



12168/02/DA
WP 80

Arbejdsdokument om biometri

Vedtaget den 1. august 2003

Gruppen, der er nedsat i henhold til artikel 29 i direktiv 95/46/EF, er et uafhængigt EU-rådgivningsorgan vedrørende databeskyttelse og beskyttelse af privatlivets fred. Dens opgaver er fastsat i artikel 30 i direktiv 95/46/EF og artikel 14 i direktiv 97/66/EF. Gruppens sekretariat varetages af:

Europa-Kommissionen, GD for det Indre Marked, Direktorat E (Tjenesteydelser, intellektuel og industriel ejendomsret, medier og databeskyttelse), B-1049 Bruxelles, Belgien, Kontor C100-6/136.

Websted: www.europa.eu.int/comm/privacy

GRUPPEN VEDRØRENDE BESKYTTELSE AF FYSISKE PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER,

som er nedsat i henhold til Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995¹,

som henviser til direktivets artikel 29 og artikel 30, stk. 1, litra a), og artikel 30 stk. 3,

som henviser til gruppens forretningsorden, særlig artikel 12 og 14,

har vedtaget nærværende arbejdsdokument:

1. INDLEDNING

De seneste års store fremskridt inden for biometrisk teknologi og den bredere anvendelse heraf kræver en grundig undersøgelse af databeskyttelsen². En omfattende og ukontrolleret udnyttelse af biometri skaber bekymring med hensyn til beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder. Der er her tale om en særlig form for data, idet de vedrører en fysisk persons adfærdsmæssige og fysiologiske karakteristika og gør det muligt at foretage en entydig identifikation³ af vedkommende.

I dag anvendes biometrisk databehandling ofte i automatiske autentifikations-/verifikations- og identifikationsprocedurer, navnlig ved adgangskontrol til såvel fysiske som virtuelle områder (dvs. adgang til bestemte elektroniske systemer eller tjenesteydelser).

Tidligere var biometri fortrinsvis baseret på en undersøgelse af dna og fingeraftryk. Sidstnævnte blev især benyttet af de retshåndhævende myndigheder (f.eks. ved strafferetlige undersøgelser). Hvis samfundet opfordrer til videreudvikling af fingeraftryks- eller andre biometridatabaser til brug ved rutineundersøgelser, kan det betyde, at tredjemand får større mulighed for at benytte disse til eget formål, selvom det ikke oprindeligt har været intentionen. Den nævnte tredjemand kan omfatte retshåndhævende myndigheder.

Det er betænkeligt, at offentligheden grundet den øgede brug af biometriske data kan blive mindre opmærksom på, hvorledes behandling af dataene kan påvirke deres

¹ EFT L 281 af 23.11.1995, s. 31. Tilgængeligt på:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

² Efter den 11. september 2001 er biometri ofte blevet fremhævet som et middel til at forbedre den offentlige sikkerhed. I EU pågår der drøftelser om brug af biometri i ID-kort, pas, rejsedokumenter og visa. USA vil inden længe stille krav om anvendelse af biometri ved identifikation af udlændinge, der ankommer til eller forlader landet. ILO's konvention nr. 108 blev i 2003 ændret, så det bliver muligt at indføre obligatorisk brug af biometri for søfarende. Disse emner drøftes også i andre internationale fora såsom G8, OECD osv.

³ Den entydige identifikation afhænger dog af forskellige faktorer, herunder databasestørrelse og biometriske typer.

hverdag. Brug af biometri på skolebiblioteker kan f.eks. gøre eleverne mindre bevidste om eventuelle risici vedrørende databeskyttelse senere i livet.

Formålet med dette dokument er at bidrage til en effektiv og ensartet gennemførelse af de nationale bestemmelser om databeskyttelse, der er vedtaget i henhold til direktiv 95/46/EF om biometriske systemer. I dokumentet fokuseres fortrinsvis på anvendelse af biometri til autentifikation og verifikation. Gruppen har til hensigt at fremsætte fælles EU-retningslinjer, navnlig til branchen for biometriske systemer og brugere af disse teknologier.

