ikke nødvendigvis afgives ved adgang. Modsat er der en række problemer ved mange biometriske systemer. For eksempel kan man ud fra irisscanning, ansigtsscanning og ganganalyse afsløre en række sygdomme og handicap. Disse informationer vil være yderst attraktive for forsikringsselskaber, der på den baggrund vil kunne vælge at opsiges samarbejdet med en kunde eller hæve prisen på vedkommendes forsikring. De biometriske systemer bør derfor altid konstrueres på en sådan måde, at der ikke kan læses mere ud af biometrien, end hvad der er relevant til det pågældende formål.

Medtænk privacy fra starten

Mange af de biometriske systemer, der bruges i dag, er baseret på systemer med ikke-krypterede data. Brug af ikke-krypterede, biometriske data har blandt andet den fordel, at det er lettere for myndighederne at sammenligne og sammenkøre forskellige registre og databaser. I effektivitetens og paradoksalt også i sikkerhedens navn bliver hensynet til privacy hermed kraftigt nedtonet. Hvis man derimod ønsker at lave et teknologisk design, der tager hensyn til privacy, bør privacy indbygges i teknologierne helt fra start – det kaldes også "Privacy by Design". Når først et system er opstillet, er det meget vanskeligt og dyrt at indbygge bedre privatlivsbeskyttelse.

Biometri kan rent faktisk bruges på en måde, der tager hensyn til beskyttelse af personoplysninger. For det første bør man sikre de biometriske data i sig selv. Det gøres bedst i de såkaldte "system on card"-løsninger, hvor både den biometriske læser og lagringen af data foregår på selve kortet. Man kan endvidere sikre, at de nøgler, som ligger på kortet, er privatlivsbeskyttende. Det vil i praksis sige, at der genereres koder, som giver brugeren rettigheder, men som ikke muliggør identifikation af for eksempel personens navn, cpr-nummer, adressen, køn og etnicitet.

PRISE-projektet

Det EU finansierede projekt om PRIVacy og SEcurity, PRISE har analyseret udviklingen af sikkerhedsteknologier såvel som aktuelle sikkerhedspolitikker, specielt med sigte på det centrale spørgsmål, hvorvidt mere flere sikkerhedsforanstaltninger, herunder overvågning, nødvendigvis altid vil indebære et tab på privatlivskontoen. PRISE konkluderer, at i en række tilfælde er det muligt at opnå større sikkerhed, uden at det går ud over privatlivet, i visse tilfælde kan privatlivets fred endda blive beskyttet bedre.

Projektet har desuden udviklet kriterier til at evaluere ansøgninger til EU's forskningsprogrammer inden for sikkerhed, et konkret værktøj til at undersøge, om en given sikkerhedsteknologi lever op til både lovgivning om persondata- og privatlivsbeskyttelse, og om teknologien er i konflikt med etik og holdninger blandt borgere i Europa.

PRISE-modellens tre niveauer

Grundlæggende er der tre forskellige niveauer for privatlivsbeskyttelse, som udviklere eller brugere af sikkerhedsteknologi skal forholde sig til.

Det første niveau kaldes *Baseline* med minimumskravene til beskyttelse af privatsfæren, med andre ord en kerne-sfære af privatliv som aldrig må krænkes. Baseline-testen tjekker, om teknologien, som ansøgeren vil udvikle eller brugeren vil benytte, giver mulighed for at overvåge personer og indsamle oplysninger, som krænker personens menneskeværdighed og fysiske integritet. Det giver bl.a. anledning til spørgsmål såsom: Vil teknologien gøre det muligt at overvåge i private hjem? Eller: Tillader den foreslåede teknologi indsamling og bearbejdning af personfølsomme data som eksempelvis seksuelle præferencer, intime tanker og samtaler?

Det næste niveau kaldes *Data Protection Compliance* og kigger på, hvorvidt den foreslåede teknologi er i overensstemmelse med relevante love og regler inden for databeskyttelse. På dette trin stilles der spørgsmål som: Indeholder teknologien aktiviteter som samkøring af data og tværgående analyser? Eller: Muliggør teknologien anonymitet hos de personer, som der indsamles data om (borgerne)?

Det øverste trin, *Context-Sensitive Trade-Off*, beskæftiger sig med de situationer, hvor en teknologi reelt overskrider grænserne for begge de foregående niveauer, men alligevel mener at have en berettigelse på grund af den øgede sikkerhed for samfundet, teknologien medfører. På dette niveau accepterer man altså et trade-off, men PRISE-metoden skal samtidig sikre, at der er proportionalitet mellem gevinsten på sikkerhedssiden og tabet for privatlivets beskyttelse på den anden, hvorfor der spørges der ind til konteksten - hvilke sikkerhedsfordele teknologien konkret medfører.

Sådan fungerer PRISE-modellen i praksis

Ud over at identificere niveauet for privatlivsbeskyttelse, tilbyder PRISE-modellen også konkrete værktøjer og metoder til at overkomme en eventuel privacy-krænkelse. F.eks. i forbindelse med en af tidens mest omdiskuterede sikkerhedsteknologier, den såkaldte "nøgenmaskine", som bruges i bl.a. USA og England. Nøgenmaskinen bruges typisk i lufthavne til at scanne den enkelte passager med det formål at identificere farlige materialer som f.eks. plastisk sprængstof. Det indebærer imidlertid at afbilde passageren uden tøj på, og det virker krænkende på mange mennesker. Reaktionen hos de borgere, der deltog i PRISE projektets interviewmøder var da også, at de afviste brugen af den type teknologi. "Hvis en nøgenmaskineløsning har problemer med at klare eksempelvis baseline-kriterierne, vil PRISE's værktøjer formentlig kunne hjælpe med gode råd. F.eks. ved at billedet kun viser konturerne på personen, men ikke er kropsspecifik. En anden løsning kunne være, at den person der betjener scanneren, og dermed ser personen, ikke er den samme, som kigger på billederne. En juridisk løsning kunne være at teknologien kun må blive brugt i specifikke situationer eller under specielle, prædefinerede omstændigheder. De samme principper gør sig gældende på de to øvrige niveauer.

Kilde: Fra Rådet til Tinget nr. 259

PRISE-projektet er blevet varetaget af det danske Teknologiråd deltog Institute of Technology Assessment (Østrig), Uafhængiges Landeszentrum für Datenschutz Schleswig-Holstein (Tyskland) samt Teknologirådet i Norge.

Se mere om PRISE på www.prise.oeaw.ac.at og www.tekno.dk

Sikkerhed

Hovedbegrundelserne for at benytte biometriske teknologier er primært bekvemmelighed og øget sikkerhed. Men af mange årsager vil man ikke kunne skabe et system, der er 100 procent sikkert. Det er derfor afgørende, at biometriske systemer ikke tillægges en ultimativ sandhedsværdi, men at man derimod i hver enkelt situation vurderer fordele og ulemper ved brug af biometri.

Biometri er aldrig 100 procent sikkert. For eksempel kan kunstige gummifingre eller masker bruges til at omgå mange biometriske scannere. Men selv i situationer, hvor der ikke gøres forsøg på at snyde de biometriske systemer, er der ofte en betydelig andel falske "matches" – også kaldet "non-matches". En fejlrate på bare 1 procent i store landsdækkende eller internationale biometriske systemer er ensbetydende med et stort antal forkerte afgørelser. Der er derfor god grund til at tænke sig grundigt om, inden man vælger at bruge biometri til identifikation i stor skala. Når det er sagt, kan de fejlprocenter, der er forbundet med ren menneskelig kontrol, i nogle tilfælde være meget højere.

Bekvemmelighed eller datasikkerhed?

Der kan være flere grunde til at opstille biometriske systemer. En af hovedbegrundelserne for at benytte biometriske teknologier er bekvemmelighed – ofte kaldet "convenience". Men biometri bliver ligeledes anvendt med henblik på at opnå en bedre sikring af såvel data og materielle genstande som mennesker. Selv om bekvemmelighed er hovedformålet med et biometrisk system, er det desuden vigtigt også at være opmærksom på, hvilke andre sikkerhedsmæssige effekter brugen af biometri medfører.

Øget sikkerhed kan også være målet for brug af biometri. Der er dog mange faldgruber. Selv om man i princippet altid burde kryptere biometriske data, har erfaringer vist, at dette langt fra altid sker. Ligeledes er såkaldte "system-on-card", hvor både lagring, scanning og matchning forgår på et smartcard med en biometrisk læser, set i forhold til datasikkerhed at foretrække frem for systemer, hvor matchning og lagring af data foregår uden for brugeres kontrol. Krav til effektivitet og lavest mulige omkostninger gør dog, at biometriske løsninger baseret på "system-on-card" endnu ikke har fået sit store gennembrud.

Sikkerhed for hvem?

Høj datasikkerhed er langt fra altid det, der bliver talt om, når politikere og andre beslutningstagere diskuterer sikkerhedsspørgsmål. I en diskussion om biometriske systemers sikkerhed kan man med fordel skelne mellem sikkerhed for brugeren og sikkerhed for opstilleren.

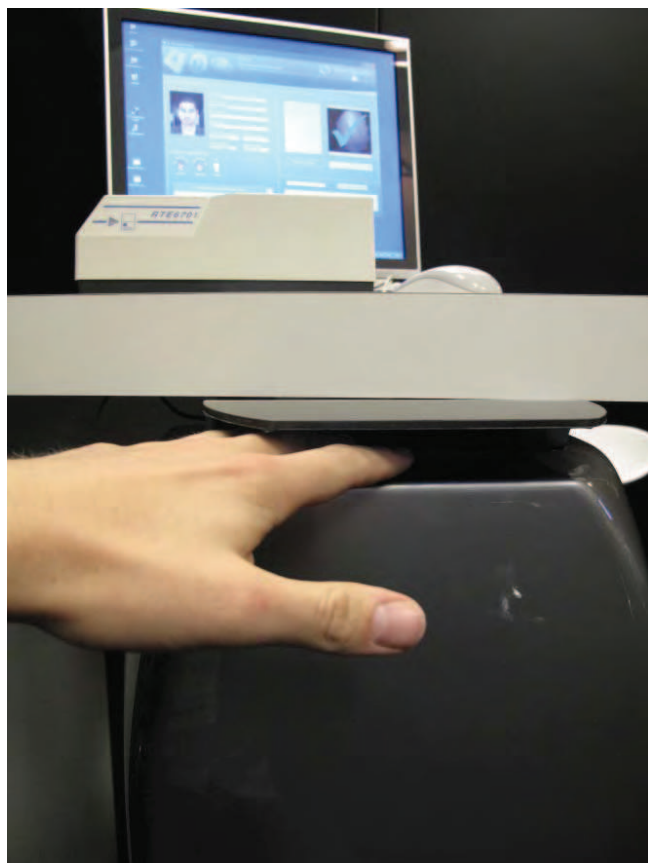
Sikring af den enkelte bruger, hvad enten denne er borger, kunde eller en ansat i en virksomhed, er ofte ikke målet for opstillerne af biometriske systemer, som typisk er myndigheder, organisationer eller virksomheder. For eksempel blev de biometriske pas indført med det formål at skabe et mere sikkert samfund. Men kritikerne af det nye pas vil hævde, at det repræsenterer et skridt i retning af det stik modsatte. At passet indeholder biometriske karakteristika, kan på den ene side skabe øget sikkerhed for, at en person er den, vedkommende giver sig ud for at være. Modsat har man som individ ikke særlig stor kontrol med, hvad myndighederne bruger ens biometriske oplysninger til. Det vil for eksempel i princippet være muligt at sammenligne ens fingeraftryk med profiler i det nationale kriminalitetsregister i det pågældende land. På denne måde kan der sagtens være et modsætningsforhold mellem på den ene side

sikring af individets rettigheder i form af høj datasikkerhed og på den anden side statens sikkerhed.

Templates og grænseværdier er afgørende for systemets sikkerhed

Templates er dannet på baggrund af specifikt udvalgte dele af selve de biometriske karakteristika – for eksempel bestemte punkter i et fingeraftryk eller en bestemt rytme knyttet til en persons gangart. Nogle templates er meget simple og eksempelvis baseret på 5-10 punkter i brugerens fingeraftryk – en sådan løsning bruges for eksempel til udlevering af skolemad i England -, mens andre indeholder mere avancerede data. De enkelte systemer er meget forskelligt konstrueret, og der er fra teknologi til teknologi stor forskel på, hvor kompliceret det er at rekonstruere velfungerende biometriske data ud fra templates. Dog er dette, i modsætning til hvad mange tror, rent faktisk muligt.

Det er en udfordring at konstruere et koncept for templates, som på den ene side ikke stiller så store krav til match, at man bliver afvist, fordi man for eksempel smiler, og på den anden side ikke slipper andre igennem, fordi der er visse sammenfald i udseendet. Forandringer i udseendet som følge af aldring er også en udfordring for mange biometriske systemer.



Biometriske teknologier vinder frem overalt

Kunderne til biometri har traditionelt været efterretningstjenester. De senere år har biometriske løsninger imidlertid vundet indpas på mange forskellige samfundsområder – både som et værktøj til kriminalitetsforebyggelse og som en service-forbedrende løsning i utallige sammenhænge. Danske og udenlandske virksomheder slås om kunderne på et allerede stort marked, der vurderes at ville vokse markant fremover.

Den internationale it-koncern Logica har p.t. omkring 500 mennesker ansat til blandt andet at udvikle biometriske løsninger baseret på standardprodukter, som Logica tilpasser til den enkelte kundes behov. Kunderne har traditionelt været efterretningstjenester og politienheder i lande som England, Holland, Frankrig, Tyskland, Sverige og Danmark, men de seneste år har biometri som forretningsområde oplevet enorm vækst, og alt tyder på, at erhvervsmulighederne vil fortsætte med at vokse fremover, fortæller afdelingsleder Martin Kiær, der har ansvar for Logicas danske aktiviteter på sikkerhedsområdet.

Han er samtidig idémanden bag forskellige biometriske løsninger – blandt andet et biometrisk koncept kaldet FaceVault, som Logica har store forventninger til. Hovedtanken bag FaceVault er at udvikle et biometrisk grundkoncept – ikke for at forebygge terror eller lignende, men med det ene formål at skabe bedre service. FaceVault er baseret på ansigtsgenkendelse og kan tilpasses en lang række forskellige formål.

”Vi er i fuld gang med at udvikle forskellige FaceVault-standardløsninger. En løsning er målrettet identifikation og udskrivelse af gæstekort med foto til besøgende i en virksomhed. En anden er til plejehjem for demente beboere. Plejehjemmets udgange overvåges af kameraer, der giver besked til det nærmeste personales PDA eller telefon, hvis en dement beboer forlader bygningen. Herefter kan medarbejderen opsøge den demente og stille og roligt hjælpe ham eller hende sikkert tilbage,” siger Martin Kiær.

Logica er også i gang med at udvikle en hospitalsløsning. Tanken er her, at der ved siden af den enkelte hospitalsseng er opsat en skærm med indbygget ansigtsgenkendelse¹⁰, som genkender den enkelte læge eller sygeplejerske, der går stuegang, og straks giver adgang til den relevante patients journaloplysninger på skærmen.

”Lægen skriver nye noter ind i journalen via for eksempel et lysbaseret tastatur. Løsningen er tidsbesparende og samtidig mere hygiejnisk i forhold til den PDA, lægerne normalt bærer med sig fra stue til stue,” siger han.

Genkender kriminelle

Martin Kiær lægger dog ikke skjul på, at de biometriske løsninger, som Logica indtil videre har leveret, først og fremmest har haft til formål at forhindre terrorisme, vold, tyveri, bedrageri, hvidvaskning af penge, identitetstyveri, trusler mod virksomheder, ulykker og katastrofer. Til disse formål har Logica udviklet et koncept kaldet i-Catcher, som blandt andet er målrettet overvågning af utrygge ”hot spots” i storbyer. Pladser, hvor mange mennesker samles, veje og midlertidige mødesteder såsom koncerter og sportsbegivenheder.

i-Catcher kan genkende registrerede personer og sende en advarsel til nærmeste politienhed. Men systemet er også målrettet genkendelse af særlige handle- og bevægelsesmønstre, som man erfaringsmæssigt ved med stor sandsynlighed vil føre til kriminalitet. i-Catcher registrerer mistænkelige mønstre og rapporterer dem ligeledes til nærmeste politienhed, som herefter kan gribe ind og i bedste fald forebygge, at kriminaliteten finder sted.

¹⁰ Ansigtsgenkendelse med enten RFID eller NFC teknologi.

Udover at løsningen i forskellige versioner og til forskellige formål benyttes af en række efterretningstjenester, hvilket Martin Kiær af naturlige årsager ikke kan gå i detaljer med, bliver i-Catcher blandt andet også brugt til overvågning af en lang række benzinstationer i Holland. Tyveri af benzin er et stort problem, og en kæde af benzinstationer har derfor hyret Logica til at udvikle et overvågningssystem, som kan forhindre tyve i at vende tilbage og gentage deres kriminalitet.

”Vi har opsat en overvågningsløsning med henholdsvis ansigts- og nummerpladegenkendelse. Systemet er forbundet med den hollandske politis database med fotografier af mere end 45.000 personer. Her er også tidligere benzintyve og nummerpladerne på deres biler registreret. Når der optræder et match, bliver personen forhindret i at tanke, og systemet sender samtidig besked til politiet,” siger Martin Kiær, der videre fortæller, at Logica har udviklet tilsvarende løsninger til afsløring af voldelige Hooligans på en række engelske og hollandske fodboldstadioner.

Logica har været i dialog med både FC København og Brøndby om lignende løsninger, der dog ikke har kunnet realiseres på grund af den danske lovgivning om persondatabeskyttelse. Ifølge Martin Kiær forhindrer dansk lov ligeledes, at Danmark indfører en løsning som den på de hollandske benzinstationer.

