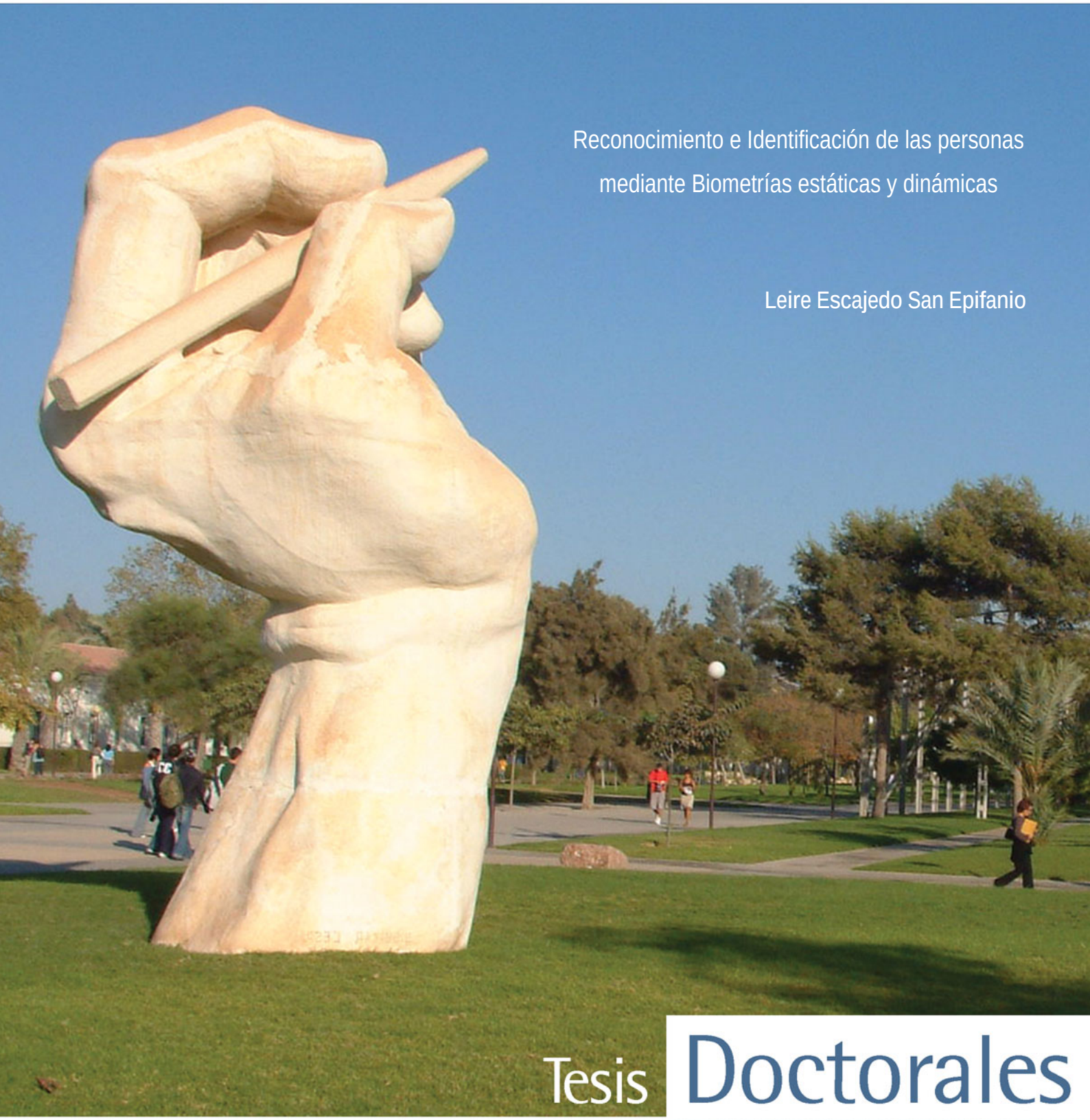
Universitat d'Alacant
Universidad de Alicante



Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas

Leire Escajedo San Epifanio

Tesis Doctorales

www.eltallerdigital.com

UNIVERSIDAD de ALICANTE

Universitat d'Alacant
Universidad de Alicante

Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas

Leire Escajedo San Epifanio

Tesis doctoral

Alicante, diciembre de 2015

Universitat d'Alacant
Universidad de Alicante

DEPARTAMENTO DE BIOTECNOLOGÍA
FACULTAD DE CIENCIAS

Reconocimiento e Identificación de las personas mediante Biometrías estáticas y comportamentales

Leire Escajedo San Epifanio

Memoria presentada para aspirar al grado de Doctora en Ciencias Biológicas *por la Universidad de Alicante.*

Programa de Doctorado en "Antropología Biológica y de la Salud" *(R.D. 778/1998).*

Tesis doctoral dirigida por:

Joaquín de Juan Herrero.
Catedrático de Biología Celular de la Universidad de Alicante.

Esther M. Rebato Ochoa.
Catedrática de Antropología Física de la Universidad del País Vasco.

Universitat d'Alacant
Universidad de Alicante

AUTORIZACION DEL/LA DIRECTOR/A DE TESIS PARA SU PRESENTACION

El Dr. Joaquín de Juan Herrero con D.N.I. 22091706Ey la Dra. Esther M. Rebato Ochoa con D.N.I. 14933158 como Directores de la Tesis Doctoral: ***Reconocimiento e Identificación de las personas mediante Biometrías estáticas y comportamentales*** realizada en el Departamento de Biotecnología de la Facultad de Ciencias de la Universidad de Alicante por Dña. **Leire Escajedo San Epifanio**, autorizan la presentación de la citada Tesis Doctoral, dado que reúne las condiciones necesarias para su defensa.

Universitat d'Alacant
Universidad de Alicante

En Alicante a 24 de Octubre de 2015

LOS DIRECTORES DE LA TESIS

Fdo.: Joaquín de Juan Herrero

Fdo.: Esther M. Rebato Ochoa

Universitat d'Alacant
Universidad de Alicante

La constancia hace posibles muchas cosas;
Incluso algunas que pueden parecer imposibles.
(B. FRANKLIN)

Nuestras huellas dactilares
no se borran de las vidas que tocamos.
(M. GHANDI)

Universitat d'Alacant
Universidad de Alicante

Universitat d'Alacant
Universidad de Alicante

Agradecimientos

Si siempre suele dar un poco vértigo echar la vista atrás y valorar el camino recorrido, qué decir de aquellos procesos que han visto el paso de varios años. Este trabajo de investigación comenzó en enero de 2011 tras la obtención del DEA en el Programa de Doctorado en Antropología Biológica y de la Salud del Departamento de Biotecnología de la Universidad de Alicante. Habían trascurrido algo más de seis años desde la defensa de la tesis que me dio acceso al grado de Doctora en Derecho y preparaba, al tiempo que este trabajo, la oposición a la plaza de Profesora Titular de Derecho Constitucional que ocupo en la actualidad en la Universidad del País Vasco. Cuántas cosas han sucedido desde entonces. En este momento de cierre del trabajo, siento que dos sentimientos son los que destacan sobre el resto. De una parte, la satisfacción personal por haber conseguido llegar a la presentación de esta tesis doctoral; y de otra, un profundo sentimiento de gratitud hacia las personas que me han acompañado en este tiempo y sin cuyo apoyo no hubiera sido posible llevar a buen puerto este proyecto.

Siento gratitud, en primer lugar, hacia aquellas personas que han hecho posible que mi curiosidad sobre los sistemas de reconocimiento automatizado mediante Biometría, sobre los retos que plantean en el contexto de nuestra sociedad global y la defensa de los derechos de las personas, haya fraguado hacia la realización de esta tesis doctoral. Agradezco la oportunidad y el estímulo, así como el tiempo y la atención que tanto en la realización de la tesina final del Programa de Doctorado (defendida a finales de 2010) como en estos años de realización de la tesis doctoral han prestado a mi trabajo y a mi persona los dos directores de esta tesis: el Profesor Joaquín de Juan Herrero, Catedrático de Biología Celular y director del Departamento de Biotecnología de la Universidad de Alicante; y la Profesora Esther Rebato Ochoa, Catedrática de Antropología Física de la Universidad de la Universidad del País Vasco/ Euskal Herriko Unibertsitatea. Leí que la palabra *investigar* se construyó a partir de la expresión *in vestiguim ire* (ir en pos de las huellas). En ese seguimiento de las pistas y señales, en la interpretación crítica de los hallazgos y resultados que se iban alcanzando ha sido para mí una experiencia muy

Universitat d'Alacant
Universidad de Alicante

gratificante, un privilegio contar con la retroalimentación y el contraste de dos personas de vuestra calidad científica y humana. Esther, Joaquín: espero, confío, deseo que el futuro cercano nos brinde oportunidades para encontrarnos y seguir caminando a donde la curiosidad nos lleve. Un fuerte abrazo a ambos.

Cuando en el año 2004 defendí mi tesis doctoral en Derecho recogí en ella una frase inspiradora del presidente estadounidense Benjamín Franklin: una frase que con insistencia ha vuelto a mí al redactar estas líneas. *La constancia hace posibles muchas cosas; incluso algunas que parecían imposibles*. A ella se añade una frase que pronunció Mahatma Ghandi en la crisis del Transvaal, en Sudáfrica: *nuestras huellas no se borran de las vidas que tocamos.* Tampoco se borran las huellas de aquellos que han tocado nuestra vida. La constancia ha sido, sí, una herramienta clave para poder realizar este trabajo; pero también ha sido imprescindible el contexto humano que me rodea en el día a día. Agradezco el apoyo de mi familia, de mis padres y hermanos, y de David y Gabriel. Deseo dejar también constancia de mi gratitud al profesor Alberto López Basaguren, Catedrático de Derecho Constitucional, a la profesora Carmen González Murua, Catedrática de Fisiología Vegetal y a la profesora Mertxe de Renobales Scheifler, Catedrática de Bioquímica, todos ellos de la Universidad del País Vasco. El entorno universitario es un espacio tan enriquecedor como complejo; a veces muy complejo. Me siento afortunada de compartir espacio con personas que creen y apuestan por la Universidad, con sus luces y sus sombras; personas convencidas del valor de la libertad de investigación y que apuestan por un avance del conocimiento comprometido con la sociedad; su experiencia me orienta y me guía, y me enseña a valorar las cosas, las buenas y las menos buenas, en su justa medida. Gracias de corazón.

En Getxo, Vizcaya, a 24 de octubre de 2015

Universitat d'Alacant
Universidad de Alicante

Índice

Número de página

Abreviaturas y acrónimos xiii

Listado de ilustraciones xvii

Parte I
Planteamiento y metodología de la investigación

1. INTRODUCCIÓN 3

1.1 Resumen de la investigación y de su contexto 3
1.1.1 Abstract 3

1.1.2 Identidad(es), identificación e interacción social: el contexto de la aplicación del reconocimiento mediante Biometría. 6
1.1.2.1 Identidad de la persona, identidad social e identificación 6
1.1.2.2. *El ansia por centralizar los datos y asociarlos a identificadores únicos* 7
1.1.2.3 *Informaciones y objetos tradicionalmente empleados como apoyo en la identificación* 9
1.1.2.4 *El miedo a los sistemas de identificación a gran escala* 11
1.1.2.5 *La llegada de los sistemas automatizados de reconocimiento biométrico* 13

1.2. Biometría, Antropometría e identificación biométrica: precisiones históricas y primeras delimitaciones conceptuales. 15
1.2.1. Los conceptos clásicos de Biometría (en la definición propuesta por FRANCIS GALTON) y Antropometría. 15
1.2.1.1. Medir humanos porqué y para qué 16
1.2.1.2 Biometría y Antropometría 17
1.2.1.3 Biometría y características psíquicas, algunas notas 19
1.2.1.4 La Biometría que sirve de base a los sistemas automatizados de reconocimiento 20

1.2.2. Categorías de estudios y de datos biométricos 21
1.2.2.1 La clasificación tripartita de IRWIN: tipología de los estudios 22

atendiendo a su objeto
1.2.2.2. La clasificación bipartita de los datos biométricos según las características de las que son tomados: datos biométricos estáticos y datos biométricos dinámicos. 22
1.2.2.2. a Datos biométricos estáticos 23
1.2.2.2.b. Datos biométricos dinámicos 24
1.2.3 La primera experiencia biométrica, en el sentido actual del concepto: el sistema antropométrico de identificación diseñado por ALPHONSE BERTILLON (el *Bertillonage* o *Signalement anthropométrique*). 26
1.2.3.1 El signalement anthropométrique: un hito en la historia del reconocimiento mediante Biometría 26
1.2.3.2 El mito de cómo la crisis del Bertillonage (supuestamente) impulsó el reconocimiento dactilográfico. El caso de los "dos Will West" 28

1.3. El reconocimiento biométrico contemporáneo y los factores que impulsan su desarrollo científico y tecnológico 30
1.3.1 La automatización de la captación de la información biométrica y de su procesamiento como elementos diferenciales 30

1.3.2. La confluencia temporal entre el desarrollo de estos sistemas y un contexto de creciente necesidad por métodos fiables de identificación 33
1.3.2.1 La promesa biométrica y su aura mítica 33
1.3.2.2. De cara al control de los nacionales de terceros países y de los "indocumentados" 34

1.3.3 Más allá de los mitos, las cifras económicas 36

1.3.4 El efecto difusor que ha tenido la decisión de incorporar la Biometría a los pasaportes europeos 39

1.3.5 Pero, ¿es oro todo lo que reluce? 40

2. MOTIVACIÓN Y OBJETIVOS DE LA INVESTIGACIÓN 44

3.1 Motivación (rationale) 44

3.2 Objetivo general 44

3.3. Objetivos específicos 45

3. MATERIALES Y MÉTODOS 47

3.1. Metodología de la investigación y materiales empleados 47

3.2. Estructura de la exposición de resultados 49

Universitat d'Alacant
Universidad de Alicante

Parte II
Resultados y discusión

Capítulo 1

La información biométrica y los datos biométricos. La base científica de los sistemas automatizados de identificación mediante Biometría. 53

1. ¿QUÉ TIPO DE *INFORMACIÓN BIOMÉTRICA* MANEJA UN SISTEMA DE RECONOCIMIENTO BIOMÉTRICO? 53

1.1. Algunas observaciones sobre la diversidad terminológica y el modo en que se ha abordado 53

1.2. Principales conceptos 54

1.2.1 *Información biométrica, dato biométrico y característica biométrica (o fuente de datos biométricos).* 54

1.2.2. *Datos en crudo y en fresco, y muestras biométricas* 56

1.2.3. *Atributos biométricos y plantillas o patrones biométricos* 57

1.2.4. Una distinción relevante: dato biométrico versus identificador biométrico 59

2. LAS *CUALIDADES* QUE DEBEN REUNIR LAS CARACTERÍSTICAS BIOMÉTRICAS PARA PODER SERVIR DE SOPORTE A UN SISTEMA DE RECONOCIMIENTO MEDIANTE BIOMETRÍA. 60

2.1. Cualidades que tienen que ver con la entidad de los rasgos y con el conocimiento científico que se tiene sobre ellos. *Universalidad, singularidad y permanencia.* 63

2.1.1. *Universal, disponible* 64

2.1.2. *Singularidad o, al menos, cualidad para una diferenciación suficiente* (variabilidad interpersonal) 65

2.1.3 *Permanente, invariable o suficientemente estable (respecto del sujeto fuente)* 66

2.2. Cualidades que tienen que ver con la capacidad de los dispositivos y las aplicaciones informáticas. *Colectividad, capacidad de rendimiento y fiabilidad* 69

2.2.1. *Colectividad, accesibilidad* 69

2.2.2. *Rendimiento y fiabilidad* 70

2.3. Cualidades que tienen que ver con la interacción entre los sistemas y las personas o el conjunto de la sociedad. La *aceptabilidad*. 70

3. CRITERIOS DE CLASIFICACIÓN DE LAS BIOMETRÍAS QUE SIRVEN DE BASE A LOS SISTEMAS DE RECONOCIMIENTO 71

3.1. Clasificación de los métodos biométricos que sirven de base a los sistemas de identificación, atendiendo a la naturaleza dinámica o estática de la información que les sirve de referencia. 72

3.2. La clasificación cronológica o la explicación de las *generaciones* de sistemas de reconocimiento mediante Biometría 73

3.2.1. *La generación cero (o los antecedentes de los sistemas automatizados de* 74

Universitat d'Alacant
Universidad de Alicante

reconocimiento biométrico)
3.2.2. *La primera generación de sistemas de reconocimiento automatizado mediante Biometría* 75
3.2.3. *La segunda generación de tecnologías biométricas* 76
3.3. *Strong-weak, hard-soft* biometrics 77
3.4. Sistemas 1D, 2D y 3D 80

4. BIOMETRÍAS ESTÁTICAS 80
4.1. Biometría de los dermatoglifos (crestas y surcos dérmicos de las manos, plantas de los pies y dedos). 80
4.1.1. *El concepto de dermatoglifo.* 80
4.1.2. *La Biometría de los dermatoglifos dactilares* 81
4.1.3 *La impresión de los dermatoglifos de la palma de la mano* 85

4.2. Biometría facial. 86
4.2.*1 El estudio de los rostros en la historia: diferentes utilidades* 86
4.2.2 *La utilización de fotografías con fines de identificación: algunas notas históricas* 88
4.2.3 Los sistemas automatizados de captura del rostro 89
4.2.4. Gestión de las variaciones inter- e intra -clase. En especial, las expresiones faciales. 90
4.2.5 El reconocimiento facial en ambientes no controlados (videovigilancia) 91

4.3. Biometría (geometría) de la mano. 92

4.4. Biometría ocular (datos obtenidos de la retina y el iris). 93
4.4.1. Biometría del iris. 94
4.4.2. Biometría de la retina. 97

4.5 Biometría auricular (datos biométricos obtenidos de la oreja) y el otograma o la llamada *huella de la oreja*. 98
4.5.1. Biometría auricular 98
4.5.2. El otograma (huella de la oreja) en los procesos judiciales 100

4.6 La Biometría del ADN y el debate sobre si debe o no considerarse entre las características que pueden servir de base a los sistemas automatizados. 101

4.7. Otras Biometrías estáticas 104
4.7.1. *Biometría del olor corporal* 104
4.7.2. Biometría del esmalte dental y la huella de la lengua 105
4.7.3 Biometría del lecho ungueal (nail bed) 105
4.7.4 Patrones vasculares de la mano 105

5. SISTEMAS BIOMÉTRICOS CON BASE EN CARACTERÍSTICAS DINÁMICAS. (I) BIOMETRÍA DE LAS HABILIDADES MOTORAS. 107
5.1. Biometría de la escritura 108
5.2. Biometría de las pulsaciones en teclado 109
5.3. Biometría del movimiento labial 110
5.4. Biometría de la marcha 110
5.5. Biometría vocal 111
5.6. Biometría de los patrones del comportamiento 113
5.7. Biometría de las señales electrofisiológicas y parámetros corporales 115

6. FORTALEZAS Y SISTEMAS DE LOS SISTEMAS BIOMÉTRICOS, ATENDIENDO A LAS CARACTERÍSTICAS QUE LES SIRVEN DE BASE PARA EL RECONOCIMIENTO Y AL ESTADO DEL ARTE DE LOS MÉTODOS CON QUE SE CAPTAN 119
6.1. Valoración de las característica biométrica desde la perspectiva de las cualidades necesarias para servir de base a un sistema de reconocimiento 120

mediante Biometría
6.1.1 Universalidad 120
6.1.2 Potencial singularizante 120
6.1.3 Estabilidad de los rasgos o características 120
6.1.4 Colectividad y accesibilidad, y resistencia al fraude 121
6.1.5. Difusión, madurez tecnológica y aceptabilidad social 123
6.2. Tabla comparativa de fortalezas y debilidades de los sistemas (valoración relativa, desde la perspectiva de la característica que emplean como referencia) 124

Capítulo 2
Funcionamiento, utilidades y limitaciones de los sistemas automatizados de identificación mediante Biometría. Los riesgos y su tratamiento.

1. LAS UTILIDADES SOCIALES QUE OFRECE EL RECONOCIMIENTO MEDIANTE BIOMETRÍA: VERIFICACIÓN, IDENTIFICACIÓN EN SENTIDO ESTRICTO Y CRIBADOS BIOMÉTRICOS. 127
1.1 Introducción a los usos de los sistemas de reconocimiento mediante Biometría 127
1.2. Sistemas de verificación: *¿soy quien digo ser?* 128
1.2.1 Verificación o comprobación de la identidad alegada *128*
1.2.3 *La toma de decisiones y los tipos de error que pueden generarse* 129
1.3. Sistemas de identificación: *¿quién soy?* 131
1.3.1. Identificar, en sentido estricto *131*
1.3.2. *Complejidad* 132
1.3.3 *La toma de decisiones y los errores que pueden producirse* 134
1.4. Sistemas de cribado biométrico: *se busca* 134
1.4.1 *Sistemas open set y sistemas closed set de verificación e identificación, y sistemas de cribado* 134
1.4.2. Los problemas del cribado "sin enrolamiento" 135

2. EL FUNCIONAMIENTO BÁSICO DE LOS SISTEMAS AUTOMATIZADOS DE RECONOCIMIENTO MEDIANTE BIOMETRÍA 137
2.1 La estructura básica 138
2.1.1 *Elementos estructurales (arquitectura de los sistemas)* 138
2.1.2 *Fases de los procesos* 139
22 El enrolamiento (o reconocimiento primario), la captación de la información biométrica y la creación del patrón. 141
2.3 El almacenamiento del patrón biométrico 142
2.4. La captación del dato en fresco, la comparación con los patrones almacenados y la toma de decisiones 144

3. LAS LIMITACIONES Y LOS RIESGOS DE LA IDENTIFICACIÓN BIOMÉTRICA CONFORME AL ESTADO ACTUAL DE LA CIENCIA Y LA TECNOLOGÍA (I). LIMITACIONES Y RIESGOS QUE TIENEN RELACIÓN CON LA BASE CIENTÍFICA DE LOS SISTEMAS. 146
3.1. Hasta qué punto pueden darse por cumplidos los *Seven Pillars of Biometric Wisdom* 147
3.2. Limitaciones relativas a la *universalidad* de las características biométricas que sirven de soporte a los sistemas de reconocimiento mediante Biometría. 148
3.3. Limitaciones relativas a la *singularidad* (uniqueness) 150

3.3.1 *Reconocimiento mediante Biometría y unicidad.* 150
3.3.2. *La distribución de la variabilidad y la menagerie biométrica* 153
3.3.3. Pero, ¿qué hacemos con este "*zoo*"? 154
3.4. Limitaciones que afectan a la *permanencia* (o estabilidad) de las características biométricas. 155
3.4.1 *Deterioro temporal o definitivo de algunas características biométricas, por enfermedad* 156
3.4.2. *El envejecimiento* 157
3.5. ¿Cómo atender a la incidencia de estas limitaciones? 161

4. LAS LIMITACIONES Y LOS RIESGOS DE LA IDENTIFICACIÓN BIOMÉTRICA CONFORME AL ESTADO ACTUAL DE LA CIENCIA Y LA TECNOLOGÍA (II). LIMITACIONES RELATIVAS A LA ARQUITECTURA DE LOS SISTEMAS AUTOMATIZADOS DE RECONOCIMIENTO MEDIANTE BIOMETRÍA. 161
4.1. Fallos intrínsecos de los sistemas. 162
4.1.1 Seguridad y fiabilidad de los sistemas, ¿versus tiempo y negocio? 162
4.1.2 Los fallos intrínsecos de la captación en fresco 162
4.1.3 Fallos intrínsecos en la digitalización o elaboración de los patrones (ya sea en el enrolamiento o en la captación en fresco) 164
4.2. Problemas de seguridad de los sistemas. 165
4.2.1. Ataques al nivel del sensor (o captación del dato en fresco en la identificación secundaria) 165
4.2.2. Ataques a nivel de los módulos de procesamiento y ataques en los módulos no biométricos 166
4.2.3 *Fallos en los módulos no-biométricos: la política de administración del sistema* 167
4.3. Las consecuencias de los fallos del sistema y las propuestas de solución 168
4.4. Sobre la lectura que se hace de los fallos tecnológicos 170

5. PROBLEMAS QUE PLANTEA EL RECONOCIMIENTO BIOMÉTRICO PLANTEA DESDE LA PERSPECTIVA ÉTICO-SOCIAL. 171
5.1. Cuerpo, identidad y privacidad, ante los sistemas automatizados de reconocimiento mediante Biometría. 173
5.1.1 *El enrolamiento biométrico, en esencia, ante la tutela de la vida privada* 174
5.1.2. *El riesgo de vigilancia excesiva* 176
5.2. ¿Cómo de "privada" es la información biométrica? 179
5.2.1. *¿Son datos sensibles, en el sentido de la LOPD?* 179
5.2.2 *¿Son sensibles en algún otro sentido?* 183
5.3. Cuestiones que plantea la información personal directa o indirectamente expuesta ante los sistemas y procesos de reconocimiento mediante Biometría. 183
5.3.1 *El estigma de los outliers* y de los que tienen *perfiles "buscados"* 184
5.3.2. *Datos relativos al genero, la identidad sexual y la orientación sexual* 186
5.3.3 *Datos sobre el origen de las personas* 188
5.3.4 *Datos relativos a la salud de las personas* 190
5.4 Los datos biométricos en relación con las prácticas de perfilado y la explotación de los *Big Bata.* 193