2. BESKRIVELSE AF BIOMETRISKE SYSTEMER

Biometriske systemer er teknologiske biometriapplikationer, der gør det muligt at foretage en automatisk identifikation og/eller autentifikation/verifikation af en fysisk person⁴. Autentifikations-/verifikationsapplikationer anvendes til opgaver på meget forskellige områder, og ansvarsmæssigt hører de ind under en række forskellige instanser.

De enkelte biometriske metoder er, uanset om de benyttes til autentifikation/verifikation eller identifikation, mere eller mindre afhængige af de biometriske parametre:

- **De universelle:** Det biometriske element eksisterer hos alle fysiske personer⁵.
- **De entydige:** Det biometriske element er særegent for hver enkelt person.
- **De bestandige:** Det biometriske elements egenskab ændrer sig ikke hos den enkelte fysiske person.

Der skelnes mellem to hovedtyper af biometriske teknikker afhængigt af, hvorvidt der anvendes faste data eller dynamiske adfærdsmæssige data⁶.

For det første findes der fysiske og **fysiologisk baserede** teknikker, som bestemmer en given persons fysiologiske karakteristika, herunder f.eks. verifikation af fingeraftryk, analyse af fingrenes geometri, irisgenkendelse, nethindeanalyse, ansigtsgenkendelse, håndens mønstre, genkendelse af ørets form, detektion af kropslugt, stemmegenkendelse, analyse af dna-mønstre⁷ eller hudens svedporer.

For det andet anvendes **adfærdsbaserede** teknikker, der måler en given persons adfærd, dvs. underskriftsverifikation, analyse af tastaturanslag, analyse af gangarter osv.

⁴ Forskellen mellem autentifikation (verifikation) og identifikation er vigtig. Autentifikation besvarer spørgsmålet: Er jeg den, jeg udgiver mig for at være? Systemet bekræfter en given persons identitet ved at behandle vedkommendes biometriske data, og spørgsmålet besvares med ja eller nej (sammenligningen er 1:1). Identifikation besvarer spørgsmålet: Hvem er jeg? Systemet genkender spørgeren ved at skelne vedkommende fra andre personer, hvis biometriske data ligeledes er lagret. Systemet skelner mellem denne person og resten af de registrerede og svarer, at spørgeren er X.

⁵ Ikke alle biometriske elementer har samme værdi, og sondringsfrekvensen – dvs. evnen til at skelne mellem personer – afhænger nøje af den benyttede biometri. De mest karakteristiske biometriske elementer synes at være dna, nethinde og fingeraftryk.

⁶ Nogle teknikker kan både være fysiologiske og adfærdsmæssige.

⁷ Brugen af dna til biometrisk identifikation afføder særlige overvejelser, som det vil føre for vidt at drøfte i nærværende dokument. Dog kan det nævnes, at det for øjeblikket ikke synes muligt at anvende tidstro generering af en dna-profil til autentifikation.

På grund af den hurtige teknologiske udvikling og den voksende bekymring for sikkerheden kombinerer mange biometriske systemer forskellige biometriske målinger med andre identifikations- eller autentifikationsteknologier. F.eks. benyttes der både ansigtsgenkendelse og stemmeregistrering i visse systemer. Ved autentifikation kan tre forskellige metoder anvendes samtidig. Disse er henholdsvis baseret på en bestemt viden (password, PIN-kode osv.), en bestemt ting (mærke, CAD-nøgle, smartkort osv.) og et bestemt personkarakteristika (et biometrisk kendetegn). Til computerbrug kan der indsættes et smartkort, indtastes et password og fremvises fingeraftryk.

De biometriske prøver, de såkaldte biometriske data (f.eks. fingeraftrykkets geometri, iris- eller nethindescanning eller stemmeoptagelser), indsamles i en "registreringsfase" ved hjælp af specifikke sensorer for hver enkelt biometrisk metode. Først uddrager det biometriske system brugerspecifikke biometriske data og derefter opbygges en biometrisk "skabelon". Skabelonen er en struktureret beskæring af et biometrisk billede, nemlig den registreredes biometriske mål. Det er denne skabelon i digitaliseret form, der lagres, og ikke selve det biometriske element. Ydermere kan de biometriske data behandles som rådata (et billede), afhængigt af hvilke funktioner det pågældende biometriske system har⁸.