Privacy by design

Men betyder det, at dansk lovgivning er en stopklods for, at vi kan udnytte biometriens mange positive muligheder herhjemme?

”Ja, som lovgivningen ser ud i øjeblikket,” siger Martin Kiær. ”Men jeg tror, der vil ske en gradvis opblødning, så vi bliver knap så strikse. I mange andre lande har man allerede erfaret, at fordelene ved de biometriske løsninger er meget større end de mulige ulemper. Jeg er overbevist om, at convenience-faktoren er så stærk, at den i sidste ende vil vinde, fordi vi mennesker altid søger efter det, der kan lette vores arbejde og hverdag mest muligt – uanset om det er til efterretnings- eller serviceformål,” siger Martin Kiær, der samtidigt understreger, at respekten for menneskers privatliv også er et uhyre vigtigt aspekt for Logica.

”Derfor er alle vores biometriske løsninger baseret på en Privacy by Design-tankegang, hvor vi allerede i udviklingsfasen sikrer, at den relevante persondatalovgivning er overholdt. Det har vi for eksempel gjort i forhold til den FaceVault-løsning, vi i en testperiode har afprøvet på en restaurant i en dansk forlystelsespark. Data er krypteret, hvilket betyder, at hverken hackere, politi eller andre kan få adgang til det bagvedliggende system og trække data ud. Løsningen kører i et lukket netværk, og data slettes fra systemet hver dag, når restauranten lukker,” fortæller Martin Kiær

Han forudser, at multifaktoridentifikation, hvor mindst én af faktorerne er biometri, fremover vil få en nøglerolle i de sammenhænge, hvor der er brug for optimal sikkerhed.

”Der er ingen tvivl om, at man ved at kombinere biometrisk genkendelse med for eksempel en pinkode – og derved kombinere noget, man er, med noget, man har – kan opnå et meget højt sikkerhedsniveau,” siger Martin Kiær, der samtidig ikke lægger ikke skjul på, at flertallet af de biometriske løsninger stadig lader en del tilbage at ønske rent teknologisk.

”Det er stadigvæk ny teknologi, og der er et stykke vej endnu, før alle mulighederne folder sig ud. Systemernes nøjagtighed kan for eksempel blive endnu bedre, men det går utrolig stærkt i øjeblikket. Konkurrencen er enorm, og producenterne slås om at komme først med det nyeste og bedste, og vi andre slås om at udvikle målrettede løsninger til bestemte segmenter. Om 10 år vil biometriske teknologier som dem, man ser i en film som *Minority Report* og en tv-serie som *CSI*, være standard. Samtidig vil biometri være en helt integreret del af vores hverdag på mange områder – for eksempel når vi besøger netbanken eller skal gennem adgangskontrollen på arbejdspladsen eller i lufthavnen,” spår han.

Biometriske udfordringer

Herhjemme er den danske supermarkedskæde Fakta frontløber, når det gælder biometri. Kæden har i løbet af de seneste år indført fingeraftrykslæsere i samtlige butikker. En evaluering viser stor tilfredshed

med løsningen hos Faktas ledelse og blandt medarbejderne. Men det betyder ikke, at der ikke har været udfordringer i forbindelse med systemet, siger Lars Kornbek, administrerende direktør for Vitani, der udvikler løsninger inden for biometri og overvågning.

”Det har blandt andet vist sig, at man i nogle af Faktabutikkerne ikke var omhyggelige nok under selve registreringen af medarbejdernes fingeraftryk i systemet. Problemet er, at hvis det første fingeraftryk, der bliver lagt ind, er dårligt, vil systemet sandsynligvis ikke godkende medarbejderen senere hen. I værste fald kan man risikere at blive genkendt som en anden,” siger Lars Kornbek.

”Det viste sig også at være en udfordring i forbindelse med brugen af systemet, at medarbejdere, der lige havde været i kølerummet og derfor havde meget tørre fingre, fik problemer med at få adgang til kassen ved hjælp af fingeraftrykket. Her skulle de blot lære at gnide fingrene mod hinanden eller komme lidt næsefedt på fingeren – så virkede systemet igen,” fortæller Lars Kornbek, der kategoriserer de to problemstillinger som begyndervanskeligheder.

Han fortæller videre, at kvaliteten af de biometriske teknologier udvikler sig med lynets hast. Faktaløsningen er baseret på en traditionel afbildning af fingeraftrykket. En nyere teknologi måler mængden af luft mellem pladen og fingerens forskellige revner og fordybninger og generer et fingeraftryk derudfra. En tredje løsning sender radiosignaler ind i fingeren og danner fingeraftrykket på baggrund af det, der reflekteres, og en fjerde løsning danner fingeraftrykket ud fra en registrering af temperaturforskelle mellem fingerens forhøjninger og fordybninger. Den allernyeste teknologi kaldes spektral-analyse. Det går ud på, at man sender fire forskellige bølglængder af lys mod fingeren. Fordelen er, at det ikke er selve fingeraftrykket, der bliver aflæst, men derimod de små blodårer inde bagved aftrykket. Det betyder, at systemet fungerer selv under meget vanskelige forhold, hvor en finger for eksempel er beskidt, tør eller våd.

Biometriens mangfoldighed

Vitani har praktiske erfaringer med at udvikle og opsætte en række forskellige biometriske teknologier. For it-hosting-selskaberne Interaction og Fuzion har Vitani installeret systemer med irisgenkendelse ved indgangen. I praksis stiller brugeren sig hen foran et kamera, hvorefter iris aflæses på 0,3 sekund. På Ringkøbing Bibliotek har Vitani installeret en fingeraftryklæser, som borgerne kan bruge ved udlån i stedet for sygesikringsbeviset. For MidtVest Bredbånd har Vitani udviklet en biometrisk løsning med fingeraftryklæsere på adgangssluserne til virksomhedens tekniske lokationer. Medarbejderne har deres fingeraftryk lagret digitalt på et plastikkort. Proceduren er her, at man præsenterer sit kort til en enhed ved siden af fingeraftryklæseren, som indlæser data og sammenligner dem med data fra den finger, man samtidig placerer på læseren. ”Fordelen ved denne løsning er, at medarbejdernes fingeraftryk og tilknyttede data ikke skal opbevares i en database med potentiel risiko for misbrug,” siger Lars Kornbek,

Fakta – en biometrisk frontløber

Supermarkedskæden Fakta har installeret Skandinaviens hidtil største biometriske løsning. I alle kædens 340 butikker er der installeret en fingeraftryklæser ved henholdsvis kasseterminalerne og butikkens pengeskab. Det tager ca. 0,5 sekund for medarbejderen at få adgang til kassen ved hjælp af sit fingeraftryk. Kun medarbejdere med den rette autorisation kan få adgang.

Den biometriske løsning har erstattet de gamle magnetkort. Det er både billigere og lettere rent administrativt for Fakta at benytte sig af fingeraftryk i stedet for at udstede magnetkort til de mange nye ansatte, virksomheden får hvert eneste år. Hvor det før tog tre dage at få lavet et medarbejderkort, er en ny medarbejder på det nye system i løbet af ét minut.

Løsningen er baseret på en standardfingeraftrykløsning, som er udvidet med specialudviklet software, der er målrettet Faktas arbejdsprocesser. Løsningen opdateres fra Faktas centrale personalesystem.

Ifølge selskabet bag Fakta-løsningen, Vitani12, har en evaluering vist, at de forventede fordele er opnået. Samtidig har medarbejderne generelt reageret positivt. Fakta fremhæver blandt andet, at sikkerheden i butikkerne er blevet bedre, og at arbejdsmiljøet også er forbedret.

der også kan fortælle, at Vitani arbejder på flere projekter, som benytter ansigtsgenkendelse – og det er ikke mindst hér, vi skal finde fremtidens biometriske løsninger, forudser han.

”Et fællestræk ved fremtidens løsninger bliver sandsynligvis, at brugerne ikke bemærker dem. Ansigtsgenkendelse er interessant, fordi man ikke skal standse op foran et kamera eller sætte sin finger eller en hånd på en læser, men kan gå lige forbi den biometriske installation og få den ønskede adgang – eller blive stoppet. Samme fordele har de systemer, der er på vej på markedet, som kan aflæse iris på relativt lang afstand,” siger Lars Kornbek, der ikke er ubetinget glad for dén udvikling.

”En ting er at bruge fingeraftryk, håndgenkendelse, venegenkendelse eller andre biometriske løsninger, der forudsætter, at man som borger ved, man bliver registreret. Noget andet er at blive genkendt og registreret i en eller anden kæmpe database, uden man ved, det sker. Det sidste, mener jeg, er etisk uacceptabelt og noget, vi skal modarbejde.”

Samtidig pointerer han på linie med Martin Kiær fra Logica, at biometri også vil vinde indpas på en lang række områder, hvor teknologien udelukkende har en positiv, serviceorienteret anvendelse. Det gælder en løsning, bilmærket Lexus har introduceret, som via ansigtsgenkendelse giver signal fra sig, hvis føreren gør tegn til at falde i søvn bag rattet. Det kan få stor betydning for trafiksikkerheden. Et andet bilmærke, BMW, er på vej med et biometrisk identifikationssystem, som gør, at bilen genkender ansigtstrækkene hos alle, der har ret til at køre i den. Der er også biometriske løsninger på bedding, som er baseret på den unikke ledningsevne, som hvert eneste menneske ifølge den nyeste forskning er udstyret med. Ledningsevnen måles ved, at personen holder i to forskellige håndtag. Biometri ved hjælp af ledningsevne vil kunne implementeres i for eksempel store håndværktøjer, som automatisk klarlægger, om man har autorisation til at bruge det pågældende værktøj.

Som et sidste eksempel kan nævnes biometri til scanning af passagerer – også kaldet ”The Naked Machine” - , som ved hjælp af for eksempel terahertz-stråling kan anvendes til sporing og visualisering af genstande, der er gemt under tøjet. Apparatet kan blandt andet afsløre, om der er våben eller eksplosiver gemt på en persons krop. Der er forskellige systemer i anvendelse, hvoraf nogle afslører alt, hvad der er under tøjet – deraf navnet ”The Naked Machine”. Denne type lufthavnssikkerhed testes i øjeblikket i mange lufthavne verden over.

Biometriske pas – redskab mod terror og illegal indvandring

Det biometriske pas er ét af den rige verdens modsvar på især terrortruslen, men det vil også få en bremsende effekt i forhold til det voksende indvandringspres på grænserne. En række EU-lande har arbejdet målrettet hen imod at indføre fuldautomatiseret, elektronisk paskontrol, men på den front halter Danmark bagefter.

Siden efteråret 2006 har alle nye pas i Danmark og resten af EU indeholdt biometriske data, som er lagret i en ikke umiddelbart synlig computerchip, der foruden en række personlige oplysninger og en landekode rummer en elektronisk kopi af pasbilledet. Og der er flere årsager til, at det traditionelle pas ikke længe er tilstrækkeligt, fortæller Lene Gisselø, chefkonsulent i Rigspolitiet med ansvar for udvikling og implementering af den kommende version af det biometriske pas i Danmark.

”Terrorangrebet i USA den 11. september 2001 skabte behov for større sikkerhed om rejsedokumenterne, end man var vant til. Derfor stillede USA som den første nation krav om, at pas fremover skulle indeholde et digitalt foto, som af mange årsager er overordentlig svært af forfalske. Siden fulgte EU efter med en tilsvarende pasløsning, der nu udbygges på en sådan måde, at pasindehaverens fingeraftryk også skal ligge på passets chip,” siger hun og fastslår, at indførelsen af det biometriske pas vil medføre, at det både bliver sværere at lave og nemmere at afdække falske pas.

”Dermed gør vi også livet sværere for mennesker, der med et falsk eller stjålet dansk pas uretmæssigt forsøger at få adgang til Danmark. Det biometriske pas vil også på lidt længere sigt – og især hvis paskontrollen automatiseres – være et middel til at sikre et kontinuerligt passagerflow og minimere kødannelse i blandt andet lufthavne, som uvægerligt opstår, fordi højere sikkerhed tager længere tid,” siger Lene Gisselø.

EU's begrundelse¹¹ for at indføre biometriske pas

”Integrering af biometriske identifikatorer er et vigtigt skridt hen imod ... at gøre rejsedokumentet sikrere og etablere en mere pålidelig forbindelse mellem indehaveren på den ene side og passet og rejsedokumentet på den anden side og dermed bidrage væsentligt til at sikre, at det beskyttes mod svigagtig brug.

Det skal sikres, at der ikke lagres andre oplysninger i passet end dem, der er foreskrevet i denne forordning eller i bilaget hertil, eller som det fremgår af det relevante rejsedokument.

Pas og rejsedokumenter skal omfatte et lagringsmedium, der indeholder et ansigtsbillede. Medlemsstaterne skal også indsætte fingeraftryk i interoperable formater. Oplysningerne skal sikres, og lagringsmediet skal have tilstrækkelig kapacitet og være i stand til at sikre oplysningernes integritet, ægthed og fortløbe karakter.

For at sikre, at de omhandlede oplysninger ikke bliver tilgængelige for flere personer end nødvendigt, er det også vigtigt, at hver medlemsstat kun udpeger ét organ som ansvarlig for fremstilling af pas og rejsedokumenter.”

Grønt eller rødt lys

Hun understøtter, at der ikke er aktuelle danske planer om at indføre automatiseret, elektronisk paskontrol på samme måde, som man de senere år har eksperimenteret med i blandt andet Portugal og England.

¹¹ Citater fra Rådet for den Europæiske Unions forordning nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometrisk identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:DA:PDF>

Her arbejder man målrettet på at indføre et system, som på et tidspunkt helt skal afløse det personlige møde med paskontrolløren.

Konkret vil det foregå sådan, at man som rejsende går hen til en scanner og får sit ansigt og eventuelt også fingeraftryk scannet. Samtidig præsenterer man sit pas for systemet, der nu sammenligner billederne af ansigt og fingeraftryk på computerchippet i det biometriske pas med de nye optagelser og giver grønt eller rødt lys.

I England begyndte man at teste et sådant system i sommeren 2008, og det har vist sig nødvendigt med bemandede scannere, da systemet endnu trækkes med en række uløste udfordringer. For eksempel har man erfaret, at det bagvedliggende biometriske it-system ikke altid er i stand til at tage højde for forandringer efter for eksempel en ansigtsløftning. I testperioden – og formentlig også efterfølgende – vil passagerer, der af forskellige årsager afvises af det biometriske kontrolsystem, blive henvist til en kø med manuel paskontrol.

På vej mod automatisk paskontrol

Ifølge EU's forordning om biometriske pas¹² skulle det biometriske pas med både ansigtsbillede og fingeraftryk lanceres senest i sommeren 2009. Det er ifølge Lene Gisselø også sket i en række EU-lande – dog ikke i Danmark. Forsinkelsen herhjemme henfører hun til den enorme kompleksitet i forbindelse med at indføre de nye biometriske pas.

”Vi har et udbud i gang i øjeblikket med henblik på at skaffe det datafangstudstyr og den it-systemløsning, der skal til, for at vi kan håndtere de nye pas. Det handler blandt andet om, at de ude i kommunerne skal have det rette udstyr, så de kan scanne borgernes fingeraftryk og tage pasfotos. Vi vil indføre elektronisk pasudstedelse, så alle informationer sendes elektronisk fra kommunen til pas-producenten. Komplexiteten vokser yderligere, fordi der er så mange myndigheder involveret – det gælder politiet, kommunerne, Integrationsministeriet, øvrige udlændingemyndigheder og Udenrigsministeriet,” fortæller hun.

Men hvis man fra EU's side skaber et passystem, som åbner for at indføre fuldautomatiseret, elektronisk paskontrol, hvorfor skal Danmark så ikke også gå efter det?

”Det er en politisk beslutning, og jeg kan kun sige, at der ikke er konkrete planer på det område herhjemme. Jeg ved, at der foregår overordnede overvejelser om det på EU-plan, men ikke noget, de er så langt med, at man kan sige noget konkret. Men jeg tør dog godt sige, at det er meget sandsynligt, at automatisk paskontrol på et vist tidspunkt vil blive introduceret i EU-regi,” slutter hun.

Biometriske pas er ikke 100 procent sikre

Kravet om større sikkerhed i forbindelse med indrejsende personer har fået mange lande til at overveje, hvordan de kan stramme op på kontrollen ved grænserne. USA, EU og andre har valgt at indføre digital biometrisk identifikation som en del af passet. I nye danske pas er der indlagt en chip med en hemmelig kode og et digitaliseret, krypteret foto af passets ejer. Næste skridt bliver, som det fremgår af artiklen herover, at indføre fingeraftryk i passet. Brug af avanceret biometrisk identifikation i passet vil have den effekt, at man får bedre muligheder for at kontrollere personens identitet. Paskontrollen kan sammenholde de biometriske kendetegn, som er lagret i passet, med den konkrete person og se om de matcher. Dermed mindskes risikoen for misbrug af personoplysninger. Ifølge Niels Christian Juul, ph.d. og lektor ved Institut for Kommunikation, Virksomhed og Informationsteknologier på RUC, er et sammenfald mellem oplysningerne i passet og personen dog ikke ensbetydende med, at matchet er 100 pct. sikkert. ”Ethvert system er ikke stærkere end det svageste led, og man må tage den mulighed i betragtning, at en person ved hjælp af falske identifikationspapirer har indrulleret sig i systemet under falsk identitet,” fastslår Niels Christian Juul.