Universitat d'Alacant
Universidad de Alicante

Capítulo 3

Análisis operativo de los sistemas de reconocimiento biométrico. Estudio de casos en diferentes escenarios

1. ANÁLISIS DEL FUNCIONAMIENTO DE LOS SISTEMAS BIOMÉTRICOS EN DIFERENTES ESCENARIOS OPERATIVOS: PLANTEAMIENTO Y METODOLOGÍA 195

1.1. ¿Cómo se juzga la aceptabilidad de una tecnología biométrica? La pregunta 195

1.2. Nuestra respuesta: con la misma referencia que juzgamos, en la actualidad, los sistemas que con otros elementos ofrecen servicios similares 196

1.2.1 Los principios de finalidad y proporcionalidad. Y la exigencia de que la información recabada sea pertinente, adecuada y no excesiva 196

1.2.2 El consentimiento, para ser libre, debe disponer de alternativas 197

1.2.3. El derecho al olvido 198

2.TIPOLOGÍA DE LOS SISTEMAS DE RECONOCIMIENTO, ATENDIENDO A SU OPERATIVIDAD. 199

2.1. Clasificaciones basadas en las *generaciones* tecnológicas y clasificaciones basadas en el tipo de entornos en los que se aplican, o las funciones que satisfacen 199

2.2. Clasificaciones que atienden al tipo de espacios o entornos en que tiene lugar la aplicación 200

2.3. Atendiendo a sus objetivos operativos 201

2.4 Clasificación empleada en este trabajo: atendiendo tanto a la tipología de escenarios operativos como a los objetivos que en ellos persigue el reconocimiento mediante Biometría 202

3. LA BIOMETRÍA EN EL CONTROL DE LOS MOVIMIENTOS TRANSFRONTERIZOS Y EN LOS ESCENARIOS DE CONFLICTO BÉLICO 203

3.1 El control de las personas que cruzan fronteras. Los legales y los ilegales. Algunas advertencias 203

3.2. Los programas de pasajeros frecuentes 204

3.3. El control "del resto" de los movimientos transfronterizos, especialmente la llamada *inmigración económica* y de los solicitantes de asilo 206

3.3.1. *La diferente motivación de las personas que viajan a otro país* 206

3.3.2. *Biometrías en los documentos de viaje (visados y pasaportes)* 207

3.3.3. *Los sistemas de control de las personas que viajan "sin titulo válido" y de las que solicitan asilo. En especial EURODAC* 208

3.4. Biometría y conflictos bélicos. El control "encubierto" y preventivo de futuros movimientos transfronterizos 212

4. LA BIOMETRÍA EN LAS RELACIONES ENTRE LOS ESTADOS Y SUS NACIONALES Y RESIDENTES 215

4. 1. Entre el miedo al control y la necesidad de identificación 216

4.2. La lucha contra la criminalidad 218

4.3. Documentos de identidad nacional y sistemas de identificación en las relaciones entre la Administración y los Administrados (pago de impuestos, administración electrónica, etc.) 220

4. 3.1 La emisión de tarjetas de identidad de ciudadanos y residentes. 221

4.3.2 *El Aadhaar.* 223

4.3.3. *Licencias y sufragio biométrico* 224

4.3.4. El control de las ayudas sociales 226

5. LA BIOMETRÍA EN LAS RELACIONES ENTRE EMPLEADORES Y EMPLEADOS 228
5.1. El control de recintos de seguridad (zonas militares y aeropuertos) 228
5.2. El control biométrico en las relaciones entre empleadores y empleados 229

6. LA BIOMETRÍA EN LAS PRISIONES, HOSPITALES Y CENTROS DE ENSEÑANZA 234
6.1 Control de accesos y seguimiento; y la protección de zonas restringidas 234
6.2. Control de asistencia de los alumnos y geolocalización en los centros de enseñanza 238
6. 3. Control de uso y sistemas de pago de servicios como las cafeterías o bibliotecas 237
6. 4. Identificación de pacientes 238

7. LA BIOMETRÍA EN LA OFERTA DE BIENES Y EN LA PRESTACIÓN DE SERVICIOS A LOS CONSUMIDORES 239
7.1. La Biometría en la identificación de los consumidores y usuarios, en sentido estricto 239
7.1.1. *El control de los abonados y los socios y el ejercicio del derecho de admisión* 239
7. 1.2. Sistemas de pago y Banca electrónica, y acceso a teléfonos inteligentes y a otros dispositivos electrónicos 244
7.1.3. Evaluación del uso del reconocimiento biométrico en la relación con los consumidores y los usuarios 246

7.2 La captación de datos de las personas *fuera* de los contratos de compraventa de bienes y prestación de servicios. 247
7.2.1. Que los datos sean interesantes, no quiere decir que sea *legítimo recabarlos* 247
7.2.2 Como excusa, intentan decir que no son datos de carácter personal 249
7.2.3. El reconocimiento biométrico en este contexto 250

8. EL RECONOCIMIENTO BIOMÉTRICO EN LA LLAMADA "VIGILANCIA INTELIGENTE", EN LAS REDES SOCIALES Y EN RELACIÓN CON LOS BIG DATA. 250
8.1. Cribado biométrico con Biometrías estáticas y Biometrías dinámicas. Los escenarios de la vigilancia inteligente 250
8.2. *Los datos biométricos en el minado de los Big Data* 253
8.3. Qué podemos rescatar de la normativa vigente 255

9. COMPARATIVA DE LOS RESULTADOS DE LA EVALUACIÓN DEL USO DE SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO EN DIFERENTES ESCENARIOS OPERATIVOS. 256

Parte III

Recopilación de conclusiones 263

Anexo de Ilustraciones 271

Bibliografía y Referencias Documentales 303

Abreviaturas y acrónimos

Aadhaar	Número de identidad único (de 12 cifras) expedido en la India
ACC	Autoridad Común de Control (de Schengen)
ACLU	American Civil Liberties Union
ADABTS	Automatic Detection of Anormal Behaviour and Threats in Crowded Spaces (Proyecto EU FP7)
AFIS	Automated Fingerpring Identification System
AGPD	Agencia Española de Protección de Datos personales
Ann Ist Super Sanitá	Annali dell'Istituto Superiore di Sanitá
AöR	Archiv des öffentlichen Rechts
BAG	Bundesarbeitsgericht (Tribunal Federal de lo Social, República Federal de Alemania)
BGBl	Bundesgesetzblatt
BGH	Tribunal Supremo de la República Federal de Alemania
BioFACE	Estudio Comparativo del Reconocimiento Facial (Proyecto del Ministerio de Interior Alemán).
Biometrics (Journal)	Journal of the International Biometric Society (Wiley-Blackwell)
BIOTEST	BIOTEST Biometric Testing Services.
BSI	Bundesamt für Sicherheit in der Informationstechnik - Autoridad Federal de Seguridad en las Tecnologías de la Información (República Federal de Alemania)
BT-Drs.	Bundestagsdrucksache (Diario Oficial de la Cámara Baja del Parlamento Alemán)
BVerfG	Bundesverfassungsgericht (Tribunal Constitucional Alemán)
CASCADE	Proyecto de encriptación de información biiométrica
CBPL	Commissie voor de Bescherming van de Persoonlijke Levensfeer – Autoridad de Proteccion de Datos de Bélgica
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CEDH	Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.(1950)
CNIE	Carte Nationale d'Identité Electronique (Francia)
CNIL	Commission Nationale Informatique et Libertés (Francia)
CoE	Consejo de Europa
Comisión LIBE	Comisión de Libertades Civiles, Justicia e Interior (Parlamento Europeo)
Comité del Convenio	Comité Consultivo del Capítulo V del Convenio nº 108 del Consejo de

Universitat d'Alacant
Universidad de Alicante

108	Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
CSIS	Central Schengen Information System
DEC	Duplicate Enrollment Check
Digma	Digma. Zeitschrift für Datenrecht und Information Sicherheit (Schulthess, Zürich)
DJ	Deutsche Justiz
DJZ	Deutsche Juristenzeitung
DOC COM	Documento de la Comisión Europea
DÖV	Die Öffentliche Verwaltung
DOXA	Cuadernos de Filosofía y Derecho
DuD	Datenschutz und Datensicherheit (Revista)
EJML	European Journal of Migration and Law
EURODAC	European Dactylographic System - Sistema de apoyo a la tramitación de los visados por parte de los Estados Miembros de la UE
FAR - TFA	False Acceptance Rate (Tasa de Falsa Aceptación)
FAST	Proyecto FAST (US Department of Homeland Security) - Future Attribute Screening Technology
FDI	Forum des Droits sur l'Internet (Francia)
FJ	Fundamento Jurídico
FRR. TFR	False Rejection Rate – Tasa de Falso Rechazo
FRVT	Face Recognition Vendor Test
FTA	Failure to Acquire
FTE	Failure to Enrol
FVC	Fingerprint Verification Competition
GAO	Government Accountability Office (EE.UU)
Garante	Garante per la protezione dei dati personali (Italia)
GT-WP 29	Grupo de Trabajo del Artículo 29 (UE)
HIDE Project	Proyecto Homeland Security, Biometric Identification & Personal Detection Ethics, financiado por la Comisión Europea.
HIPAA	Health Insurance Portability and Accountability Act, Estados Unidos de América (1996)
iAFB	International Association for Biometrics
IATA	Asociación Internacional de Transporte Aéreo, (en inglés "International Air Transport Association")
ICAO	OACI (en inglés)
ICO	Information Commissioner - Reino Unido
IEEE	Institute of Electrical and Electronics Engineers
IHESI	Institut des Hautes Etudes de la Sécurité Intérieure (Francia)
INS	Servicio de Inmigración y Naturalización (EE.UU)
INSPASS	Sistema para el tránsito acelerado de los viajeros frecuentes (EE..UU.) - Immigration and Naturalization Service Passenger Accelerated Service

Universitat d'Alacant
Universidad de Alicante

	System
Int J L Med	International Journal of Legal Medicine
IPTS	Institute for Prospective Technological Studies
ISO	International Organization for Standardization
ITP	Journal Information Technology & People
JA	Juristische Ausbildung
JASS	Journal of Anthropological Sciences
JBl	Juristische Blätter
JD	Revista Jueces para la Democracia
Juridikum	Juridikum. Zeitschrift für Kritik – Recht- Gesellschaft
La Ley	Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía: La Ley
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
MRTD	Machine Readable Travel Documents
NIST	National Institute of Standards and Technology (EE.UU.)
NJ	Neue Justiz, Zeitschrift für Rechtsetzung und Rechtsanwendung, Nomos, Berlin
NJW	Neue Juristiche Wochenschrift
NSIS	National Schengen Information System
OACI	Organización de la Aviación Civil Internacional (ICAO)
OGH	Tribunal Supremo (Austria)
Pers Ubiquit Comput	Personal and Ubiquitous Computing (Springer)
PETs	Privacy Enhancement Technologies1
PIA	Privacy Impact Assesment
PIN	Personal Identification Number
PWP SIS	Permanent Working Party SIS
RDS	Revista Derecho y Salud
REDA	Revista Española de Derecho Administrativo
REDC	Revista Española de Derecho Constitucional
ReDCE	Revista de Derecho Constitucional Europeo
Rev Der G H	Revista de Derecho y Genoma Humano
RFID CHIP	Chip de Identificación por Radio frecuencia
RGD	Revista General de Derecho
RGLJ	Revista General de Legislación y Jurisprudencia
RNIPP	Répertoire National d'Identification des personnes physiques (Francias)
RPC	Revista de Política Comparada
RTP	Registered Traveller Programme
RVAP	Revista Vasca de Administración Pública

[1] DOC COM (2007) 228 final.

Universitat d'Alacant
Universidad de Alicante

Sci Justice	Science & Justice. Journal of the Forensic Science Society
SEPD	Supervisor Europeo de Protección de Datos
SIA	Sistema de Información Aduanera
SICH	Sistema Integrado de Control Horario – Aprobado por Orden del Consejero de Presidencia, Justicia y Seguridad del Gobierno de Canarias, el 7 de agosto de 2009.
SIS	Sistema de Información Schengen (si se indica II, es el sistema de segunda generación)
SIS II	Sistema de Información Schengen de Segunda Generación
STC	Sentencia del Tribunal Constitucional (España)
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STIC	Systéme de Traitement des infractions constatées (Francia)
STS	Sentencia del Tribunal Supremo (España)
TC	Tribunal Constitucional (si no se indica otra cosa, el de España)
TCE	Tratado de la Comunidad Europea
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamienoto de la Unión Europea
TGI	Tribunal de Grande Instance - se indica región- (Francia)
TJCE	Tribunal de Justicia de las Comunidades Europeas
Trans R.l Society Edinb	Revista Earth and Environmental Science Transactions of the Royal Society of Edinburgh (Cambridge Journals)
TS	Tribunal Supremo (si no se indica otra cosa, el de España)
TSJ	Tribunal Superior de Justicia (se indica Comunidad Autónoma)
TUE	Tratado de la Unión Europea
UIDAI	Unique Identification Authority of India
US Patriot Act	"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act, Estados Unidos de América, 2001
US-VISIT	En la actualidad OBIM (Office of Biometric Identity Management), Estados Unidos
VersR	Juristische Rundschau für die Individualversicherung
VIS	Sistema Información de Visados
Vol.	Volumen
VWP	Visa Waiver Programm (EEUU las expide a visitantes de 36 países)
ZöRV	Zeitschrift für ausländisches und öffentliches Recht und Völkerrecht
ZRP	Zeitschrift für Rechtspolitik

Universitat d'Alacant
Universidad de Alicante

Listado de Ilustraciones

		Número de página
Imagen 1. Panorámica de escenarios operativos en los que se aplica el reconocimiento mediante Biometría.	……	271
1. Puerta de acceso con pasaporte biométrico europeo (ePass lane).	……	271
2. Control biométrico en las zonas de conflicto bélico (Afganistán).	……	271
3. Control de refugiados, ACNUR, Tailandia.	……	271
4. Sistema de acceso Privium para pasajeros frecuentes.	……	271
5. Sala de tránsito de viajeros Privium, aeropuerto de Schiphol.	……	271
6. Tarjeta de Identidad Aadhaar, India.	……	271
7. Sistema de sufragio biométrico.	……	271
8. Control de inmigración en aeropuerto norteamericano.	……	271
9. Sistema de control de beneficiarios de ayudas sociales (SASSA Card).	……	271
10. Sistema de visado electrónico en ELPASO.	……	271
11. Pago con Palm Secure en una escuela de EE.UU.	……	271
12. Acceso biométrico al parque Disney, en Orlando, EE.UU.	……	271
13. Sistema de geometría manual de acceso de los trabajadores.	……	271
14. Acceso biométrico (apertura de puerta).	……	271
15. Cajero automático biométrico.	……	271
16. Máquina expendedora de soda.	……	271
17. Sistema de acceso a banca electrónica (Barclays).	……	271
18. Captación de huellas en el Iphone de Apple.	……	271
19. Sistema de control horario de trabajadores.	……	271
Imagen 2. Ejemplos de características biométricas.	……	272
Imagen 3. Ejemplos de aplicaciones biométricas.	……	273
Imagen 4. Cueva de *Chauvet*.	……	273
Imagen 5. Huellas dactilares del tiempo de Babilonia.	……	273
Imagen 6. El muro de las huellas, en la ciudad de Tongling.	……	274
Imagen 7. Leonardo Da Vinci, *El hombre de Vitruvio*.	……	274
Imagen 8. El hombre de Vitruvio, en el Euro que acuña la República de Italia.	……	274

Universitat d'Alacant
Universidad de Alicante

Imagen 9. Proporciones de Durero. …… 274

Imagen 10. Lombroso. *L'Homme Criminel*, …… 274

Imagen 11. Primer número de la revista *Biometrika* (1901). …… 274

Imagen 12. Diagrama de medidas de Bertillon. …… 275

Imagen 13, Aplicación del Diagrama de Bertillon, prisión de Illinois. …… 275

Imagen 14. Toma de medidas de Bertillon, Policía de Nueva York. …… 275

Imagen 15. Ficha de Bertillon (Bertillon Card) de Francis Galton. …… 275

Imagen 16. Tabla sinóptica de rasgos fisionómicos (uso policial). …… 276

Imagen 17. Caso *Will West*, fotografías del frente y el perfil de los dos detenidos. …… 276

Imagen 18. Huellas dactilares (índice izquierdo) de *Will y William West*. …… 276

Imagen 19. Cálculo de los ingresos obtenidos por las tecnologías biométricas entre los años 1999 y 2003. …… 277

Imagen 20. Beneficios del sector de las tecnologías biométricas, 2009-2014. …… 277

Imagen 21. Sistema biométrico de determinación del sexo. SexNet. …… 277

Imagen 22. Clasificación de huellas dactilares según el esquema de Galton-Henry. …… 278

Imagen 23. Reconocimiento biométrico de la tipología de huellas dactilares. …… 278

Imagen 24. Transformación de muestra biométrica en patrón digital. …… 278

Imagen 25. Ejemplo de búsqueda de coincidencia en las minucias. …… 278

Imagen 26. Diferentes tipos de sensores de captación de huellas dactilares. …… 278

Imagen 27. Captación de la geometría del rostro. …… 279

Imagen 28. Fotoantropometría. …… 279

Imagen 29. Variabilidad de la Biometría facial (intra- e interclase). …… 279

Imagen 30. Sistema de cribado facial remoto. …… 279

Imagen 31. Localización de los puntos de medida en la geometría manual. …… 280

Imagen 32. Diferentes perspectivas del prototipo de captación de la geometría manual. …… 280

Imagen 33. Dispositivo de captación de la huella palmar y muestra digital que se obtiene. …… 280

Imagen 34. John DAUGHMAN y los ojos de Sharbat GULA. …… 280

Imagen 35. Esquema de IANNARELLI. …… 281

Imagen 36. Huella de la Oreja. …… 281

Imagen 37. Huella de la Oreja (2). …… 281

Imagen 38. Obtención de la Biometría auricular mediante ondas. …… 281

Imagen 39. Obtención de la Biometría auricular en 3 dimensiones. …… 281

Imagen 40. Muestras biométricas del IRIS almacenadas en distintas …… 282

Universitat d'Alacant
Universidad de Alicante

bases de datos.

Imagen 41. Biometría periocular. …… 282

Imagen 42. Diferentes tipos de cámaras que captan la Biometría del IRIS. …… 283

Imagen 43. Patrón de ADN representado en imagen. …… 283

Imagen 44. Representación del perfil de ADN en carnet de identidad. …… 283

Imagen 45. Diagrama de la nariz electrónica *ENose* y prototipos. …… 283

Imagen 46. Biometría dental (bandas *Hunter Scheger*). …… 284

Imagen 47. Huella de la lengua (*tongue print*). …… 284

Imagen 48. Lecho ungueal. …… 284

Imagen 49. *Tattoo Matching*. …… 284

Imagen 50. Reconocimiento de Marcas faciales. …… 284

Imagen 51. Biometría de la firma dinámica. …… 285

Imagen 51b. Biometría de la marcha (*Gait biometrics*). …… 285

Imagen 52. Sensor *Enobio*. …… 285

Imagen 53. Biometrías dinámicas- Proyecto *FAST*. …… 286

Imagen 54. Poder de discriminación de las tecnologías de reconocimiento biométrico y riesgo que implican para la privacidad. …… 286

Imagen 55. "Muestra biométrica" (o dato en crudo). …… 287

Imagen 56. Los carteles de "se busca", ejemplos históricos. …… 288

Imagen 57. Oferta de recompensa por *El Chapo Guzmán*, México 2015. …… 288

Imagen 58. Retrato Robot de *Bin Laden* elaborado parcialmente a partir de la imagen de *Gaspar Llamazares* …… 288

Imagen 59. Esquema del funcionamiento básico de los sistemas de reconocimiento mediante Biometría. …… 289

Imagen 60. Ejemplo de SISTEMAS MULTIBIOMÉTRICOS (que emplean varias fuentes de información biométrica). …… 289

Imagen 61. Distintas posibilidades de sistemas multibiométricos. …… 290

Imagen 62. Categorías de vulnerabilidades de los sistemas biométricos, expresadas en un modelo *fishbone (*espina de pez). …… 290

Imagen 63. Simulación de características biométricas. …… 291

Imagen 64. Problemas de enrolamiento. …… 291

Imagen 65. Problemas de captación de las huellas. …… 291

Imagen 66. Problemas de captación del iris. …… 291

Imagen 67. Exposición involuntaria de la Biometría. Das *biometrische Sammelabum*, Álbum para colección biométrica, del *Chaos Computer Club* (CCC), …… 292

Imagen 68. Influencia de los factores ambientales y de iluminación en el reconocimiento biométrico (reconocimiento facial). …… 292

Imagen 69. Impacto del envejecimiento. …… 292

Imagen 70. Sistemas que requieren habilidades específicas de los …… 293

Universitat d'Alacant
Universidad de Alicante

usuarios.

Imagen 71. Ejemplo de patologías del iris. …… 293

Imagen 72. Ejemplos de algunas enfermedades de la piel que afectan a las impresiones dactilares. …… 293

Imagen 73. Pasaporte biométrico europeo destacando el logotipo que indica que lleva incrustado un microchip. …… 293

Imagen 74. Programa de viajeros frecuentes. *SmartGate* …… 294

Imagen 75 Sistemas de control biométrico de personas desplazadas por conflictos bélicos (refugiados). …… 294

Imagen 76. Mapa del mundo en el que aparecen en gris los países que tienen implantado (a fecha de 2014) un sistema biométrico civil o de registro del sufragio. …… 294

Imagen 77. Padrón electoral de Bolivia. …… 295

Imagen 78. Geolocalización. *Mapa de Marauder* de Harry Potter. …… 295

Imagen 79. Control de abonados en *Mouseplanet*. …… 295

Imagen 80. *SodaTron*. …… 295

Imagen 81. Máquina expendedora con sistema de reconocimiento biométrico de la edad. …… 295

Imagen 82. Teléfono inteligente con captación de huella biométricas. …… 296

Imagen 83. Sensor de huellas dactilares EIKON. …… 296

Imagen 84. Sistema de pago PALM SECURE. …… 296

Imagen 85. Estudiantes de la Escuela Elemental de Crawnberry, en Westminster, abonan la comida en el comedor escolar mediante escáner palmar. …… 296

Imagen 86. Etiquetado voluntario de fotos en Facebook. …… 297

Imagen 87. Vigilancia (re-identificación). …… 297

Imagen 88. Procesamiento de imágenes (vigilancia biométrica en espacios abiertos). …… 297

Imagen 89. *Multicamera Tracking*. …… 297

Imagen 90. Reconocimiento facial tipo *Terminator*. …… 298

Imagen 91 Captación de atributos de la vestimenta. …… 298

Imagen 92. Vigilancia que pasa inadvertida (viñeta de humor). …… 299

Imagen 93. La Biometría en el cine. …… 299

Universitat d'Alacant
Universidad de Alicante

Parte I
PLANTEAMIENTO, OBJETIVOS Y METODOLOGÍA DE LA INVESTIGACIÓN

Universitat d'Alacant
Universidad de Alicante

Universitat d'Alacant
Universidad de Alicante

1. Introducción

1.1 RESUMEN DE LA PRESENTE INVESTIGACIÓN Y DE SU CONTEXTO.

1.1.1. Abstract

Aunque resulta difícil ofrecer una definición unívoca, en su acepción amplia se describe como *información biométrica* aquella que se obtiene *mediante estudios mensurativos o estadísticos de los fenómenos o procesos biológicos*[1]. En coherencia, y dentro del conjunto de los biodatos humanos – o datos que pueden obtenerse del cuerpo humano- los datos biométricos se caracterizan por ser el resultado de uno o varios procedimientos destinados a medir la peculiaridad de alguna característica anatómico-física o comportamental de una persona o un grupo de personas. De ahí que en ocasiones la literatura comparada se refiera a los datos biométricos como *representaciones numéricas* o matemáticas de los fenómenos biológicos. La diversidad de los datos biométricos que pueden obtenerse de una sola persona es infinita. Como describía Francis GALTON en el primer número de la revista *Biometrika* (1901), la disciplina de la Biometría agrupa *todos aquellos métodos* que permiten describir tanto las variables continuas como el más pequeño de los cambios que acontecen en el mundo de lo vivo, de lo orgánico[2]. Tan diversos como los datos que se obtienen son los instrumentos y métodos que en el último siglo se han desarrollado para captar métricamente y obtener así información de los seres vivos, incluyendo a los seres humanos.

Tanto los grupos de individuos como cada individuo singular son referencias ineludibles en los estudios biométricos, porque, si bien al presentar los resultados del conjunto parecerá que se desvanecen los individuos, lo cierto es que no es posible alcanzar resultados biométricos de un conjunto sin un estudio singularizado de cada individuo. Vistos desde el conjunto, en los estudios que tratan de hallar el conocimiento biológico mediante métodos cuantitativos, ya lo advertía

---

[1] ALBRIZIO, A: "Biometry and Anthropometry", *Journal of Anthropological Sciences*, vol. 85, 2007, pp101-123, p102-106; ABS, M. "Biometrik", en *Historisches Wörterbuch der Philosophie*, pp945-946; GHILARDI, G./ KELLER, F.: "Epistemological Foundations of Biometrics", en *Second Generation Biometrics* 2012, pp23 y ss, 24-25.