Det er kun i registreringsfasen, at der kan trækkes på både rådata, ekstraktions- og beskyttelsesalgoritmer (kryptografi, nøgletransformation osv.) samt skabeloner. Det skal i den henseende understreges, at hvis der fremkommer oplysninger i forbindelse med de rådata, der kan betragtes som følsomme i betydningen af artikel 8 i direktiv 95/46/EF, skal registreringen af dataene ske i overensstemmelse med bestemmelsen (se punkt 3.7 nedenfor).

I forbindelse med databeskyttelse spiller det også en vigtig rolle, hvorledes brugernes skabeloner lagres. Det afhænger af, hvilken type applikation den biometriske anordning skal anvendes i, og skabelonernes størrelse. Skabelonerne kan lagres på følgende måder:

- a) - I en biometrisk anordnings hukommelse
- b) - I en central database
- c) - I plastickort, optiske kort eller smartkort. Denne metode tillader, at brugeren kan benytte sin skabelon til identifikationsformål.

I princippet er det ikke nødvendigt at lagre referencedata til autentifikation/verifikation i en database, det er tilstrækkeligt at gemme de personlige data decentralt. Til gengæld er det nødvendigt at lagre referencedata til identifikation i en central database, idet systemet for at kunne fastslå den registreredes identitet skal kunne sammenligne vedkommendes skabeloner eller rådata (billede) med de tilsvarende skabeloner/rådata fra alle de personer, hvis data er lagret centralt.

Ved databeskyttelse er det endvidere afgørende, at nogle biometriske systemer bygger på information, f.eks. fingeraftryk eller dna-prøver, der kan indsamles, uden at den registrerede er klar over det, dvs. at vedkommende uafvidende kan efterlade sig spor. Ved at anvende en

⁸ Dette dokument vedrører biometriske systemer, som bygger på skabeloner og derfor kan anvendes til rådata. De særlige forhold, der gør sig gældende vedrørende rådata, kan dog betyde, at kravene til databeskyttelse skal tilpasses.

biometrisk algoritme på fingeraftrykket på et glas er det muligt⁹ at undersøge, om en person er registreret i en database indeholdende biometriske data og i givet fald kontrollere, hvem vedkommende er, ved at sammenligne de to skabeloner. Det samme gælder andre biometriske systemer, f.eks. sådanne, som bygger på analyse af tastaturanslag eller ansigtsgenkendelse på afstand, på grund af de særlige teknologiske metoder, der benyttes¹⁰. Der knytter sig to problemer hertil: For det første kan indsamlingen og behandlingen af data gennemføres uden den registreredes vidende, og for det andet kan disse biometriske teknologier uanset deres vederhæftighed udnyttes groft, da det er svært at opdage brugen af dem. Det er derfor nødvendigt at fastlægge særlige beskyttelsesforanstaltninger, der omfatter disse teknologier.

3. ANVENDELSE AF PRINCIPPERNE I DIREKTIV 95/46/EF

3.1. Anvendelse af direktiv 95/46/EF

I artikel 2, litra a), i direktiv 95/46/EF forstås "personoplysninger" som "enhver form for information om en identificeret eller identificerbar fysisk person (...); ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske (...) identitet". I betragtning 26 uddybes dette: "For at afgøre, om en person er identificerbar, tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person".

I henhold til ovennævnte definition anses de biometriske identifikationsmålinger eller de digitale udgaver heraf (dvs. skabelonerne) i de fleste tilfælde for at være personoplysninger¹¹. Biometriske data kan åbenbart altid betragtes som "information om en fysisk person", da de vedrører data, som i kraft af deres art indeholder oplysninger om en given person. Ved biometrisk identifikation er en person som hovedregel identificerbar, idet de biometriske data benyttes til identifikation eller autentifikation/verifikation ved at skelne den registrerede fra andre personer¹². I henhold til artikel 3, stk. 1, i direktiv 95/46/EF skal bestemmelserne om databeskyttelse anvendes på behandling af personoplysninger, der helt eller delvist foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Dette direktiv gælder ikke for behandling af personoplysninger, som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter. En række biometriske applikationer af familiemæssig art henhører under denne kategori.