¹² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:DA:PDF>

Biometri kan ikke løse alle sikkerhedsproblemer

Biometri har nået et udviklingsstade, hvor mange løsninger er ved at være færdigudviklede og bliver markedsført som sikkerhedsløsninger. Men der er stadig mange fejlkilder, og løsningerne er langt fra 100 procent sikre. Derfor skal man fortsat være opmærksom på den sikkerhed man får – og særligt ikke får –, når biometrien tages til hjælp, mener RUC-forsker.

Biometri er ikke noget nyt. Vi har i årtier haft pas med foto og beskrivelse af hårfarve, øjenfarve og højde. I moderne biometri digitaliseres processerne. Teknologierne bag biometriske løsninger opsamler personens kendetegn. Hvad enten de sidder i fingeren, øjet, ansigtet eller et helt fjerde sted på kroppen eller kommer til udtryk gennem måden, personen opfører sig – for eksempel gangart, håndskrift eller tastaturtryk.

Ifølge Niels Christian Juul, ph.d. og lektor ved Institut for Kommunikation, Virksomhed og Informationsteknologier på RUC, får man generelt set alt for mange uvæsentlige data, når man opsamler biometriske informationer fra eksempelvis et tredimensionelt billede af et ansigt. Derfor udtrækker et biometrisk system kun de kendetegn, som er karakteristiske.

”Inden for hver enkelt biometrisk teknologi findes der et stort antal karakteristiske kendetegn, som kan bruges til at skelne mellem brugerne af systemet. De enkelte løsninger baserer sig på hver sit sæt af karakteristika, som samles i en ”template”, forklarer han.

En template er en sekvens af 0- og 1-taller, som det biometriske system danner hver gang det præsenteres for en persons pegefinger, hånd, ansigt eller andet. Og da man kan trække rigtig mange karakteristika ud af ét enkelt fingeraftryk, kan det også resultere i mange forskellige templates.

”Et godt biometrisk system baseres på et udvalg af karakteristika, så det danner den samme template hver gang den samme person præsenterer sig for systemet, og to forskellige templates, hvis der er tale om to forskellige personer. Et andet system kan bruge andre karakteristika, ligesom man kan justere et biometrisk system, så den enkelte persons template dannes ud fra et nyt sæt af karakteristika,” siger Niels Christian Juul.

Uenighed om sikkerheden

Han fortæller, at der er uenighed blandt eksperter om, hvorvidt det er muligt at genskabe det oprindelige billede af personen ud fra templaten. Men hvis det er muligt, vil det åbne for, at en person med kriminel hensigt kan iklæde sig en anden identitet.

”Mit synspunkt er, at man må gå ud fra, at der enten allerede er reel mulighed for at spole tilbage fra templaten, eller at det bliver muligt på et senere tidspunkt. Derfor bør vi i dag medtage det som en konkret risiko i forbindelse med brugen af alle biometriske teknologier. Men det er en risiko, man kan gøre en hel del for at mindske ved dels at stille høje sikkerhedskrav til den underliggende teknologi og dels kombinere flere forskellige biometriske teknologier i den samme løsning, så man for eksempel skal identificere sig både med ansigtsgenkendelse og fingeraftryk,” siger Niels Christian Juul.

En template fylder stadig meget, og da den måske kan føres tilbage til en person, er der tale om persondata, som ikke bare kan flyde ubeskyttet rundt mellem it-systemerne. Derfor forskes der i dag i at omforme templaten ved hjælp af en såkaldt ”hashfunktion” til en ny og kortere sekvens af 0- og 1-taller. En hashfunktion er en envejsfunktion, som er kendetegnet ved, at man kan gå fra ét datasæt til et andet og kortere datasæt uden mulighed for at komme tilbage igen.

En hashfunktion har også, forklarer Niels Christian Juul, en spredningseffekt med det resultat, at hvis man underkaster to tal, der ligger tæt på hinanden, for en hashfunktion, så vil de to nye tal, der kommer ud i den anden ende, ligge langt fra hinanden.

"I et biometrisk system, hvor templates gemmes som hashværdier, er det derfor en særlig udfordring at sikre, at præcis den samme template dannes hver gang for den samme person, da hashværdierne ellers vil være helt forskellige," siger han.

Biometrien udfordres

Niels Christian Juul fremhæver, at en anden vigtig teknologisk udfordring i forbindelse med al biometri er at sørge for, at der sker et præcist match mellem de data, der er lagret i systemet om den enkelte person, og de data, den biometriske løsning har opsamlet på stedet, når man for eksempel skal have adgang til en virksomhed eller til en "fast lane" gennem lufthavnen. Man skal med andre ord undgå, at systemet afviser personer, der har ret til adgang, eller godkender personer, som ikke har ret til adgang.

"Problemet er her, at man kan risikere et sammenfald i templates i forhold til to næsten ens ansigter, fordi templates ikke giver et fuldstændigt billede af de oprindelige karakteristika, men kun et udtræk af dem. Udfordringen er at konstruere et koncept for templates, som på den ene side ikke stiller så store krav til match, at man bliver afvist, fordi man for eksempel smiler, og på den anden side ikke slipper andre igennem, fordi der er visse sammenfald i udseendet," siger han.

Niels Christian Juul fastslår samtidig, at den måske største risiko for tyveri af persondata skal findes i den fase, hvor de biometriske oplysninger lægges ind i systemet. Det er i den fase, de biometriske templates bliver dannet.

Forandringer i udseendet som følge af aldring er også en massiv udfordring i forhold til et biometrisk system, der skal kunne håndtere aldring. Her kan det være en mulighed at gennemføre en dynamisk opdatering af systemet, så det registrerer ændringerne, siger han.

"En af problemstillingerne her er, at det blandt andet forudsætter, at folk bruger systemerne jævnlige, så der ikke når at ske så store ændringer med udseendet, at man ikke bliver genkendt. En anden og nok så alvorlig udfordring er, at en svindler ved hjælp af sminke mv. kan udgive sig for en anden person, som systemet kender, og derefter gradvist ændre på sit udseende, indtil han antager sit naturlige udseende, og systemet accepterer det. Dermed har han stjålet den andens persons identitet," siger Niels Christian Juul og nævner, at der også er særlige forhold omkring børn, fordi deres biometriske kendetegn ændrer sig massivt, indtil de når en vis alder. Og der er mange flere udfordringer på den konto:

"Det er også et problem, at folk kan komme til skade og miste for eksempel en hånd eller et øje, så de ikke kan give fingeraftryk eller benytte irisgenkendelse længere. Tilsvarende ses det relativt ofte, at arbejdsforhold kan påvirke kroppen så meget, at de biometriske kendetegn ændrer sig markant. Det så man blandt andet med de bornholmske keramikere, der sled så eftertrykkeligt på deres fingeraftryk, at de i mange tilfælde ikke kunne benytte Bornholmstrafikkens fingeraftryklæsere¹³. Det er klart, at man på den ene eller anden måde bliver nødt til at tage højde for disse og mange andre forhold i udformningen af biometriske løsninger," siger Niels Christian Juul og tilføjer, at man også må tage i betragtning – og søge at dæmme op for –, at personer med kriminelle intentioner kan bruge tvang over for et menneske, hvis biometriske data kan give adgang til for eksempel computersystemer, bankkonti og bygninger.

Danskerne ønsker overvågning

Ifølge Niels Christian Juul er der også utallige anvendelsesmuligheder for biometriske teknologier, som kan hjælpe mennesker i hverdagen – for eksempel nem adgang til offentlig transport og hurtig passage gennem lufthaven. Sidstnævnte er allerede en realitet i lufthavne i London og Amsterdam. Men han ser også en meget tydelig tendens til mere kameraovervågning af borgerne – for eksempel i Jomfru Ane Gade

¹³ Det bekræfter IT-chef på Bornholmstrafikken i interview i DR-programmet Viden Om. Her udtaler han følgende; "For enkelte passagerer kan systemet ikke fungere. Det drejer sig om 2,5 %, hvis finger simpelthen slet ikke kan blive scannet i første omgang, når der skal laves en referencescanning til chipkortet. Det er typisk keramikere eller håndværkere, som kan have slidt deres fingeraftryk helt væk af deres arbejde: "Man må acceptere, at man med et biometrisk system ikke kan få alle igenem." <http://www.dr.dk/DR2/VidenOm/Temaer/Biometri/20070530163036.htm>

i Aalborg¹⁴ – i kombination med biometriske løsninger, som registrerer borgerens gøren og laden i hverdagen.

”Vi er på vej til at etablere et system, hvor alting er overvåget, og hvor mennesker ikke skal give deres accept af eller er klar over, at de bliver overvåget. Der findes allerede biometriske overvågningssystemer, som kan danne et tredimensionelt billede af et ansigt, som er godt nok til, at man kan slå det efter i en database og identificere personen. Vel at mærke uden at personen ved det eller har givet tilsagn om, at det er i orden, at vedkommende identificeres,” siger han.

Niels Christian Juul pointerer, at der bør være en diskussion i samfundet om, hvorvidt det er okay at identificere folk uden deres viden og accept, eller om man for eksempel skal skilte med, at der ikke blot videoovervåges, men også foretages personidentifikation via kameraer i bestemte områder.

Ifølge Niels Christian Juul tyder meget på, at et flertal af danskerne har en positiv holdning til overvågning.

”Vi stoler åbenbart så meget på vores politikere, at vi som et af de eneste folkefærd i verden ikke har noget imod at blive overvåget. Tiltroen til, at overvågning ikke vil blive misbrugt, er nok et dansk/skandinavisk fænomen og en holdning, de ryster på hovedet af mange andre steder. Det gælder for eksempel i England, hvor Tony Blair mødte massiv modstand i befolkningen, da han ville indføre et borgerkort med indlagt biometri. Det forudsatte oprettelsen af et centralt personregister, men det ønskede borgerne ikke, og så måtte man droppe ideen,” siger han og understreger, at den øgede overvågning i samfundet for ham at se er en forkert udvikling.

Han peger på, at jo mere overvågning og registrering af adfærd, vi får, des færre muligheder bliver der for den enkelte til at eksperimentere med, hvem man egentlig er – finde sin identitet og prøve grænser af.

Men hvad har vi egentlig at skjule? En masse!, siger Niels Christian Juul:

”Det kan være teenageren, der prøver at ryge en smøg eller eksperimenterer på anden vis, selv om han har en aftale med forældrene om ikke at gøre det. Det kan være 117 forskellige ting, hvor folk ikke gør det, de siger de gør, uden at det er kriminelt. I et samfund, hvor din fysiske færden og dine bevægelser på nettet bliver registreret, er den slags ikke muligt. Efter min mening er det et dødt samfund, der er som taget ud af en science fiction roman som ”1984”.

Magten tilbage til borgerne

Niels Christian Juul er ikke i tvivl om, at de biometriske kendetegn, man afgiver, kan opsamles af andre, der derved kan opbygge en kunstig person. Identitetstyveri er allerede et hyppigt forekommende problem i blandt andet USA – også uden brug af biometri. Her er der typisk tale om tyveri af personers navne, fødselsdatoer og social security-numre, som blandt andet bliver misbrugt til oprettelse af kreditkort, bankkonti og mobiltelefonabonnementer¹⁵.

”Man har altid kunnet klæde sig ud og udgive sig for en anden. Forskellen i forhold til tidligere opstår, hvis man tillægger det biometriske system for stor vægt. Det vil sige, at hvis systemet siger, at det er mig, der passerer, så ér det mig. Også selv om det er en anden, der ligner mig til forveksling. Problemet er, at de biometriske kendetegn er ude i det åbne, og jeg har endnu ikke set det biometriske kendetegn, som ikke kunne eftergøres. Derfor mener jeg ikke, at biometriske kendetegn kan bruges til at bevise, at jeg er mig,” siger han.

På den baggrund opfordrer Niels Christian Juul til, at biometri bruges som erstatning for ens brugernavn men ikke ens password. Dog mener han, at en række traditionelle biometriske løsninger kan være okay i situationer, hvor man i dag ikke forlanger nogen særlig sikkerhed og for eksempel kan komme ind på et område ved blot at oplyse sit navn eller forevise sygesikringsbevis. Man må blot ikke tillægge systemerne en ultimativ sandhedsværdi.

¹⁴ Der er også intensiv kameraovervågning på vej på Strøget i København. Overvågningen ventes igangsat i slutningen af 2009.

¹⁵ ”Passet og (u)sikkerheden”. Kapitel forfatter af Birgitte Kofod Olsen i bogen ”Pas – Identitet, kultur og grænser”, Jesper Gulddal og Mette Mortensen (red), Informations Forlag, 2004.

Han mener, vi bør stile efter løsninger, hvor man udover den biometriske identifikation også skal identificere sig på anden vis. En biometrisk løsning, hvor borgeren bevarer en del af kontrollen selv, kan for eksempel baseres på et kort i kreditkortstørrelse med fingeraftrykslæser indbygget. Her kan brugeren af kortet lukke op for kortet ved hjælp af sit eget fingeraftryk.

”Man kan have alt muligt gemt på sådan et kort – for eksempel elektroniske nøgler og forskellige koder, som giver adgang til netbank, arbejdspladsen og offentlig transport. Fordelen er, at ens fingeraftryk, andre biologiske data og personlige informationer ikke ligger i en database, hvor de i teorien kan blive stjålet og misbrugt. Det giver også mulighed for at bruge fælles nøgler og adgangskoder i de situationer, hvor man blot skal være én af en gruppe af personer for at få adgang. Herved eliminerer man unødigt overvågning. Det er magten tilbage til borgerne, og det er jeg tilhænger af,” slutter Niels Christian Juul.

Biometri på flyrejsen

I april 2007 indførte SAS muligheden for at identificere sig med fingeraftryk ved check-in på indenrigsruter fra Aalborg Lufthavn. Det er ikke første gang, SAS har benyttet sig af fingeraftryksscanneren. Allerede i 2006 blev systemet implementeret på pilotbasis i Sverige, hvilket viste sig at fungere så godt, at SAS senere valgte at indføre det i Danmark. Systemet blev først implementeret i Aalborg lufthavn, da lufthavnen kun har to gates og derved relativt nemt kunne indkøre systemet. I dag har SAS også indført systemet på indenrigsruter i Århus og Københavns lufthavn. I praksis afgiver man sit fingeraftryk ved check-in-skranken og igen ved gaten. Det sikrer, at ingen checker bagage ind uden selv at gå om bord på flyet. En proces, der efter sigende går meget hurtigere end ved brug af almindelig identifikation. Den såkaldte biometriboks aflæser to eller tre punkter på din finger og godkender fingeren. Du behøver ikke at være i systemet i forvejen, og alle informationer bliver slettet igen, når du er landet.

Grethe Skovmose, der er Stationsleder for SAS i Aalborg Lufthavn, har udelukkende gode erfaringer med fingeraftryksscanneren: ”Det går meget mere smidigt og hurtigt efter den biometriske løsning er blevet installeret i gaten. Det sker meget sjældent, at scanneren ikke kan aflæse fingeren. Der er selvfølgelig de passagerer, som ikke ønsker denne service, men så kører vi bare efter den gamle procedure, men det er sjældent; de fleste er positive og synes, det er sjovt at prøve noget nyt”. Grethe Skovmose forklarer, hvorfor SAS valgte netop fingeraftryksscanneren til fordel for andre biometriske løsninger: ”Jeg tror, at det er fordi, at det er det første system, der er blevet udviklet og derfor det, man hurtigst kunne gå til. Vi havde faktisk talt om irisscanning, men vi trak på Sveriges gode erfaringer med fingeraftryksscanningen”. Til spørgsmålet, om der er noget som andre, der overvejer at installere en biometrisk løsning, bør overveje, svarer Grethe Skovmose: ”Det er selvfølgelig stadig vigtigt at have en backup-procedure, hvis systemet ikke virker, men det har vi som sagt ikke haft de store erfaringer med”.

Etik i det biometriske design

For at undgå negative samfundskonsekvenser og efterfølgende lappeløsninger bør etiske overvejelser fremover være en fast bestanddel i udviklingen og videreudviklingen af enhver biometrisk løsning. Samtidig er det på tide at droppe skrækken for "big brother" og i stedet bruge kræfter på at diskutere, hvordan vi anvender biometri og overvågning konstruktivt, så det gør demokratiet endnu stærkere, mener filosof fra Aalborg Universitet.

Anders Albrechtslund, filosof ved Institut for Kommunikation på Aalborg Universitet, mener, at vi generelt i samfundet skal blive langt bedre til at inkorporere etiske overvejelser i beslutninger om overvågning, og vi skal tage fat på opgaven med det samme, da udviklingen mod et overvågningssamfund går særdeles hurtigt. Der er efterhånden kameraer mange steder, staten ved stort set alting om os, og overvågning koblet med biometriske teknologier dukker op på fodboldstadioner, i lufthavne, på arbejdspladser og mange andre steder.

Nogle frygter, at vi er på vej mod et totalitært "big brother-samfund", hvor den enkelte borger er overvåget og undertrykt. Men Anders Albrechtslund foretrækker at anskue overvågning som en grundpille i et demokratisk samfund. Han mener, at et samfund uden overvågning vil være et anarki, og at man bør stoppe med at fokusere på skrækken for "big brother".

"I stedet skal vi bruge kræfterne på en løbende diskussion i samfundet af, hvordan vi kan anvende overvågning konstruktivt, så det gør vores demokrati endnu stærkere og skaber et sikrere fundament for samfundsudviklingen," siger Anders Albrechtslund, der ser et tilsvarende behov for at indarbejde etiske overvejelser i forhold til overvågning på arbejdspladsen – men også hér anskuet ud fra en positiv synsvinkel.