[2] Véase también FISHER, R. en "The Correlation Between Relatives on the Supposition of Mendelian Inheritance", *Trans R. Society Edinb* 52, 1918, 399-433,, en el que procedía a medir los rasgos y a fijar las variables continuas, como base para abordar la heredabilidad de aquéllos.

GALTON, es difícil no impresionarse *por la poca importancia que en el conjunto parece tener cada individuo*[3]. Parece ser una minúscula entrada de datos en un fenómeno masivo. Pero en ese fenómeno masivo se nos ofrecerá también la oportunidad de volver a esas minúsculas entradas de datos, a esas que dentro de la diversidad permiten establecer la cercanía entre los individuos son determinantes para poder establecer las variables continuas de los fenómenos biológicos. Con esa contemplación de los individuos dentro del conjunto guarda estrecha relación este trabajo; con la oportunidad de captar y expresar métricamente no sólo lo constante, sino también lo variable; no sólo lo común, sino también lo singular. La naturaleza, decía el matemático belga QUETELET[4], "*muestra variaciones de formas ilimitadas e infinitas"* y *"nunca reproduce exactamente sus obras"*, y esa impresionante diversidad tiene también su expresión en cada persona, en cada ser humano único e irrepetible.

Un hito histórico para el enfoque de la Biometría que interesa a este trabajo –el de la potencialidad de servir de base a sistemas de reconocimiento de seres humanos – llegará de la mano de Alphonse BERTILLON. Este experto francés diseñó para la policía un sistema de reconocimiento de criminales reincidentes que, entre otras cosas, completaba las fichas policiales con estudios mensurativos de algunos de sus rasgos anatómico-físicos (véanse las IMÁGENES 12, 13, 14). En las últimas dos décadas se han instalado en nuestro entorno sistemas informatizados que, partiendo del potencial singularizante de la Biometría, ofrecen la posibilidad de reconocer la identidad de una persona de forma rápida y eficiente, y no sólo con base en rasgos anatómico-físicos sino atendiendo también a lo que se conoce como biometrías dinámicas o comportamentales, que atienden a las expresiones de la fisiología, el funcionamiento de las habilidades motoras o las señales electrofisiológicas del cuerpo humano (véanse en el anexo las IMÁGENES 1,2 y3).

El control de los movimientos transfronterizos, la identificación de las personas indocumentadas que solicitan asilo o la seguridad en espacios como instalaciones militares o prisiones; el acceso a los sistemas sanitarios o el control del fraude en las ayudas sociales; la verificación de la titularidad de los abonos de parques e instalaciones de ocio o los programas que facilitan el embarque a pasajeros frecuentes en los aeropuertos internacionales; o procedimientos de control de los procesos electorales son sólo algunos de los escenarios en los que se han implantado ya sistemas de estas características. Importantes referentes en lo que se refiere a la protección de los derechos civiles o de la privacidad vienen advirtiendo desde comienzos del siglo XXI del peligro

[3] GALTON, F. *Spirit of Biometrika*, editorial del primer número de la revista *Biometrika*, 1901; COX, R. "Biometrika: The First 100 Years". *Biometrika* 88 (1), 2001, 3–11.

[4] Citado por DE ANTÓN Y BARBERÁ, F. "Las Huellas Dactilares a Examen", 2009, 020-026.

de este conjunto de tecnologías que, entre otras cosas, emplean *la corporeidad* como elemento de gestión y control de las identidades de las personas. Pero la decisión de la Unión Europea de incorporar datos biométricos a los pasaportes de sus ciudadanos y al control de los solicitantes de asilo en la Unión Europea hizo que, en muy poco tiempo, pasasen de ser tecnologías emergentes a implementarse en multitud de escenarios.

Este proceso se ha producido sin excesivo debate público y con muy pocos estudios multidisciplinares que se adentren en abordar la naturaleza del reconocimiento biométrico, sus potencialidades y sus límites, y las consecuencias sociales que conlleva su aplicación. En ese contexto surge la inquietud, finalmente encauzada en este trabajo, por dar respuesta a la siguiente cuestión. *No hay duda de que en el actual contexto social necesitamos sistemas ágiles y fiables para gestionar la identidad de las personas. Pero, ¿son los sistemas automatizados de reconocimiento biométrico, esos sistemas "agiles y fiables" que necesitamos?*

Dar respuesta a esta cuestión requiere profundizar, por una parte, en la naturaleza y características de la información biométrica con potencial de identificación y, por otra, en la configuración y funcionamiento de estos sistemas automatizados. Desde esa base y con la experiencia de los sistemas que están en funcionamiento, se ha abordado críticamente su empleabilidad, precisión y fiabilidad en diferentes contextos operativos, y se ha procedido a valorar la aceptabilidad y legitimidad de los mismos con la referencia comparativa de otros mecanismos de identificación social que se han empleado y se emplean con la misma finalidad. Se trata, en suma, de dar respuesta a la cuestión de hasta qué punto las tecnologías de reconocimiento biométrico pueden, en el actual estado de la ciencia y de la tecnología, ofrecer calidad y eficiencia en el reconocimiento de las personas, y cuáles son los beneficios y el coste de su aplicación en diferentes formatos y escenarios operativos.

A la realización de este trabajo han contribuido, entre otros, dos ayudas de investigación: una del Instituto Vasco de Administración Pública y otra del programa de ayudas a Grupos del Sistema Universitario Vasco, además de las facilidades que la Universidad del País Vasco/ Euskal Herriko Unibertsitatea ofrece a los miembros de su PDI en el acceso al Sistema de Documentación y Préstamo Interbibliotecario. A lo largo de la realización de este trabajo se han realizado cuatro estancias breves de investigación: dos en el *Max-Planck Institüt für offentliches Recht und Völkerrecht* de Heidelbeg (Alemania, 2012 y 2015), una en el *Institute for Advanced Legal Studies* de la *University of London* (Reino Unido, 2013) y otra en la Academia Europea EURAC de Bolzano (Italia, 2014).

1.1.2. Identidad(es), identificación e interacción social: el contexto de la aplicación del reconocimiento mediante biometría.

1.1.2.1 *Identidad de la persona, identidad social e identificación*

Los de *identidad* e *identificación* son dos conceptos más complejos de lo que a primera vista puede parecer. Apelan en ultimo término a cuestiones de las que viene ocupándose históricamente la filosofía, cómo es el caso de las preguntas relativas a la naturaleza de la individualidad, del *ser* o incluso del *alma*[5]. Explica HILDEBRANDT que *ipse* (el uno mismo) e *idem* (la observación que la persona tienen los demás) interaccionan en un modo que su intersección permite la construcción de la identidad personal[6]. Pero en el espacio cotidiano la necesidad de identificar o atribuir "identidad" a una persona rara vez tiene un alcance tan metafísico[7]; difícilmente puede prestarse el tiempo que requeriría conocer en profundidad *quién es realmente cada persona.*

Para expresar gráficamente en qué consisten los sistemas de identificación suele decirse que tratan de reflejar con certeza en qué condiciones y situaciones podemos tratar a alguien como *idéntico.* Pero, ¿idéntico *a qué* o *a quién*? Idéntico a dos objetos referenciales diferentes. Idéntico en el sentido de que la persona *es a alguien con quien bien nosotros, bien otros ya interactuaron con anterioridad*; esto es, idéntico a *sí mismo*, aunque a un sí mismo en otro momento y contexto. Aplicando esta idea, quien roba la identidad de un tercero no es que, propiamente, sustraiga a alguien su individualidad, sino que consigue suplantarse en aquello que frente a terceros identificaba a la víctima y, con ello, se hace falsamente ser merecedor del trato que esa persona recibía por parte de una administración, una empresa o un particular. Pero también cabe establecer que alguien es *idéntico* a otro objeto referencial; esto es, *idéntico* en el sentido de que se parece en algo a otras personas que ya conocemos y, por esa identidad, merece el mismo trato que les dispensamos a ellas. Es decir, idéntico en el sentido de que comparte algunas cualidades o características[8], sea éste un conjunto más o menos grande[9] de individuos. Así, en algunos casos, la pretensión de un sistema de reconocimiento puede ser la de establecer que alguien es nacional,

---

[5] CLARKE, R. "Human Identification in Information Systems", 1994, pp. 6-3.

[6] HILDEBRANDT, M. "*Profiling* and the Identity of European Citizens", 2009, p274. Entre los primeros en exponer esta tesis, RICOEUR, P. "La personne et la référence identifiant", en *Soi-même comme un autre*, 1990, pp39-54. También distingue entre *mismidad* y *self*, *idem* e *ipse*, el CCNE en su Avis nº 98 "Biométrie, donnés identifiants et droits de l'homme", 2007, pp7-8 ; ERICKSON, E. H. *Identity and the Life Cycle*, Norton & Company, 1994, p109.

[7] OLORIZ AGUILERA (1855-1912), citado por ANTÓN BARBERÁ, F./ DE LUIS Y TARAGANO, J. V., *Policía científica*, 2004, p9.

[8] MORDINI, E. / TZOVARAS, D. *Second Generation Biometrics*, cit., p1.

[9] CLARKE, R. "Person location and person tracking", 2001, 2 pp. 206-231.

mayor de edad o mujer, que tiene derecho al voto o que pertenece a un país que por estar en conflicto da derecho a sus nacionales a ser recibidos en Europa, tal y como sucede con todos aquellos que estimamos que son *idénticos a él.*

Una serie de elementos materiales, combinados con informaciones tales como el origen, sexo, filiación o el nombre y los apellidos producen, lo que en algunos países se denomina *identidad civil* –ante el Estado- y que se establece entre el nacimiento y la defunción de una persona. Pero lo que llamamos *identidad social* es un artefacto más complejo. Explica Alain DAMASIO[10] que se trata de un "artefacto" que comprende un conjunto más o menos difuso de *fragmentos individuales* con los que se identifica a una persona; modos de comportarse, tipos de actividades, perfiles de consumo o de voto; esto es, versiones abreviadas y funcionales de la identidad de alguien. Desde tiempos ancestrales las personas son juzgadas y calificadas por su medio social para facilitar su rápida ubicación. Mientras el buen nombre o el hecho de que se asociaban a una persona características positivas reportaba importantes ventajas, el mal nombre le condenaba al ostracismo. Y lo malo es que muchas veces, una vez formulado ese mal nombre ya no era posible librarse de éste. La doctrina explica que los abusos en este segundo sentido y aquello del "*calumnia, que algo queda*" llevaron a proclamar en las Cartas de Derechos un derecho fundamental al "*buen nombre*". Una nueva versión de esta situación se produce en la actualidad, por ejemplo, con los motores de búsqueda y el llamado derecho al olvido o derecho que el titular de un dato tiene a que se borre de internet una información personal que le afecta y está obsoleta. Y es que los fragmentos individuales que el contexto social contemporáneo toma de nosotros, sobre todo en nuestro uso de las redes digitales, dan lugar cantidades ingentes de información. Nunca antes en la historia habíamos estado tan expuestos a los demás, ni en formas tan diversas.

Universitat d'Alacant
Universidad de Alicante

1.1.2.2. *El ansia por centralizar los datos y asociarlos a identificadores únicos*

El hecho de que quienes captan la información lo hagan de forma fragmentada no hace perder de vista, ni mucho menos, el valor potencial de una colección de identidades en la que se puedan ir cuidadosamente ensamblando todos los *fragmentos de identidad* y llegar así a captar el resultado de las complejas relaciones que una persona tiene con la sociedad y en las que refleja la riqueza y multidimensionalidad de su persona[11]. Desde el punto de vista de quien almacena la información, de poco sirve el esfuerzo de almacenamiento si la información no está organizada y accesible para poderla emplear de forma eficaz en el futuro. Si lo pensamos bien, sólo en internet

[10] En su intervención en los debates del *FDI*, de 12 de marzo de 2002.

[11] TRUCHE P. / FAUGERE, J. -P./ P. FLICHY, *Administration électronique et protection des données personnelles – Livre Blanc*, 2002, pp31 y ss.

participamos en muy diferentes espacios y asumimos diversos roles, expresamos maneras de sentir y de pensar, pseudónimos y motes que complican la vinculación de esos fragmentos de identidad a una única persona. Piénsese el interés que, desde el punto de vista de quienes están interesados en captar los perfiles de las personas y analizar éstos con diferentes fines, puede tener no sólo el poder vincular fragmentos de identidad sino el hecho de construir los mosaicos sobre una base, un núcleo de identidad que pueda darse como fijo, estable y permanente[12]; un núcleo de identidad que nos permita localizar física o virtualmente a una persona y trazar sus movimientos o actividades de cualquier tipo.

Visto desde la perspectiva de la persona cuyos datos son almacenados y del riesgo de que se produzcan accesos no consentidos o no conocidos a estos, la fragmentación (o balcanización) de las parcelas de identidad favorece en la actualidad el ejercicio de sus derechos. Es más, Alain DAMASIO explica cómo la administración electrónica debería preservar nuestro derecho a tener múltiples identidades, el derecho a reinventarnos cuantas veces lo estimemos oportuno y a expresar de forma diferente nuestra identidad como estudiante, consumidor de diferentes bienes o servicios, contribuyente o afiliado a la seguridad social. Y es que el perfilado corre el riesgo de ocasionar construcciones sociales de la identidad de una persona que queden más o menos lejos de lo que una persona es o siente ser. Pocas falacias hay de mayor calibre que tomar una parte por el todo.

En algunas cartas de derechos, entre ellas las europeas, se reconoce a todas las personas un derecho a la identidad personal y en la última década este derecho ha sido objeto de una interpretación jurisprudencial cada vez más amplia. No se trata sólo de un derecho de cada persona a conocer su origen, su filiación o su nacionalidad; tampoco se trata de proteger *el constructo social* que de la identidad de alguien se ha hecho; no. Como explica la jurisprudencia del Tribunal Europeo de Derechos Humanos, lo que este derecho protege es *la verdad personal* que cada individuo proyecta hacia el exterior. Esa verdad[13] comprende tanto elementos estáticos, como aspectos dinámicos, en el sentido de que forman parte de la identidad de una persona aquellas decisiones que a lo largo de su vida toma para guiarse y adoptar de forma autónoma decisiones sobre su vida. Entre esas decisiones están comprendidas, incluso, aquellas que modifican aspectos estáticos de su identidad. El nombre, las relaciones paterno-filiales o la nacionalidad pueden modificarse, como también pueden modificarse elementos de la corporeidad que son empleados por la sociedad como referencia en la construcción social de las identidades

[12] DAMASIO, Alain: "Construisons ensemble la civilité de l'internet", *Le Forum des droits sur l'internet*.

[13] ESCAJEDO, L. "Identidad genética y libertad de ciencia", en *Identidad, Derecho y Política*, 2013, pp19-29.

(como es el caso de la asignación del sexo con base en los órganos sexuales). No tendría, por tanto, mucho sentido no poder ejercer ese mismo derecho cuando se trata de modificar la construcción que de nuestra identidad se ha hecho virtualmente en determinados entornos digitales como los de adquisición de bienes y servicios.

1.1.2.3. *Informaciones y objetos tradicionalmente empleados como apoyo en la identificación*

Re-identificar a alguien con quien se ha tenido trato o determinar si alguien pertenece al conjunto de personas autorizadas o legitimadas para acceder a un entorno (físico o digital) concreto resulta en ocasiones muy complejo; más en contextos en los que se tiene relación cotidiana y rápida con multitud de sujetos y se encomienda la identificación a personas que –no habiendo tenido nunca trato con un sujeto- no identifican desde sus recuerdos, sino a partir de alguna información que la persona ofrece o algún objeto que ésta porta. Los historiadores recogen diferentes elementos y sistemas que a lo largo de la historia se han empleado, en sentido amplio, para esta función. Las huellas de manos en las cuevas de *Chauvet,* de aproximadamente entre 32000 y 36000 años de antigüedad[14] (IMAGEN 4) o la creencia de que los reyes de Babilonia imprimían su mano derecha en las tablas de barro a modo de *refrendo real* [15]son citados por la literatura como prácticas que guardan cierta relación con los sistemas de identificación contemporáneos. Pero entre los primeros sistemas de identificación social de los que se tiene constancia suele citarse el desarrollado en la ciudad de Jericó, en el valle del Jordán(en torno al año 9000 a. C.)[16]. De este sistema se tuvo noticia por textos muy posteriores, como la Odisea de Homero. Descripciones de la apariencia física, modificaciones en el cuerpo (como tatuajes o cicatrices), el hecho de portar objetos identificativos o el demostrar que se conocían datos, memorias o elementos característicos de determinadas familias o tribus son citados como medios para reconocer o ser reconocido[17] en una ciudad cuyo desarrollo y crecimiento, unido al tránsito frecuente de viajeros, ya no era posible un conocimiento directo de las personas.

---

[14] KINDT, E. *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013, p14.

[15] ASHBOURN, J. "The social implications of the wide scale implementation of Biometric and related technologies", Background paper for the IPTS, DG JRC, EU Commission, January 2005, p4; BIOMETRIC TASK FORCE, *Biometric History Timeline*, Department of Defense, Estados Unidos.

[16] GATES, C. *Ancient Cities: The Archaeology of Urban Life*, 2003.

[17] MORDINI, E./ TZOVARAS, *Second Generation Biometrics*, pp2-3; CCNE, Avis nº 98, cit., 2007, pp4-5.

En los primeros imperios (Egipcio, Chino o Asirio)[18], -IMAGEN 5- aparecen sistemas más sofisticados. Documentos de la dinastía TANG (616-907) hacen referencia a un uso de huellas impresas en los contratos como un método que se cree que se había venido usando desde hace al menos dos mil años[19]. El cobro de impuestos, la identificación de criminales reincidentes o esclavos y el reconocimiento de condiciones como la de ser propietario o (en Roma) *ciudadano político* son algunos de los ejemplos de necesidades de organización social que llevaron a desarrollar sistemas de identificación. En el Antiguo Egipto la altura, complexión, rasgos faciales u otras características destacables –como las cicatrices- se empleaban junto al nombre en la identificación de los obreros que participaron en la construcción de las Pirámides[20]. Con todo, los nombres y apellidos han venido siendo uno de los elementos de identificación más importantes[21].

Sobre la base de un sistema establecido en la antigua Roma, los nómadas que circulaban por Europa en la Edad Media solían portar distintos tipos de salvoconductos que, emitidos por distintas autoridades, los acreditaban como peregrinos, soldados profesionales, comerciantes[22]. Otro hito que se reseña es la ley por la que de Enrique VIII de Inglaterra (1538) ordenó a los clérigos anglicanos que mantuvieran registros de nacimientos, decesos y enlaces matrimoniales, incluyendo los apellidos de los padres en el caso de los nacimientos en el seno matrimonial[23]. Dichos registros se mantuvieron bajo la responsabilidad de las instituciones religiosas hasta que en 1837 la ley de registro de Nacimientos y Decesos (*Births and Deaths Registration Act*) lo transformó en un asunto civil. Existieron asimismo sistemas para la identificación de los mendigos por parte de las autoridades civiles o religiosas. Por la obra *Decadas da Asia. Dos feitos que os Portuguezes fizeram na conquista e descobrimento dos mares e terras do Oriente*, de João DE

Universitat d'Alacant
Universidad de Alicante

[18] INTRONA, L. D./ NISSENBAUM, H. *Facial Recognition Technology*, 2009, pp9-10; LANGENDERFER, J./ LINNHOFF, S. "The Emergence of Biometrics and its Effect on Consumers", 2005, pp314 y ss.

[19] KINDT, E. *Privacy*, 2013,p16.; MCMAHON, Z. *Biometrics: History*, Indiana University, citado por el NSTC, *Biometric History*, 2006; FARELO, A. *A History of Fingerprints*, Interpol, abril de 2009, p2; Bridges, B. C. *Practical fingerprinting*, 1963.

[20] DAVIS, R. "Biometric Myths: Six of the Best", 2006, p1; GIROTTO, S. "Il tratamento dei Dati Biometrici", 2011, p1237.

[21] POLEMI, D. 1997, p4.

[22] EHRLICH, T. "Passports", *Standford Law Review*, v. 19, 1966-1967, pp129-149; LORENTE ACOSTA, J. A. "Identificación genética criminal", 2002, pp1-2; MORDINI, E./ TZOVARAS, D. (eds.), *Second Generation*, pp3-4.

[23] CLARKE, R. *Human Identification*, 1994, p11.

BARROS (1496-1570), también conocido como el *Tito Livio* portugués[24], sabemos que en esa época los comerciantes chinos imprimían con tinta las huellas de la palma de las manos y de los pies[25].

La vinculación entre los registros de nacimientos y la expedición de los documentos de viaje llegará en Francia, de la mano de la Revolución Francesa. Si bien Luis XIV expidió los que son considerados como primeros pasaportes de la historia, será tras la Revolución de 1789 y con una clara vinculación con el principio según el cual los seres humanos nacen libres e iguales en derechos, cuando se impulse un reconocimiento de las identidades personales vinculado con un *registro de los nacimientos*[26]. MORDINI/ TSOVARAS/ ASHTON[27] destacan este hito como el momento que implica dejar atrás esquemas de identificación basados en la "*pertenencia a una comunidad*" o en elementos como la religión, la casta, la pertenencia étnica, la condición social. A partir de entonces se avanza hacia sistemas de identificación con vocación de ser expedidos al conjunto de la ciudadanía, basados en un documento creado por el Estado y que contienen información relativa al nombre, la nacionalidad y la fecha y lugar de nacimiento. Un ciudadano existirá, dicen estos autores, "*en tanto su nacimiento haya sido certificado y no conste registralmente su defunción*" y esa existencia se acreditará con un documento expedido por el Estado.

1.1.2.4. *El miedo a los sistemas de identificación a gran escala*

Hasta la primera Guerra Mundial convivían dentro de cada país multitud de sistemas de registro de los habitantes y documentos de identificación emitidos por diferentes entidades. Pero el final de la guerra llevará a revisar esa situación y a reforzar la calidad de los documentos. Se introducirán las fotografías (y en algún caso huellas dactilares) con dos fines: la identificación de las personas que –en numero creciente- cruzan las fronteras y la de las personas con derecho a recibir algún tipo de ayuda social. Además, una conferencia internacional en 1920 impulsó el sistema de los pasaportes actuales[28] tratando de acercar los esquemas de identificación que venía empleando cada estado. Desde el punto de vista interno de cada Estado el registro de los ciudadanos tenía fines administrativos, entre ellos la recaudación fiscal o el derecho al trabajo, y

[24] COSTA, J. A. P. D. (1993): «História da dactiloscopia em Portugal», Separata de *O Médico*, n° 1469, Vol.. 93. pp.174-175; PEREIRA, R. (1987): «O desenvolvimento da ciência antropológica na empresa colonial do Estado Novo», en *Estado Novo das origens ao fim da autarcia*, Lisboa, Fragmentos. Vol. II, pp. 89-106.

[25] J. DE BARROS, Capítulo II de la Tercera década: "imprimindo toda a figura da mão, & outro tanto faz com a planta do pé direito{…}".

[26] WALKER, G. de Q.,"Information as Power", CIS – Centre for Independent Studies, Policy Report, 1986.

[27] MORDINI, E./ TSOVARAS, D./ ASHTON, H. en *Second Generation Biometrics*, cit. pp4-5.

[28] CLARKE, R. Human Identification, cit. 1994, p12.

la referencia empleada para la identificación se extenderá para otros propósitos como la administración de las ayudas sociales o el control de la legitimidad de los procesos electorales. Abusos como los cometidos en los métodos de control poblacional de los nazis en los territorios ocupados hicieron, eso sí, que en algunos países se desconfiase de los registros estatales y se potenciasen más los registros municipales, pero en estatales o locales lo cierto es que los esquemas coincidían en sus elementos fundamentales.

La segunda posguerra, con el paso hacia los Estados sociales en los que la riqueza es redistribuida mediante sistemas impositivos y prestaciones sociales, abrió en Europa el camino hacia sistemas más robustos de identificación. Entre tanto, en los Estados Unidos de América, país en el que no se contaba con un sistema de identificación similar al de los documentos nacionales de identidad, una serie de acontecimientos llevaron a instituir *de facto* el número de la seguridad social (SSN – Social Security Number) como un identificador a nivel nacional. En tiempos de la represión de los años 30 en los Estados Unidos un número importante de norteamericanos estaba sin empleo ni vivienda, y carecían de acceso al alimento y a los cuidados médicos[29]. Como respuesta a dicha situación, el presidente Franklin D. Roosevelt propuso un conjunto de normas de seguridad económica entre las que estaba la Ley de seguridad social de 1935. Dicha Ley estableció dos programas de seguro: uno para los ancianos y otro los desempleados. Y como piezas necesarias para su puesta en marcha estableció un sistema de cobro de tasas a empleados y empleadores y una fórmula por la que se asignaba a cada trabajador un número de identificación personal. Entre la Segunda Guerra mundial y el año 1951 también existió en Reino Unido un sistema de ayudas sociales para el cuál se expidió una tarjeta de identidad asociada al domicilio de las personas[30] y en Canadá se desarrolló un sistema similar al número de la seguridad social estadounidense, el SIN (Social Insurance Number).