⁹ Visse forudsætninger kræves dog opfyldt, såsom indsamling af fingeraftrykket fra glasset uden at ødelægge det, teknisk udstyr til at behandle fingeraftryksdataene, adgang til producentens algoritme og/eller fingeraftryksdatabasen.

¹⁰ Se punkt 3 om anvendelsen af direktiv 95/46/EF, navnlig punkt 3.3 om forpligtelsen til at informere den registrerede.

¹¹ I tilfælde, hvor de biometriske data ligesom skabelonerne lagres på en sådan måde, at den registrerede ikke kan identificeres af den registeransvarlige eller en anden person, betragtes dataene ikke som personoplysninger.

¹² Muligheden for at identificere en person afhænger også af, om andre data er tilgængelige, som sammen eller hver for sig kan medvirke til identifikationen. I artikel 2, litra a) i direktiv 95/46/EF nævnes udtrykkeligt muligheden for at definere personoplysninger som information, "der direkte kan identificeres" ved hjælp af "et eller flere elementer, der er særlige for denne persons fysiske identitet".

Bortset fra disse undtagelser er behandling af biometriske data udelukkende lovlig, såfremt alle procedurer – begyndende med registreringen – gennemføres i henhold til bestemmelserne i direktiv 95/46/EF.

Dette dokument omfatter ikke alle de problemer, der kan opstå ved anvendelsen af direktiv 95/46/EF i forbindelse med biometriske data. Kun de mest relevante behandles, hvilket betyder, at der ikke gives en udtømmende beskrivelse af konsekvenserne af anvendelsen af direktiv 95/46/EF.

3.2. Formåls- og proportionalitetsprincippet

Ifølge artikel 6 i direktiv 95/46/EF skal personoplysninger indsamles til udtrykkeligt angivne og legitime formål, og senere behandling heraf må ikke være uforenelig med disse formål. Endvidere skal de være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles (formålsprincippet).

Overholdelse af dette princip kræver, at formålet med at indsamle og behandle biometriske data fastlægges. Desuden er det nødvendigt at undersøge proportionalitet og lovgrundlag under hensyntagen til beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig hvorvidt målet kan nås på en måde, der ikke griber så meget ind i disse rettigheder. Indtil nu har proportionalitet været det vigtigste kriterium for næsten alle de beslutninger, som tilsynsmyndighederne har taget om behandling af biometriske data.¹³

I henseende til adgangskontrol (autentifikation/verifikation) mener gruppen, at biometriske systemer med fysiske karakteristika, som ikke efterlader spor (f.eks. håndens omrids, men ikke fingeraftrykket), eller biometriske systemer med fysiske karakteristika, der efterlader spor, men som bygger på, at data, der er i en anden persons besiddelse end den registreredes, ikke overføres til et internt lager (dvs. i en anordning til adgangskontrol eller en central database), gør det lettere at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder¹⁴. Adskillige tilsynsmyndigheder har tilsluttet sig dette synspunkt og anført, at biometriske data helst ikke skal lagres i en database, men i stedet i en ting som brugeren alene har adgang til, f.eks. et mikrochipkort, en mobiltelefon eller et bankkort¹⁵. Med andre ord bør man ikke benytte omfattende identifikationsteknikker i autentifikations-/verifikationsapplikationer, der kan anvendes uden at lagre de biometriske data centralt.

Derfor mener gruppen, at brugen af andre typer applikationer (dvs. baseret på digitale fingeraftryksskabeloner i en terminal eller central database) skal undersøges nøje inden anvendelse. Hvis systemet skal gennemføres, f.eks. i forbindelse med installationer, der

¹³ Det gælder f.eks. beslutninger taget af myndighederne i Nederlandene, Frankrig, Tyskland, Italien og Grækenland.

¹⁴ Der kan skelnes mellem biometriske data, som behandles centralt, og biometriske referencedata, der lagres på en mobil anordning, hvor genkendelsesprocessen finder sted på kortet, men ikke på sensoren, eller hvor sensoren er en del af den mobile anordning.