"Hvis man vælger et udgangspunkt, der hedder, at overvågning af performance er med til at disciplinere og motivere medarbejderne, og samtidig muliggør større frihed under ansvar for den enkelte, så er overvågning på arbejdspladsen noget positivt, som fremmer den enkelte medarbejders karriere. Jeg kalder det "deltagende overvågning", når ens synlighed på den måde bliver en styrke. Men det forudsætter, at man indfører en organisationsform, der gør det muligt. I en topstyret organisation, hvor chefen ser sig selv som et orakel, der skal vide og kontrollere alt, er der stor risiko for, at medarbejderne ender som ulykkelige borgere i en diktaturstat," siger han.

Designorienteret etik

Det relativt nye begreb "designorienteret etik" betyder, at man allerede i designprocessen udvikler en løsning, der lever op til bestemte etiske krav. Tankegangen kendes blandt andet fra "privacy by design", hvor krav om at beskytte privatlivets fred ligeledes bliver tilgodeset i designfasen. Etiske overvejelser om teknologi har ellers traditionelt været noget, der blev bragt på banen i en evalueringsproces, hvor man analyserede teknologien og gav en etisk vurdering af den.

"Ideen med designorienteret etik er at foregribe etiske problemstillinger med en given teknologi – for eksempel en biometrisk løsning. Det kan ske via dialog mellem etiske konsulenter og teknologiudviklere, hvor man diskuterer de problematiske situationer, teknologien kan give anledning til, og derudfra udvikler løsningen på en sådan måde, at de etiske problemfelter elimineres," siger Anders Albrechtslund, der forsker i krydsfeltet mellem teknologi og etik.

Han peger på, at det blandt andet er oplagt at kortlægge de informationer, man ønsker at indsamle ved hjælp af den biometriske løsning, og afklare, om de kan misbruges eller føre til, at de mennesker, der skal bruge løsningen, kan blive diskrimineret eller på anden måde udsat for andet, der er uacceptabelt set fra en etisk synsvinkel.

Etikere og teknologer

Ifølge Anders Albrechtslund er designorienteret etik et logisk næste skridt i den udvikling, som siden oplysningstiden gradvist har bragt etiske overvejelser frem til at spille en stadig vigtigere rolle på stort set alle samfundsområder. Men det er ikke tilstrækkeligt at tilknytte en etisk konsulent i designfasen, når en ny biometrisk løsning skal se dagens lys; etikere bør være en konstant følgesvend til teknologerne, pointerer han:

”Teknologiudviklingen går som bekendt hurtigt, og man vil hele tiden videreudvikle og forbedre en given biometrisk løsning. Derfor er det vigtigt, at etiske konsulenter og teknologiudviklere kører parløb og sikrer, at etikken også er tænkt ind i nye versioner af løsningen. Samtidig kan etikkerne via brugerundersøgelser og lignende afdække og gøre opmærksom på de etiske problemstillinger, som man ikke havde fantasi til at forestille sig i designfasen.”

Anders Albrechtslund deltager som designetiker i et stort forsknings- og udviklingsprojekt på Aalborg Universitet, der går ud på at udvikle en mobiltelefon, som kan lette hverdagen for autistiske borgere¹⁶. Sideløbende udvikler han et koncept for, hvordan sådan et samarbejde rent praktisk kan struktureres for at fungere optimalt. Håbet er, at konceptet vil kunne tjene som rettesnor for fremtidig integration mellem etik og teknologi.

Sortering af mennesker

Anders Albrechtslund mener, at et vigtigt fokusområde for designorienteret etik i forbindelse med udvikling af biometriske løsninger bør være, om løsningerne kan have en klassificerende, ekskluderende eller diskriminerende bieffekt i forhold til bestemte befolkningsgrupper.

Han peger på, at hvis man forestiller sig, at biometri bruges til at tilbyde en særlig service, som man kan fravælge eller vælge – for eksempel en ”fast lane” i lufthavnen –, så indebærer et fravalg af denne service, at man bliver ringere stillet end dem, der vælger servicen. Men hvis ikke alle har mulighed for at vælge/fravælge, vil dem, der ikke har opnået servicen, fremstå som andenrangsborgere. Men det kan blive værre endnu, siger han.

”Det engelske begreb ”social sorting” betyder i praksis, at en biometrisk løsning er programmeret til at holde øje med bestemte handicap, racemæssige og religiøse kendetegn, og at man på den baggrund udtrækker folk til et særligt grundigt eftersyn i for eksempel lufthavnens sikkerhedskontrol eller helt afviser at give adgang til diskoteket, storcentret eller restauranten. Det er efter min mening en uacceptabel måde at bruge biometri på,” siger han og fortæller om forskning¹⁷, der viser konsekvenserne af, at politiet i USA langt oftere kontrollerer unge sorte i 20’erne for kriminalitet end andre befolkningsgrupper.

”Når man tjekker en bestemt profil oftere, vil man af samme årsag også finde mere kriminalitet inden for den profil end hos andre befolkningsprofiler. Derfor vil statistikkerne vise, at der bliver begået relativt mere kriminalitet her, hvilket animerer politiet til endnu mere kontrol af denne gruppe. Der er altså en selvforstærkende effekt her, som kan være med til at grave de sociale grøfter dybere. Det er en risikofaktor, man i høj grad skal være opmærksom på ved indførelse af biometriske teknologier,” siger Anders Albrechtslund.

Inkluderende biometri

Men indførelse af biometriske teknologier indebærer også en række fordele, som kan give et kvalitetsløft i dagligdagen for særligt udsatte grupper. Det fremhæver Birgitte Kofod Olsen, jurist og ph.d. i identifikationsteknologi og individbeskyttelse og CSR-konsulent og forfatter, foruden forhenværende vicedirektør i Institut for Menneskerettigheder. Hun peger blandt andet på, at blinde eller mennesker med nedsat syn

¹⁶ Projektet hedder HANDS – se <http://hands-project.eu>

¹⁷ Omtalt i bogen ”The Panoptic Sort – A Political Economy of Personal Information (Critical Studies in Communication and in the Cultural Industries)” (Paperback), af Oscar H. Grady.

på grund af sygdom kan få adgang til betalingsautomater via sikkerhedssystemer, der bygger på stemmeidentifikation i stedet for en pinkode.

”Tilsvarende kan erstatning af foto med irisgenkendelse eller finger- eller håndaftryk i passet sikre, at muslimske kvinder, der af religiøse årsager bærer tørklæde, ikke tvinges til at blotte ansigtet. Et tredje eksempel er transseksuelle mænd, der endnu ikke har fået en kønsskifteoperation. De klæder sig som kvinder, men har et pas med et billede af en mand. Det kan give anledning til ydmygende situationer, som man kan undgå ved hjælp af biometri,” siger Birgitte Kofod Olsen.



Biometri udfordrer demokratiske rettigheder

Opgaven kan synes uovervindelig: på én gang at skabe effektiv service, forvaltning og forebyggelse af terror og samtidig at sikre borgernes demokratiske ret til beskyttelse af værdighed, integritet og privatliv. Dilemmaet afspejler sig i ny lovgivning, som åbner for øget overvågning og registrering. Vi befinder os på en glidebane, som vil blive forværret med udbredelsen af biometriske teknologier – med mindre vi giver kontrollen tilbage til borgerne, siger ekspert.

”Hver gang man begrænser respekten for den enkelte borgeres privatsfære, rører man ved basale principper som frihed, respekt for værdighed, integritet og selvbestemmelse, som danner selve fundamentet for det demokratiske samfund, vi sætter så højt,” siger Birgitte Kofod Olsen.

Hun mener, at samfundet, hvis man virkelig ønsker at prioritere individets interesse og eliminere overvågning, bør stoppe al registrering af borgerne. I stedet skal alle oplysninger om den enkelte samles på et borgerkort, som borgeren selv råder over. Kortet skal indeholde alle almindelige personoplysninger men også sundhedsoplysninger og andre følsomme og fortrolige oplysninger. Samtidig fjernes oplysningerne fra centrale offentlige og private databaser. Det vil herefter være én selv, der bestemmer hvem, der skal have adgang til oplysningerne, og som giver samtykke til at anvende dem.

”Borgeren skal have pligt til at udlevere bestemte oplysninger til for eksempel skattemyndighederne. Og jeg er overbevist om, at hvis man udnytter moderne teknologi som e-mail og sms optimalt, vil det ikke kræve uoverstigelig administration at spørge borgerne, hver gang en myndighed har brug for information,” fastslår Birgitte Kofod Olsen, der ikke mener, at den nuværende lovgivning beskytter individet godt nok.

”Vi befinder os tværtimod på en glidebane, som betyder, at andre gradvist får stadig større råderet over stadig flere af vores private oplysninger. I stedet bør vi sætte borgeren i centrum som den, der har kontrol med egne informationer,” siger hun.

Borgeren vs. samfundet

I 1995 trådte EU's direktiv¹⁸ om privatlivsbeskyttelse i kraft. Baggrunden var et ønske fra EU's side om at beskytte oplysninger om borgerne og sikre et frit flow af information mellem medlemsstaterne. Bestemmelserne i direktivet blev siden integreret i dansk lovgivning. Den nuværende lovgivning herhjemme om beskyttelse af privatlivet er spredt mellem henholdsvis forvaltningsloven, offentlighedsloven, retsplejeloven og persondataloven.

Privatlivsaspekterne i de forskellige lovkomplekser sætter grænser for, hvordan og til hvilke formål man må indsamle, opbevare og anvende oplysninger om borgerne. Det fremgår blandt andet, at myndighederne kun må foretage husundersøgelser, beslaglægge breve og papirer, og bryde meddelelshemmeligheden, når der foreligger en dommerkendelse. Lovgivningen foreskriver også, at det kræver samtykke fra en borger før myndighederne må udveksle følsomme oplysninger om samme borger. Der er dog den

Privatliv er en menneskeret

Privatlivsbeskyttelsen er en grundlæggende rettighed i den Europæiske Menneskerettighedskonvention. Af artikel 8 fremgår det, at både personen selv, herunder krop og udseende, og hans eller hendes adfærd i forhold til for eksempel familie, seksualitet og kommunikation er omfattet af beskyttelsen, ligesom de materielle ting, der tilhører vedkommende, og de oplysninger, der er knyttet til ham eller hende. EU's direktiv om privatlivsbeskyttelse bygger herpå.

¹⁸ Direktiv 95/46 af 24.06.1995 i EFT L 281/31.

undtagelse, at hvis der er forhold, som gør, at samfundets interesse overstiger borgerens interesse, behøver man ikke indhente samtykke – og det har vi set flere eksempler på, siger Birgitte Kofod Olsen.

”De danskere, der vendte hjem fra Thailand efter tsunamien, blev for eksempel modtaget af myndigheds personer i lufthavnen, som registrerede dem og sendte oplysninger videre til de sociale myndigheder, der efterfølgende foretog ændringer i tildelingen af sociale ydelser for dem, der ikke måtte befinde sig i udlandet, fordi de fik sociale ydelser i Danmark og stod til rådighed for arbejdsmarkedet. I den situation vurderede man altså, at afklaring af mistanken om misbrug vejede højere end den enkeltes ret til at give samtykke.”

Men er det ikke uhyre nemt at argumentere for, at samfundets interesse i en given sag næsten altid vil veje højere end det enkelte individs interesse?

”Jo, i hvert fald i et samfund som det danske, som bygger på en kombination af den traditionelle socialdemokratiske velfærdsstat og den nuværende regerings visioner om at effektivisere samfundets systemer. Den cocktail fører let til, at man tillægger samfundsinteressen alt for stor vægt og i samme åndedrag giver køb på individets ret til en privatsfære,” siger Birgitte Kofod Olsen.

Stadig mere overvågning

Hun fortæller, at der bliver opsat stadig flere kameraer overalt i Europa – ikke mindst i Danmark. De overvåger trafikken på motorvejene, passagerne i togene, kunderne på posthusene, i bankerne, på benzinstationerne, i butikkerne, i indkøbscentrene og tilskuerne til fodboldkampe. På mange arbejdspladser registreres de ansattes aktivitet på internettet, på mailen og telefonen. På biblioteket registreres alle udlån med cpr-nummer som reference, i virksomheder og detailhandlen registreres kunderne og deres indkøb. Med folketingets vedtagelse af den første såkaldte Terrorpakke¹⁹ i 2002 blev teleselskaberne pålagt at registrere al teletrafik og opbevare oplysningerne, så politiet kan få adgang til dem i en sag. På samme måde kan alle med en mobiltelefon i dag spores døgnet rundt på grund af registrering og opbevaring af oplysninger fra sendemasterne. Flyselskaberne indsamler passageroplysninger om destinationer og madpræferencer, som politiet har direkte adgang til uden dommerkendelse.

Følsomme biometriske oplysninger

Nogle biometriske teknologier resulterer i oplysninger, der kan betegnes som følsomt materiale efter dansk lovgivning – det vil sige oplysninger om blandt andet sundhed, sygdom og etnisk baggrund. Der er forbud mod behandling af oplysninger af denne art, med mindre der er givet samtykke af den berørte person, eller der er samfundsmæssige eller andre hensyn, som vægtes højere end hensynet til personen.

Ansigtsgenkendelse er en af disse teknologier. Man kan ud fra en ansigtsscanning blandt andet aflæse oplysninger om race, alder, køn og handicap. Ansigtsgenkendelse kan desuden kombineres med termisk scanning, som måler det mønster, der opstår som følge af varmeafgivelsen i de forskellige ansigtsområder. Disse oplysninger kan anvendes til at vurdere persons sundhedstilstand og følelsesmæssige tilstand, og om vedkommende for eksempel har et alkoholmisbrug.

Hver for sig giver mulighederne for at indsamle personoplysninger ikke anledning til problemer, hvis det sker inden for lovgivningen, men hvad sker der, hvis vi åbner for at sammenkøre alle de oplysninger, der nu ligger i separate databaser, spørger Birgitte Kofod Olsen og giver selv svaret:

”Så kan vi udvikle avancerede og detaljerede profiler over alle borgers adfærd, vaner, præferencer, økonomi, sociale forhold, sundhed og meget mere. Og argumenter om effektivitet og bedre service hos offentlige myndigheder, sikkerhed mod terrorisme, målrettet service i butikkerne, målrettet markedsføring og bedre indtjening i den private sektor, øget sikkerhed i trafikken, øget sundhed i befolkningen osv. vil let kunne føre os til at lempe på de nuværende regler.”

¹⁹ Den anden terrorpakke kom i 2006 efter en embedsmandsgruppe i Justitsministeriet havde udarbejdet en rapport med 50 forslag.

Det transparente menneske

Birgitte Kofod Olsen ser både positive og negative aspekter i den voksende brug af biometri i forhold til sikring af privatsfæren for den enkelte.

”På den ene side kan biometri understøtte en udvikling, hvor al information ligger hos borgeren. Den biometriske autenticitet er meget stærk, og ved at udnytte biometri og koble det med kryptering kan vi være tæt på 100 procent sikre på, at de oplysninger, en borger afgiver, faktisk stammer fra denne borger. Hvis man derimod fortsætter den nuværende udvikling og samler flere og flere informationer hos myndighederne og så lægger biologiske informationer fra ansigtsgenkendelse og andre biometriske teknologier oveni, som har karakter af følsomme oplysninger og i nogle tilfælde vil kunne afsløre blandt andet kroniske sygdomme, ender vi med en stat, hvor alle borgere er transparente – og så er spørgsmålet, hvad der er tilbage af vores frihed,” siger Birgitte Kofod Olsen, der mener, at vi allerede i dag er tæt på at nå den situation i Danmark.

”Det foruroligende er, at jo mere overvågning og registrering vi tillader, jo mere nærmer vi os en samfundsform med totalitære træk, som vi så udfoldet i for eksempel Sovjet under den kolde krig. Og vi skal huske, at den eneste reelle beskyttelse mod en sådan udvikling er lovgivning. Men lovgivning kan som bekendt ændres i morgen af et flertal i Folketinget. Og med den accelererende terrortrussel kan der hurtigt opstå nye incitamentter til, at man fortsætter med at gå på kompromis med de grundlæggende demokratiske principper og rettigheder, som vores samfund bygger på,” siger hun og tilføjer, at den embedsmands- og ekspertgruppe, som udarbejdede en rapport forud for Folketingets vedtagelse af den anden terrorkpakke, ikke fandt det nødvendigt at øge samfundets overvågning og registrering af borgerne. Gruppen mente, at man kunne opnå en ligeså effektiv efterforskning og forebyggelse af terrorisme inden for den eksisterende lovgivning. Den øgede overvågning og registrering med Terrorkpakken er blevet til på politikernes initiativ.

Beskyttelse af borgerens privatliv

”Vi må ikke falde i den forkerte grøft ved med en omfattende og indgribende brug af teknologi at krænke netop en af samfundets grundlæggende værdier – borgernes privatliv. Beskyttelsen af privatlivets fred er af central betydning i et demokratisk samfund, og det er vigtigt, at vi til stadighed værner om den enkeltes privatliv. Med den teknologiske udvikling følger således muligheden – nogle vil sige risikoen – for blandt andet øget indsamling og registrering af oplysninger om borgerne, længere opbevaringstid samt nemmere adgang til udveksling af personoplysninger. Det er vigtigt, at vi i forhold til blandt andet sådanne muligheder sikrer en nødvendige balance mellem på den ene siden hensynet til effektivt at løse forskellige samfundsmæssige opgaver ved hjælp af moderne teknologi og på den anden side hensynet til beskyttelsen af den enkelte borgers privatliv.”²⁰

²⁰ Udenrigsminister Lene Espersen, forhenværende Erhvervs- og Økonomiminister (K) i bogen ”Overvågning eller omsorg – privatlivets grænser”, Forlaget Thomson, 2005, red. Af Birgitte Kofod Olsen og Rikke Frank Jørgensen.