El SSN, expedido por la *Social Security Administration*, estaba pensado como un mecanismo para registrar los beneficios que un empleado iba acumulando para el futuro –de hecho se indicaba expresamente en el carnet que "no era para identificación"[31]-. La ausencia de otro tipo de identificador nacional hizo que, sin embargo, se terminara empleando en otros escenarios operativos, como las finanzas, la educación, la identificación de contribuyentes a los efectos de

[29] DOTSON, K. A. "Your Good Name: Identity Theft and the Consumer", *Quinnipiac Law Review* (QLR) Vol. 22, nº 3, 2004, pp618-619, con referencias oficiales a las estadísticas de la oficina de investigación sobre seguridad social.

[30] RULE, J. "*Social control and modern social structure",* 1974, pp. 314-15

[31] DEPARTMENT OF HEALTH, EDUCATION AND WELFARE – HEW, "Records, Computers and the Rights of Citizens", US Department of Health, Education and Welfare, MIT Press, Boston, 1973, pp114-22.

tributación o la concesión de licencias como las de conducción[32]. Esta difusión del uso del SSN ha resultado con el tiempo un problema, porque los terceros que conocer el número de identificación de alguien junto con alguna otra información facilita en ocasiones suplantar su identidad.

En el caso de España, el DNI se emplea como "documento público que acredita la auténtica personalidad de su titular" en el sentido de "justificante completo de la identidad de la persona" (L.O 1/ 1992[33]) y su uso está extendido tanto ante las autoridades como ante los particulares[34]. Se expide tanto a los nacionales como a los extranjeros a los que se ha autorizado la permanencia en el país más allá de los tres meses. La facilidad para acceder al número del DNI de las personas y suplantar con ello su personalidad se compensa en cierta medida con la exigencia de mostrar el documento original (o versión electrónica).

1.1.2.5. *La llegada de los sistemas automatizados de reconocimiento biométrico*

Los sistemas de reconocimiento automatizado mediante Biometría han llegado en un momento en el que los conceptos de frontera se han transformado y los Estados se enfrentan a nuevos retos para su seguridad nacional ocasionados, entre otros, por el aumento de la población, la mayor velocidad o intensidad de los movimientos poblacionales y las nuevas formas de criminalidad. Históricamente las fronteras, como líneas de demarcación claramente determinadas, habían sido defendidas con objetivos de defensa y han contribuido también a la construcción de identidades colectivas (en el sentido de líneas divisorias entre el *nosotros* y *los otros*). Pero a lo largo del siglo XX el concepto de frontera ha sufrido importantes transformaciones. Entre los más de 7000 millones de personas que habitan el planeta, centenares de miles se desplazan cotidianamente con las motivaciones más diversas. El crecimiento de la población y de la movilidad han llevado a repensar de forma radical los sistemas de reconocimiento[35]. Preocupan las actividades del crimen organizado, amenazas terroristas y de

[32]COMPTROLLER GENERAL-CG, "Re-issuing Tamper Resistant Cards Will Not Eliminate Misuse of Social Security Numbers", 1980; FEDERAL ADVISORY COMMITTEE ON FALSE IDENTIFICATION – FACFI, "The Criminal Use of False Identification", 1976; OFFICE OF TECHONLOGY ASSESMENT – OTA, "Computer-based National Information Systems: Technology and Public Policy Issues", 1981.

[33] El art. 9.1 de la LO 1/ 1992, sobre Protección de la Seguridad Ciudadana.

[34] SÁNCHEZ BARRILAO, J. F. "Identificación documental de Nacionales y Extranjeros", *Revista Española de Derecho Constitucional*, 2002, 219-220.

[35] INTRONA, L./ NISSENBAUM, H. *Facial Recognition Technology*, cit., 2010, p8.

salud pública, junto a los robos y usurpaciones de identidad con diferentes fines[36], y éstos han sido esgrimidos como problemas ante los que se buscan soluciones *eficaces*[37]; entre ellas la necesidad de contar con herramientas para una identificación indubitada de las personas. En este año 2015, además, las guerras y la pobreza han llevado a cientos de miles de personas, procedentes de África o de países como Irak, Afganistán o Siria, a tratar de entrar desesperadamente al territorio de la UE y es de seguro que, tras esta crisis, volverán a revisarse por enésima vez los sistemas de control transfronterizo.

El reconocimiento de identidad mediante Biometría tiene como base una asociación automatizada entre la identidad social del individuo y características anatómico-físicas o comportamentales singularizantes que son captadas de su corporeidad o de su comportamiento. Para esta captación no siempre es imprescindible que la persona colabore (o siquiera conozca) que se está analizando su corporeidad con el objetivo de determinar su identidad (IMÁGENES 1, 89, 90). Estos métodos de captación de información pueden ofrecernos *fragmentos individuales* de la identidad de alguien que asociados a algún otro elemento sirvan para identificar, pero –por sí solos- no resultan suficientes. Pero es posible también emplear la Biometría para establecer *identificadores únicos;* esto es, de IDs únicos y estables a los que vincular los fragmentos de identidad que se van recogiendo de una persona. En la India, por ejemplo, se ha procedido a instaurar un sistema de identificador que a partir de la información biométrica de una persona le otorga una numeración única y distinta respecto del resto de los cientos de millones de personas que habitan en dicho país.

Universitat d'Alacant
Universidad de Alicante

En ambos casos, y con el soporte de un sistema automatizado que garantiza un reconocimiento en el menor tiempo posible, el planteamiento de estos sistemas de reconocimiento descansa en la idea de que "el cuerpo nunca miente" y que resulta prácticamente imposible imitar (o suplantar) las características biométricas de otra persona[38]. Convertida la huella dactilar de alguien en un algoritmo digital singularizante, la aparente comodidad de colocar la huella en un escáner en vez de tener que completar extensos formularios de registro, permitiría potencialmente ir acumulando nueva información a toda la que ya tengamos asociada a dicha huella. Si esto es

[36] SAUNDERS, K. M. / ZUCKER, B. "Counteracting Identity Fraud in the Information Age", *Cornell Journal of Law*, 1999/8, pp661-663; DOTSON, K. A. "Your Good Name", *Quinnipiac Law Review* (QLR), 2004, pp611-612; TOWLE, H. K. "Identity Theft", *Rutgers Computer*, 2004, pp237 y ss.

[37] DOBRIŠEK, S.:" Workshop report. Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, security and defense", en *HIDE Newsletter*, vol. 2 (7), 2009, pp2 y 3.

[38] INTRONA, L. D. / NISSENBAUM, H. *Facial Recognition*, cit., pp9-10; REID, P. *Biometrics for Network Security*, Upper Saddle River, Prentice Hall PTR, Nueva Jersey, 2004; BOLLE, R./ CONNELL, J. H./ ET ALTERE, *Guide to Biometrics*, Springer, 2004.

posible desde el punto de vista científico y técnico, si resulta o no aceptable desde el punto de vista ético y en qué medida lo permitiría la legalidad vigente, son preguntas a las que se busca respuesta con la presente investigación.

1.2. Biometría, Antropometría e identificación biométrica: precisiones históricas y primeras delimitaciones conceptuales.

1.2.1. El concepto clásico de *Biometría* (en la definición propuesta por FRANCIS GALTON) y el de *Antropometría.*

En la literatura reciente encontramos la voz Biometría como referida al *reconocimiento automatizado de individuos basado en sus características comportamentales o biológicas*[39]. El foro *EuBiometrics* completa esa definición escogiendo como ejemplos las técnicas de reconocimiento basadas en huellas dactilares, escaneo del iris o la retina, la captación de la geometría manual o dactilar, los patrones de voz y otras técnicas como el reconocimiento facial. Pero se trata ésta de una acepción nueva y limitada de la voz biometría, que se aleja del sentido que se dio originariamente al concepto y que aún hoy día se maneja en las Ciencias biológicas y biomédicas. De hecho, en la reunión de 1998, en Sudáfrica, el presidente de la *International Biometrics society* afirmó que habían registrado la expresión *biometrics* como marca comercial para evitar la tendencia popular a emplear esa voz para referirse a las técnicas de reconocimiento automatizado[40]; pero parece que de poco sirvió.

En el lenguaje común se está relegando el uso de la expresión en sentido amplio, en el sentido de "*estudio mensurativo o estadístico de los fenómenos o procesos biológicos*". La voz Biometría etimológicamente proviene de las voces griegas *bios=vida* y *metron=medir*. Esa acepción agrupa, en sentido amplio, a todos los estudios que persiguen contribuir al conocimiento biológico a través, entre otras cosas, del establecimiento de variables continuas[41]. En ese punto, en la coincidencia de que estamos ante algo que tiene que ver con lo vivo y con las medidas, coinciden prácticamente todos los que hacen uso de la voz Biometría (Biométrie, Biometry, Biometrie).

---

[39] ISO 2006a. Citado por BUSCH, C.: "Biometrische Verfahren – Chancen, Stolpersteine und Perspectiven", en P. SCHAAR, cit.. 2007, p29; TELETRUST DEUTSCHAND, G. LASSMAN, *Bewertungskirterien zur Vergleichbarkeit Biometrischer Verfahren*, 2002.

[40] WILSON, S. R. "Evolution and Biometry", Biometrics 55, nº2/ 1999, p334.

[41] HOCKING, R. R. "A Biometrics Invited Paper: the Analysis and Selection of Variables in linear regression", *Biometrics. International Biometric Society*, vol. 1/32, 1976, pp1-49; CATTELL, R. B. "An Introduction to Essentials", *Biometrics. International Biometric Society*, vol. 21/1, 1956, pp1190-215.; BRILLINGER, D. R. The National variablity of vital rates and associated statistics, Biometrics, vol. 42/4, 1986, pp693-734.

1.2.1.1 *Medir humanos por qué y para qué*

El encuentro entre las Ciencias de la Vida y la métrica, advierte ALBRIZIO, representa *un inmenso capítulo* de la Historia de la Ciencia[42]. Comprende métodos matemáticos que son empleados con diferentes fines por la Biología, la Medicina o la agronomía, entre otros[43]. Los datos biométricos se emplean asimismo en la investigación y en las aplicaciones biomédicas, en este último caso con fines diagnósticos y/o terapéuticos[44].

Ya desde la Antigüedad se venía midiendo a los seres humanos con la intención de emplear los datos obtenidos para elaborar cánones de referencia en la arquitectura y en la escultura[45]. Entre los conocidos, el más antiguo fue hallado en una tumba en la que fuera capital del Antiguo Imperio egipcio (Menfis) y se calcula que data en torno al año 3000 a.C. Los artesanos Egipcios empleaban cuadrículas y proporciones estándares para producir imágenes humanas y de otro tipo, estableciendo fórmulas diferentes para los hombres y las mujeres [46]. Varios siglos más tarde, encontramos referencias en el escultor griego Policleto o del arquitecto romano Marco Vitruvio (siglo I a C), que en su libro *De Architectura* describe cómo si un hombre está tumbado sobre su espalda, con sus manos y pies extendidos, sus dedos tocarán la circunferencia imaginaria trazada tomando como centro su ombligo[47]. Este último se interesó por las proporciones del cuerpo y el uso de éstas como referencia metodológica en la arquitectura. En alusión a este arquitecto dio Leonardo Da Vinci el nombre de "*El hombre de Vitruvio*" al famoso dibujo que en la actualidad es el logotipo de la moneda de un Euro que acuña la República de Italia (IMÁGENES 7 Y 8).

Cabe citar, asimismo, ejemplos sobre sus usos industriales, especialmente en casos en los que es necesario establecer el espacio que un ser humano medio necesita para desenvolverse (por ejemplo en un avión, un asiento de cine o un pupitre escolar)[48], en el diseño ergonómico de

---

[42] ALBRIZIO, A. "Biometry and Antrophometry", *Journal of Anthropological Sciences*, vol. 85, 2007, pp101-123, p102-106; ABS, M. "Biometrik", 1971, págs. 945-946; GHILARDI, G./ KELLER, F. "Epistemological Foundations of Biometrics", en *Second Generation*, pp24-25.

[43] Con más referencias, SCHAAR, P. (ed.), *Biometrie Und Datenschutz*, 2007, págs. 7-8.

[44] ZHANG, D. / SONKA, M. (eds), *Medical Biometrics*, Springer 2010.

[45] SPENCER, F. (ed.), *History of Physical Anthropology: an Encyclopedia*, vol I, 1997, voz *Anthropometry*, cita entre otros el tratado de DURERO: DÜRER, A. *Bücher von menschlicher Proportion* (Cuatro libros sobre las proporciones humanas, publicados póstumamente en 1528).

[46] ROBINS, G. *Proportion and Style in Ancient Egyptian Art*, University of TexasPress, Austin, 1994.

[47] MARCUS VITRUVIUS, *De Architectura*, Book III, Chapter 1, p3.

[48] GOUVALI, M. K./ BOUDOLOS, K. "Match between school furniture dimensions and children's anthropometry", *Applied Ergonomics* 37 (2006), 765-773; FAIZ SYUAIB, M. "Anthropometric study of farm workers on Java Island, Indonesia, and its implications for the design of farm tools and equipment", *Applied Ergonomics* 51

muebles o máquinas que debe manejar un ser humano, así como en el diseño de prendas de vestir o complementos ajustados al cuerpo[49]. Quizá se recuerde la polémica que en 2007 suscitó en España una iniciativa del Gobierno destinada a promocionar *cánones de belleza saludable*. Al efecto, se firmó un acuerdo con la *Asociación de Creativos de Moda* que incluía, entre otras cosas, la realización de un estudio antropométrico a 8500 mujeres de entre 12 y 70 años con la finalidad de conocer las medidas corporales más frecuentes en la población española y unificar las tallas de la ropa que se comercializa[50].

La toma de datos biométricos con estos fines se hace en la actualidad tanto de forma manual como con el apoyo de sistemas parcial o totalmente automatizados. Así, entre estos últimos, hemos encontrado en la literatura la referencia de sistemas de análisis respiratorio que detectan elevados niveles de acetona y pueden emplearse en la detección y tratamiento de la diabetes[51]; sistemas digitales que procesan las huellas plantares de los recién nacido con fines de investigación o su llanto con el objetivo de detección precoz de afectaciones en el sistema nervioso central[52]; así como sistemas de Biometría vocal que contribuyen a la detección precoz del Parkinson[53].

1.2.1.2. *Biometría y Antropometría*

Resulta difícil explicar porqué se ha adoptado la expresión *Biometría* (en lugar de *Antropometría*) como disciplina que sirve de soporte a los sistemas de reconocimiento de seres humanos. Tradicionalmente se había venido empleando la primera de las voces para los estudios de los fenómenos biológicos –con independencia del organismo que fuera objeto del estudio-

(2015), 222-235; HSIAO, H./ WHITESTONE, J./ WILBUR, M./ ROGER, J. LACKORE/ ROUTLEY, J. G., "Seat and seatbelt accommodation in fire apparatus: Anthropometric aspects", *Applied Ergonomics* 51 (2015), 137-151.

[49] YOKOTA, M. "Head and facial anthropometry of mixed-race US Army male soldiers", *Applied Ergonomics* 36 (2005), pp379-383, estudio destinado a ajustar los respiradores y las máscaras de protección ante riesgos químico-biológicos.

[50] Acuerdo firmado el 23 de enero de 2007 entre, de una parte, el Ministerio de Sanidad y consumo (Ministra Doña Elena Salgado), y, de otra, la *Agrupación Española de Género de Punto, la Federación Española de Empresas de la Confección*, junto con empresas como El Corte Inglés, Cortefiel, Inditex y Mango, para homogeneizar la información de las tallas y promover una imagen saludable; vid. detalladamente LLANOS, M. "Modelos: riesgo, profesión y vacío legal", *Trastornos de la Conducta Alimentaria* 5/ 2007, pp507-543.

[51] ZHANG, B/ KUMAR, B. V./ ZHANG, D. "Detecting Diabetes Mellitus and Non- Proliferative Diabetic Retinopathy using Tongue Color, Texture, and Geometry Features,", *IEEE Trans. on Biomedical Engineering*, 2013.

[52] DING, S./ ZHU, H./ JIA, W./ ET ALT, "A survey feature extraction for pattern recognition", *Artificial Intelligence Review*, 2012.

[53] GUO, P. F. / BHATTACHARYA, P./ ET ALT, "Advances in Detecting Parkinson Disease", I*CMB* 2010, LCNS 6165, pp306-314.

reservando la expresión Antropometría para referirse a determinados estudios específicamente relacionados con las dimensiones del cuerpo humano.

Aunque hay expertos que usaron la voz años antes que él[54], la primera definición formal de *Biometría* se atribuye a Francis GALTON (1822-1911)[55] –IMAGEN 15-. Él y Karl PEARSON (1857-1936), fundadores de la revista *Biometrika* son considerados los pioneros de la Biometría, por su contribución a la introducción sistemática de métodos cuantitativos en el estudio de los fenómenos biológicos. En el primer número de la revista *Biometrika* (1901) –IMAGEN 11- GALTON explicaba que el objetivo de esta disciplina es el de *proporcionar materiales que, del modo más exacto posible, nos permitan descubrir hasta el más pequeño de los cambios que incesantemente fluyen en el mundo orgánico*. Fue a partir de la citada publicación cuando comenzó a hacerse un uso frecuente del término. En esa tesis de GALTON se fijó Ronald FISHER (1890-1962) cuando describió la *Biometría* como una búsqueda del conocimiento biológico por medios cuantitativos[56], independientemente de que se realice con fines biomédicos, biocientíficos o de otro tipo[57]. En términos similares, la Sociedad internacional de Biometría, fundada en 1947 y con presencia en más de 60 países, se describe a sí misma como promotora del "*desarrollo y la aplicación de la teoría y los métodos matemáticos y estadísticos a las Biociencias, incluyendo la agricultura, las ciencias biomédicas y la salud pública, la ecología, las ciencias ambientales forestales y disciplinas afines"*[58].

El término *Antropometría*[59], por su parte, se atribuye a Johan Sigismund ELSHOLTZ (1633-1688). Los historiadores afirman que ELSHOLTZ diseñó un sistema de medidas para investigar la relación intrínseca que según HIPÓCRATES existía entre las proporciones del cuerpo humano y algunas enfermedades. Sobre esa base ELSHOLTZ diseñó una serie de estudios de las proporciones del cuerpo humano con fines biomédicos. Desde entonces, el significado del término *Antropometría* se ha enriquecido con aportaciones muy diversas y fue a partir de la segunda mitad

[54] En 1841 Christoph BERNOULLI empleó la expresión *biometría* para referirse a tomas de medidas en seres humanos con fines estadísticos. Vid. SABOROWKSI, M. "Die Pluripotenz der Biodaten. Beobachtungen zu einem Verwertungsgeschehen", en POTTHAST, T./ HERRMANN, B./ MÜLLER, U. (eds.), *Wem gehört der menschliche Körper?*, Mentis, Paderborn, 2010, p380.

[55] BULMER, M. *Francis Galton: Pioneer of Heredity and Biometry*, John Hopkins Univ. Press, 2003; MORDINI, E./ MASSARI, S., *Bioethics J*, 2008, p489.

[56] Destaca entre sus trabajos "The Correlation Between Relatives on the Supposition of Mendelian Inheritance", *Trans R. Society Edinb* 52, 399-433, (1918), en el que procediendo a medir los rasgos y fijando las variables continuas, abordaba la heredabilidad de aquéllos.

[57] STIGLER, S. M. "The Problematic Unity of Biometrics", *Biometrics* (Journal), 2000, p654.

[58] http://www.biometricsociety.org/about/

[59] GIULIANO, A. *Dieci e tutti diverse o Studio sui dermatoglifi umani*, 2004, pp1ss.

del siglo XVIII cuando el término se adoptó de forma amplia, acercándose prácticamente a una *Biometría especializada en el ser humano*. Entre las aportaciones destacadas en este sentido, hay que mencionar al matemático belga QUETELET.

QUETELET estructuró la Antropometría en 1870, con su libro *Anthropométrie,* aunque la historia de la Antropometría física comienza a contarse a partir del siglo XVIII, con los trabajos de C. LINNEO (1707-1778), BUFFON (G.L. Leclerc, 1707-1788) y G. WHITE (1720-1793) para la comparación racial. Es considerada una especialidad dentro de la antropología biológica y abarca el estudio de las dimensiones y medidas humanas con diferentes propósitos. Entre ellos, la comprensión de los cambios físicos que se producen a lo largo del ciclo vital, o las diferencias entre las etnias. Tras un extenso estudio mensurativo QUETELET advirtió que los datos biométricos de las personas varían en torno a determinados promedios que parecen constantes; formuló el que aún se conoce como Indice Quetelet – o índice que determina el peso ideal de una persona – así como un concepto de *hombre medio*[60]. Sin embargo, en su obra "*Sur l'homme et le developpement de ses facultés. Essay d'une physique sociale*" (1835) Quetelet amplió su estudio tratando de establecer las reglas que determinan al ser humano desde una perspectiva fisiológica, intelectual y moral, sus conclusiones en relación con estas dos últimas perspectivas fueron muy criticadas.

1.2.1.3. *Biometría y características psíquicas: algunas notas*

El médico alemán Franz Joseph GALL (1758-1828) mostró fascinación por la hipótesis de una vinculación que el carácter y la capacidad tenían con el cerebro y la apariencia física de las personas. Defendió la disciplina de la craneoscopia (posteriormente conocida como frenología), como método para determinar la personalidad y el desarrollo de las facultades mentales y morales con base en la estructura craneal. Esta perspectiva de estudio guarda relación con la fisiognomía de César LOMBROSO (1835-1909), que consideraba posible establecer una correlación entre las características físicas –especialmente las características craneales y faciales- y determinados rasgos de la personalidad[61]. Proyectó sus conclusiones en la esfera de la criminalidad y en 1872 presentó su tesis sobre la existencia de una serie de rasgos biológicos y psíquicos característicos del *uomo delincuente*[62] -IMAGEN 10-. En su opinión, aún antes de que delinquieran, existía una base suficiente como para considerar que las personas que presentaban

[60] KINDT, E. *Privacy and Data Protection*, 2013, p17.

[61] GATTI, U. / VERDE, A., "Cesare Lombroso: Methodological ambiguities and brilliant intuitions", *International Journal of Law and Psychiatry* 35 (2012), 19-26.

[62] CURTO, D. R. (1995): "Crimes e Antropologia Criminal", *Revista Lusitana,* n°13-14. pp.179-199; URRUELA MORA, A. "La actual discusión sobre las bases genéticas de la criminalidad", en *Características Biológicas, Personalidad y Delincuencia*, 2003, p.131; DEL MISMO AUTOR, *Imputabilidad penal y anomalía o alteración psíquica*, 2003, pp339-342.

dichos rasgos eran una suerte de *delincuentes natos*[63], tesis sobre la que continuaron trabajando sus discípulos GAROFALO y FERRI[64].

Muchas de las conclusiones de los estudios que vinculaban elementos anatómico-físicos y perfiles de personalidad, o de quienes defendían un determinismo biológico de la criminalidad fueron rebatidas por la comunidad científica, aunque algunos sistemas totalitarios encontraron en ellos argumentos para cometer atroces crímenes contra la humanidad. Existe, con todo, un debate que no se ha cerrado del todo y que, como se verá en la exposición de resultados, en cierta medida se ha vuelto a reavivar con ocasión de los sistemas de reconocimiento biométrico de segunda generación.

1.2.1.4. *La Biometría que sirve de base a los sistemas automatizados de reconocimiento: la acepción estricta*

La acepción estricta, contemporánea, de Biometría se aleja de la original en dos sentidos. En primer lugar, cuando se habla de Biometría en el contexto de las tecnologías automatizadas de reconocimiento, se está haciendo referencia a estudios mensurativos sobre los seres humanos, mientras que el concepto amplio se aplica sobre cualesquiera organismos vivos. Una segunda diferencia, es que más allá del establecimiento de variables continuas existe un objetivo de establecer métricamente la singularidad de un sujeto respecto de un conjunto, hasta el punto que permita su reconocimiento indubitado respecto al resto.

Es decir, que se emplea la expresión *Biometrics* para referirse a los sistemas automatizados de identificación de seres humanos y existe una tendencia, en algunos foros, a referirse con la expresión *Biometry* a la disciplina que sirve de soporte a estos sistemas de reconocimiento. Así, la *Encyclopedia of Genetics, Genomics, Proteomics and Informatics* (2008), describe como *Biometric* la codificación electrónica de una característica física (huella dactilar, escaneado del iris) y que puede ser empleada en la identificación personal digital. Y en el *Biometric Institute Privacy Code* (2006) se define como tal una característica biológica o comportamental única de un individuo que es capturada por un sistema automatizado con el propósito de identificación o verificación.

---

[63] SERRANO MAÍLLO, A. "La posición de las variables biológicas en la teoría criminológica contemporánea", en *Características Biológicas*, 2003, pp49-53.

[64] Vid. GARÓFALO, R. *La Criminología. Estudio sobre el delito*, 1900, pp142 y ss –versión digital DOI:968-7804-11-4-; FERRI, E. *Principios de Derecho Criminal* (trad. J. A. RODRÍGUEZ), Reus, Madrid, 1933, pp45 y ss.

1.2.2. Categorías de estudios y de datos biométricos.

La medición aplicada a los seres vivos y su procesamiento matemático han dado pie a multitud de categorías biométricas que son difíciles de sistematizar de cara a una presentación conjunta. Aquí se ha optado por reseñar dos categorías que resultan especialmente útiles de cara a la exposición de los resultados de esta investigación. En primer lugar la clasificación o categorización tripartita que realizó IRWIN en 1959 y que consistió en agrupar los estudios biométricos atendiendo a las características del grupo de población que hubiera sido tomado como muestra de referencia. En segundo lugar se presta atención a la clasificación o categorización entre datos biométricos *estructurales* y datos biométricos *dinámicos*, que –con matices diferenciales- algunos autores expresan como datos biométricos físicos y datos biométricos comportamentales.