¹⁵ Det er nødvendigt at tage hensyn til de foranstaltninger, der indføres for at løse problemer, som opstår med tabte, stjålne eller ødelagte kort, og fremme dem, der ikke fører til lagring af biometriske data. Om muligt skal dataene derefter indsamles igen direkte hos den registrerede.

skal have et højt sikkerhedsniveau¹⁶, må det overvejes, hvorvidt man skal anvende databehandling, som i henhold til artikel 20 i direktiv 95/46/EF kan indebære særlige risici og derfor skal underkastes tilsynsmyndighedernes forudgående kontrol i overensstemmelse med den nationale lovgivning (se punkt 3.5).

Direktiv 95/46/EF indeholder et forbud mod senere behandling, der er uforenelig med formålet med dataindsamlingen. Det ville f.eks. være tilfældet, hvis biometriske data til brug ved adgangskontrol blev anvendt til at bedømme den registreredes psykiske tilstand eller overvåge arbejdspladsen. Derfor skal der indføres foranstaltninger for at undgå et sådant genbrug¹⁷. Direktiv 95/46/EF åbner mulighed for undtagelser fra forbuddet mod yderligere databehandling, men kun på specifikke betingelser.

Generelt anses risikoen for at genbruge fysiske biometriske data, som enkeltpersoner uafvidende efterlader sig (dvs. fingeraftryk), til uforenelige formål for relativt lav, såfremt dataene ikke lagres i centrale databaser, men forbliver hos den registrerede og er utilgængelige for tredjemand. Central lagring af biometriske data øger risikoen for, at dataene kan anvendes til at forbinde forskellige databaser, da det vil gøre det muligt at udarbejde detaljerede profiler over enkeltpersoners vaner både i den offentlige og den private sektor. I henseende til forenelighed er det også vigtigt at drøfte interoperabiliteten mellem forskellige systemer, hvor der anvendes biometriske parametre. Den nødvendige interoperabilitetsstandardisering kan føre til en tættere sammenkædning af databaser.

Set i lyset af formålet med at behandle dataene rejser brugen af biometri endvidere spørgsmålet om hver enkelt gruppe behandlede datas proportionalitet. Biometriske data må kun anvendes, hvis de er relevante, tilstrækkelige og ikke omfatter mere, end hvad der kræves for at opfylde formålet. Derfor skal nødvendigheden og proportionaliteten af de behandlede data vurderes grundigt¹⁸. F.eks. har den franske tilsynsmyndighed, CNIL, afvist at anvende fingeraftryk til identifikation af børn, der skulle have adgang til en kantine¹⁹, men i stedet godkendt brugen af genkendelse ved hjælp af håndens mønstre. Den portugisiske tilsynsmyndighed har for nylig afvist at give et universitet lov til at benytte fingeraftryk til at kontrollere, hvor flittige og punktlige de ikke-undervisende medarbejdere er²⁰. Til gengæld har den tyske tilsynsmyndighed tilladt anvendelsen af biometriske karakteristika på identitetspapirer for at hindre forfalskninger. Tilladelsen

¹⁶ Det er endnu ikke muligt at anvende den biometriske teknologi til pålidelig, tidstro identifikation af en befolkning af en vis størrelse, og en sådan løsning ventes ikke at foreligge inden for den nærmeste fremtid.

¹⁷ Som nævnt ovenfor skal formålet tydeligt angives.

¹⁸ Det skal i visse tilfælde være muligt at bibeholde anonymiteten eller anvende pseudonym. Det er nødvendigt at tage hensyn til de foranstaltninger, der indføres for at løse problemer, som opstår med tabte, stjålne eller ødelagte kort, og fremme dem, der ikke fører til lagring af biometriske data. Om muligt skal dataene indsamles igen direkte hos den registrerede.

¹⁹ Tilsyneladende har tilsynsmyndighederne i Det Forenede Kongerige tilladt brug af fingeraftryksidentifikation i lignende situationer, såfremt de nødvendige sikkerhedsforanstaltninger er blevet indført.