Stop glidebanen mod overvågnings- og kontrolsamfundet

Biometriens indtog har accelereret glidebanen mod et overvågnings- og kontrolsamfund, hvor borgerne til sidst hverken har frihed eller privatliv tilbage, og hvor al innovation er forsvundet, mener it-direktør Stephan Engberg.

Stephan Engberg, direktør i virksomheden Priway, der beskæftiger sig med it-sikkerhed og innovation, er grundlæggende modstander af brug af biometrisk teknologier, som indebærer, at borgeren skal afgive biometriske data. Uanset hvor uskyldigt et biometrisk redskab kan forekomme, er der tale om et skridt i den forkerte retning, og den lagrede biometriske information vil altid kunne misbruges et andet sted, mener han.

”Det er en glidebane mod et allerede fremskredent overvågnings- og kontrolsamfund, som jeg ikke tror, ret mange danskere har lyst til at leve i, og som også vil betyde velfærdssamfundets endeligt, fordi innovationen går i stå. Hvis vi først accepterer usikker biometri som en naturlig del af den måde, vi indretter samfundet på – og det er i høj grad ved at ske –, er der ingen vej tilbage,” siger Stephan Engberg.

Han pointerer, at der her er tale om, at helt basale, samfundsbærende rettigheder og principper er i farezonen. Det understregede også den Europæiske Menneskerettighedsdomstol for nyligt i sagen ”S & Marper vs. United Kingdom” ved at dømme UK for overtrædelse af Menneskerettighedskonventionens artikel 8 for ulovligt at registrere dna, fingeraftryk og vævsprøver på ikke-dømte borgere.

”Det er desværre noget, man i Danmark ikke tøver med at udsætte diskoteksgæster for,” siger Stephan Engberg.

Biometri på borgernes præmisser

Det betyder ikke, at Stephan Engberg er modstander af biometri som sådan. Teknologien skal bare anvendes på borgernes præmisser, så den enkelte bevarer fuld kontrol med eget liv, og biometrien isoleres til udelukkende at forebygge kriminalitet.

”Jeg er tilhænger af biometri, som via for eksempel en kombination af fingeraftryk og en talkode giver adgang til et individuelt borgerkort med nøgler eller koder, der styrer borgerens kontakter, borgerens data, giver adgang til borgerens netbank osv. Det ideelle borgerkort giver dig både frihed og sikkerhed. Det skal sikre, at den næste transaktion hverken kan kobles til forudgående eller fremtidige transaktioner, medmindre du selv ønsker det. Og det skal ske på en sådan måde, at man forebygger mange forskellige former for kriminalitet,” siger han og fortsætter:

”Det står i skærende kontrast til det truende overvågnings- og kontrolsamfund, hvor store databaser sammenkøres, hvorefter informationer om den enkelte vil flyde frit på tværs af de sammenhænge, hvor de opstod. Med det resultat at man er totalt blottet og ikke har hverken sikkerhed eller privatliv tilbage.”

Nærmest retsløs

Han mener, at samfundet nødvendigvis må tage ansvar for at sikre en minimumssikkerhed i forhold til den borgerkortsløsning, han foreslår. Borgere, der ønsker mere sikkerhed derudover – det kan for eksempel være højtstående politikere og erhvervsfolk –, skal kunne købe sig til alternative korttyper, som for eksempel kræver identifikation med flere forskellige biometriske metoder og en længere pinkode, foreslår Stephan Engberg.

”Vi kan sagtens på rent kommercielt plan sikre specielle sammenhænge, men det vil kræve fælles tiltag at rette op på de mange fejl, man begår i øjeblikket, fordi man fokuserer mere på at kontrollere end på at sikre borgerne,” siger han.

Stephan Engberg ville aldrig acceptere at udlevere sit fingeraftryk eller anden biometrisk identifikation til noget som helst andet end sit eget borgerkort.

”På den måde reducerer jeg risikoen for, at jeg på et eller andet tidspunkt ender i en retssag, hvor en anklager med henvisning til ”biometrisk login” påstår, at jeg har deltaget i en kriminel sammenhæng. I et samfund, hvor biometri misbruges til adgangskontrol, kan den virkelige forbryder jo have hentet mit fingeraftryk alle mulige steder, og jeg vil på det nærmeste være retsløs. Den eneste måde at beskytte sig mod dette er ved at opretholde en nultolerance overfor biometrisk registrering, der ligger uden for ens egen kontrol,” siger Stephan Engberg og understreger, at alle typer af biometri kan forfalsskes.

”Det kan godt være, at for eksempel veneskanning er sværere at fake end fingeraftryk, men pointen er, at der i begge tilfælde er tale om fysiske konstanter – og alle fysiske konstanter kan kompromitteres. Det er præcis derfor, at biometriske data er ubrugelige som nøgler; de kan ikke lukkes, ikke sikres og man kan ikke få nye biometriske nøgler, hvis de bliver ”stjålet”.

I Stephan Engbergs optik er et af formålene med en god borgerkorts-løsning endvidere, at den kan redde samfundet fra den sikkerhedsmæssige katastrofe, som han mener, de nye biometriske pas udgør. Ifølge Stephan Engberg er det biometriske pas alt for let at forfalsske.

Borgeren suverænitet

Han peger videre på, at der i dag er kommercielle, statslige, politiske, sociale og mange andre interesser, som ønsker at kontrollere mennesker, og at det derfor er så afgørende ud fra både en demokratisk og en samfundsøkonomisk betragtning, at vi holder fast i, at det vigtigste aktiv overhovedet i samfundet er borgeren og borgerens suverænitet – adgangen til at bestemme selv.

”Det er livsvigtigt at bevare en struktur, hvor det er forbrugernes valg, som er styrende for værdikæderne og innovationen i samfundet. Men biometriens udbredelse er direkte destruktiv for den samfundsstruktur, vi kender og sætter pris på,” siger Stephan Engberg, der fastslår, at biometri er en af de stærkeste magtteknologier i dag.

”I takt med at man indfører biometri, sker der en destabiliserende bevægelse af magt fra borgerne til politikerne/embedsværket og de store virksomheder. En af konsekvenserne af central styring er, at man både i det offentlige og det private magtapparat tror, at man via overvågning og registrering kender befolkningens behov på forhånd og derfor ikke længere behøver at indrette sig efter borgerens faktiske behov. Resultatet er, at man tilpasser kunden til det som udbyderen ønsker – med den konsekvens, at markedsmekanismene, inklusiv innovationen i samfundet, stille og roligt går i stå. Det er en proces, som allerede har stået på længe, og som er yderst uheldig i et land som Danmark, hvor vi skal leve af innovation. Hvis vi skal undgå fortsat innovationsnedbrud, er det helt afgørende, at det enkelte menneskes daglige ønsker og valg bestemmer udviklingen; ikke overordnede, diffuse offentlige eller erhvervsøkonomiske interesser,” siger Stephan Engberg.

Mange bække små

Han peger på, at mennesker generelt har svært ved at forholde sig til risikoen ved de mange små transaktioner i hverdagen, hvor man afgiver nogle få informationer om sig selv – for eksempel via biometriske teknologier, dankort, mobiletelefonen, IP-adressen, etc.

”Men realiteten er, at der sker en akkumulering af informationer, og at den enkelte bliver mere og mere blottet. Og når dét på et tidspunkt går op for folk, er det i realiteten for sent at ændre. Så ligger de informationer i systemerne for good,” siger Stephan Engberg, der afviser, at man kan spole tiden tilbage og slette alle informationer, hvis man på et tidspunkt måtte ønske at gøre det.

”Det er ikke muligt på troværdig vis at slette data, fordi man ikke kan bevise, at data er slettet. Samtidig viser al erfaring, at der ofte er så stærke interesser i at bevare data, at det heller ikke sker,” siger han.

Den gode nyhed er, pointerer Stephan Engberg, at der begynder at komme løsningsmodeller på banen, som fastholder det enkelte menneskes suverænitet – og det er den rigtige vej at gå.

”Selvbestemmelse drejer sig først og fremmest om at kunne træffe uafhængige valg. Hvis du kan gøre det via et borgerkost med en ny nøgle uden biometrisk eller anden kobling til andre steder, så kan samfundet overleve selv det kritiske, digitale miljøsvineri med persondata og fundamentale rettigheder, som finder sted i øjeblikket.”

Danmark på forkant

Stephan Engberg er netop vendt hjem fra en konference om sikkerhed i Sundhedssektoren. Her observerede han ”ganske pæne løsninger fra både Schweiz og Polen, hvor borgeren kontrollerede deres egne data via et kort.” Men også i Danmark er vi faktisk langt fremme, siger han.

”I SIME-projektet arbejder vi med konkrete projekter om at sikre online diagnosesupport uden at arbejde med personhenførbare data, og i Sundhedsministeriet arbejder vi med SDSD23 om et stifinderprojekt til at sikre bio-banker ved at anonymisere prøven fra starten. Dette projekt udspringer af et kæmpearbejde med at analysere og designe, hvordan man kan sikre nogle af vores allermest sensitive systemer, nemlig patientjournalerne,” siger han og fortsætter:

”I årenes løb har disse projekter skabt flere afledte innovationer. I SIME-projektet arbejder vi for eksempel med en biometrisk løsning, hvor lægen kan validere sin autorisation som læge uden at identificere sig direkte eller indirekte. Samme løsning kan anvendes på diskoteker for at holde voldsmænd ude – vel at mærke uden opsamling af biometri eller persondata. I begge tilfælde løser systemet den ønskede opgave og skaber merværdi, men uden at borgernes privatliv kompromitteres,” siger Stephan Engberg og pointerer, at vi må holde op med at skabe personhenførbare data, når vi ikke kan beskytte dem:

”Vi skal også stoppe med at designe teknologier, som skaber sikkerhedsproblemer, vi kunne have undgået. I stedet må vi skabe en verden med systemer, der er opbygget på borgernes præmisser og til gavn for borgerne på alle måder, og det er faktisk muligt i dag. Vi skal bare gøre det.”

Scenarie 1: Biometriens velsignelser

Den 36-årige kommunikationschef Sofie Løvenrose strakte sig veltilpas under den varme dyne og missede mod den skarpe vintersol, der trængte ind gennem en sprække i gardinet. Hun udbrød et stille "sluk" ud i rummet, hvorefter den insisterende hyletone forsvandt, og loftslýset holdt op med at blinke. Hun kastede et blik på årstallet, datoen og tidspunktet, der stod at læse med lysskrift på væggen: 2020, 23. december, 09.00. Hun havde arbejdet over til langt ud på natten. Nu stod juleferien for døren, men der var endnu meget, hun skulle nå – for eksempel havde hun endnu ikke købt en eneste julegave. Sofie Løvenrose havde sine to børn hver anden uge, og de skulle være hos faren i julen, men gaver skulle de have. Det var på høje tid at komme ud af fjerene.

Da hun trådte ud i køkkenet, blev hun som altid genkendt af husets servicekamera-4, der sendte besked til det intelligente styringssystem om at aktivere gulvvarmen i køkkenet og på badeværelset. Hun blev mødt af den logrende robothund Solvej, der bjæffede et "Godmorgen, Sofie – har du sovet godt?" med sin hæse, charmerende røst. Hun klappede det lille dyr og bemærkede, at den bevægede sig langsommere end sædvanligt. Hun kyssede hundens bløde snude, deaktiverede dens elsystem, knappede op ind til solcellepanelet og placerede den i solen i vindueskarmen. Nu satte hun sin højre tommelfinger på den biometriske aflæser på køleskabets front og fik adgang. Hun tømte kartonen med vitamin- og mineralberiget drikkeyoghurt med ægte jordbærekstrakt i ét drag og supplerede med en håndfuld tørrede goji-bær. Så tog hun et hurtigt bad og kom i tøjet. Før hun løb ud ad døren, aktiverede hun atter hunden og satte den ned på gulvet. "Pas nu godt på huset i julen," smilede hun og klappede sin lille ven på hovedet.

Hun låste huset af med en kode, hun opbevarede i sit smart-card – et plastikkort i kredittkortstørrelse, som hun åbnede med sit fingeraftryk. Kortet indeholdt alle de koder og password, hun brugte i hverdagen – til netbank, kredittkort, bil, båd, sommerhus, arbejdsplads, offentlige parkeringspladser og meget andet. Kortet rummede også sundhedsoplysninger, skatteoplysninger og andre beskyttede informationer om hende. Hun kunne stadig gribe sig i at føle stor lettelse over ikke længere at skulle huske alle livets koder og bekymre sig om, at myndighederne vidste stort set alt om hende. Der var trods alt et og andet, hun gerne ville holde for sig selv.

Et par minutter senere svingede Sofie Løvenrose sin elbil, der var blevet ladet op i løbet af natten, ned på motorvejen, og kørte gennem den biometriske registrering, der gav adgang til fast track-banen. Hun betalte et fast beløb om måneden til selskabet Fast Track Biometrics Inc., som håndterede alle fast track-tilbud i Danmark, inklusiv dem i lufthaven, som via en kombination af ansigts- og irisgenkendelse bragte hende hurtigt gennem security og ud til flyet. Det seneste, hun havde hørt, var, at der var fast track offentlig transport på vej i storbyerne. Hun susede forbi bilkøerne på den ordinære motorvej og fik lidt ondt af dem, der ikke var så privilegerede. Kort efter svingede hun gennem registreringszonen ved indkørslen til sin arbejdsplads. Fra dét øjeblik var hun genkendt, og kameraer med ansigtsgenkendelse fulgte hvert skridt, hun tog på arbejdspladsen, ligesom it-systemerne registrerede alt, hvad hun foretog sig på sin computer. Hun skyndte sig op på sit kontor, og priste sig endnu engang lykkelig for, at ledelsen et par år tidligere havde besluttet at skrotte de åbne kontormiljøer. Hun lagde benene op og gav sig i kast med at skrive et udkast til den fondsbørsmeddelelse, der skulle udsendes tredje juledag.

I det samme tikkede en besked ind på Sofie Løvenroses mobilenhed. Det var ugerapporten fra plejehjemmet, hvor hendes mor havde boet det seneste års tid på grund af demens. Hjemmets biometriske overvågningssystem havde detekteret moren 14 gange på vej væk fra institutionen, men personalet var hver gang trådt til og havde ledsaget hende tilbage til rummet. Midt i sorgen over sin mors sygdom glædede det hende, at plejehjemmet ved hjælp af den biometriske teknologi var i stand til at passe så godt på moren.

Sofie Løvenrose hentede en sandwich i kantinen og satte den til livs i bilen. Der var for en gang skyld kø i fast track-banen. Hendes blik gled ud ad vinduet, og i det samme bevægede tankerne sig tilbage i tiden.

Det gjorde hende en smule urolig, at hun ikke kunne kontrollere sine tanker. Den menneskelige hjerne havde sine egne love, som forskerne langt fra havde gennemskuet. Og tankerne – de levede deres eget liv. I det øjeblik mindede de hende om dengang i barndommen, hvor der ikke fandtes overvågning, og hun kunne bevæge sig rundt uden at andre vidste, hvor hun var, og hvad hun lavede. Hun mærkede en uvant ro brede sig i kroppen ved tanken. Men så var der en, der dyttede, og hun vågnede op med et ryk, satte bilen i gear og accelererede i retning mod byen. Næste stop var den store legetøjsbutik på gågaden, dernæst afleverede hun gaverne og tog grådkvalt afsked med de små pus, der for første gang skulle undvære deres mor juleaften. Men hun havde forfærdelig travlt, og der var ikke tid til de store afskedsscener. Hun skulle nå flyet til Stockholm klokken 18, for i det svenske ventede hendes far med julemaden. Hun kastede bilen fra sig i lufthavnen og skyndte sig gennem fast track-passagen, der førte direkte fra parkeringsanlægget til security-afsnittet. Foran hende trådte først en burka-klædt kvinde og dernæst en tydeligt transseksuel mand problemfrit gennem security, da de blev identificeret ved hjælp af irisgenkendelse. Hun kunne ikke lade være med at glæde sig over biometriens velsignelser, der blandt meget andet også gjorde det muligt for blinde at bruge betalingsautomater, hvor der var installeret et sikkerhedssystem, som byggede på stemmeidentifikation. Endelig sank hun ned i flysædet. Hun sukkende og smilede ved sig selv. Nu kunne hun med god samvittighed holde juleferie.

Scenarie 2: Identitetstyveri med livstruende konsekvenser

Det var en lun sensommermorgen i året 2020. Overlæge ved Hjertecentret på Rigshospitalet Thomas Holberg låste sin cykel fast til stativet og gik fløjtende over mod hospitalets indgangsparti i tonet glas. Endnu engang strøg det gennem ham, hvor glad han var for sit liv. Han havde en kone, der elskede ham, og sammen havde de tre dejlige teenagebørn, der var akkurat så besværlige og frihedshungrende, som de skulle være. Familien manglede heller intet materielt. De boede i en stor, moderniseret Frederiksbergvilla med plads til det hele og lidt til og meget mere, som en dansk trubadur sang i hans barndom i fattigfirserne. Thomas Holberg smilede ved tanken og satte farten op. Foran ham ventede en udfordrende hjer-teoperation på en nyfødt, som han var en af de eneste i Norden, der kunne udføre. Han var allerede fokuseret på opgaven og havde gennemtænkt de passager, han erfaringsmæssigt vidste, ville blive mest udfordrende. Nu ringede hans mobilenhed med en talebesked fra bankrådgiveren, der havde forsøgt at få fat på ham de seneste dage. Det må vente, tænkte han, og passerede i det samme den biometriske overvågning ved indgangen, der registrerede hans bevægelsesmønster og ansigtstræk. I dette tilfælde ikke hans iris, fordi han var iført solbriller. Med det nye system med flere, mere avancerede kameraer, behøvede man ikke længere rette blikket mod et bestemt punkt over luftslusen, men kunne gå lige igennem. Systemet spottede hans kendetegn og sammenholdt dem på en brøkdel af et sekund med hans biometriske data i hospitalets centrale database. I samme nu fik hans kolleger på afdelingen besked om, at han var i bygningen, og kunne gå i gang med at klargøre de sidste teknikaliteter forud for operationen. Samtidig gik der besked til Rigshospitalets tidsregistreringssystem om, at han var mødt på arbejde. Men det biometriske system havde også en anden funktion, som Thomas Holberg ikke kendte til.