1.2.2.1. La Clasificación tripartita de IRWIN: tipología de estudios biométricos atendiendo a su objeto

Según IRWIN[65], los estudios biométricos pueden clasificarse en 3 categorías atendiendo al objeto de estudio biométrico. Encontramos así:

a) Estudios que implican la toma de medidas a *amplios grupos de individuos* o, incluso *a toda una población*[66].

b) Estudios que implican la toma de medidas aplicada a *pequeños grupos de individuos.*

c) Estudios que implican la obtención de los datos biométricos de *un individuo que ha sido identificado*. Estas tomas de datos no se refieren sólo a informaciones biométricas con perfil singularizante, si no que comprenden también lo que algunos autores describen como biomarcadores[67], incluyendo desde medidas macroscópicas (como la talla o el peso corporales), como medidas para cuya obtención son necesarios instrumentos más complejos e incluso análisis de laboratorio, como sucede en el estudio mensurativo de los componentes sanguíneos (hematimetrías).

---

[65] IRWIN, J. O., "Biometric method: past, present, future", *Biometrics*, 1959, nº 15, pp363-365, p366.

[66] BULMER, M.: *Francis Galton: Pioneer of Heredity and Biometry*, 2003; MORDINI, E./ MASSARI, S. en *Bioethics J.*, 2008, p489; SCHNEIDER, W., "Towards the impact of the Human Race: The history of eugenics in Modern France", en *Journal of Modern History*, 1982, vol. 54, n. 2 Jun 1982, pp.268-291; PROCTOR, R. (1988): "From Anthropologie to Rassenkunde", en *Bones Bodies, Behaviour*, STOCKING, G. W. (ed.) Madison, University of Wisconsin.

[67] Con más referencias, HANK, K./ JÜRGES,H./ SCHAAN, B., „Die Erhebung biometrischer Daten im Survey of Health, Ageing and Retirement in Europe. Befunde und Perspectiven", *Methoden – Daten-Analysen*, 2009 3(1), pp97ss: son datos intercambiables con los que es posible referirse a datos que miden características físicas de una persona.

En los años 60, cuando IRWIN publicaba esta distinción, la Biometría todavía prestaba más atención a las poblaciones que a los individuos singulares. A partir de Bertillon, como se verá en el próximo apartado, consideran los historiadores que se impulsa definitivamente la rama de la Biometría que orienta sus aplicaciones a la identificación inequívoca de las personas[68]. Esta es la base sobre la que tiempo después se terminarán creando infraestructuras informáticas que, si bien con más precisión y en menos tiempo[69], siguen consistiendo en comparar los rasgos de un individuo con aquellos que en su día fueron fichados y almacenados en algún tipo de soporte. En la actualidad, la asociación entre la Biometría y los sistemas de reconocimiento tiene tal relevancia que tiende a ser la acepción que prevalece en el uso corriente de la voz *dato biométrico*.

1.2.2.2. Clasificación bipartita de los datos biométricos atendiendo a la tipología de las características humanas de las que son tomados: estáticos y dinámicos.

La segunda categorización que nos interesa es la que clasifica las características biométricas – o los datos que se toman de éstas- en estructurales y dinámicas. Ha de advertirse que, aunque no de forma unívoca, se emplean en la literatura las distinciones entre datos biométricos anatómico-físicos y comportamentales, o datos biológicos, fisiológicos y comportamentales. En nuestra opinión, y como se explicarán a continuación, no todos los datos dinámicos encajan en la categoría de comportamentales aunque la literatura emplea con mayor frecuencia este último término para referirse al conjunto de los datos dinámicos. Además de a estos conceptos, se prestará atención a continuación a las características biométricas que los distintos autores agrupan en una u otra categoría.

Universitat d'Alacant
Universidad de Alicante

1.2.2.2.a *Datos biométricos estáticos*

Se describen como datos biométricos anatómico-físicos aquellos que se obtienen en un *momento puntual* a partir de las *características anatómico-físicas de un ser humano*[70]. Destacamos esos dos elementos, el temporal y la referencia a la estructura corporal como elementos distintivos de este conjunto de datos, porque consideramos que es la conjunción de ambos las que los distingue del segundo grupo de datos al que nos vamos a referir.

---

[68] APARICIO SALOM, J. A. *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 2000, p54; BIASOTTI, A. *Le tecnologie biometriche. Sicurezza, contrattualistica e privacy*, 2002, p13.

[69] GARFINKEL, S. *Database Nation: The Death of Privacy in the 21st Century*, 2000, Chapter 3; ALTERMANN, A. "A Piece of your Self", 2003, pp139s..

[70] PEACOCK, C./ GOODE, A./ BRETT, A. "Automatic forensic face recognition from digital images", *Sci Justice*, 2004 jan-Mar, 44 (1), 29-34.

En el área de la Antropometría se emplea la diferenciación entre Antropometría estática y Antropometría dinámica o funcional para distinguir las tomas de medidas con el cuerpo en una posición fija y determinada de aquellas otras en las que la toma de medidas se realiza teniendo en cuenta, por ejemplo, el movimiento corporal asociado a determinadas actividades. En nuestra opinión ese elemento temporal es muy relevante para distinguirlos de los datos dinámicos, aunque la literatura contemporánea no hace tal precisión.

Pueden, por ejemplo, obtenerse datos biométricos *anatómico-físicos* o estáticos del escaneado de las huellas dactilares, de la captación de la geometría de la mano, de la obtención del patrón del iris o del fondo venoso de la retina, así como –por ejemplo- de la composición química del olor corporal[71]. En todos esos casos en un momento puntual se capta del sujeto lo que se conoce como *muestra biométrica* o *dato en crudo* y sobre esa muestra se procederá a realizar el estudio mensurativo que dará como resultado el dato o patrón biométrico. Quiere ello decir que aquellos parámetros corporales que pueden tomarse de forma estática –en un momento temporal fijo- quedarían también comprendidos en este conjunto, a diferencia de aquellos parámetros que – como se verá en el segundo grupo de datos – requieren algún tipo de monitorización de la personas.

En el capítulo primero de los resultados se abordará con más detalle la obtención de información biométrica a partir de estas características, pero se ofrece aquí una tabla con detalle de algunos ejemplos.

Universitat d'Alacant
Universidad de Alicante

FUENTES DE BIOMETRÍAS "ESTATICAS"	CARACTERÍSTICA A MEDIR
Huella dactilar	Forma de los dermatoglifos; localización de las minucias.
Geometría de la mano	Longitud, grosor y situación de los dedos; perfil de la mano, etc.
Iris	El patrón del iris en torno a la pupila del ojo.
Retina	El patrón de la circulación sanguínea en el fondo del ojo.

[71] BEHRENS, M./ ROTH, R. (eds), *Biometrische Identifikation*, 2001, p13; BREITENSTEIN, M. "Überblick über Biometrische Verfahren", 2002, pp35ss.

Rostro	Características geométricas típicas, como las medidas y distancia entre los ojos, la nariz, la boca, las cejas, etc.

Tabla: Principales características biométricas de tipo físico o fisiológico[72]

1.2.2.2.b *Datos biométricos dinámicos*

El de Biometría dinámica o comportamental es el conjunto más complejo de datos. En la Opinión 80/ 2003 el GT-WP se refería a estos como datos obtenidos de "características fisiológicas", por oposición a las anatómico-físicas, y en el año 2012 completó esa descripción refiriéndose a este conjunto como "*datos obtenidos de fuentes biométricas dinámicas*" [73]. Más allá de esa descripción genérica, lo cierto es que no se ha consensuado aún una única categorización y la literatura discrepa a la hora de situar en uno u otro grupo determinados datos biométricos[74]. La tendencia es de la ubicar en este grupo todos los datos biométricos que *no se han obtenido de una característica o rasgo físico*[75], aunque se discute cuál debe ser la ubicación más adecuada para el caso de las señales corporales o datos biométricos obtenidos de la medición de determinados parámetros corporales. Ello implica agrupar datos entre los cuáles hay importantes diferencias.

Entre las descripciones más detalladas están la que recoge el informe ENISA[76] y la publicada por YAMPOLSKI/ GOVIDARAJU[77]. En ambas descripciones se distinguen tres subgrupos en esta categoría de datos:

1) *Datos obtenidos de las habilidades motoras* (basados en el control y movimiento muscular). Es el caso de los datos biométricos obtenidos, entre otros: del modo en que una persona firma o escribe; de la mecánica de su habla o del espectro de su voz; de la dinámica de los rasgos faciales, o del modo en que emplea un teclado o un ratón de ordenador.

[72] BEHRENS, M./ ROTH, R. (eds), *Biometrische Identifikation* (2001) 13; BREITENSTEIN, *Überblick Über Biometrische Verfahren*, en NOLDE, V. /LEGER, L. (ed.), *Biometrische Verfahren*, 2002, pp35ss.

[73] Documento WP 193, Opinión 1/2012.

[74] Los advierten WANG, L./ GENG, X. en su manual *Behavioral biometrics for human identification*, 2009; SCHÜMACHER, G. "Behavioural Biometrics: Emerging Trends and Ethical Risks", en *Second Generation*, p216.

[75] *Glossary of Terms for Voice Biometrics*, Biometric Security Ltd. 2009.

[76] ENISA. *ENISA briefing: Behavioural biometrics*. European Network and Information Security Agency, 2010,.

[77] YAMPOLSKY, R./ GOVINDARAJU, V. "Behavioural biometrics", *International Journal of Biometrics* 2008 1(1): 81–113; SCHUMACHER, "Behavioral biometrics"m pp218 a 220.

2*) Señales corporales o datos biométricos obtenidos de la medición de determinados parámetros corporales*. A modo de ejemplo cabe citar los electrocardiogramas, perfiles de temperatura corporal, actividad cerebral (electroencefalograma), frecuencia de la respiración, parpadeo de los ojos, transpiración y agitación (como parámetro cambiante ante el estrés). El proyecto FAST del Departamento de Seguridad Interior de los Estados Unidos, por ejemplo, persigue detectar las (malas) intenciones de los sujetos en determinadas señales comportamentales y motoras, y evitar así su ejecución.

3) *Información biométrica que se obtiene de la interacción con máquinas o dispositivos automatizados* (programas, juegos, patrones de compra, análisis del fraseado en los email o conversaciones, etc.).

En nuestra opinión, es posible reconducir estas tres categorías a solo dos. Lo característico de las Biometrías dinámicas es la captación de información generada por el funcionamiento del cuerpo humano durante un lapso más o menos amplio de tiempo. Consideramos que las dos fuentes principales de dicha información son, de una parte, los datos que se obtienen de las habilidades motoras y, de otra parte, las señales y parámetros corporales. Estos autores incluyen un tercer grupo sobre la base de aquellos casos en los que la información se genera a partir de la interacción con máquinas o dispositivos, pero la información a obtener creemos que será en todo caso agrupable en una de las dos primeras categorías; eso es, al interactuar con la máquina el cuerpo de la persona pondrá en funcionamiento alguna habilidad motora o, en su caso, expresará señales corporales que serán objeto de captación biométrica. Asimismo, creemos que, la captación de los datos biométricos a los que se refieren el primero y el segundo de los conjuntos puede realizarse con implicación activa del sujeto o sin que éste interactúe con el sistema de reconocimiento automatizado. En coherencia con esta consideración, entendemos que no es adecuado el uso de términos como los de características pasivas y características activas para distinguir entre las fuentes de datos biométricas estáticas y las fuentes de datos biométricas dinámicas.

FUENTES DE BIOMETRÍAS DINÁMICAS	CARACTERÍSTICA A MEDIR
La firma dinámica	La figura y el trazo de la firma, la velocidad, la presión, etc.
La voz	Espectro acústico.

El Movimiento corporal	Oscilación en el torso, contoneo de caderas, forma en la que doblan las rodillas y tobillos, etc.
La forma de teclear	Ritmo de tecleado, Velocidad, presión, corrección, comportamiento durante las pausas, etc.
Señales corporales	Ritmo de la respiración o agitación ante determinados estímulos, obtención de señales que captan el funcionamiento del cerebro, patrones del latido cardíaco, etc.

Tabla: Principales características biométricas comportamentales[78]

1.2.3. La primera experiencia biométrica, en el sentido actual del concepto: el sistema antropométrico de identificación diseñado por Alphonse BERTILLON (el *Bertillonage* o *signalement anthropométrique*).

1.2.3.1 El signalement anthropométrique: un hito en la historia del reconocimiento mediante Biometría

A pesar de que investigadores como GALTON concentraban su atención en estudios poblacionales –y no tanto en individuos singulares- los trabajos que abordaron aquellos *rasgos mensurables de los seres humanos, sean físicos o comportamentales,* advertían con frecuencia de la potencialidad de la Biometría en relación de cara al reconocimiento de los individuos. Es el caso, entre otros, de las investigaciones de antropólogos como Paul BROCA, fundador de la Sociedad de Antropología de París. Antes de que GALTON acuñase el término *Biometry*, BROCA venía empleando medidas y cálculos estadísticos en la descripción de las características de grupos de individuos. Por cuanto se refiere propiamente a la toma de medidas con fines de identificación, será clave un discípulo de su escuela: Alphonse BERTILLON.

El sistema antropométrico de identificación de delincuentes de BERTILLON se considera el primer hito destacado en la aplicación histórica de la Biometría con fines de con la finalidad de evitar la agravación en la pena que solía acarrear la reconocimiento. El 31 de agosto de 1832 se abolió en Francia la marca de fuego de los condenados y, desde el punto de vista práctico, determinar en qué casos un delincuente merecía una sanción agravada, en tanto reincidente, se

[78] Lo incluyó POLEMI en el Informe *ETS Biometrics*, 1997, p 5; también el IPTS, en el informe *Biometrics at the Frontiers,* 2005, p17; BEHRENS, M./ ROTH, R. (eds.), *Biometrische Identifikation*, 2001, p13; BREITENSTEIN, M. "Überblick über Biometrische Verfahren", 2002, pp35ss.

hizo más complejo. La única referencia eran los archivos documentales pero, como es comprensible, los delincuentes reincidentes trataban de ocultar su identidad civil para evitar que se les aplicase la agravante por reincidencia. Se comprende y comenzó a ser frecuente que los delincuentes reincidentes tratasen de ocultar su identidad civil para evitar que se les impusiera una agravación de la condena por reincidencia[79].

Esa y otras circunstancias propiciaron la aparición de un cuerpo especializado dentro de la policía: la llamada policía técnica[80]. A finales del siglo XIX los ficheros judiciales franceses contaban con datos de más de 5 millones de personas, si bien la consulta de los ficheros en papel, clasificados por orden alfabético, no resultaba muy operativa. Nótese que en el caso de que el detenido no facilitase su nombre o falsease su identidad, las posibilidades de asociarlo con una de las fichas almacenadas dependería de la confluencia de circunstancias tales como el hecho de que algún testigo pudiera ofrecer información o al menos indicios que llevasen al nombre (real o no) con el que el individuo estuviera ya fichado. Será el reconocimiento mediante características físicas el que hizo progresar estas tareas. Alphonse era hijo del antropólogo y estadista Louis Adolphe BERTILLON[81], miembro fundador de la *Escuela de Antropología de París de Paul BROCA*[82]. Se incorporó en 1879 a la Prefectura de Policía de París, con la tarea de elaborar una serie de fichas "signaléticas" (en español vendría a ser algo así como *señaléticas*) [83] de determinados individuos. VÉANSE LAS IMÁGENES 13, 14, 15.

Apasionado de la ciencia aplicada al ser humano, se había interesado anteriormente en los trabajos de Lambert QUETELET , quien como se ha visto afirmaba que no existían sobre la tierra dos esqueletos humanos de medidas completamente idénticas. Demostró también que algunos huesos humanos no experimentaban modificaciones después de los 20 años de edad. En sus fichas BERTILLON registraba detallada información sobre los individuos. Describía marcas individuales como tatuajes y cicatrices y algunas características morfológicas como el color del pelo y de los ojos, y además tomaba fotografías y medidas antropométricas siguiendo, se ha dicho ya, las

---

[79] AUGER, D. *Biométrie: l'équilibre entre «liberté individuelle» et promesse sécuritaire serait-il impossible?*, 2005, pp26-27.

[80] DIAS, C. *La police technique et scientifique*, PUF, Paris, 2000, p12.

[81] SÁNCHEZ VIGIL, J. M./ FERNÁNDEZ FUENTES, B. "La fotografía como documento de identidad", *Documentación de las Ciencias de la Información*, 2005, vol. 28, pp189-195.

[82] SPENCER, F. (ed.), *History of Physical Anthropology: an Encyclopedia*, vol I, 1997, voz *Anthropometry* y voz *Bertillon*; JAIN, A. K./ FLYNN, P./ ROSS, A. A. (eds.), *Handbook of Biometrics*, Springer 2007.

[83] MADUREIRA, N. "Policía sin ciencia: la investigación criminal en Portugal: 1880-1936", *Política y Sociedad,* 2005, Vol. 42, núm. 3, pp45-62. Vid. A. BERTILLON, *Signaletic instructions including the theory and practice of anthropometrical identification*, Werner, Chicago, 1896.

técnicas desarrolladas por BROCA y sus colaboradores en el Laboratorio de Antropología de la *École Pratique des Hautes Études* de París. Esa será la base del diseño del sistema de "signalement anthropométrique" que desarrollará BERTILLON[84] y que sería conocido como *Bertillonage*. No se trataba únicamente de un sistema métrico, sino que vinculaba la información que se tenía de los sujetos con un sistema de descripciones métricas detalladas de sus cuerpos, basando en este último conjunto de datos la clasificación y ordenación de la base de datos manual.

Entre sus escritos más destacados están *La photographie judiciaire* (1890) y *L'Anthropologie métrique* (1909). Su sistema fue adoptado extensamente en occidente antes de la introducción de la dactiloscopia y consistía en tomar diferentes medidas de los detenidos (como la envergadura, el tamaño del cráneo o del codo, los pies o las orejas). En *Scotland Yard* lo introdujo Edward HENRY. Recogía fichas de los detenidos, detallando con precisión ciertas longitudes y anchuras de la cabeza y del cuerpo, como por ejemplo la longitud de los dedos de las manos[85].

1.2.3.2 *El mito de cómo la crisis del Bertillonage (supuestamente) impulsó el reconocimiento dactilográfico. El caso de los "dos Will West"*

En la narrativa histórica del reconocimiento mediante Biometría se ha venido insistiendo de forma recurrente en cómo *el caso de los dos Will West* (Will y William West*)* supuso la crisis definitiva del Bertillonage y su sustitución por la identificación mediante la impresión dactilar. En la actualidad se revisa críticamente esta forma de narrar los hechos, advirtiendo de que los datos sobre lo acontecido y sus consecuencias fueron publicados en las primeras décadas del siglo XX, en un momento en el que de forma interesada algunos sectores doctrinales querían impulsar definitivamente el uso de las huellas dactilares en la identificación.

Ciertamente, el *Bertillonage* planteaba dificultades relacionadas con la calidad de la toma de medidas y el hecho de que en algunos lugares se empleasen unidades métricas diferentes. Carecemos, sin embargo, de estudios que nos permitan conocer con detalle cuál era la tasa de error en la aplicación del *Bertillonage* y desconocemos, asimismo, qué porcentaje de los errores se debía al método y cuál a la falta de pericia de quien tomaba las medidas.

---

[84] STIGLER, S. M.: "Galton and Identification by fingerprints", en *Statistics on the Table*, 1999, pp131-189; HACKING, I. *The taming of chance*, 1990, pp186-188; COLE, S. A. *Suspected identities*, 2001.

[85] Detalladamente, TRUCCO, L., *Introduzione allo Studio dell'identità individuale nell'ordinamento costituzionale italiano*, 2004, pp24 y ss.

Muy distinto es lo sucedido en el caso West, en el que el capricho del azar atrajo una serie de circunstancias cuyo concurso, a todas luces, parecía extremadamente improbable. En el año 1903 llegó a la prisión de Leavenworth un nuevo recluso: *Will West*. Él insistía en que nunca antes había estado en dicha prisión, pero una persona de la secretaría de la administración decía conocerle sin el menor atisbo de duda. Analizados los ficheros, se obtuvo la ficha de un recluso anterior, que no sólo tenia las mismas medidas craneales que Will, sino que –como muestran las fotografías- guardaba con él un asombroso parecido[86].

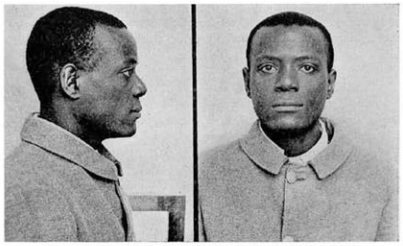


Fig. 5. The Bertillon photograph of Will West, No. 3426 of the United States Penetentiary at Leavenworth, Kans.

Por si ello fuera poco, el nombre recogido en aquella ficha no era otro que West, *William West*. La probabilidad de que existieran dos delincuentes, encarcelados en un relativamente breve lapso de tiempo en la misma prisión estadounidense, y que además coincidieran no sólo en medidas craneales sino también en el nombre se consideraba algo tan remoto, que es comprensible que en primer término se concluyera que se trataba de una única persona. Sólo la comparación de las huellas dactilares de Will con las de la ficha de William fue la que determinó que, tal y como aquel afirmaba, se trataba de dos personas diferentes (IMAGEN 18).

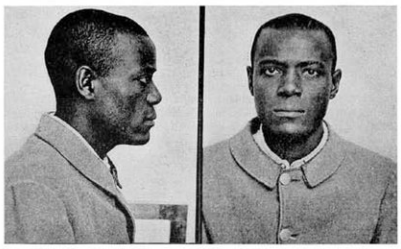


Fig. 6. The Bertillon photograph of William West, No. 2626 of the United States Penetentiary at Leavenworth Kans. This is a different man from the foregoing (Fig. 5.), bu has practically the same Bertillon measurements, and almost the same name. Both were at Leavenworth at the same time.

Coincidimos, con Simon A. COLE[87], en que no fue el caso de *los dos Will West* lo que desbancó al *Bertillonage*. A pesar de la identidad de medidas craneales, las fichas de ambos mostraban diferencias destacables en otras medidas corporales, como por ejemplo los pies. Al parecer el mito se creó veinte años después del suceso, para impulsar el uso de las huellas dactilares y alentado por voces que afirmaban que el *Bertillonage* – de origen europeo- no era adecuado para distinguir a los delincuentes de raza afroamericana o asiática, estadísticamente más frecuentes en el territorio norteamericano. Es fácil apreciar que comparativamente la obtención, clasificación, almacenamiento y comparación de las huellas dactilares resultaba mucho más sencilla que el *Bertillonage*, y que además facilitaba la distinción entre hermanos o gemelos que guardaban importantes semejanzas.

[86] SHONIREGUN, C. A. / CROSIER, S. *Securing Biometrics Applications*, 2008, p16.

[87] COLE, S. A. "Suspect Identities: A History of Fingerprinting and Criminal Identification" (Harvard University Press, 2002), en la entrevista que le hizo Errol MORRIS en "What's in a Name? (II)", *The New York Times*, 2012.

Fue esa constatación la que progresivamente fue haciendo que las medidas antropométricas dejasen de ser la única base de identificación policial y progresivamente se completasen con otros tipos de datos. Debe tenerse en cuenta, además, que si bien desde la década de 1880 existían referencias -aún sin método- sobre la posibilidad de una identificación cuantitativa de los individuos a través de sus huellas (de autores como Henry FAULDS, William HERSCHEL o Francis GALTON[88]), hubo que esperar aún unos años para que se propusieran métodos de obtención, clasificación y gestión de este tipo de muestras. La madurez de estos sistemas (como los de VUČETIČ o, en España, Federico OLORIZ AGUILERA[89]) coincidió temporalmente con *el caso West*, lo que sirvió de caldo de cultivo a la leyenda.

En los países anglosajones se había ido extendiendo el sistema que Scotland Yard adoptó en 1901 –con una oficina de fuellas dactilares dirigida por Edward HENRY. Éste había desarrollado un sistema de clasificación de las huellas cuando era administrador en Bengala (India) y completó el sistema propuesto por GALTON, dando lugar al que se conoce como sistema *Galton –Henry*. En Alemania se había adoptado el sistema de ROSCHER[90]. –IMAGEN 22-.

1.3. El reconocimiento biométrico contemporáneo y los factores que impulsan su desarrollo científico-tecnológico

1.3.1. La automatización de la captación de la información biométrica y de su procesamiento como elementos diferenciales

Universitat d'Alacant
Universidad de Alicante

El reconocimiento biométrico contemporáneo es el objeto de estudio de esta investigación, lo cual nos lleva a la necesidad de situarlo respecto de sus precedentes. Pero la comprensión del desarrollo de esta área científico tecnológica y sus niveles de implementación actual requieren, además, situar adecuadamente una serie de factores que han propiciado el impulso de estas tecnologías. Los sistemas de reconocimiento biométrico contemporáneo son descritos en la literatura como "*métodos automatizados de verificación o reconocimiento de la*

[88] WAYMAN, J./ JAIN, A./ MAIO, D. "An Introduction to Biometric Authentication Systems", en WAYMAN, J./ JAIN, A./ MALTONI, D./ MAIO, M. (eds,), *Biometric Systems. Technology, Design and Performance Evaluation*, Springer, 2008, pp18 citan los siguientes trabajos: FAULDS, F. "On the skin furrows of the hand", *Nature*, 22, 605, 28 de octubre de 1880; HERSCHEL, W. "Skin furrows of the hand", *Nature*, 23, 76, 25 de noviembre de 1880; GALTON, F. "Personal identification and description", *Nature*, 21 y 28 de junio de 1888, pp. 173–177, 201–202.