²⁰ Den portugisiske tilsynsmyndighed mente, at indførelsen af et sådant system var ude af proportioner set i forhold til formålet med databehandlingen. Systemet skulle lagre dataene i en biometrisk anordning. I alt skulle kontrollen omfatte ca. 140 personer.

blev dog givet under forudsætning af, at dataene lagres i kortets mikrochip og ikke i en database, hvor man kan sammenligne den registreredes fingeraftryk med andres.

Der kan opstå særlige problemer vedrørende ovennævnte, idet biometriske data ofte indeholder flere oplysninger end nødvendigt for identifikationen eller autentifikationen/verifikationen. Det gælder dog snarere det oprindelige billede (rådata), da skabelonen rent teknisk kan – og bør – udformes, så behandling af unødvendige data undgås. Overflødige data bør destrueres så hurtigt som muligt²¹. Desuden kan visse biometriske data give personoplysninger om racemæssig baggrund og oplysninger om helbredsforhold (se punkt 3.7 nedenfor).

Endelig skal det nævnes, at biometriske systemer kan udformes, så de kan anvendes til at beskytte privatlivets fred bedre. De kan bl.a. begrænse behandlingen af andre personoplysninger såsom navn, adresse, opholdssted osv.

3.3. Rimelig indsamling og informering af den registrerede

Behandling, og især indsamling, af biometriske data skal ske på en rimelig måde²². Den registeransvarlige skal informere den registrerede i overensstemmelse med artikel 10 og 11 i direktiv 95/46/EF²³. Derfor er det afgørende, at den registeransvarliges formål og identitet (ofte den person, som har ansvaret for det biometriske system eller den anvendte biometriske teknik) klart defineres.

Det er vigtigt at undgå systemer, der indsamler biometriske data uden den registreredes vidende. Ud fra den synsvinkel udgør visse biometriske systemer en større risiko end andre, f.eks. ansigtsgenkendelse på afstand, indsamling af fingeraftryk og aflytning af stemmer.

3.4. Principper vedrørende grundlaget for behandling af oplysninger

Behandling af biometriske data skal ske på grundlag af bestemmelserne i artikel 7 i direktiv 95/46/EF. Gruppen understreger, at i tilfælde hvor den registeransvarlige angiver samtykke som grundlag for behandling af oplysninger, skal bestemmelserne i artikel 2 i direktiv 95/46/EF overholdes (enhver frivillig, specifik og informeret viljetilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling).

3.5. Forudgående kontrol – anmeldelse

Som tidligere nævnt støtter gruppen anvendelsen af biometriske systemer, som ikke lagrer spor i en terminal eller en central database (se punkt 3.2). Hvis det planlægges at anvende disse systemer, anbefaler gruppen imidlertid i lyset af faren for (gen-)brug til

²¹ Dette understreges i artikel 6, stk. 1, litra e), i direktiv 95/46/EF, hvor det hedder, at personoplysninger *ikke* må opbevares i et længere tidsrum end det, der er nødvendigt, af hensyn til formålet med databehandlingen.

²² Artikel 6, litra a), i direktiv 95/46/EF.

²³ Oplysningspligten omtalt i artikel 10 og 11 i direktiv 95/46/EF kan kun fraviges, såfremt den bygger på lovmæssige foranstaltninger og er nødvendig for at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 13 i direktiv 95/46/EF (den offentlige sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager osv.).

forskellige formål samt specifikke problemer i forbindelse med ikke-autoriseret adgang, at medlemsstaterne overvejer, hvorvidt dataene skal underkastes en forudgående kontrol hos tilsynsmyndighederne i henhold til artikel 20 i direktiv 95/46/EF, da en sådan behandling kan indebære særlige risici for personers rettigheder og frihedsrettigheder. Såfremt medlemsstaterne påtænker at indføre forudgående kontrol ved behandling af biometriske data, bør de nationale tilsynsmyndigheder høres først.