Systemet registrerede bevægelsesmønstre og fremtoning, der var blevet klassificeret som overvågningskrævende af det biometriske overvågningssystem. Systemet foretog sine vurderinger ud fra et sæt af kriterier om blandt andet en persons bevægelseshastighed og -målrettethed, omfanget af medbragt eller efterladt bagage og bagagens udseende, religiøst betinget påklædning, etnisk oprindelse og race. Kriterierne var fastsat internationalt ud fra en statistisk baseret opgørelse af karakteristika ved personer, der havde udført forskellige kriminelle handlinger. Alle biometriske data om de personer, der trådte ind på hospitalsområdet, blev sendt til dansk politis og Interpols centrale databaser og sammenholdt med data for tusinder af personer, der var efterlyst i Danmark og den øvrige verden. Hvis der var et match, sendte systemet automatisk en alarmmeddelelse i en bestemt trusselskategori til henholdsvis hospitalets vagt-personel og til nærmeste politienhed. Allerede inden Thomas Holberg var nået halvvejs over til elevatoren, der skulle bringe ham op på afdelingen, havde systemet afsendt en kode-rød-advarsel, og i det øjeblik hans finger ramte elevatorknappen, greb stærke arme ham bagfra. Kort efter befandt han sig i et tomt, hvidt lokale uden vinduer.

"Jeg må bede dig om at finde dit borgerkort frem," sagde en høj muskuløs betjent i uniform.

"Hvad drejer det her sig om?" råbte Thomas Holberg vredt og begyndte at gå over mod den blanke ståldør, men betjenten stillede sig i vejen.

"Jeg skal have dit borgerkort lige nu!" sagde han skarpt.

Thomas Holberg opgav sin modstand. Han forstod ikke, hvad der foregik omkring ham. Nu trak han sin pung frem og fandt kortet.

"Vær venlig at aktivere det!" sagde betjenten.

Thomas Holberg så vantro på ham. Hele hans liv befandt sig på dét kort. Alle passwords og koder til oplysninger om hans sundhedsmæssige og finansielle forhold. Med informationerne på kortet kunne man få adgang til hans konti og se, hvad han brugte sine penge til. Og man kunne afdække hans præferencer og vaner. Oplysningerne ville blotte ham fuldstændig.

”Du kan ligeså godt gøre det med det samme. Min kollega er på vej med en dommerkendelse. Der er ingen vej udenom.”

Thomas Holberg følte sig både vred og forvirret, da han lagde sin tommelfinger på kortet og aktiverede det. Nu førte betjenten sin skanner hen til kortet og overførte indholdet. Fra dét øjeblik havde Thomas Holberg stort set ikke én hemmelighed tilbage i verden.

”Jeg vil gerne vide, hvorfor du gør det her mod mig?” mumlede han.

”Du er mere naiv, end politiet tillader, hvis du tror, du kan slippe af sted med at røve en pengetransport og skyde en mand ned på åben gade i et totalovervåget samfund,” brummede betjenten.

”Jeg ved ikke, hvad du taler om – jeg har ikke røvet eller skudt nogen.”

”Du kan fortælle dine løgnehistorier til dommeren.”

I det samme ringede Thomas Holbergs mobile enhed, som politimanden havde beslaglagt. Den store mand tændte den og førte den op til øret. ”Det er din kone,” mumlede han.

”Må jeg ikke få lov at fortælle hende, hvor jeg er. Hun er højgravid og kan føde hver time det skal være?” løj han.

En mild vind blæste henover betjentens ansigt og han rakte ham telefonen.

”Du får ét minut.”

”Hvad er der sket, Thomas?” hviskede hun. ”Rådgiveren nede fra banken har ringet og fortalt, at du har tømmt alle vores konti i løbet af de sidste tre døgn. Jeg er også blevet kontaktet af den amerikanske ambassade. De siger, de har lejet vores hus i tre år, og at du har fået udbetalt et depositum på 125.000 euro. Souschefen i handelsafdelingen flytter ind på mandag.”

Før Thomas Holberg nåede at svare, havde vagten fortrudt sin velvillighed og taget telefonen fra ham igen. Nu gik døren op og yderligere to betjente trådte ind.

”Jeg vil gerne tale med min advokat,” sagde Thomas Holberg med dirrende stemme, da hans arme blev låst på ryggen med plastikstrips. Men ingen svarede ham, og kort efter befandt han sig i en varevogn med tonede ruder, der kørte af sted gennem byen i høj fart. Nu kom han i tanke om det lille drengebarn med hjerteproblemer. Drengens overlevelse afhang af ham. Thomas Holberg slog sit hoved mod ruden, men ingen reagerede.

Langt om længe sank han om på siden med lukkede øjnene, og mens bilen bragte ham længere væk fra alt det, der betød noget i hans liv, begyndte en sætning at gentage sig i hans hjerne: ”Der er én, der har stjålet mine biometriske data og overtaget min identitet”. Han kunne slet, slet ikke overskue konsekvenserne. Det eneste, han vidste, var, at forbryderen ville have et stort forspring, når politiet forhåbentlig engang blev klar over, at de havde begået en utilgivelig fejl.

Scenarie 3: Ingen skjulesteder i overvågningssamfundet

Det var en kølig efterårsdag i året 2020. Fuldmægtig ved Det Nationale Sikkerhedskontrolcenter Ingolf Koll havde netop sat sig til rette ved skrivebordet, da skærmen foran ham afgav et advarselssignal. Det gibbede i ham, og han mærkede adrenalinet pumpe – hvor han dog elskede sit job! Der var ikke noget bedre end at se en svindler gå i fælden – og jo flere, der faldt i, des mere fik han i lønningsposen. Jo, det var dejligt at være tilbage på pinden efter en lang efterårsferie i familiens skød. I det samme tonede ansigtet af en ung mand frem på vægprojektoren. Under ansigtet stod følgende informationer: "Objektets navn: Jonathan Hokusan. Alder: 27 år. Cpr: 130393-2457. Civilstand: Ugift, et barn. Bemærkning: Udtaget til totalovervågning i 24 timer (nu 23 timer, 59 minutter, 9 sekunder) – derefter status til Centralkontrolenheden, der træffer beslutning om eventuel fortsat overvågning. Årsag: Manglende indbetaling af børnebidrag. Anklaget for forsikringssvindel (under 100.000 Euro) i sag om trafikskade. Anklaget for ureglementeret arbejdsforhold, såkaldt "sort" arbejde, samtidig med, at objektet modtager sygedagpenge fra det offentlige."

Ingolf Kolls fingre bevægede sig hurtigt hen over tastaturet, og snart havde han ved hjælp af GPS-systemet i den unge mands lovpligtige mobilenhed, hvorigennem al kommunikation med det offentlige foregik, indfanget en person, som kameraer med indbygget biometrisk genkendelse i det samme bekræftede var Jonathan Hokusan. Den unge mand bevægede sig med rolige skridt hen over Rådhuspladsen i retning mod Strøget. Uden at han på noget tidspunkt fik den fjerneste mistanke om det, ville Ingolf Koll i det kommende døgn følge alle objektets bevægelser og al kommunikation, han var involveret i. Kolls opgave var ganske klar: Han skulle identificere mulige beviser i forhold til anklagepunkterne.

Med nogle få tryk på skærmen rekvirerede Koll en oversigt over objektets kommunikation via sin mobilenhed – såvel taletelefoni som e-mail – i de forløbne 30 dage. Næste skridt var at indhente samtlige oplysninger, der fandtes om objektet i offentlige databaser, blandt andet om bopæl, indtægtsforhold, skat, pension og helbred. Endelig fik Ingolf Koll adgang til en fælles kommerciel database, som objektet selv på et tidspunkt havde tilmeldt sig for at modtage målrettede reklametilbud. Den indeholdt detaljerede informationer om hans indkøbsmønstre fordelt på samtlige varekategorier inden for de seneste tre år, foruden informationer om, hvor han havde været på ferie. Samtlige oversigter skulle vedlægges den endelige 24-timers rapport til Centralkontrolenheden.

Ingolf Koll gik nu ind i Det Nationale Sikkerhedskontrolcenters centrale database og placerede en overvågningsalarm på Jonathan Hokusan. Alarmen betød, at databasen fra dette øjeblik ville sende information direkte til ham, hver gang objektets biometriske data blev genkendt af et hvilket som helst overvågningskamera med biometrisk genkendelse. I de seneste 10-15 år var der blevet sat biometriske kameraer op overalt i landet på blandt andet gader og stræder, posthuse, banker, benzinstationer, butikker og indkøbscentre, stadioner, stationer, lufthavne, toge, busser og i offentlige bygninger. I praksis kunne sikkerhedsmyndighederne følge en borger tæt fra det øjeblik, vedkommende trådte ud ad døren fra sin private bolig, og meget af det, borgeren foretog sig i privatsfæren, kunne man få indblik i ved at overvåge hans eller hendes aktiviteter i cyberspace.

Jonathan Hokusan fortsatte ned ad Strøget og gik ind på cafeen Bobs Superfood, hvor han bestilte en "Total Active" – en friskpresset kåljuice med algepulver og tangkrymmel på toppen. Han løftede tilsyneladende uden problemer papkruset med den arm, han havde anmeldt svært skadet efter trafikulykken til sit forsikringselskab, og fortsatte sin vandring. Få minutter senere drejede han ned ad en sidegade og forsvandt ind i en butik ved navn "Urban Living". Her kunne Koll ikke følge objektet og slog derfor systemet på "automatik", hvorefter det ville afgive en alarm i det øjeblik, Jonathan Hokusan atter trådte ud i det offentlige rum.

Der skete ingenting de følgende to timer. Derefter aktiverede objektet sin mobilenhed, og hans stemme trængte ud i lokalet i Det Nationale Sikkerhedskontrolcenter.

"Hej skat."

"Hvor er du henne?"

"Jeg er på arbejde i min søsters forretning. Jeg har fri klokken 18, tænkte på, om du ikke henter mig – vi kunne gå ud og spise bagefter?"

"Troede du havde ondt i armen."

"Det er væk for længst. Ses vi?"

"Selvfølgelig. Kys."

Ingolf Koll havde i mellemtiden fået to yderligere overvågningssager at tage sig af. Derfor passede det ham fint, at Jonathan Hokusan var på arbejde nogle timer og ikke krævede særlig opmærksomhed. Men han var klar, da alarmen lød og objektet trådte ud ad butikken lidt over seks med sin påståede dårlige arm om skulderen på en ung kvinde. Han fulgte dem til indgangsdøren til en indisk restaurant og senere gennem gaderne til Jonathan Hokusans bolig.

Kameraet i gaden overvågede entredøren natten igennem, mens Koll sov, men der blev ikke afgivet alarm, hvilket betød, at objektet ikke havde forladt sin bolig. Den følgende morgen kunne Koll derfor afslutte sin 24-timers rapport. Der var for ham ingen tvivl om, at mistanken mod Jonathan Hokusan var berettiget, og at han ville blive dømt. Dermed havde Det Nationale Sikkerhedskontrolcenter og han selv som medarbejder endnu engang bevist sin berettigelse. Det styrkede hans selvfølelse i forhold til de stadig flere mennesker, der mente, at overvågning af borgerne truede demokratiet. Ingolf Koll mente tværtimod, at den voksende samfundstransparens var en garant for demokratiets overlevelse. Og med de digitale fodspor, ethvert menneske blandt andet ved hjælp af biometrisk identifikation satte sig i cyberspace, var beviserne ikke til at skyde igennem. Det gavnede sikkerheden i samfundet – og fuldmægtig Kolls løncheck.

Teknologierne

Der udvikles hele tiden nye biometriske teknologier, og det kan derfor være vanskelig at holde sig opdateret omkring teknologiernes aktuelle udviklingsstadiet. De udvalgte teknologier, der bliver gennemgået i det følgende, skulle gerne demonstrere mangfoldigheden blandt de forskellige teknologier. Samtidig er mindre anvendte teknologier baseret på målinger af for eksempel øreform, retina og lugt ikke medtaget. For yderlige beskrivelser af disse teknologier henvises der til den engelsksprogede litteratur på området. Links til engelsksprogede rapporter kan findes på hjemmesiden: www.biometri.info.

Ansigtsgenkendelse

Ansigtsgenkendelse benytter karakteristika ved det menneskelige ansigt til at verificere eller identificere personer. Teknologien bliver typisk brugt til at overvåge offentlige steder samt til logisk og fysisk adgangskontrol. Ansigtsgenkendelse spiller på nuværende tidspunkt en relativt stor rolle på det globale marked for såkaldt 1:N (én til mange) identifikation. 1:N identifikation er den type af identifikation, der anvendes til at identificere en person blandt en gruppe af registrerede personer. Ansigtsgenkendelse bliver derfor ofte brugt i situationer, hvor der i forvejen er opsat kameraer. Teknologien anvendes dog også til såkaldt 1:1 verifikation, hvor ens karakteristika kun sammenholdes med data fra én registreret bruger. Denne anvendelse af teknologien vil for eksempel kunne findes i PDA'er, laptops og lignende samt i forbindelse med automatiseret grænsekontrol.

Ansigtet er for det menneskelige øje den vigtigste kilde til identifikation af de personer, vi er sammen med. Biometriske teknologier baseret på ansigtsgenkendelse "ser" typisk det menneskelige ansigt som ca. 80 forskelligartede orienteringspunkter – for eksempel afstanden mellem øjnene, næsens bredde, øjenhulernes dybde, kindben, kæbelinje og hage. Disse orienteringspunkter bliver målt, og der bliver derudfra skabt en kode bestående af en lang række tal, som udgør en digital beskrivelse af ansigtet.

Et videoovervågningssystem med ansigtsgenkendelse gennem søger konstant det pågældende område for ansigter. Når et ansigt kommer til syne, registreres det på en brøkdelen af et sekund. I denne del af identificeringsprocessen opererer kameraet med en relativt lav opløsning. Men så snart et ansigt er identificeret, slår systemet over til optagelse med høj opløsning. Herefter bestemmes ansigtets størrelse og position. Det er afgørende, at ansigtet er drejet i kameraets retning, men typisk vil systemet acceptere en vinkel på maksimalt 35 grader. Herefter foregår der en såkaldt "normalisering" af billedet, så det, på trods af at det er filmet fra en bestemt afstand og vinkel, bliver konverteret til en standardiseret form. Dette billede bliver nu transformeret til en unik digital kode – en "template" –, der gør det muligt at sammenligne den med de data, der allerede er registreret i en database. Hvis denne digitale kode ligger tilstrækkeligt tæt på en kode, som er registreret i databasen, vil computeren komme op med et match. Hvis ansigtsgenkendelsesteknologien bliver anvendt i forbindelse med overvågning, vil resultatet af dette match typisk blive gennemset af en operatør for at sikre, at de to digitale koder, som computeren har identificeret som ens, nu også tilhører den samme person.

Styrker og svagheder ved ansigtsgenkendelse

Ansigtsgenkendelse har en række styrker, som gør, at teknologien allerede har vundet vid udbredelse. For det første kan ansigtsscanning gennemføres uden fysisk kontakt. Dette gør teknologien velegnet til overvågning og til applikationer på steder, hvor der stilles hygiejniske krav om at undgå berøring. For det andet kan ansigtsgenkendelse udnytte allerede eksisterende kameraer og vil derfor i mange henseender være en relativt billig teknologi at implementere. Endelig kan ansigtsgenkendelse indlæse brugere fra stillbilleder, hvilket blandt andet gør teknologien kompatibel med store databaser med ansigtsbilleder. Ansigtsgenkendelse har dog også en række svagheder. Teknologien kan for eksempel have vanskeligt ved at genkende ansigter over afstand og under forskellige lysforhold. Herudover kan ændringer af frisure, skæg og hovedbeklædning reducere systemets evne til at fortage sammenligninger. Kvaliteten af ansigtsgenkendelse varierer desuden på tværs af personers etniske baggrund, fordi algoritmerne kan være udviklet og testet på bestemte befolkningsgrupper. Endelig er der en betydelig risiko for, at ansigtsgenkendelse kan blive misbrugt til at overvåge personer uden deres samtykke eller viden.

Trends

I dag bliver ansigtsgenkendelse primært baseret på 2D-billeder. Dette vil dog formentligt ændre sig, da der bliver forsket intensivt i at udvikle teknologier til 3D-ansigtsgenkendelse. 3D-ansigtsgenkendelse vurderes på sigt at have et stort potentiale på grund af en langt højere præcision end de nuværende teknologier baseret på 2D. 3D-sensorer er dog på nuværende tidspunkt både meget dyrere og langsommere end 2D-sensorer. Endvidere er de nuværende 3D-modeller forholdsvis sarte og skal kalibreres med jævne mellemrum for at bevare deres præcision.

En anden trend er at kombinere ansigtsgenkendelse med hudteksturanalyse. Sidstnævnte teknologi konverterer linjer, mønstre og tydelige områder i personens hud til en matematisk kode, der anvendes til at genkende registrerede brugere. Det anslås, at hudteksturanalyse kan forbedre nøjagtigheden af traditionel ansigtsgenkendelse med 20-25 procent.