[89] ANTÓN BARBERÁ, F./ DE LUIS Y TARAGANO, J. V. *Policía científica*, 5ª edición, Tirant lo Blanch, 2004, p9.

[90] BARNES, J. C. *History of Fingerprints*, cit.

identidad de una persona viva con base en características fisiológicas o comportamentales" [91], descripción en la que destaca por su novedad el componente de *automatización*[92][93] aunque destaca también el objetivo de identificación que se atribuye a estas técnicas. Ello explica que algunos autores hablen de una *Biométrica* como ciencia emparentada –aunque diferente- respecto a la Biometría, definiéndola como "*la ciencia del establecimiento de la identidad de un individuo con base en sus atributos físicos, químicos o comportamentales*"[94] o "la ciencia de emplear información biológica con fines de identificación o verificación"[95]. –IMÁGENES 1, 2, 3 Y 55-.

Por otra parte, y aunque suele hacerse referencia abreviada al conjunto de estas tecnologías como *biometrics* o *biometric technologies*, en opinión de autores destacados como James WAYMAN o Anil K. JAIN, bien pudiéramos referirnos a estos sistemas como una "*autenticación antropométrica*" automatizada, en el sentido de que: en primer lugar, en la actualidad quedan fuera de este conjunto aquellos métodos de identificación forense que nos disponen aún de versiones tecnológicas[96]; y en segundo lugar, en tanto estos sistemas se emplean en una única especie: la humana. La propuesta terminológica ISO de 2012 matiza, además, que la expresión verificación o reconocimiento es más correcta que *autenticación*, lo cual nos dejaría el concepto en "*reconocimiento antropométrico automatizado*".

Otra diferencia sustancial reside en el hecho de que algunos sistemas de reconocimiento mediante Biometría –aunque no todos- no recogen más información sobre el sujeto fuente que la Biometría misma. En comparación con la Antropometría de GALTON o el *Bertillonage*, que concebían el cuerpo como una fuente complementaria de información, la Biometría contemporánea tiende a concebir el cuerpo como *única fuente* de patrones singularizantes que pueden almacenarse y a futuro compararse con nuevos patrones tomados del cuerpo. Si un patrón

[91]Con más referencias, WAYMAN, J./ JAIN, A./ MAIO, D. "An Introduction to Biometric Authentication Systems", en *Biometric Systems*, 2008, pp1-2.

[92] El *Biometrics Institute Privacy Code* (2006) los describe como "*métodos automatizados para identificar sobre la base de una característica biológica o comportamental única*".

[93] Vid. INTERNATIONAL BIOMETRICS GROUP (IBG), *How is "Biometrics" defined?*, en *Biometrics explained*, 2001; Documento de la OCDE - WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based Technologies*, 2004, pp10-11; NANAVATI, S. / THIEME, M./ NANAVATI, R. *Biometrics. Identity verification in a networked World*, 2002, p15 yss; SETHI, I. K.: "Biometrics", en STRANDBURG, K. J. / RAICU, D. S. *Privacy and Technologies of Identity. A Cross-Disciplinary Conversation*, Springer, 2006, pp117-134.

[94] JAIN, A. K./ FLYNN, P./ ROSS, A. A. *Handbook on Biometrics*, Springer, 2008, p. 1

[95] MAGNET, S. A. *When Biometrics Fail: Gender, Race and the Technology of Identity,* 2011, p 21.

[96] MEUTH, L. *Zulässingkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen*, Duncker& Humblot, Berlin, 2005, pp35-36.

en fresco coincide con el almacenado previamente el sujeto será re-identificado; y si los patrones no coinciden, no se confirmará la identidad[97] (IMAGEN 24).

El desarrollo de técnicas de procesamiento de señales digitales (DSP – *Digital Signal Processing*) y sus proyecciones en posibles sistemas reconocimiento a través de la voz[98] o las huellas dactilares[99] llevaron a reconocer ya a comienzos de los años 60 el importante potencial de estas tecnologías de cara a garantizar elevados niveles de seguridad en los controles de acceso, uso de claves personales o transacciones financieras[100]. Como veremos, con el desarrollo e implementación de los primeros sistemas se dará ya por comenzada *la primera generación* de sistemas de reconocimiento automatizado mediante Biometría desarrollados fundamentalmente sobre fuentes de datos biométricos estáticos. En los años 70 se desarrollaron e implementaron sistemas de reconocimiento basados en la geometría manual[101] y comenzó el testado de los sistemas a gran escala[102]. La literatura considera que fue a partir de ese momento cuando comenzó a evidenciarse un creciente interés por los posibles usos gubernamentales de las tecnologías de identificación automatizada[103]. En los años 80 se desarrollaron sistemas de reconocimiento por Biometría de la retina[104] y mediante firma dinámica, a los que siguieron sistemas de reconocimiento facial[105]. Las tecnologías que tienen su base en el patrón del iris, por

---

[97] MORDINI, E. / REBERA, A. P. "Biometrics and Ageing: social and ethical considerations", en FAIRHURST, M. (ed.), *Age Factors in Biometrics Procesing*, 2013, p 39.

[98] PRUZANSKY, S. "Pattern-matching", *Journal of the Acoustical Society of America,* 1963, 35, p354–358; LI, K. P./ DAMMANN, J. E./ CHAPMAN, W.D. "Experimental studies in speaker verification", *J. Acoust. Soc. Am*., 1966, 40, 966–978; LUCK, J. "Automatic speaker verification using spectral measurements", *J. Acoust. Soc. Am*., 1969, 46, 1026–1031; STEVENS, K./ WILLIAMS, C. / CARBONELL, J./ WOODS, B. "Speaker authentication and identification: a comparison of spectrographic and auditory presentation of speech material", *J. Acoust. Soc. Am*., 1968, 44, 596–607; ATAL, B. "Automatic recognition of", *Proc. IEEE*, 1976, 64(4), 460–474; ROSENBERG, A. "Automatic speaker recognition", *Proc. IEEE*, 1976, 64(4), 475–487.

[99] TRAURING, M. "Automatic comparison of finger-ridge patterns", *Nature*, 1963, 197, 938–940.

[100] TRAURING, M. "On the automatic comparison of finger-ridge patterns", *Hughes Laboratory Research Report* 1961, n. 190.

[101] El primer sistema totalmente automatizado de reconocimiento biométrico fue el sistema basado en geometría manual que patentó Robert P. Miller en 1971. ZUNKEL, R. "Hand geometry based verifications", en A. JAIN, ET ALT. (eds.) *Biometrics: Personal Identification in Networked Society*, 1999.

[102] FEJFAR, A./ MYERS, J. "The testing of 3 automatic ID verification techniques for entry control", *2nd Int.Conf. on Crime Countermeasures*, Oxford, 25–29 de julio de 1977.

[103] NATIONAL BUREAU OF STANDARDS, *Guidelines on the evaluation of techniques for automated personal identification*, 1977.

[104] CRANE, H. D./ OSTREM, J. S. "Automatic signature verification using a threeaxis force-sensitive pen", *IEEE Trans. on Systems, Man and Cybernetics*, *SMC*- 13(3), 329–337, 1983.; NALWA, V. S. "Automatic on-line signature verification", *Proc. IEEE*, 85(2), 215–239, 1997.

[105] HARMON, L. D./ KHAN, M. K. / LASCH, R./ RAMIG, P. F. "Machine recognition of human faces", *Pattern Recognition,* 31(2), 97–110, 1981; SAMAL, S./ IYENGAR, P. "Automatic recognition and analysis of human faces and facial expressions", *Pattern Recognition*, 25, 65–77, 1992; CHELLAPPA, R./ WILSON, C. L./ SIROHEY, S.

su parte, fueron propuestas a mediados de los años 80, pero la primera patente de un algoritmo es de los años 90 (1994)[106].

1.3.2. La confluencia temporal entre el desarrollo de estos sistemas y un contexto de creciente necesidad por métodos fiables de identificación.

Algunas tesis parecen presentar los avances y desarrollos tecnológicos como fenómenos impulsados por "*una fuerza autónoma*", como si tuvieran una lógica ajena a los asuntos humanos[107]. En ausencia de tomas de decisiones asertivas y claras a las que achacar el impulso de las tecnologías biométricas, pareciera que ni es posible cuestionar su avance, ni contamos con un sujeto o sujetos de referencia a los que atribuir la responsabilidad por las consecuencias negativas que hubiere deparado su acción o su omisión. Pero lo cierto es que la vigilancia masiva no se extiende por sí sola, sino por una dinámica que impulsan instituciones públicas y corporaciones privadas que, con diferentes intereses, buscan satisfacer su creciente necesidad de información sobre las personas. Y a ello ha de sumarse el importantísimo potencial económico de estas tecnologías y una narrativa que presenta al reconocimiento biométrico con un aura mítica, en el sentido de pieza clave para garantizar la seguridad de las personas a escala planetaria. Vamos a presentar con más detalle estos factores.

1.3.2.1 *La promesa biométrica y su aura mítica*

A grandes rasgos, el reconocimiento mediante Biometría implica atribuir a las personas una referencia algorítmica, digital, que se diferencia de otros códigos alfanuméricos (como el DNI) en el hecho de que la referencia para su atribución los rasgos estáticos o comportamentales inherentes a la persona. Eso hace que, en hipótesis al menos, pueda considerarse inherente, permanente y difícil de falsear[108]. A ello se une la celeridad y la eficiencia de la automatización del reconocimiento. Ofrece así la posibilidad de un reconocimiento rápido y además indubitado de la

---

"Human and machine recognition of faces", *Proc. IEEE*, 83(5), 705–740, 1995; SIROVICH, L./ KIRBY, M. "Low-dimensional procedure for the characterization of human faces", *J. Optical Soc. Am.*, 1987, 4, 519–524; TURK, M./ PENTLAND, A. "Eigenfaces for recognition", *J. Cognitive Neuroscience*, 1991, 3(1), 71–86; ZHANG, J./ YAN, Y./ LADES, M. "Face recognition: eigenface, elastic matching and neural nets", *Proc. IEEE*, 1997, 85(9), 1423–1436; DAUGMAN, J. D. "High confidence visual recognition of persons by a test of statistical Independence", *IEEE Trans. Pattern Analysis and Machine Intelligence*, 15(11), 1148–1161, 1993.

[106]WILDES, R. P. "Iris recognition: an emerging biometric technology", *Proc. IEEE*, 85(9), 1348–1364, 1997; JAIN, A. / BOLLE, R./ PANKATI, S. *Introduction to biometrics*, en JAIN, A. / ET AL. (eds.) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999. Vid. NSTC *Biometrics History*, 2006.

[107] RULE, J. B. *Privacy in Peril. How we are sacrificing a fundamental right in exchange for security convenience*, Oxford University Press 2007, pp. 18-19.

[108]INTRONA, L. D./ NISSENBAUM, H. *Facial Recognition Technology*, 2009, pp9-10; REID, P. *Biometrics for Network Security*, 2004; BOLLE, R./ CONNELL, J. H./ ET ALTERE, *Guide to Biometrics*, Springer, 2004.

identidad de las personas resulta muy atractiva. si se había venido diciendo que el ADN estaba llamado a ser el estándar de oro de la identificación, por su inmutabilidad y su variabilidad interpersonal, el reconocimiento automatizado mediante Biometría parece estar llamada a complementar una eficiencia asimilable con la ventaja de la celeridad en el reconocimiento.

Esto a llevado a que algunas voces celebren la identificación biométrica como una *tecnología de identificación perfecta*[109]. Paul REID, por ejemplo, en su libro *Biometrics for Network Security*[110] refleja cómo se ha creado en torno al reconocimiento biométrico la imagen de una tecnología altamente desarrollada, eficiente y precisa. Se le asocia, además, un altísimo potencial y una gran variedad de usos posibles. En la vida cotidiana de los países occidentales la identidad se alega con medios que una persona conoce (una clave o contraseña) o mediante objetos que porta (documentos de identidad, tarjetas inteligentes) y contamos con diferentes tipo de identificadores: identificadores biográficos (relativos al nacimiento, la profesión o el estado civil, por ejemplo) e identificadores atribuidos (como los apellidos, números de DNI o de la seguridad social, números de cliente, etc.). Pero conocemos factores que hacen a cada uno de ellos *vulnerable*. Lo que se sabe puede olvidarse, los objetos identificativos pueden perderse y en muchas situaciones es posible acceder a los identificadores biográficos o atribuidos de las personas.

En cambio, por su naturaleza, las características biométricas no pueden –en principio—olvidarse, robarse o falsearse y ello además de presentarse como una oportunidad para superar los inconvenientes de otros sistemas de reconocimiento. Invitan además, a pensar que el reconocimiento mediante Biometría podrá contribuir a solucionar los problemas que se plantean por la debilidad o inexistencia de documentos identificadores.

1.3.2.2. *De cara al control de los nacionales de terceros países y de los "indocumentados"*

A lo largo y ancho del Planeta nuestra identidad personal es uno de nuestros principales *valores*[111], afirmaba CHERTOFF. El ansia de aquellos individuos que, por diferentes motivaciones, tratan de suplantar identidades de otras personas plantea un importante problema de seguridad personal y nacional al que resulta difícil dar respuesta cuando las fronteras deben supervisar la

[109] MAGNET, S. *When Biometrics Fail*, 2011, p21.

[110] REID, P. *Biometrics for Network Security*, 2001.

[111] CHERTOFF, M. "Managing Identity", en *Orbis - A Journal of World Affairs*, vol. 53, nº 1/ 2009, pp. 137 y ss.

validez de más de 8000 documentos diferentes[112]. A ello se suman las personas que carecen de documentos que den alguna seña de su identidad. Aunque la tasa de registro de nacimientos alcanzó el 56% entre los años 2000 y 2010, 230 millones de niños menores de 5 años están sin registrar. Fundamentalmente sucede en los países del África subsahariana y Asia, pero también en bolsas de población excluidas en los países industrializados [113] o en los grupos de población que son víctimas de los conflictos bélicos –IMAGEN 75-. La falta de registro impide a las personas demostrar la existencia de vínculos familiares sin expresión biológica (como las adopciones o los matrimonios) o acontecimientos como los divorcios y defunciones, y les excluye del ejercicio de derechos como el derecho a la educación y a la salud o el derecho a la nacionalidad y la ciudadanía sociales[114], y ese es el argumento que países como India y otras regiones de América del Sur y África han esgrimido para implementar sistemas de registro biométrico de las personas. La IMAGEN 76 muestra los países que en 2014 contaban con algún sistema biométrico aplicado a la población civil. En el caso de las personas más vulnerables, sobre todo los menores de edad, la falta de registro propicia que víctimas de los matrimonios precoces, de la trata de personas o de la esclavitud. En ausencia de datos biográficos o de identificación de otro tipo, las características biométricas son vistas como soporte para el establecimiento de un identificador único sólido. Pero el mero hecho de que las características biométricas presenten algunas características diferenciales respecto de los elementos que sirven de soporte a otros sistemas no debe interpretase, sin más, en el sentido de que los sistemas de reconocimiento biométrico basados en ellas no sean *vulnerables*[115].

Desde que en torno a la Segunda Guerra Mundial comenzara a fraguarse la idea de una *economía global* y hasta la actualidad, la evolución del mercado ha hecho del mundo contemporáneo una compleja realidad que tiende a resumirse en la literatura con una palabra: *globalización*. Aunque se trata de un proceso *multidimensional* y no sólo económico, es decir, un proceso que se extiende a la ciencia, la política, la cultura o la misma sociedad, no puede negarse que la expresión más determinante de este fenómeno es la interdependencia global de los mercados financieros, favorecida, entre otras cosas, por la desregulación y la liberalización de

---

[112] Véase al respecto el Informe de la *Comisión 9/11* sobre fraudes y su debate en el Congreso de los Estados Unidos de América.

[113] MUZZY, M.: "UNICEF good practices in integration birth registration into health systems (2000-2009), UNICEF 2010, http://www.unicef.org/protection/Birth_Registration_Working_Paper%282%29.pdf (ultimo acceso julio de 2015).

[114] ALTO COMISIONADO DE LA ONU PARA LOS DERECHOS HUMANOS, Informe *Birth registration and the right of everyone to recognition everywhere as a person before the law*, presentado en a la Asamblea General de las Naciones Unidas, A/HRC/27/22, 17 de junio de 2014.

[115] REBERA, A. P. / MORDINI, E. "Biometrics and Ageing: social and ethical considerations", en M. FAIRHURST, pp39-40.

aquellos. Tampoco cabe pasar por alto la complejidad de nuestro mundo. Una amplia parte de la población no tiene acceso a la satisfacción cotidiana de necesidades básicas como el alimento, la vivienda, la sanidad o la educación. Según la UNICEF más de un 40% de las personas no son registradas al nacer, lo cual hace poco fiables los pasaportes y documentos de identidad a los que en el futuro puedan tener acceso[116]. A ello ha de sumarse que conforme a las estadísticas publicadas por la IATA en el año 2014 más de 850 millones de personas se desplazan en avión[117] y según el servicio de migración de UNICEF en torno a 215 millones de personas viven fuera del país del que son originarios[118].

Transferencias bancarias inmediatas, contratos que se elaboran sin necesidad de una reunión física, incluso sin la necesidad de cables, la comunicación planetaria instantánea ofrece unas posibilidades antes solo soñadas. Incluso sin salir de casa y a cualquier hora del día o de la noche, con un ordenador y un módem podemos toparnos con alguien que vive en el lado opuesto del Planeta. Pero tampoco resulta difícil sentirse solo, aislado entre la multitud que nos rodea física y virtualmente. Nos sentimos rodeados de muchos, sí; pero de muchos desconocidos. Y los nuevos perfiles del terrorismo y la delincuencia internacional nos hacen sentir cada vez más inseguros. ¿Cómo elegir en quién se puede confiar? Para interactuar hay que identificar, es un acto elemental en la vida social[119]. Pero, ¿cómo hacerlo en este contexto?

En este contexto la promesa que se asocia a la Biometría no es insignificante[120]:

> "*Si pudieras identificar a un ser humano como único en el mundo, ¿qué razón te impediría construir una infraestructura que, a nivel mundial, te permitiera obtener en cualquier momento una identificación indubitada?*".

Esa es la pregunta con la que John M. McConnel abrió su intervención en la Conferencia del *Biometric Consortium* en el año 2009[121]. Desde cualquier perspectiva organizacional, la posibilidad de un reconocimiento rápido y además indubitado de la identidad de las personas resulta muy atractiva. Parece, además, "que ha llegado en el momento más oportuno", o eso quiere darse a entender.

---

[116] MORDINI, E. / TZOVARAS, D. / H. ASHTON, H., en *Second generation*, cit., pp5-6.

[117] Estadísticas publicadas en su página web por la Asociación Internacional de Transporte Aereo (IATA – International Air Transport Association), *World Air Transport Statistics* (WATS), 59th edition.

[118] Vid. detalladamente BARBERO GONZÁLEZ, I. *Globalización, Estado y Ciudadanía*, 2012, pp27-29.

[119] En el mismo sentido, BART, J. *Histoire du droit privé, de la chute de l'Empire Romaine au XIXéme siecle*, editorial Montchrestien, Paris, 1998, p213; GIROTTO, S.: "Il tratamento dei Dati Biometrici", en *Tratatto di Biodiritto*, 2011, p1237; LORENTE ACOSTA, J. A. "Identificación genética criminal", cit., pp1-2.

[120] LANGENDERFER, J./ LINNHOFF, S. "The Emergence of Biometrics", 2005, pp314 y ss.

[121] MCCONNEL, J. M. "Identity, Security, and the World Wide Web", 2009.

1.3.3 Más allá de los mitos, las cifras económicas

Cualquiera de los elementos que en la actualidad se emplean para controlar el acceso físico o virtual de seres humanos a algún espacio (sean claves, llaves, carnets u otro tipo de objetivos identificativos) pueden ser potencialmente sustituidos por tecnologías biométricas; de hecho lo están siendo ya. Si nos cuesta imaginar en cuánto dinero puede traducirse una transformación actual, no debemos preocuparnos; ya otros se han tomado la molestia de realizar en detalle estos cálculos. Un informe del Departamento del Tesoro de los Estados Unidos, presentado en el año 2003[122] destacaba cómo hasta comienzos el siglo XXI el uso de las tecnologías biométricas se había reservado a parcelas muy exclusivas de la realidad social (como la seguridad de las altas operaciones financieras, o el control de instalaciones militares o instancias de alta seguridad nacional).

En poco menos de una década, sin embargo, estas tecnologías se han extendido hasta lo cotidiano, como por ejemplo: al acceso a los teléfonos móviles, tabletas o portátiles, en la apertura de automóviles o puertas de acceso a las viviendas, así como en el acceso a estancias, armarios o cajas de seguridad en el interior de edificios. Los elementos biométricos están incorporados a sistemas que controlan el transito transfronterizo de viajeros, el ejercicio del derecho de sufragio o los accesos y movimientos internos en zonas como las instalaciones aeroportuarias o las prisiones, pero también el acceso de abonados a comedores escolares, gimnasios o parques temáticos, sistemas de acceso a clubes nocturnos o servicios hospitalarios y operaciones financieras cotidianas.

Universitat d'Alacant
Universidad de Alicante

Los aeropuertos de Shiphol (Ámsterdam, Países Bajos), Frankfurt Internacional (Frankfurt am Main, Alemania) y Heathrow (Londres, Reino Unido), y desde hace poco siete aeropuertos españoles, cuentan con un programa de viajeros frecuentes que agiliza su embarque escaneando su biometría y en España los Ayuntamientos de Villena o el Puerto de la Cruz o los gobiernos autonómicos de Andalucía y Castilla la Mancha establecieron sistemas de reconocimiento mediante Biometría en el control horario de sus empleados. Un hito clave en esa expansión lo constituyen sin duda los atentados del 11 de septiembre de 2001 en los Estados Unidos de América y una serie de decisiones del Congreso de dicho país, que propició que otros –como los Estados Miembros de la UE y Suiza- se vieran en la necesidad de incorporar elementos

[122] JAIN, A. K./ FLYNN, P. / ROSS, A. A. *Handbook on Biometrics*, Springer, 2008, p1.

biométricos a sus visados y pasaportes[123]. Entre estas decisiones destacan la *Us Patriot Act*[124] y la *Us Military Commissions Act*[125]. La primera de estas leyes, con el argumento de reforzar la seguridad en los movimientos transfronterizos, exigió la incorporación de datos biométricos a los documentos de viaje expedidos por terceros países (pasaportes y tarjetas de identidad). Como ya advirtiera el IPTS en 2005, en su informe a la Comisión de Libertades del Parlamento Europeo (LIBE), al acostumbrarse los ciudadanos al reconocimiento biométrico en las fronteras, apenas han opuesto resistencia a su expansión al sector privado[126].

Esto, entre otras cosas, tienen una clara traslación económica. Tras el 11/S el mercado de las tecnologías de la seguridad aumentó de forma espectacular en todo el mundo y en ese espacio de oportunidad comenzó el desarrollo de las tecnologías biométricas en los movimientos transfronterizos, programas de viajeros frecuentes y operaciones financieras. Más lentamente se fueron extendiendo a la prestación de servicios a los consumidores, las prisiones las escuelas o la atención sanitaria, así como a aplicaciones en dispositivos personales de todo tipo. En el año 2006 circulaban ya 500 millones de documentos de viaje de lectura mecánica, que implicaron el establecimiento de tecnologías de enrolamiento y renovación, y mecanismos de verificación de la autenticidad de los documentos. Sólo en tecnología facial los 2,9 millones de dólares de ingresos del año 2002 ascendieron hasta 240, y de 13,9 millones a 93 millones en tecnologías de verificación vocal. El crecimiento más espectacular, con todo, se produjo en el reconocimiento por Biometría digital, que pasó de 100 millones de dólares a casi mil[127].

Universitat d'Alacant
Universidad de Alicante

El conjunto de los sistemas de autenticación las tecnologías biométricas creció del 9% al 21% en el año 2001 (VÉASE LA IMAGEN 19), aunque decreciendo algo respecto de los valores relativos de los años 2008 y 2009 en que llegaron al 25%. Según CLARKE aunque son cada vez más aceptados, retiene su crecimiento el hecho de que no consiguen alcanzar un 100% de fiabilidad[128]. Atendiendo a su distribución por sectores en el mercado mundial, en el año 2007 un 64'6% de las biometrías se empleaban en entornos públicos; en 2015 el sector comercial, con un 52,4% supera ya al sector público según los datos del informe *The Future of Biometrics, de Acuity*. En cuanto a las

---

[123] Véase el Prólogo de Viviane REDING, Vicepresidenta de la Comisión Europea, en S*econd Generation Biometrics*, 2012, pp. v-vi.

[124] El nombre oficial de esta Ley es:"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001".

[125] HR-6166, aprobada por el Congreso y refrendada por George W. Bush el 17 de Octubre de 2006.

[126] IPTS, *Biometrics at the Frontiers*, 2005, pp32-34.