3.6. Sikkerhedsforanstaltninger

I henhold til artikel 17 i direktiv 95/46/EF skal den registeransvarlige iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelse af oplysninger i et net, samt mod enhver anden form for ulovlig behandling. Der skal gennemføres sikkerhedsforanstaltninger ved behandling (lagring, udsendelse, uddragning af karakteristika, sammenligning osv.) af biometriske data, navnlig hvis den registeransvarlige udsender dataene via internettet. Disse foranstaltninger kan f.eks. omfatte kryptering af skabeloner og beskyttelse af krypteringsnøgler samt indførelse af adgangskontrol og -beskyttelse, så det nærmest bliver umuligt at rekonstruere de oprindelige skabelondata.

I sammenhæng hermed skal der tages hensyn til visse nye teknologier. Det bliver f.eks. muligt at anvende biometriske data som krypteringsnøgler. Det gør den registrerede mindre udsat for risici, da nøglerne kun kan afkodes på basis af en ny indsamling af data fra den registrerede selv. Derved undgår man at oprette databaser, som indeholder skabeloner med biometriske data, der kan genbruges til formål, der ikke har forbindelse hermed.

De nødvendige sikkerhedsforanstaltninger skal gennemføres allerede fra begyndelsen af behandlingen, og de er især vigtige i "registreringsfasen", hvor de biometriske data omdannes til skabeloner eller billeder. Manglende integritet, fortrolighed og tilgængelighed i forbindelse med databaserne vil være ødelæggende for alle fremtidige applikationer, der bygger på oplysninger fra disse databaser, og tilføje de registrerede uoprettelig skade. Hvis en autoriseret persons fingeraftryk f.eks. blev forbundet med en ikke-autoriseret persons identitet, kan sidstnævnte få adgang til de samme tjenester som den autoriserede uden at være berettiget hertil. Det kan medføre identitetstyveri, og uanset om det opdages eller ej, vil det betyde, at personens fingeraftryk fremover vil fremstå som utroværdige. Det vil begrænse vedkommendes frihed.

Fejl, der opstår i de biometriske systemer, kan få store konsekvenser for de registrerede, navnlig kan forkert afvisning af autoriserede personer og forkert godkendelse af ikke-autoriserede personer skabe alvorlige problemer på flere niveauer. Brug af biometriske data bør på forhånd nedsætte risikoen for fejl. Det kan dog også skabe en illusion af, at identifikation eller autentifikation/verifikation af den registrerede altid er korrekt. Det kan gøre det svært eller endda umuligt for den registrerede at bevise det modsatte. Hvis systemet ved en fejl identificerer den registrerede som en person, der ikke har tilladelse til at gå ombord på et fly eller rejse til et bestemt land, vil det være vanskeligt for vedkommende at tilbagevise de "indiskutable" beviser og dermed løse problemet. Derfor skal det i overensstemmelse med artikel 15 i direktiv 95/46/EF understreges, at afgørelser, der kan få retsvirkning for den registrerede, kun har gyldighed, såfremt resultatet af edb-behandlingen er blevet bekræftet.

Endelig skal det nævnes, at anvendelse af biometri kan forbedre kontrolprocedurerne bl.a. i forbindelse med adgang til personoplysninger vedrørende tredjemand, f.eks. tyveri og misbrug (bemyndigelsesprocedurer).

3.7. Følsomme oplysninger

Visse biometriske data kan i henhold til artikel 8 i direktiv 95/46/EF anses for følsomme, det gælder navnlig personoplysninger om racemæssig eller etnisk baggrund og oplysninger om helbredsforhold. Biometriske systemer baseret på ansigtsgenkendelse kan f.eks. behandle personoplysninger om racemæssig eller etnisk baggrund. I så tilfælde gælder både de særlige sikkerhedsbestemmelser nævnt i artikel 8 og direktivets generelle beskyttelsesbestemmelser.

Det betyder dog ikke, at enhver behandling af biometriske data nødvendigvis indbefatter følsomme oplysninger. Det er en vurderingssag, som afhænger af de specifikke biometriske karakteristika, der anvendes, og selve den biometriske applikation. Det er mere sandsynligt, at biometriske data i form af billeder vurderes som følsomme, da de rådata i princippet ikke må rekonstrueres på baggrund af skabelonen.