Dna-analyse

Analyse af deoxyribonukleinsyre (dna) i de menneskelige celler er en anden metode til at identificere personer på. Dna findes i alle mennesker og er, dog med undtagelse af enæggede tvillinger, uden sammenligning den mest sikre måde at identificere personer på. Dna-analyse bliver af mange ikke opfattet som en egentlig biometrisk teknologi, da der endnu ikke findes en fuldt automatiseret proces, og fordi det på nuværende tidspunkt tager nogle timer at gennemføre en dna-analyse.

Dna bliver i dag i vidt omfang brugt til at diagnosticere sygdomme, til faderskabstests, til efterforskning og i forbindelse med retsmedicinske undersøgelser. Dna bliver også i mindre grad brugt til personlig identifikation. For eksempel er det i USA muligt at købe et såkaldt DNA PAK (Personal Archival Kit), som kan bruges til at gemme en dna-prøve, som senere kan anvendes til at identificere en person, hvis vedkommende skulle blive udsat for en ulykke, naturkatastrofe eller andet. Dog er den kommercielle brug af dna endnu meget begrænset.

Styrker og svagheder

Dna har en række markante fordele i forhold til andre biometriske teknologier. For det første har alle personer dna, mens alle for eksempel ikke har fingeraftryk. For det andet er dna 100 procent uforanderlig gennem hele livet, og for det tredje er selve dna-analysens meget store præcision en stor fordel.

På den anden side er der også en række betydelige ulemper ved brugen af dna. Først og fremmest er dna-analyse stadig langsom, besværlig og dyr. Yderligere er brugen af dna forbundet med en betydelig risiko for krænkelse af den enkeltes privatliv, da det er nødvendigt at tage en fysisk prøve fra personens krop. Et andet problem med dna-analyse er, at selve dna-prøven – for eksempel et hår – indeholder en lang række personlige oplysninger om blandt andet arveanlæg og helbred. Endelig kan der være etiske problemer knyttet til brugen af dna-analyse, da information fra en dna-profil ikke kun siger noget om en enkelt person, men også kan afsløre forhold om andre personer fra samme familie.

Trends

De allerede eksisterende teknikker til dna-analyse vil i de kommende år blive mere automatiserede, billigere og hurtigere. Desuden vil der blive udviklet nye teknikker, der blandt andet vil gøre det muligt at adskille enæggede tvillingers dna fra hinanden. Ifølge James A. Loudermilk, der er Senior Level technologist i FBI, forskes der i USA intensivt i at udvikle en teknik til at gennemføre dna-analyse på nogle få minutter – også kaldet "Rapid DNA". Loudermilk vurderer, at det om 5-7 år – det vil sige i 2015-17 – vil være muligt at anvende "Rapid DNA" i den praktiske efterforskning i FBI-regi.

Fingeraftrykslæsning

Fingeraftrykslæsning er formentligt den mest velkendte metode til biometrisk identifikation. På grund af deres unikhed og relative ensartethed gennem livet har fingeraftryk været brugt til identifikation i mere end hundrede år.

Metoden er baseret på registrering af de mønstre, som findes på fingerspidserne. En persons fingeraftryk er unikt, og selv enæggede tvillinger har forskellige fingeraftryk. Udviklingen af mønstret i en persons fingeraftryk er delvist bestemt af den genetiske kode i dna, der mere generelt bestemmer, hvordan huden skal udvikles, mens den mere specifikke udvikling er et resultat af fosterets position i livmoderen og det omgivende fostervand.

Der findes to hovedmetoder til matchning af fingeraftryk. Den ene foretager en simpel sammenligning af mønstret i to forskellige billeder. Den mest brugte teknik er dog såkaldt "minutiae matchning", hvor specielle punkter i fingeraftrykkets mønster sammenlignes i forhold til placering og retning – for eksempel de steder, hvor linjerne i fingeraftrykket ophører eller deler sig i flere linjer.

Fingeraftryksscanning anvendes på nuværende tidspunkt blandt andet til biometriske pas og borgerkort i en lang række lande, til økonomiske transaktioner, til check-in i lufthavne, betaling af skolemad og til logisk og fysisk adgangskontrol.

Fingeraftryksscannere

En fingeraftryksscanner scanner fingerens unikke mønster og omdanner dette til en talkode – en såkaldt "template". Der findes dog en række forskellige metoder til fingerscanning, hvoraf de vigtigste er optisk scanning, siliciumscanning, ultralydsscanning og termisk scanning. De to mest anvendte metoder er optisk scanning og siliciumscanning.

Optiske scannere

En optisk scanner fungerer ved at sammenligne billedet af en scannet finger med et tidligere indscannet billede, der er lagret i en database. En optisk scanner fungerer stort set som det lyssensorsystem, der bruges i et almindeligt digitalkamera. Den centrale enhed i en optisk scanner er en såkaldt "Charge Coupled Device" (CCD), som baserer sig på lysfølsomme dioder – også kaldet "photosites". Disse små photosites fungerer ved at generere et elektrisk signal, når de bliver påvirket af lysfotoner. Hver photosite registrerer én pixel, hvorved der ud af lyse og mørke pixels dannes et billede af den scannede finger. Før softwaren i scanneren sammenligner det scannede fingeraftryk med det tidligere lagrede fingeraftryk, kontrollerer programmet kvaliteten af det netop scannede billede. Det er derfor afgørende, at billedet er skarpt, og at det hverken er for lyst eller mørkt. Når eller hvis billedet er godkendt, sammenligner systemet det med de billeder, der er lagret i databasen.

Siliciumscannere

Siliciumscannere har vundet stor udbredelse siden deres kommercielle introduktion i 1998. Denne scannertype genererer ligesom den optiske scanner et billede af fingeraftrykket. Siliciumscanneren anvender dog ikke lys men derimod elektrisk strøm til dette formål. Denne teknologi er baseret på det forhold, at

der er forskel på fingerspidsens evne til at lede elektrisk strøm alt efter, om der er tale om toppen eller dalen af de riller, som findes i hudens overflade. På baggrund af disse forskelle i den elektriske ledeevne registreres et meget præcist billede af fingeraftrykket.

En af de store fordele ved siliciumscannere er den høje billedkvalitet, som er på niveau med de bedste optiske scannere. Ydermere fylder en siliciumscanner ikke særlig meget og kan derfor nemt integreres i små svagstrømsapparater. Denne scannertype kan desuden ikke "snydes" med for eksempel et printet billede af et fingeraftryk, da teknologien måler på både højden af bakker og dale i fingerspidsens hud. På negativsiden hører mindre hårdførhed og kortere levetid, end hvad der for eksempel kendetegner optiske scannere.

Styrker og svagheder ved fingeraftryksscanning

Scanning af fingeraftryk er en relativt moden teknologi sammenlignet med andre metoder til biometrisk verifikation og identifikation. Denne modenhed kombineret med en konkurrencedygtig pris betyder, at der på markedet findes et bredt udbud af forskellige fingeraftryksscannere, som man kan anvende i mange forskellige sammenhænge. Analysen af de data, der er resultatet af scanningen, er relativ simpel i forhold til andre biometriske teknikker og kræver kun begrænset computerkraft. Fingeraftryksscanning kan derfor også foregå decentralt på for eksempel et Smartcard. Ydermere kan det virke mere bekvemt at få scannet netop fingerspidserne frem for eksempelvis sin øjne eller andre kropsdele.

En af svaghederne er, at fingeraftryksscannere er relativt lette at snyde med for eksempel en kunstig finger. Der kan dog opnås større sikkerhed ved for eksempel at scanne flere fingre eller ved at kombinere fingerscanning med andre teknologier. Samtidig kan afgivelse af fingeraftryk lede tankerne hen på politi- og efterforskningsmæssige aktiviteter, hvorfor nogle kan føle det ubehageligt at skulle afgive netop fingeraftryk.

Trends

Der er stor vækst i salget af udstyr til biometrisk identifikation baseret på fingeraftryk. Årsagerne er blandt andet den lave pris, og at fingeraftryksscanning er anvendelig på en lang række forskellige områder. Yderligere er der store økonomiske interesser på spil blandt de firmaer, der er involverede i markedsføringen af fingeraftryksscannere, hvilket i sig selv kan være med til at forklare teknologiens hurtigt voksende udbredelse.

Inden for nærmeste fremtid forventes voksende udbredelse af biometriske løsninger, som kombinerer Smartcards og biometriske læsere til at lette medarbejderes adgang til blandt andet bygninger og computersystemer og borgeres adgang til borgerservices. Der vil sandsynligvis også ske en markant udbredelse af fingeraftryksscannere i blandt andet mobiltelefoner, PDA'er og til computerapplikationer. Samtidig vil der formentlig blive opstillet flere robuste fingeraftryksscannere på befærdede steder såsom grænseovergange, lufthavne og i forbindelse med adgang til offentlige tjenester.

Ganganalyse

Biometrisk ganganalyse udspringer af det forhold, at det enkelte menneskes gangart er forholdsvis særegen. På samme måde som vi med det menneskelige øje kan genkende personer på lang afstand blot ved at iagttage den måde, de går på, er det via biometrisk ganganalyse muligt at identificere personer ud fra blandt andet højde, bredde, skridtlængde og gangrytme. På trods af at det menneskelige perceptionssystem er meget komplekst, er biometrisk ganganalyse et af de få områder, hvor computeren udkonkurrerer den menneskelige perception.

En persons gangart er bestemt af både fysiologiske karakteristika såsom skelettets og musklernes strukturer, men er samtidig afhængig af adfærdsrelaterede karakteristika. Biometrisk ganganalyse måler derfor både på kroppens form og på de bevægelser, der bliver udført. Kroppens form bliver målt i bestemte positioner – eksempelvis når en person har venstre fod fladt placeret på jorden samtidig med højre hæl, eller når højre fod er placeret fladt på underlaget, mens venstre tå rører jorden.

Bevægelsesrytmen måles som varigheden mellem disse forskellige faser. Den kombinerede registrering af kroppens form og bevægelser gør det relativt vanskeligt at udvikle præcise algoritmer, som kan omdannes til templates. Specielt er det en stor udfordring at lave algoritmer, der er uafhængige af, om den person, man ønsker at identificere, for eksempel går i det samme tempo, på det samme underlag, i de samme sko, med den samme taske og er iført det samme tøj. Desuden skal det billede, der bliver brugt, helst optages fra siden, og den præcision, hvormed teknologien kan identificere personer, afhænger derfor også af, om det er muligt at filme fra den rigtige vinkel. Grunden til, at ganganalyse typisk er baseret på billeder, der er taget fra siden, er, at både skridtlængde, armens svingninger og overkroppens position og bevægelser i op- og nedadgående retning fremstår relativt tydeligt i dette perspektiv. Der arbejdes dog også på at udvikle en pålidelig ganganalyse baseret på 3D-teknologi.

Styrker og svagheder

Den største force ved biometrisk ganganalyse er, at teknologien kan anvendes til at identificere personer på stor afstand. Teknologien er langt mindre afhængig af gode lysforhold end for eksempel ansigtsgenkendelse, og den kan desuden anvendes om natten ved brug af infrarødt lys. Teknologien har desuden den fordel, at den er kontaktløs og derfor hygiejnisk – modsat for eksempel fingeraftryksscanning. Endelig kan teknologien anvendes til overvågningssystemer, da den ikke er baseret på fysisk kontakt.

Ganganalyse er ikke særlig præcis i forhold til de øvrige biometriske teknologier, og teknologien vil primært kunne bruges til at identificere personer, hvis identitet derefter vil blive be- eller afkræftet enten manuelt eller via andre biometriske teknologier. Ganganalyse er dermed ikke hensigtsmæssig til brug med henblik på logisk eller fysisk adgangskontrol, men vil i højere grad være nyttig som en integreret del af biometriske overvågningssystemer.

Trends

Præcisionen af biometrisk ganganalyse bliver løbende forbedret. Der er dog stadig et behov for at forbedre teknologien, så den bliver mindre afhængig af faktorer så som underlag, tøj og sko. Der bliver forsket intensivt i at udvikle systemer, der kombinerer ganganalyse og ansigtsgenkendelse, og i at udvikle biometrisk ganganalyse baseret på 3D-teknologi. Begge dele viser indtil videre lovende resultater.

Håndscanning

Ved biometrisk håndscanning anvendes håndens geometriske karakteristika til at be- eller afkræfte en persons identitet. Håndscanning fungerer typisk ved, at man placerer sin højre hånd på en flad metalplade, hvorpå der sidder en række ”pigge” (typisk lavet af plastik), der sørger for, at hånden er placeret korrekt på scanneren. Fingrene skal være spredte, og håndfladen skal hvile fladt på metalpladen. Når hånden er korrekt placeret, bliver den affotograferet. Nogle håndscannere har kun ét indbygget kamera og genererer 2D-billeder, mens andre anvender flere kameraer og spejle til at danne et 3D-billede. Herefter bliver der - afhængig af den anvendte teknologi - målt på håndens længde, bredde, højde, afstand mellem leddene og håndens knoglestruktur. De karakteristika, der måles, er ikke specielt unikke, og teknologien bruges derfor ikke til identifikation men kun til verifikation.

Den samme teknologi, som anvendes til håndscanning, bliver ligeledes brugt til at lave fingerscannere, der måler på pege- og langfingerens geometriske karakteristika.

Hvor bruges håndscanning?

De første håndscanningssystemer kom på markedet i sidste halvdel af 1980'erne, og teknologien har siden da været brugt til en række forskellige formål. Arbejdstidsregistrering og fysisk adgangskontrol på arbejdspladser har været det mest udbredte anvendelsesområde – for eksempel har alle atomkraftværker i USA opstillet adgangskontrolsystemer baseret på biometrisk håndscanning. Teknologien anvendes også i det såkaldte INSPASS-program, der tillader registrerede passagerer at springe køen over ved immigrationskontrollen i en række internationale lufthavne i USA. I Disney World anvendes fingerformsscanning til at sikre, at ens adgangskort ikke misbruges.

På steder, hvor der kræves et højere sikkerhedsniveau, bliver håndscanning dog ofte kombineret med andre biometriske teknologier. Dette er for eksempel tilfældet ved en række trafikerede checkpoints ved den israelsk-palæstinensiske grænse.

Teknologiens styrker

Geometrisk håndscanning er velegnet til krævende miljøer, da teknologien er meget modstandsdygtig over for variationer i for eksempel temperatur og fugtighed. De fleste håndscannere har desuden en meget lav ”Failure To Enroll Rate” (FTER) og ”False Match Rate” (FMR) og kan fungere fejlfrit på trods af, at brugerne for eksempel har beskidte hænder eller bærer tynde plastikhandsker. Teknologien er dermed specielt velegnet til fysik adgangskontrol, hvor scannerenheden ofte vil være placeret på et mere eksponeret sted end systemer til logisk adgangskontrol.

Håndscanning har efterhånden været brugt i årtier, og teknologien har ikke forandret sig betydeligt indenfor de sidste år. Om end mange af de nyere biometriske teknologier er mere præcise, er de ikke så gennemtestede som håndscanning. Desuden betragtes håndscanning af mange som mindre indgribende i den enkeltes privatsfære end for eksempel fingeraftryk, der ofte forbindes med politi og efterforskning af forbrydelser. Endelig er håndens dimensioner forholdsvis stabile gennem voksenlivet og ændrer sig ikke nævneværdigt med alderen, da det primært er form og knoglestruktur, der bliver målt på. Aldrings-tegn i huden er derfor ikke af større betydning for matchningsresultatet.

Teknologiens svagheder

Håndscanning har dog også en række svagheder i forhold til andre biometriske teknologier. Som nævnt er håndscanning ikke særlig præcis i forhold til andre biometriske teknologier såsom finger- og irisscanning, hvilket gør teknologien uegnet til 1:N identifikation. Selve scanneren er desuden så stor, at den ikke er velegnet til logisk adgangskontrol. Endelig er håndscanning en relativt dyr teknologi sammenlignet med for eksempel fingeraftryksscanning.

Trends

Håndscanning er efterhånden en ældre teknologi, som på mange områder er blevet overhalet af andre biometriske teknologier. Der sker dog stadigvæk forbedringer af teknologien blandt andet i form af bedre kameraer og forøgelse af template-størrelsen. Der arbejdes desuden på at udvikle systemer, hvor man ikke behøver at placere hånden på en plade, men blot holder den foran scanneren. Den generelle tendens på det biometriske område med at kombinere forskellige teknologier vil sandsynligvis også resultere i kombinationer af hånd- og fingerscanning og hånd- og venescanning.

Irisgenkendelse

Irisgenkendelse er en meget sikker biometrisk teknologi, der kan anvendes til såvel verifikation som identifikation. Faktisk vurderes chancen for, at der findes to identiske iris til at være én ud af 1078. Iris forbliver uændret hele livet og er bedre beskyttet bag øjenlåget end for eksempel et fingeraftryk, der sli-des dagligt. Irisscanning er en af de mere inkluderende biometriske teknologier. For eksempel kan blinde også anvende irisscannere, så længe de har iris. Ligeledes er der kun meget sjældent problemer med upræcise læsninger forårsaget af briller eller kontaktlinser.

Hvordan fungerer en irisscanner?

En fordel ved irisscanning er, at den kan baseres på en relativt simpel teknologi. Hjørnестenen i en iris-scanner er et digitalt kamera baseret på CCD-teknologi. For at kunne tage klare billeder af iris bruges både synligt og infrarødt lys. Det infrarøde lys er med til at skabe højere kontrast og dermed gøre det lettere at adskille pupillen fra iris. Når kameraet har taget et billede, lokaliseres pupillens centrum og yderkant, iris' kanter, øjenlåget og øjenvippen. Herefter bliver mønstret i iris analyseret og transformeret til en unik numerisk kode – også kaldet en "template".