[127] Datos obtenidos de *The Biometric Industry Repot* – Forecasts and Analysis to 2006, editado por M. LOCKIE.

[128] CLARKE, N. *Transparent User Authentication*, 2011, p17.

previsiones a futuro, el informe anual del *International Biometric Group* destaca que entre los años 2009 y 2014 se produjo un crecimiento de aproximadamente un 25% anual (IMAGEN 20) y se estima que para el año 2020 el mercado de las tecnologías de reconocimiento biométrico, que se estima en 10.000 millones de dólares en la actualidad, alcanzará los 25.000 millones de dólares[129].

1.3.4 El efecto difusor que ha tenido la decisión de incorporar la Biometría a los pasaportes europeos

Los documentos doctrinales e institucionales que vienen prestando atención a las implicaciones sociales, económicas, legales y técnicas han aumentado exponencialmente en los últimos diez años[130], fruto de estudios preocupados por el que se ha dado en llamar *efecto difusor* de las tecnologías de reconocimiento biométrico. Como ya advirtió el IPTS que sucedería[131], el uso de elementos biométricos en los pasaportes (VÉASE LA IMAGEN 74) y documentos nacionales de identidad ha facilitado la expansión de su uso en una sociedad que parece asimilar sin sobresaltos la erosión de la privacidad y el aumento de la vigilancia[132]. Aunque no puede decirse que las instituciones hayan asistido impasibles a esta difusión, veremos que en algunos casos han albergado importantes dudas sobre el modo en que habían de proceder ante las tecnologías de reconocimiento biométrico, en buena medida por la confluencia de dos fenómenos. De una parte, el efecto en Europa del decidido impulso de los Estados Unidos de América a determinados usos de elementos biométricos y, de otra parte, la dificultad de categorizar y aportar datos concluyentes y generales sobre el balance entre utilidades y riesgos de las tecnologías de reconocimiento mediante Biometría[133].

Universitat d'Alacant
Universidad de Alicante

Aunque no se exprese con la misma rotundidad que se ensalzan sus virtudes, es frecuente reconocer que las tecnologías biométricas están muy lejos de ser infalibles[134]. Precisamente por lo inaceptable del balance entre ventajas y limitaciones, el Gobierno de los Estados Unidos se mostró

---

[129] *Global Biometrics Market* (2014-2010), *Market Forecast By Technologies, Applications, End Use, Regions and Countries*.

[130] MORDINI, E./ PETRINI, C., "Ethical and Social Implications of Biometric Identification Technology", 2007, 43, p1.

[131] IPTS, *Biometrics at the Frontiers,* cit.

[132] LYON, D. *La societá sorvegliata*, cit., 2002, p96; J. B. RULE, J. B. *Privacy in Peril*, cit., pp. 43-39.

[133] Además del informe del IPTS a la Comisión LIBE, loc cit, véase la respuesta del Gobierno Alemán a las preguntas de la Cámara baja en DEUTSCHER BUNDESTAG, *Drucksache* 16/ 161, de 9 de diciembre de 2005. Respuesta del Gobierno a las preguntas presentadas por los parlamentarios Ulla JELPKE, Petra PAU y la Fraktion *Die Linke* – informe 16/82-.

[134] AUS, J. P. "Eurodac: A Solution Looking for a Problem?", 2006; Amgaben, G. "Bio-political tatooing", Le Monde, 11 de enero de 2004; IPTS, *Biometrics at the Frontiers*, cit., p10-11.

durante la década de los 90 claramente contrario a una expansión de la Biometría hacia los usos civiles[135]. Parece pues importante preguntarse qué es lo que ha cambiado en dicha ponderación[136]. Los sistemas actuales, ¿captan mejor la singularidad que sus predecesores? ¿Es menor el riesgo de que se traduzcan en una vigilancia excesiva de las personas o de que se haga un mal uso de la información que captan? ¿Qué es lo que justifica que se hayan extendido tanto?

1.3.5. Pero, ¿es oro todo lo que reluce?

Mucho antes de que Thomas MORE (o en expresión castellanizada de su nombre Tomás MORO)[137] construyese la voz *Utopía,* se crearon e incluso reflejaron documentalmente sociedades idealizadas, alternativas al mundo existente[138], así como *anti-utopías* o expresiones que alertaban de los destinos a los que inevitablemente parecían llevar determinados caminos. Enjuiciar adecuadamente las potencialidades y riesgos de una nueva aplicación científico-tecnológica requeriría encuadrar el debate de forma en que todos los argumentos encuentren un anclaje imprescindible en el mundo real en que vivimos. Pero como ya advirtiera BENTHAM[139], a veces por ignorancia, otras por *intereses siniestros*, esto no suele ser fácil de llevar a cabo. Son muchos los factores que, evitable o inevitablemente, inconscientemente o por intereses de algunos, dificultan que esto suceda en los procesos de toma de decisión política.

El reconocimiento mediante Biometría ha despertado temores que aparecían ya en algunas construcciones utópicas antiguas y nos ha recordado las advertencias que recogieron pensadores de otras épocas[140]; hay algo en el reconocimiento biométrico que no parece ser *tan nuevo*. En la evocación de MCCONNEL a la que hacíamos referencia se habla de rastrear y localizar con facilidad "*a los malos*" y mantenerlos alejados "*de los buenos"* y de algún modo retoma el deseo de librarse de un miedo que expresaba el escritor romano Tito Maccio Plauto (255 a. C.– 184 a. C) y que popularizó Thomas Hobbes: "*cuando se desconoce quién es el otro, lobo es el hombre para el*

[135] DEPARTMENT OF THE TREASURY (EEUU), *The Use of Technology to combat identity theft*, 2005.

[136] Cuestión que en Francia enfrentó al Consejo de Estado con la CNIL y el Consejo Constitucional, y en Suiza dividió a la población ante un referendo.

[137] En el libro: *Libellus... De optimo reipublicae statu, deque nova insula Vtopiae* (1516), en español, *Libro Del estado ideal de una república en la nueva isla de Utopía*.

[138] RÜSEN, J. "History and Utopia", *HISTOREIN*, vol. 7, 2007, pp1-10; MANUEL, F. E. "Toward a Psychological History of Utopias", *Daedalus*, vol. 94, 2/ 1965, pp293 y ss.

[139] BENTHAM, J. / LARRABEE, H. A. *Handbook of Political Fallacies*, Harper, edición de 1952, a partir del *Book of Fallacies* (1824) de Jeremy BENTHAM.

[140] CABRERA, D. H. *Lo tecnológico y lo imaginario: Las nuevas tecnologías como creencias*, Biblos, 2006, pp126-128.

hombre"[141]. Con esta tecnología, al menos en su promesa original, seremos capaces de distinguir a los hombres y a los lobos.

Ilustrado con una fastuosa tecnología[142] vemos cómo el reconocimiento mediante Biometría se aplica cotidianamente en la sociedad que sirve de escenario a la película *Minority Report* (Steven Spilberg, 2002) y en la serie *Person of Interest* (CBN, 2011) aparece una máquina capaz de realizar una intensa vigilancia sobre las personas. Muchas otras películas y series recogen sistemas automatizados de reconocimiento biométrico[143] (IMAGEN 93), pero probablemente ninguna otra ha mostrado de forma tan detallada la potencialidad de estas tecnologías: a) sensores del iris establecidos indiscriminadamente por toda la ciudad y que saludan a las personas al entrar en los comercios –ofreciéndoles servicios personalizados-, sistemas de acceso a vehículos, edificios y domicilios que incorporan Biometría y una tropa impresionante de pequeños robots policiales especializados en la localización de las personas (en *Minority Report*); b) filtrado de comportamientos atípicos de las personas dentro de la masa social, con acceso a móviles, correos electrónicos, cámaras de videovigilancia, etc., en tiempo real (*Person of Interest*).

Pero el control de los ciudadanos tiene sus riesgos. A lo largo del siglo XX diversos autores como Aldous Huxley (*Un mundo feliz*, 1932*)*, George Orwell (*1984*, publicado en 1949) o Ray Bradbury (*Fahrenheit 451*, 1953) proyectaron las consecuencias que pudiera tener un uso de las tecnologías para dar vida a *utopías de control*. Estas ambiciones han tenido mayor o menor presencia en distintos momentos de la historia[144], con consecuencias frecuentemente nefastas. HUXLEY y ORWell escenificaron métodos de condicionamiento físico y psíquico de las personas y sistemas de control masivos en sociedades repletas de personas paradójicamente *anónimas* entre sí. Coincidían estas obras en reflejar modelos temerosos de las dictaduras, si bien el tipo de

[141]HOBBES, T. *Leviathan or The Matter, Form and Power of a Common Wealth Ecclesiastical and Civil*), 1651: *"Lupus est homo homini, non homo, quomquali sit non novit*".

[142] EUROPEAN COMMISSION (ed.), *Biometrics in Europe*, 2007, p6.

[143] Film de S. SPIELBERG, 2003, en el que el protagonista modifica su iris mediante transplante para evitar su localización en una sociedad vigilada; véase también *Diamantes para la eternidad* (Guy Hamilton, 1971) de James Bond (que lleva huellas falsas). Otras películas: huellas falsas en *Fingerprints don't lie* (1951), en *Fantomas* (1964) aparecen guantes que generan huellas falsas; reconocimiento de voz en *2001: Odisea del Espacio* (1968), identificación vocal y chequeo ocular en *Blade Runner* (1982); reconocimiento mediante retina en *Star Trek 2* (1982), sustitución de globo ocular para acceder a arma nuclear en *Nunca Digas Nunca Jamás* (1983), arma con reconocimiento palmar en Licencia para matar (1989), escáner de retina, huellas y voz en *Mision Imposible 1* (1996), katana biométrica en *Blade* (1998), escáner ocular para acceso en *X-Men* (2000), reconocimiento manual para acceso en *El Planeta de los Simios* (2001). Un listado más amplio, con más de un centenar de películas, en http://fingerchip.pagesperso-orange.fr/biometrics/movies.htm (consultado en julio de 2015).

[144] ARENDT, H. *The Origins of Totalitarism*, 1973 describe la autoridad de decidir "quién pertenece" (y quién no), como un componente central de la soberanía y una preocupación que se mantiene desde las primeras formas de Estado hasta nuestros días.

control de masas hacia el que tiende nuestra era parece estar erigiéndose sobre los sistemas democráticos o, en opinión de STRASSER[145], quizá como consecuencia de la obsolescencia de éstos. También en *Minority Report* se desmonta en parte este mito, cuando el personaje interpretado por Tom Cruise trata de zafarse de la orden de búsqueda y captura que de forma injusta ha sido dictada contra él y para ello recurre a un trasplante de ojos que le proporcionará una identidad *sin antecedentes policiales*.

Fuera ya de la literatura de ciencia ficción encontramos las preocupaciones expresadas por importantes voces. Los sistemas de identificación que usan el cuerpo humano están aquí, decía el periodista del Washington Post Rajiv CHANDRASEKARAN en 1997, pero las dudas en torno a la privacidad de las personas siguen sin resolverse. El *Comité Consultatif National d'Éthique pour les Sciences de la vie et de la santé (CCNE)* francés se refirió en 2007 al *riesgo de biometrización del ser humano*[146]. De informatización del cuerpo humano[147], *el cuerpo como contraseña* o hipervigilancia de éste, así como de implantación de *códigos de barras*[148] o *tatuajes biopolíticos*[149] en las personas han hablado en la última década diferentes voces. Así el Supervisor Europeo para la Protección de Datos y el Grupo del Artículo 29, la comisión de libertades del Parlamento Europeo, o los expertos que durante meses expusieron sus tesis ante la Cámara de los Lores del Reino Unido. Todas ellas advierten de las implicaciones que para la dignidad humana y los derechos fundamentales tiene empleo de la Biometría en la identificación de las personas, destacando en especial algunas dimensiones de la privacidad y del derecho a la identidad personal. El uso de la identificación biométrica propicia, además, la geolocalización. En tiempo real nos permite saber en qué lugar del mundo está, exactamente, una persona.

Universitat d'Alacant
Universidad de Alicante

"Ya no caminamos sonámbulos hacia una sociedad vigilada", advierte el Comisionado Británico Richard THOMAS a la *Cámara de los Lores* del Reino Unido[150], "*nos estamos despertando rodeados de*

---

[145] STRASSER, P.: "Biometrie – ein Schritt in die Überwachungsdemokratie?", SCHAAR, P. (ed.), *Biometrie Und Datenschutz*, 2007, pp14-15.

[146] CCNE, *Biométrie, dones identifiants et droits de de l'homme*, 2007, cit., p3.

[147] VAN DER PLOEG, I. *The Machine Readable Body. Essay on Biometrics and the Informatization of the Body*, Shaker, 2005, p8.

[148] CREWS jr., C. W. "Human Bar Code. Monitoring Biometric Technologies in a Free Society", *Policy Analysis*, nº 452, 2002, pp1 y ss.

[149] AMGABEN, G. "Bio-political tattooing", Le Monde, 11 de enero de 2004.

[150] THOMAS, R. (Information Commissioner), *A Report on the Surveillance Society*, publicado por el ICO, Gobierno del Reino Unido, 2006; véase también el *Memorando de LIBERTY* (National Council for Civil Liberties), en HOUSE OF LORDS – SELECT COMMITTEE ON THE CONSTITUTION. *Part. 1. Borders, Citizens and Immigration Bill Report*, 2009, pp103-104.

ésta y ello debería preocuparnos". La Agencia Española de Protección de Datos de Carácter Personal incluye una viñeta de humor en su guía de videovigilancia, expresando también la preocupación por la vigilancia que pasa inadvertida (IMAGEN 92). El reconocimiento mediante Biometría no sólo se ha expandido como parte de esa sociedad vigilada, sino que además veremos que aparece en muchos discursos como herramienta con potencialidad para ofrecer una *vigilancia perfecta*.

También se presta atención a la ausencia de preocupación ciudadana. Algunos autores, como James B. RULE, llaman la atención por la aparente conformidad de los ciudadanos ante estas intromisiones. Aún y cuando no se pretendiera abusar de ésta, la mera idea de una vigilancia perfecta parece contener implícitamente una importante amenaza[151]; pero no parece que los ciudadanos se hayan percatado de ello. Las aplicaciones biométricas se expanden deforma imparable[152]. En la existencia de los salvajes, explicaba RAND en *El Manantial*, la vida es totalmente pública y controlada, siendo así que las civilizaciones vienen a caracterizarse por su progreso hacia la sociedad de la privacidad[153]. ¿Qué nos pasa que no nos sentimos amenazados? James B. RULE achaca esa tendencia al hecho de que la ciudadanía parece conformarse con facilidad con la "*erosión de la privacidad*" y que en nuestra era son relativamente pocos los que se entregan a la causa de defenderla[154]. Se trata de una visión actualizada de algo que TOCQUEVILLE proyectaba en relación con el Estado. La mentalidad individualista promueve paradójicamente el conformismo ante el refuerzo y el aumento de control por parte de quienes tienen el poder[155], sea poder político o socioeconómico.

Universitat d'Alacant
Universidad de Alicante

[151] TIEN, L. *Electronic Frontier Foundation*.

[152] LANGENDERFER, J./ LINNHOFF, S."The Emergence of Biometrics", cit., pp314 y ss; BROMBA, M. "Die 14 Märchen der Biometrie", 2007, pp36ss; documento WP 193 del GT-WP 29, 2012.

[153] RAND, A. *The Fountainhead*, Bobbs-Merril, New York, 1943 (1969), pp729-730.

[154] RULE, J. B. *Privacy in Peril*, 2007, p143.

[155] Tomado de DE TOCQUEVILLE, A. *Pratique de la Philosophie*, E. Hatier, 1994.

2. Motivación y objetivos de la investigación

2.1 MOTIVACIÓN (RATIONALE)

En tanto basados en la captura métrica de características anatómico-físicas o comportamentales singularizantes y gestionados en forma que permiten un acceso casi inmediato a tal información, los sistemas de reconocimiento biométrico se nos presentan como una tecnología perfecta. Una tecnología capaz de separar *a los malos* y mantenerlos alejados *de los buenos*. La perfección tecnológica que se les atribuye nos llamó la atención sobre este espacio en el que se alían el conocimiento científico y la ingeniería computacional, y esa idea de *separar los buenos y los malos* hizo que nos intrigase saber de qué buenos y qué malos se estaba hablando y cómo se planeaba separar a los unos de los otros.

2.2 OBJETIVO GENERAL

El objetivo de la presente investigación es abordar la realidad de los sistemas biométricos contemporáneos para, desde ese anclaje, dar respuesta a dos cuestiones: Primera, ¿hasta qué punto y cómo ofrecen las tecnologías de reconocimiento biométrico la posibilidad de identificar a un ser humano con único en el mundo? Segunda, ¿qué razones están permitiendo y cuáles deberían impedir construir infraestructuras de reconocimiento biométrico "que aseguren la identificación en todo momento"? La primera de las preguntas acepta la hipótesis científica de la que parten los sistemas de reconocimiento biométrico: la posibilidad de *expresar métricamente* (cifrar, cuantificar) la singularidad de algunas características de las personas. Pero se adentra en validar hasta qué punto el actual contexto científico y tecnológico es capaz de ofrecer y cómo sistemas de reconocimiento ágiles y fiables basados en dicha hipótesis.

Existe un rango amplísimo de tecnologías biométricas, con muy diferentes niveles de calidad y eficiencia, y se emplean en un amplio abanico de escenarios y contextos a lo largo y ancho del Planeta. También son diferentes las condiciones de procesamiento y almacenamiento de los datos,

los niveles de interoperatividad[156] o los riesgos para los derechos fundamentales de los titulares de los datos[157]. Algunas afirmaciones que asocian, sin más, Biometría y vigilancia perfecta se sostienen a veces sobre interpretaciones parciales de la verdad histórica o científica, bien directamente sobre falacias y mitos[158], y es importante analizar la realidad de los datos que manejan.

Establecida la metodología, potencialidad y limitaciones de estos sistemas de reconocimiento, nos adentraremos en la cuestión de qué razones sostienen y cuáles abogan por impedir el establecimiento de infraestructuras de reconocimiento biométrico. Al efecto, se empleará como referencia una comparativa con la realidad de los sistemas de reconocimiento a los que están sustituyendo o están llamadas a sustituir (accesos con claves o identificadores materializados en objetos tales como llaves, tarjetas o carnets).

2.3. OBJETIVOS ESPECÍFICOS

Dentro del objetivo general que se ha descrito y como concreción del mismo, se desea dar respuesta a los objetivos específicos que se formulan a continuación en forma de poreguntas:

1) Biometría, datos biométricos, sistemas biométricos: ¿en qué sentido se han venido empleando históricamente estos conceptos y en qué sentido se emplean en el siglo XXI?
2) Cuáles son las diferencias más significativas entre los sistemas de reconocimiento automatizado mediante Biometría y los sistemas que con los mismos fines se habían venido empleando hasta el momento.
3) Cuál es *la naturaleza* de la información biométrica que se emplea como base de los sistemas de reconocimiento automatizado mediante Biometría.
4) Qué cualidades deben reunir la información biométrica para poder servir de base a un sistema automatizado de identificación.
5) Qué tipo(s) de datos biométricos se emplean con fines de reconocimiento y qué tipo de clasificación o agrupación cabe hacer de los mismos.

---

[156] Las expresiones *interoperancia* e *interoperatividad* se emplean en la bibliografía y documentos relativos a la identificación biométrica, pero aún no están en el diccionario de la Real Academia de la Lengua Española.

[157] CREWS jr., C. W. "Human Bar Code", cit., p1 y ss.

[158] DAVIS, R. *Biometrics Myths: Six of the Best*, 2001; FOESSEL M./ GARAPON A., "Biométrie: les nouvelles formes de l'identité", *Esprit*, 2006, pp. 165-167.

6) Fortalezas y debilidades de los sistemas de reconocimiento mediante Biometría comparando el tipo de información que sirve de base la sistema.

7) En qué sentido ofrecen un servicio de "reconocimiento" o de "identificación" de las personas los sistemas biométricos.

8) Cómo funcionan los sistemas de reconocimiento mediante Biometrías estáticas y dinámicas.

9) Cuál es la distancia entre la información en crudo y el llamado *patrón biométrico* –o dato que almacenan los sistemas de reconocimiento biométrico.

10) Cómo afrontan el reto de la unicidad, en comparación con los métodos forenses, y cómo manejan el umbral de tolerancia.

11) Cuáles son las limitaciones y riesgos de estos sistemas desde el punto de vista de su base científica.

12) Cuáles son las limitaciones y riesgos de estos sistemas desde el punto de vista de las tecnologías que aplican.

13) Cuáles son las limitaciones y riesgos de estos sistemas desde el punto de vista ético y social.

14) En qué contextos operativos se emplean en la actualidad tanto en Europa como en otras regiones del mundo.

15) Valoración de la aceptabilidad y legitimidad en diferentes contextos operativos.

16) En comparación con los datos obtenidos del ADN humano, ¿qué estatuto tienen los datos biométricos que se emplean con fines de reconocimiento en diferentes países?

17) Conclusión final. La pregunta de partida de esta investigación era: "No hay duda de que en el actual contexto social necesitamos sistemas ágiles y fiables para gestionar la identidad de las personas. Pero, ¿Son los sistemas automatizados de reconocimiento biométrico, esos sistemas ágiles y fiables que necesitamos?". Es decir, ¿hasta qué punto y en qué sentido las tecnologías de reconocimiento biométrico pueden, en estado actual de la ciencia y la tecnología, ofrecer calidad y eficiencia en el reconocimiento de las personas y cuál es el coste social que se deriva de su aplicación en diferentes formatos y escenarios operativos?

Universitat d'Alacant
Universidad de Alicante

3. Materiales y métodos

3.1. METODOLOGÍA DE LA INVESTIGACIÓN Y MATERIALES EMPLEADOS

Se trata ésta de una investigación empírica que a través de la experiencia y la observación busca hallar la respuesta a las preguntas que acaban de describirse en el apartado anterior. En primer lugar, ¿hasta qué punto y cómo ofrecen las tecnologías de reconocimiento biométrico la posibilidad de identificar a un ser humano con único en el mundo? Y, en segundo lugar, ¿qué razones están permitiendo y cuáles deberían impedir construir infraestructuras de reconocimiento biométrico "que aseguren la identificación en todo momento"? La primera de las tareas emprendidas ha consistido en subdividir la investigación atendiendo a la metodología y al tipo de materiales previsiblemente necesarios para dar respuesta a las sub-preguntas comprendidas en esas dos grandes cuestiones, y que han sido descritas como objetivos específicos.

Universitat d'Alacant
Universidad de Alicante

En la tarea de establecer hasta qué punto y cómo ofrecen las tecnologías de reconocimiento biométrico la posibilidad de identificar a un ser humano *como único en el mundo*, la investigación ha consistido en abordar el estado del arte del reconocimiento biométrico en diferentes modalidades y comprender el diseño y el funcionamiento de las aplicaciones tecnológicas que se han creado con base en él. La taxonomía de los datos biométricos que sirven actualmente de soporte a estos sistemas y los métodos de captación de dichos datos son, sin duda, una de las piezas clave. Se han estudiado, asimismo, los modos en que las tecnologías biométricas captan, miden y almacenan las características de una persona para cuando ésta regrese a futuro y solicite una verificación de su identidad.

Esa línea de la investigación ha requerido la consulta de varios tipos de fuentes bibliográficas y documentales, correspondientes a disciplinas como la Antropología Biológica, la Medicina Forense, la Inteligencia computacional y la ingeniería informática (tanto en términos de procesamiento, como de captación de imágenes, señales corporales y otros tipos de información

obtenidos del cuerpo de las personas). La atención se ha concentrado especialmente en artículos de revistas indexadas y monografías publicadas en español, inglés, francés, alemán o italiano, algunas de las cuáles han sido consultadas en las estancias breves de investigación que en estos años se han realizado en el Instituto *Max Planck* de Heidelberg (Alemania, 2012 y 2015), en el *Institute of Advanced Legal Studies* de la Universidad de Londres (Reino Unido, 2013) y en la Academia Europea *EURAC* de Bolzano (Italia, 2014). Al resto de las fuentes se ha tenido acceso gracias a buscadores y plataformas como los de *Science Direct*, *Scopus*, *Elsevier*, o *HeinOnline*, *Emerald Insight* y JSTOR, y el servicio documental de la Universidad del País Vasco/ Euskal Herriko Unibertsitatea.

Otra importante línea de trabajo ha concentrado la atención en las limitaciones y riesgos de estos sistemas, así como en su coste social. Las limitaciones requieren tener en cuenta no sólo las disciplinas que se han advertido ya y que están implicadas en el procesamiento de los datos en crudo y los patrones de reconocimiento, sino que entran también en consideración cuestiones relativas a la seguridad de las Tecnologías de la Información y de la Comunicación para las cuáles han sido consultados trabajos de ingeniería informática y de ciberseguridad, bien publicados bien distribuidos a través de las páginas web de grupos de investigación como el de la Universidad estatal de Massachusetts o la Universidad estatal de San José (*National Biometric TEST Center* de los EEUU). Se ha atendido, asimismo, a los trabajos que la *National Bureau of Standards*, la asociación británica *Biometrics* o la norteamericana *Biometrics Industry Standards*, así como los proyectos de la UE CASCADE y BIOTEST y la ISO han realizado con el propósito de contribuir a la estandarización de diferentes aspectos de las tecnologías de reconocimiento biométrico.