3.8. Entydig identifikation

Biometriske data er entydige, og de fleste genererer en entydig skabelon (eller billede). Hvis biometriske data anvendes i vidt omfang, navnlig på en betydelig del af en given befolkning, må de i medfør af direktiv 95/46/EF anses for at være almene midler til identifikation. I disse tilfælde gælder artikel 8, stk. 7, i direktiv 95/46/EF, og det er medlemsstaterne, der bestemmer betingelserne for databehandlingen.

Der kan opstå visse problemer i tilfælde, hvor biometriske data anvendes til at forbinde databaser indeholdende personoplysninger²⁴, såfremt den registrerede ikke kan komme med indsigelser over for behandlingen af de biometriske data. Sådanne situationer kan typisk forekomme mellem borgere og offentlige myndigheder.

Derfor er det ønskeligt, at skabeloner og digitale repræsentationer heraf manipuleres matematisk (kryptering, algoritmer eller nummertegnsfunktioner) ved hjælp af forskellige parametre til de enkelte biometriske produkter. Herved undgås, at personoplysninger fra flere databaser blandes ved sammenligning af skabeloner eller digitale repræsentationer.

3.9. Adfærdskodekser og anvendelse af teknologi, der kan beskytte privatlivets fred

Gruppen opfordrer branchen til at fremstille biometriske systemer, der kan lette gennemførelsen af anbefalingerne i nærværende arbejdsdokument. Ifald der udarbejdes europæiske eller internationale standarder på dette område, bør de udformes i samarbejde med tilsynsmyndighederne, så dataene beskyttes bedst muligt, de sociale risici mindskes, og misbrug af de biometriske data hindres. I den sammenhæng ønsker gruppen at

²⁴ Se også punkt 3.2 ovenfor om genbrug, der er foreneligt med det oprindelige formål med indsamlingen.

understrege vigtigheden af teknologier, som kan beskytte privatlivets fred, så indsamlingen af data begrænses, og ulovlig behandling forhindres.

Endvidere fremhæver gruppen, at det i henhold til artikel 27 i direktiv 95/46/EF er vigtigt at udarbejde adfærdskodekser, der afhængigt af de særlige forhold i de forskellige sektorer skal bidrage til en korrekt anvendelse af principperne om databeskyttelse. EU-kodekser kan indsendes til gruppen, der bl.a. vil afgøre, hvorvidt de indsendte forslag er i overensstemmelse med de nationale bestemmelser, medlemsstaterne har vedtaget til gennemførelse af direktiv 95/46/EF.

KONKLUSIONER

Gruppen mener, at de fleste biometriske data automatisk omfatter behandling af personoplysninger. Det er derfor nødvendigt at overholde principperne om databeskyttelse i direktiv 95/46/EF under hensyntagen til de særlige muligheder, der eksisterer med biometri, bl.a. indsamling af biometriske data uden den registreredes vidende og den tilsyneladende sikre forbindelse til den enkelte person ved udvikling af biometriske systemer.

Navnlig i forbindelse med autentifikation/verifikation medfører overholdelsen af proportionalitetsprincippet, der udgør kernen i den beskyttelse, som direktiv 95/46/EF sikrer, at der foretrækkes anvendt biometriske applikationer, som ikke behandler data fra fysiske spor, som enkeltpersoner uafvidende efterlader sig, eller som lagres i et centralt system. Derved kan den registrerede udøve bedre kontrol med sine personoplysninger.

Gruppen agter at vende tilbage til dette arbejdsdokument og gennemgå tilsynsmyndighedernes erfaringer og de teknologiske landvindinger inden for biometriske applikationer. Da biometriske data allerede på nuværende tidspunkt anvendes til en lang række forskellige formål, skal disse emner omgående gøres til genstand for yderligere drøftelser, herunder især sikkerheden i forbindelse med beskæftigelse, visa, immigration og rejseaktivitet.

Selvom det fortsat er branchens ansvar at udvikle biometriske systemer, der overholder reglerne for databeskyttelse, vil en løbende dialog mellem alle interesserede parter, herunder tilsynsmyndighederne, være til stor gavn. Dialogen skal ske på grundlag af et udkast til en adfærdskodeks.

Udarbejdet i Bruxelles, den 13. juni 2003
På gruppens vegne
Stefano RODOTÀ
Formand