Teknologiens styrker

Irisscanning er karakteriseret ved at have en ekstremt lav "False Match Rate" (FMR). Det skyldes både iris' unikhed men også det forhold, at de algoritmer, der bruges til at konvertere de personlige karakteristika fra det scannede billede til templates, er meget nøjagtige og detaljerede. Irisscanning har desuden den fordel, at iris ikke forandres med tiden. Samtidig kan teknologien anvendes til både logiske og fysiske adgangssystemer, hvorfor der er mulighed for at skabe et integreret adgangssystem til for eksempel både bygninger og computersystemer.

Teknologiens svagheder

Irisscanningsteknologien er på nuværende tidspunkt mere besværlig at anvende for brugeren end for eksempel fingeraftryksscanning og ansigtsscanning. Forklaringen er, at det kræver en relativ præcis placering af hoved og øjne. Dette problem vil dog med tiden blive mindre i takt med, at teknologien forbedres.

Udfordringen med at få acceptable billeder af iris resulterer i en relativt høj afvisning af personer, der ellers er registrerede som brugere – såkaldt "False Rejection Rate" (FRR). Det forventes dog, at teknologien med tiden vil overkomme dette problem.

Det er endvidere en svaghed, at relativt mange mennesker opfatter brug af øjnene til biometrisk autorisation og identifikation som noget ubehageligt.

Der er også en udbredt bekymring for de fremtidige formål, som irisscanning kan blive anvendt til. Det er blandt andet ikke utænkeligt, at det bliver muligt at identificere en person på meget lang afstand, hvilket – i kombination med sammenkøring af centrale registre – vil øge risikoen for gennemgribende overvågning.

Trends

Irisscanning har i en årrække været brugt i forbindelse med grænsekontrol i blandt andet De Forenede Arabiske Emirater og England, af FN til uddeling af nødhjælp og af det amerikanske militær til at sikre, at kun de rette personer får adgang til bestemte faciliteter.

Irisscanning er måske den mest lovende af de nuværende fysiske biometriske teknologier, primært på grund af den høje præcision. På nuværende tidspunkt fungerer irisscannere allerede så godt, at de kan scanne iris på ca. tre meters afstand gennem både briller og bilruder, og mens personer er i bevægelse.

Forventningen er, at irisscanning i fremtiden vil kunne ses i en bred variation af enheder såsom mobiltelefoner, PDA'er og laptops. Det forventes desuden, at irisscanning hurtigt vil vinde videre udbredelse i forbindelse med autorisation af forbrugere, internt på arbejdspladser, som adgang til borgerservices og i forbindelse med grænsekontrol og immigration.

Signaturanalyse

Biometrisk signaturanalyse benytter de unikke aspekter ved håndskriften – typisk ens underskrift – til at verificere en persons identitet. Hvad der måles på varierer en smule fra producent til producent, men er typisk måling af pennestrøgenes form, rækkefølge, hastighed, acceleration, tryk og retning.

I praksis skal brugeren af teknologien registrere sin underskrift på en elektronisk "notesblok". Det skal ske gentagne gange for at udjævne variationer mellem de enkelte signaturer. Den template, der bliver gemt i systemet, rummer således data for brugerens "gennemsnitlige" underskrift.

Teknologien er endnu ikke særlig udbredt, men den kan blive det alt efter hvilke normer og standarder, der vinder indpas – for eksempel til verifikation af personers identitet på kontrakter inden for blandt andet finansverdenen, forsikringsbranchen, internethandel, i sundhedssektoren og i forbindelse med tildeling af velværdsydelser.

Styrker og svagheder

En fordel ved biometrisk signaturanalyse er, at underskriften i århundreder har været en accepteret form for verifikation af ens identitet. Det at afgive sin underskrift er en af de mindst indgribende autentifikationsformer og nyder en høj grad af accept i befolkningen. Netop af denne grund anses det for relativt uproblematisk at anvende biometrisk signaturanalyse til elektroniske transaktioner.

Teknologien er derudover relativt sikker. Man kan forholdsvist nemt kopiere en anden persons underskrift, så den - set med det blotte øje - ligner den originale underskrift. Men det er meget vanskeligt at lave en kopi, der både ligner originalen og er udført med samme rytme, tryk og hastighed. Samtidig er det muligt at ændre sin underskrift, hvis brugeren er nødsaget til at ændre identitet.

Men der er også en række ulemper forbundet med brugen af biometrisk signaturanalyse. Der er stor forskel på, hvor ensartet en given person kan skrive sin underskrift. Dermed er der også en relativt stor gruppe af personer, som vil have vanskeligheder ved at registrere og senere verificere deres personlige signatur. Specielt personer med sygdomme, der påvirker musklerne i hånden, vil have vanskeligt ved at verificere deres identitet, og de vil derfor være udsat for en væsentligt højere "False Rejection Rate" (FRR). Desuden kan brugerens mentale tilstand bevirke, at personen kommer til at udføre deres personlige signatur på en måde, der afviger fra den normale. Dertil kommer, at de fysiske omgivelser bør være de samme under den første registrering og den senere verifikation. Her er det for eksempel relevant, om brugeren står op eller sidder ned, eller om der er de samme muligheder for at hvile underarmen. Endelig skal det nævnes, at ens personlige underskrift ikke er uforanderlig, men for manges vedkommende ændrer sig betydeligt gennem livet.

Trends

Verdensmarkedet for biometrisk signaturanalyse ventes ifølge blandt andet Global Industry Analysts Inc. at vokse med stor hastighed frem mod 2015. I perioden 2010-15 forventes salget af trådløse systemer baseret på signaturanalyse at stige støt. Teknologien vil især blive anvendt til at bekræfte identiteten af forbrugere og borgere, som ønsker at modtage bestemte services eller varer.

Udviklingen mod et papirløst samfund har været med til at skabe et behov for systemer som biometrisk signaturanalyse. Om det bliver biometrisk signaturanalyse eller en af de konkurrerende biometriske teknologier, der vinder kapløbet, vil vise sig i løbet af de kommende år. Introduktionen af et biometrisk borgerservicekort vil blandt andet kunne have indvirkning på denne udvikling.

Stemmegenkendelse

Biometrisk stemmegenkendelse gør brug af både fysiologiske og adfærdsrelaterede karakteristika. Den fysiologiske del af stemmegenkendelsen er relateret til den fysiske udformning af personens stemmebånd, strubehoved, luftveje mv., mens den adfærdsrelaterede del knytter sig til den fysiske aktivitet, der er relateret til menneskers tale.

Der er to former for stemmegenkendelse: Tekstafhængig og tekstuafhængig. I systemer, der er baseret på tekstafhængig tale, præsenterer man enten et fast password, eller også beder systemet en om at sige en bestemt sætning blandt en række tidligere registrerede sætninger. Et eksempel kan være, at systemet beder en om at sige en række tilfældigt genererede tal, som man tidligere har programmeret ind i systemet – for eksempel: "1-2-32-7". På denne måde kan sikkerheden øges i modsætning til, når man bruger det samme password hver gang. Det tekstuafhængige system har ikke på forhånd kendskab til hvilke ord eller fraser, brugeren vil formulere, og kan derfor også bruges til at identificere personer i situationer, hvor den involverede er uvidende om indsamlingen. Denne teknologi anvendes for eksempel til at identificere lydoptagelser af Osama Bin Laden.

Teknologien bag stemmegenkendelse fungerer på den måde, at der dannes en række algoritmer på baggrund af målinger af de registrerede lydes frekvens, lydstyrke og rytme. Mange af de karakteristika, der anvendes til at danne templates, er unikke for den menneskelige stemme, hvorfor teknologien er meget vanskelig at kopiere selv med gode lydoptagere. På trods af at en optagelse i høj kvalitet vil ligge meget tæt op ad den menneskelige stemme, vil det ikke kunne undgås, at der bliver tilført ikke-menneskelige elementer til den afspillede stemme. Muligheden for at snyde stemmegenkendelsessoftwaren er dog stadig til stede, men det er en forholdsvis vanskelig proces.

Stemmegenkendelse har hidtil hovedsagligt været brugt til at skabe højere sikkerhed i forbindelse med økonomiske transaktioner via telefon eller mobiltelefon. Teknologien bliver også i få tilfælde brugt til fysisk adgangskontrol.

Styrker og svagheder

Stemmegenkendelse er relativt set en billig biometrisk teknologi, da den kan anvendes sammen med traditionelle teknologiske komponenter som mikrofoner, headsets, fastnet- og mobiltelefoner. Desuden er stemmegenkendelse en relativt sikker teknologi - den er for eksempel mere sikker end visse systemer baseret på fingeraftryksscanning. Stemmegenkendelse har desuden den fordel, at befolkningen ikke forbinder teknologien med overvågning og registrering, hvorfor den ikke i så høj grad opfattes som privatlivskrænkende.

Der er også en række ulemper forbundet med stemmegenkendelse. Dårlige telefonforbindelser og baggrundsstøj kan give falske "non-matches" og kan derfor skabe irritation for brugerne. Der kan for eksempel opstå problemer, hvis man har ladet sig registrere første gang på en fastnettelefon og derefter forsøger at anvende en mobiltelefon. Desuden er det stadig en generel opfattelse, at biometrisk stemmegenkendelse er en forholdsvis usikker teknologi. Der er blandt andet en udbredt men ofte ubegrundet bekymring for, at systemet ikke vil kunne genkende ens stemme i forbindelse med sygdom eller mangel på søvn. Endelig er de templates, der anvendes til stemmegenkendelse, typisk større end dem, der bliver brugt til andre biometriske teknologier, hvorfor matchning-processen foregår relativt langsom.

Tastodynamik

Tastodynamik kan anvendes til at verificere en persons identitet. Teknologien fungerer ved at måle den måde, brugeren af en computer skriver på tastaturet. Der måles både på den tid, brugeren holder hver enkelt tast nede, og den tid, der forløber mellem de enkelte anslag. Biometrisk autentifikation baseret på tastodynamik måler ikke på fysiologiske karakteristika af nogen art og er dermed en ren adfærdsrelateret, biometrisk teknologi. Teknologien bliver som regel brugt i forbindelse med indtastningen af et password og anvendes ikke til at identificere personer, der skriver på et dokument eller lignende.

Måling af tastodynamik kræver ikke ekstraudstyr som for eksempel scannerenheder eller kameraer, det kræver udelukkende, at der installeres en softwareløsning på den computer, som personen i forvejen benytter. Det installerede program registrerer brugerens brug af keyboardet og genererer på den baggrund templates, som bruges ved den senere verifikation af brugeren.

Styrker og svagheder

En af de store fordele ved brugen af tastodynamik er, at teknologien for det første baserer sig på allerede tilstedeværende udstyr, og at brugeren ikke skal gøre andet end at skrive sit password som ved en almindelig log-in-situation. Løsningen indebærer også den fordel, at ens password kan ændres, hvis der opstår behov for at skifte identitet. Det betyder, at tastodynamik ikke indebærer samme risici for krænkelse af privatlivets fred som biometriske teknologier, der er baseret på målinger af permanente fysiologiske karakteristika.

Der er dog også en række betydelige svagheder forbundet med brugen af verifikation baseret på tastodynamik. Teknologien er endnu ikke på et særligt højt udviklingsstadium og er ikke gennemtestet uden for laboratoriet. Det betyder blandt andet, at de algoritmer, der anvendes til at konstruere templates, ikke er særligt veludviklede. Det betyder også, at der stadig er for mange falske afvisninger af autoriserede brugere, og at der gives adgang til for mange uautoriserede personer. En anden stor svaghed er, at personers måde at skrive et password på ikke er uforanderlig, men derimod ofte ændrer sig fra gang til gang. Alt dette betyder i praksis, at firmaer og organisationer typisk fravælger at anvende tastodynamik i kombination med passwords. Teknologien skaber endnu ikke et væsentligt højere sikkerhedsniveau og er samtidig en kilde til irritation hos de ikke-accepterede, autoriserede brugere.

Trends

De lave omkostninger, der er forbundet med brugen af tastodynamik, kan på sigt gøre teknologien attraktiv. Dette kræver dog, at der udvikles algoritmer, som overvinder udfordringen med variation i brugernes anslagsmønstre. Hvis det lykkedes, er der gode muligheder for, at tastodynamik kan blive en meget udbredt biometrisk teknologi.

Venescanning

Biometrisk venescanning er en relativt ny biometrisk teknologi, hvor man anvender blodårerne i hænder eller fingre til at be- eller afkræfte en persons identitet. Teknologien udnytter, at det mønster, der dannes af ens blodårer, er unikt og stort set ikke forandres med alderen.

Venescanning vil i princippet kunne anvendes utallige steder på kroppen. I dag bliver teknologien brugt til at scanne blodårenes struktur i håndfladen, på oversiden af hånden og i fingrene. Teknologien er baseret på en kombination af almindelig CCD-kamerateknologi og infrarødt lys.

Brugen af infrarødt lys får hæmoglobinet i blodårerne til at fremstå mørkt, mens den resterende del af hånden eller fingeren fremstår som lys. Fra det billede, der bliver taget af CCD-kameraet, lokaliseres centrale punkter i blodåremønstret, og der dannes på baggrund heraf en template, som efterfølgende anvendes til at be- eller afkræfte en persons identitet. De centrale punkter, der registreres i template, er forgreninger i blodårerne, vinklen af disse forgreninger og tykkelsen af blodårerne.

Hvor kan venescanning anvendes?

Venescanning har tidligere hovedsageligt været brugt i Japan og Sydkorea, men har igennem de sidste år også vundet udbredelse til resten af verden. Både venescanning af håndfladen og fingervenescanning bliver i vid udstrækning anvendt i hæveautomater, til fysisk og logisk adgangskontrol, til arbejdstidsregistrering, på biblioteker og i sundhedssektoren. Fordele såsom pris og præcision forventes at medføre, at venescanning også bliver en stadig mere udbredt teknologi.

Styrker og svagheder

Teknologien måler på karakteristika inde i selve kroppen og er derfor ikke så sårbar over for ydre skader og skrammer som for eksempel fingeraftryksscanning. Problemet med at opnå den rigtige belysning i forhold til blandt andet ansigtsgenkendelse er heller ikke aktuelt for venescanning, da det, der måles på, som nævnt er inde i kroppen og ikke påvirkes af ydre lysforhold. Samtidig er personers venestrukturer med den nuværende viden ikke så lette at kopiere som for eksempel et fingeraftryk.

Venescanning er på den anden side endnu ikke særlig gennemtestet under ugunstige situationer som for eksempel kolde temperaturer og kraftigt sollys. Der er samtidig ikke foretaget studier af en persons blodåremønster gennem en lang årrække. Endvidere er der endnu ikke særligt stort kendskab til hvilke sygdomme, der kan føre til forringede match-resultater. Ud over fysiske skader vil blandt andet tumorer, aterosklerose, diabetes og højt blodtryk formentligt kunne påvirke blodårenes udseende og derved påvirke muligheden for at scanne mønstret korrekt.

Trends

Prisen på venescannere er allerede i dag forholdsvis lav, og det forventes, at prisen vil falde yderligere de kommende år. Da de nuværende testresultater for venescanning viser lovende tegn, hvad angår præcision – den er større end ved fingeraftryks- og håndscanning -, må det forventes, at venescanning bliver en udbredt biometrisk teknologi på globalt plan i de kommende år. Endelig er venescanning en oplagt teknologi at anvende i kombination med andre biometriske teknologier som for eksempel fingeraftryksscanning og håndscanning.

Deltagerliste

Teknologirådets workshop om den fremtidige brug af biometriske teknologier

Anette Høyrup	Forbrugerrådet
Bettina Tjagvad Kristensen	Udlændingesservice Arbejdsmarkedskontoret
Camila Wøldike	Sociologistudernede
Charlotte Bagger Tranberg	Aalborg Universitet - Juridisk Institut
Chrispin Smith	
Christian Damsgaard Jensen	Informatik og Matematisk Modellering
Christian Wernberg-Tougaard	In4change.com
Claus Fabricius	AIM Danmark
Flemming Faber	IT- og Telestyrelsen
Frederik Kortbek	Danish Biometrics
Helle Schaumann	Danske Institut for menneskerettigheder
Henning Mortensen	ITEK/Dansk Industri
Jacob Skjødt Nielsen	Teknologirådet
Jakob Vedelsby	Freelancejournalist
Janni Christoffersen	Datatilsynet
John Radmer	Rigspolitiet
Jonas Andersson	Precise Biometrics
Lars Kornbek	VITANI A/S
Lene Gisselø	Rigspolitiet
Martin Sølvkjær	Bispebjerg Hospital MIT-afdelingen
Mikael Hertig	Nensome
Niels Bertelsen	PROSA
Niels Rune Bøggild	Ministeriet for Flygtninge,
Nis M. Nissen	Bispebjerg Hospital
Peter Kastmand Larsen	Københavns Universitet Retsantropologisk Enhed
Peter Lemcke Frederiksen	Teknologirådet
Peter Ussing	CSC
Stephan Engberg	Priway Aps
Søren Duus Østergaard	IBM Danmark A/S
Thomas Laursen	Det Ethiske Råds sekretariat
Thomas S. Hansen	Ringkøbing-Skjern Kommune
Torben Andresen Lindhardt	Dansk Metal
Uffe Clemmensen	QUARD Technology

Referenter:

Claus Bové	Teknologirådet
Mads Hauptmann Larsen	Teknologirådet
Oliver Bo Schmidt	Teknologirådet
Sune Bjarke Stefansson	Teknologirådet
Zara Wölck	Teknologirådet