Universitat d'Alacant
Universidad de Alicante

Han sido claves también los documentos publicados con ocasión de investigaciones realizadas por consorcios entre gobiernos y empresas, o tras proyectos como BIOTEST, ESPRIT, el proyecto BANCA (de comercio electrónico) o, más recientemente, los proyectos HIDE, y en relación con las biometrías comportamentales FAST y ADABTS.

El coste social, por su parte, forma parte de las dimensiones éticas y sociopolíticas de la aplicación de las tecnologías de reconocimiento biométrico y se han realizado contribuciones a esta temática no sólo desde las áreas experimentales y técnicas ya mencionadas, sino también desde la Ciencia Política y el Derecho y la Ética aplicada a las biotecnologías. Junto con algunos trabajos académicos, se han estudiado críticamente documentos publicados por organizaciones no gubernamentales (como las asociaciones a favor de las libertades civiles o de las libertades

informáticas[159]), y materiales institucionales –de Parlamentos y de Departamentos Gubernamentales (como el Departamento del Tesoro o el Departamento de Seguridad Interior de los EEUU), e informes que expertos e instancias independientes han realizado a solicitud de gobiernos y parlamentos. Importantes también, sin duda, los pronunciamientos de las autoridades[160] a las que está encomendada la protección de datos de carácter personal, como el Supervisor Europeo para la Protección de Datos y el GT WP 29 de la Unión Europea, el Comité Consultivo del Convenio nº 108 del Consejo de Europa, la Agencia Española de Protección de Datos de Carácter Personal y otras autoridades similares en los países occidentales, como es el caso del *Garante* italiano.

Los documentos y publicaciones revisados se han analizado de forma sistemática y crítica al servicio de los objetivos de la presente investigación, procediendo a reconocer en ellos razones y conclusiones, observando la fundamentación de las diferentes afirmaciones que se realizan (las evidencias y las razones) y extrayendo de todo ello los hallazgos que han sido incorporados a los capítulos de resultados.

Por último, se ha procedido a estudiar estos sistemas dentro de diferentes sistemas operativos. Esta parte ha sido, sin duda, la más compleja de completar. Buena parte de los sistemas actualmente operativos se han implementado sin un mínimo de transparencia deseable y resulta difícil acceder a datos fiables. En primer lugar, se han obtenido referencias a partir de publicaciones como *Biometrics Tech Today* y otras de las grandes corporaciones, y de reportajes de prensa especializada; en segundo lugar, otros datos se han extraído de las publicaciones académicas en forma de monografías, capítulos de libro, artículos o actas de congresos; una tercera fuente destacada han sido informes realizados por las instituciones e informes que expertos independientes realizaron para algunos parlamentos (como los de Alemania, Estados Unidos, Reino Unido o el Parlamento Europeo); por último debe señalarse, que también se ha procedido a analizar casos que han sido sometidos a la consideración de los tribunales o de las autoridades de protección de datos de carácter personal (la Agencia Española de Protección de Datos o el *Garante* Italiano), junto con la normativa y la doctrina jurídica que ha dado respuesta a los mismos.

---

[159] *American Civil Liberties Union – ACLU*, E*lectronic Frontier Foundation, Electronic Privacy Information Center*, *Center for Democracy and Technology* y Privacy Coalition.

[160] Como, por ejemplo, el proyecto *BioIS,* elaborado en Alemania en los años 1999 y 2000 con la coordinación de los Departamentos Federales de Seguridad Informática y de Criminalidad con la colaboración de varios entes de investigación, o el proyecto IPTS (ya citado) elaborado para la comisión de libertades del Parlamento Europeo.

3.2 ESTRUCTURA DE LA PRESENTACIÓN DE LOS RESULTADOS

El primero de los capítulos de la presentación de resultados aborda el estado actual del conocimiento científico que sirve de base a la identificación mediante Biometría. Esto es, la información biométrica que sirve de soporte a las tecnologías de reconocimiento. En él se procede a establecer con rigor conceptos que, con frecuencia, aparecen confusos en los debates, como es el caso del *dato biométrico*, en relación con la *fuente de la que se obtienen los datos biométricos* y el *dato en crudo*. Se presentarán, asimismo, aquellas cualidades que debe reunir una característica biométrica para constituir la base de un sistema de identificación automatizado, y se profundizará en las formas de captación de los datos biométricos dinámicos y estáticos, procediendo en la discusión a comparar las fortalezas y debilidades de cada uno de los conjuntos.

El segundo de los capítulos de la exposición aborda el funcionamiento y las utilidades de los sistemas de reconocimiento biométrico y aquellas limitaciones que en la actualidad entendemos que los separan de la mítica perfección que se les atribuye. Como se verá, algunas tecnologías se emplean con fines de verificación, otras con fines de identificación en sentido estricto y cabe también la posibilidad de un uso fines de cribado biométrico. En este capítulo se procederá a clarificar una serie de elementos que son relevantes para determinar la eficiencia de estos sistemas. Así, determinados aspectos organizacionales y técnicos, que van desde la base científica escogida hasta las formas de enrolamiento o almacenamiento, incidirán en la calidad de las aplicaciones y en la seguridad de los correspondientes sistemas de reconocimiento mediante Biometría. Sentada esa base se abordarán las limitaciones y riesgo de los sistemas automatizados de reconocimiento mediante Biometría agrupados en tres bloques: limites que tienen origen en la base científica de los sistemas; limitaciones y riesgos que tienen su origen en aspectos de las tecnologías informáticas que sirven de soporte a los sistemas; y limitaciones y riesgos desde la perspectiva ética y social.

En el tercer capítulo de resultados se analizan los sistemas de reconocimiento mediante Biometría desde la perspectiva de su funcionamiento en diferentes escenarios operativos, se atiende a su diversidad de diseño y a los usos con los que se emplean, y se persigue evaluar la legitimidad y la proporcionalidad de cada uno de estos usos.

Universitat d'Alacant
Universidad de Alicante

PARTE II

RESULTADOS DE LA INVESTIGACIÓN Y DISCUSIÓN

Universitat d'Alacant
Universidad de Alicante

Universitat d'Alacant
Universidad de Alicante

Capítulo 1

La información biométrica y los datos biométricos. La base científica de los sistemas automatizados de identificación mediante biometría.

1. ¿QUÉ TIPO DE *INFORMACIÓN BIOMÉTRICA* MANEJA UN SISTEMA DE RECONOCIMIENTO BIOMÉTRICO?

1.1. Algunas observaciones sobre la diversidad terminológica y el modo en que se ha abordado

Con el objetivo de anclar la valoración de las tecnologías de reconocimiento biométrico en la realidad, se aborda aquí con detalle en qué consiste la información biométrica que sirve de base dichos sistemas. Hemos de realizar, en este primer apartado, una advertencia en relación con la terminología. Aunque la literatura de las diferentes disciplinas implicadas en el estudio del reconocimiento biométrico, las corporaciones empresariales del sector y las instituciones públicas llevan más de una década prestando atención a estos sistemas, lo cierto es que no se ha llegado aún a un consenso sobre el uso de términos clave como los de información biométrica o dato biométrico, entre otros[1]. Ello explica que expresiones muy similares sigan empleándose en diferentes acepciones.

Universitat d'Alacant
Universidad de Alicante

Para evitar confusiones, algunas instituciones han realizado propuestas sobre el uso de la terminología biométrica que están contribuyendo a clarificar y homogeneizar la terminología pero, en nuestra opinión, las discrepancias en el uso de algunos conceptos siguen siendo importantes. Por tal motivo hemos optado por tener en cuenta varias de las propuestas, sin ceñirnos a una única, y escoger aquellos términos que estimamos más adecuados para referirnos a los principales conceptos. Dedicaremos los primeros apartados de este capítulo a realizar esas precisiones terminológicas.

Entre las propuestas terminológicas más destacadas, y que aquí se han tenido en cuenta como referencia, están, de una parte, la propuesta del Grupo Europeo para la Protección de Datos de Carácter Personal (GT-WP 29) y, de otra, los trabajos de la Organización Internacional de Normalización (ISO), realizados con diferentes fines. Como es sabido, el GT-WP 29 o *Grupo de Trabajo del artículo 29*, creado por la Directiva 95/46/CE, es un órgano consultivo independiente

[1] LIU, Y. "Privacy Regulations on Biometrics in Australia", *Computer Law & Security* 2010, p357.

que forma parte del entramado institucional de la Unión Europea. Lo integran las Autoridades de Protección de Datos de todos los Estados Miembros de la UE, el Supervisor Europeo para Protección de Datos de carácter personal y la Comisión Europea. Oficialmente se le conoce como GT– WP 29, aunque es frecuente aludir al mismo con el nombre no oficial de Grupo Europeo de/ o para la Protección de Datos. Este grupo de trabajo ha ido realizando importantes aportaciones en relación con las tecnologías de identificación biométrica y en lo que se refiere a la armonización terminológica destaca que haya tenido en cuenta el manejo que diferentes instituciones (nacionales o comunitarias) de ámbito Europeo estaban dando a la terminología biométrica[2].

Por su parte, la Organización Internacional de Normalización (ISO) y la Comisión Electrónica Internacional (IEC) tienen un Comité conjunto sobre las Tecnologías de la Información que se conoce como ISO/IEC - JTC1. En agosto de 2002 se creó dentro de este comité conjunto un subcomité de normalización específicamente dedicado a la Identificación biométrica. Dicho subcomité cuenta con 6 grupos de trabajo, en las siguientes áreas: 1) estandarización terminológica; 2) interfaces de comunicación; 3) formatos de datos; 4) definición de arquitecturas biométricas y perfiles de aplicación; 5) mecanismos de evaluación del os sistemas desde el punto de vista de su funcionalidad; 6) efectos sociales y jurídicos de la instalación de los sistemas. En el seno de la Asociación Española de Normalización y Certificación (AENOR) existe a su vez un comité "espejo" de ese subcomité 37 (SC 37). Tras años de trabajo el Grupo 1 de los citados adoptó y publicó en diciembre de 2012 el *ISO Vocabulary for Biometrics*[3], que se ha empleado aquí entre los documentos de referencia.

Universitat d'Alacant
Universidad de Alicante

1.2. Principales conceptos

1.2.1. *Información biométrica, dato biométrico y característica biométrica (o fuente de datos biométricos).*

Conforme a las definiciones que recoge el Diccionario de la Real Academia de la Lengua, *dato* deviene de *datum*, que en latín significa *lo que se da*. De ahí que se considere que, dentro del conjunto de la información en general, los datos se caracterizan por su *disposición*. ¿Qué es lo que caracteriza a los datos biométricos? En una de las definiciones más recientes, el *Garante* italiano afirmaba que un dato biométrico es *cualquier dato* obtenido de propiedades biológicas, aspectos comportamentales, características fisiológicas, hábitos o acciones que, además, reúne las cualidades de ser único, individual y mensurable en una persona[4]. Advierte el *Garante* que a los

[2] Véase por ejemplo: GT-WP 29, *Opinion 3/ 2012 on developments in biometric Technologies*, WP 193.

[3] MCIVER, R. *Biometrics,* en *Encyclopedia of Biometrics, Springer*, 2009, pp157-158.

[4] *Guidelines on Biometric Recognition and graphometric signature*, Anexo A de la Orden del Garante de 12 de noviembre de 2014.

efectos de considerar qué tipos de datos son aceptados dentro de dicha definición no es relevante que los métodos que se emplean para proceder a la medición impliquen un cierto grado de probabilidad. En el conjunto de los biodatos o datos que se obtienen del cuerpo de una persona – que tienen multitud de usos sociales[5]- los biométricos se caracterizarían así, no tanto por describir "propiedades naturales", cuanto por captar matemática o estadísticamente dichas *propiedades*[6]. De ahí que otros autores destaquen precisamente esta última particularidad, esto es, el hecho de que los *datos biométricos* son una proyección matemática, un reflejo de un estudio mensurativo o estadístico de una particularidad captada en los fenómenos biológicos dinámicos o estáticos que acontecen en el cuerpo de una persona[7].

Las definiciones a las que acaba de hacerse referencia resultan de gran utilidad cuando se trata de explicar en qué consiste el reconocimiento mediante Biometría en comparación, por ejemplo, con otros sistemas de reconocimiento. Pero puestos a precisar el modo concreto en que funcionan los diferentes sistemas, los tipos de procesos que acontecen para llevar a cabo estas formas de reconocimiento, la voz dato biométrico puede resultar excesivamente amplia. Y es que, como advierte MCIVER, la voz *dato biométrico* en ocasiones se emplea para referirse indistintamente a cualquiera de los datos que se manejan en las diferentes fases de funcionamiento de un sistema automatizado de reconocimiento biométrico[8]; y en otros casos, en cambio, se emplea para hacer alusión a las representaciones matemáticas de las medidas corporales de una persona o, por ejemplo, al patrón que en concreto es almacenado y objeto de comparación sucesiva en el futuro[9]. De ahí que con frecuencia y en aras a la claridad, suela recurrirse como vamos a ver a continuación a voces (o sub-voces) que formarían parte de la voz general "dato biométrico" pero ofrecen una mayor precisión.

El *Código de Privacidad* del *Biometrics Institute* de Australia definía la *información biométrica* como "*cualquier dato que pueda emplearse para identificar biométricamente a un individuo*"[10],

[5] SABOROWKSI, M. "Die Pluripotenz der Biodaten", en T. POTTHAST/ B. HERRMANN/ U. MÜLLER (eds), *Wem gehört der menschliche Körper?*, 2010, pp367-368.

[6] MORDINI, E./ TZOVARAS, D./ ASHTON, H. en *Second Generation Biometrics*, 2012, pp7-8.

[7] Se ha visto esta clasificación bipartita en la parte primera, 1.2.2.2. *Clasificación bipartita de datos biométricos atendiendo a las características de las que son tomados: datos biométricos estáticos y datos biométricos dinámicos.*

[8] Los hallazgos relativos al funcionamiento de los sistemas de reconocimiento mediante Biometría y sus diferentes fases se han recogido en el segundo de los capítulos de esta exposición de resultados.

[9] MCIVER, R. *Biometric Vocabulary – Standardization*, pp157-158.

[10] *Biometrics Institute Privacy Code*, Australia, 2006. Accesible en www.biometricsinstitute.org

mientras que el *Comité consultivo del Convenio 108*[11] se refería a la información biométrica como un concepto que incluía tanto los *datos en crudo* –sin definirlos - como los *patrones biométricos*[12].

Por su parte, la voz *dato biométrico* ha sido y aún es empleada con frecuencia en dos acepciones principales. Una primera no muy precisa, cual es la de "*característica biológica mesurable*" y otra, en nuestra opinión más acertada, que es la de "*resultado de la medición de tal característica*". La *característica biológica mesurable* no es, propiamente, un dato biométrico. Se trata más bien de una *posible fuente de datos* o de información, y será la aplicación de un método científico-técnico la que nos permitirá extraer de esa fuente datos biométricos.

También es oportuno destacar que hasta fechas recientes ha sido bastante común el uso indistinto de expresiones como *característica biométrica* o *dato biométrico* para referirse en ocasiones al rasgo físico o comportamental respecto del cual se desea realizar la medición, y en otras al resultado de ésta. Así por ejemplo, la Agencia Española de Protección de Datos (AGPD) en varios de sus pronunciamientos y resoluciones[13] dice que son datos biométricos "*aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión (tales como las huellas digitales, el iris del ojo, la voz, etc.)*". Sitúa como clave del concepto *aspectos físicos* –nótese que no se refiere a los aspectos dinámicos o comportamentales-, si bien indica que deben ser aspectos físicos que *mediante un análisis técnico permiten distinguir singularidades* entre las personas.

Universitat d'Alacant
Universidad de Alicante

1.2.2. *Datos en crudo y en fresco, y muestras biométricas*

El GT-WP 29 señala en su Opinión 4/ 2007 que las características físicas, fisiológicas, comportamentales o psicológicas de un individuo son fuentes de datos biométricos y destaca la importancia de distinguir entre, de una parte, *estas fuentes* y, de otra, *los datos métricos* que se obtienen de ellas[14]. Se distingue también entre los datos almacenados, o patrones, y los llamados

---

[11] Se conoce como tal al Comité que surgió con motivo del artículo 18 del *Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.

[12] CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*, Strasbourg 2005,p. 3, http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf.

[13]https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/1999-0000_Tratamiento-de-la-huella-digital-de-los-trabajadores.pdf

[14] GP-WP 29, Opinión 4/ 2007 de 20 de junio de 2007.

fresh data o datos que son captados en un momento posterior al enrolamiento, con el objetivo de verificar la identidad del sujeto mediante la comparación entre los datos almacenados y los nuevos datos.

Con la expresión datos en crudo (*Rohdata*, en alemán, o *Raw data* en inglés, *donnée brute* en francés) se hace referencia por algunos autores al conjunto de información *que es posible captar* de forma mensurativa a partir de un rasgo biológico o comportamental. En el caso de la información dactilográfica, por ejemplo, la impresión en tinta de una huella o su captación completa por parte de un escáner representan el dato *en crudo*. En el caso de la Biometría del iris, la fuente del dato es el iris en su conjunto y el dato en crudo que de él se toma es –con frecuencia- un bucle o espiral de su estructura que es característico y singularizante para cada persona. El Vocabulario ISO/IEC 1975 propone desterrar el término dato biométrico en crudo y emplear en su lugar la voz *muestra biométrica*, por entender que este segundo concepto es más preciso. Así, define muestra biométrica como *el resultado que se obtiene mediante la captura que realiza un sistema de identificación biométrica* cuando el sujeto se enrola o cuando el sujeto se coloca ante el dispositivo de captura por segunda vez. Esa muestra puede ser una captura analógica o digital de la característica biométrica, y normalmente no se procede a almacenarla en su totalidad; la mayoría de los sistemas proceden a extraer de esa muestra biométrica aquellos rasgos o particularidades (los atributos biométricos que se expondrán en el siguiente apartado); estos atributos son los que serán objeto de tratamiento informatizado[15]. Véanse las IMÁGENES 2 Y 55.

Entre los sistemas biométricos que emplean como referencia la misma característica o fuente de datos, existen con frecuencia notables diferencias en lo que se refiere a la *muestra biométrica* o dato en crudo a partir del cuál proceden a extraer los rasgos biométricos singularizantes. En el caso de las Biometrías faciales, por ejemplo, algunos sistemas captan la geometría (en el sentido de las relaciones entre determinados puntos característicos del rostro), mientras que otros sistemas tratan el rostro como un patrón general; y en el caso de las Biometrías auriculares, existen notables diferencias entre la muestra que emplean como referencia los sistemas 2D y los sistemas 3D.

1.2.3. *Atributos biométricos y plantillas o patrones biométricos*

A partir de la muestra biométrica (o dato en crudo) se procede a crear una plantilla o patrón biométrico. ¿De qué modo? En primer lugar se extraen de la muestra una serie de atributos biométricos o elementos característicos presentes en la muestra. Si bien las muestras podían ser

[15] KINDT, E. *Privacy and Data*, 2013, p.43, con referencias detalladas al *Vocabulario de Biometría ISO* en su versión de 2012.

analógicas o digitales, en los sistemas de reconocimiento automatizados todos los atributos biométricos son ya digitales. La extracción de atributos biométricos se realiza mediante algoritmos matemáticos que son los que determinan cuántos atributos y, en concreto, cuáles (o en qué localización) han de extraerse. Por ejemplo, una vez se binariza la imagen de una impresión dactilar (que sería la muestra), el sistema escoge cuáles de las minucias características de dicha huella van a extraerse. Como resultado de esa extracción se generan uno o varios sets de atributos y, a partir de ellos, se crea el patrón biométrico y se almacena para usarlo en posteriores comparaciones. Puede decirse, en coherencia, que el patrón es el conjunto de atributos de referencia que se almacena para un individuo en concreto. A esa patrón se le pueden vincular, si se desean, la información sobre el formato y la encriptación del patrón biométrico y cuantos otros datos se considere oportunos. Véase la IMAGEN 22.

La idea, al menos en hipótesis, es que los conjuntos de atributos (o patrones) sean una versión digital y comprimida de los elementos más singularizantes de la característica biométrica de referencia. Es decir, y siguiendo el ejemplo, que de forma comprimida hayan recogido aquello que más singulariza la huella dactilar de una persona o la geometría de su rostro. Del acierto en la elección de la muestra biométrica de referencia, en la selección del método mensurativo y en la detección de atributos realmente singularizantes (y suficientes) dependerá, sin embargo, que el objetivo se alcance o no. El patrón recibe en inglés el nombre de *biometric template* y en francés el de *empreinte numérique*, voz que destaca cómo se ha transformado la información del dato en crudo en un sistema numérico.

Ha de destacarse que el formato y el tamaño de los patrones biométricos varía notablemente de unos sistemas a otros. Es posible que se cree una tabla o se formule una cadena binaria (10100001) de determinada extensión, con más o menos detalles. Por ejemplo, las minucias pueden presentarse ofreciendo una lista de las coordenadas en que están localizadas, el patrón de iris como una cadena binaria y la geometría manual puede que se expresen mediante un vector de la longitud y el grosor de los dedos. De este modo, el tamaño en bits y bytes de un patrón que recoge por ejemplo los elementos más singularizantes de la geometría del rostro es significativamente menor que el tamaño que, en ese mismo caso, requeriría el almacenamiento de la imagen del rostro de referencia. Ello permite, como se abordará en detalle en el siguiente capítulo de los resultados, que los patrones sean almacenados en espacios muy pequeños –incluso en micro-procesadores (por ejemplo chips) incrustados en tarjetas inteligentes o en pasaportes (IMAGEN 74 e IMAGEN 75.3)- y los sistemas de reconocimiento procedan a realizar la comparación entre nuevos patrones y patrones almacenados a una gran velocidad.

Nótese, sin embargo, que el potencial singularizante que tiene una característica biométrica no es el mismo que ofrecen los patrones. Dos rostros pueden ser al ojo desnudo significativamente diferentes y cabe la posibilidad, sin embargo, que para un sistema de reconocimiento biométrico las diferencias captadas no sean tan notables. Del diseño y de la calidad en la captación de muestras y atributos, y del acierto en la selección de atributos singularizantes dependerá la mayor o menor capacidad de un sistema para distinguir entre individuos en los que la muestra biométrica de referencia guarde una importante similitud.

1.2.4. *Una distinción relevante: dato biométrico versus identificador biométrico*

Los datos biométricos (más que los atributos, los patrones biométricos) pueden ser empleados como identificadores *únicos* (UID), aunque es importante señalar que no siempre lo son. Un identificador único es un identificador que, en el conjunto de todos los identificadores que con el mismo fin se han atribuido a un conjunto de personas, se considera tan singular que –sin más datos- puede potencialmente emplearse para distinguir entre las personas. Socialmente empleamos UIDs que son números (en serie o atribuidos aleatoriamente), o pueden ser también códigos alfanuméricos, como el numero de DNI o el de los pasaportes. Si de un identificador único se dice que es *universal* ello implica que tiene la potencialidad para distinguir a una persona respecto al resto de los seres humanos que viven en el mundo (o incluso en el conjunto de quienes viven, han vivido y vivirán en él).

En la esfera global los identificadores únicos venían empleándose fundamentalmente para los objetos (como los números de serie de los coches, por ejemplo) o las organizaciones, pero en la actualidad se emplean para identificar a las personas. Los emplean, por ejemplo, los gobiernos y han surgido también en la lucha contra los fraudes de identidad[16]. En España se emplean códigos alfanuméricos para el DNI, con diferente forma de numeración para los nacionales y los residentes. Esos identificadores únicos se asignan aleatoriamente, aunque si bien no tienen una vinculación con la persona si mantienen numeraciones similares en el contexto de cada provincia. Cuando la información de una persona se almacena, existe una clave, un elemento identificador entorno al cuál se produce ese almacenamiento. Ese identificador es un conjunto de datos de la persona, sí, pero un conjunto de datos que tiene la particularidad de *representar a la persona.* El nombre completo, una dirección de email, un número de teléfono móvil o el número del carnet de identidad son algunos de los identificadores que sirvan para almacenar información de la persona, pero los operadores de los sistemas suelen preferir identificadores que limiten los errores. Por ejemplo el nombre y los apellidos no siempre resultan lo suficientemente

[16] COMITÉ DEL CONVENIO 108, *The introduction and use of personal identifi cation numbers: the data protection issues*, Consejo de Europa, 1991, p. 12.

singularizantes y en algunos casos plantean problemas, mientras que los códigos alfanuméricos (como un numero de móvil o el DNI con letra) plantean menos errores. Cuanto más grande es la base de datos, más importante es que las carpetas de datos estén asociadas a buenos identificadores únicos.

¿Sería posible que esa numeración tuviera una relación con la Biometría de la persona? La respuesta es sí. En India se ha implementado el *Aadhaar*[17], un sistema en el que el número de identificación de las personas está asociado a su biometría (IMAGEN 1.6). El patrón biométrico individual queda plasmado en un numero de 12 cifras agrupadas de cuatro en cuatro. Este identificador no garantiza la ciudadanía ni otorga derechos de las personas, pero sí acredita su identidad. También en el sistema de fichado de delincuentes de BERTILLON se empleaba la referencia de las medidas craneales como clave para la realización de búsquedas de las fichas de los delincuentes; es decir, se generaba un identificador basado en tales medidas, si bien en las fichas se recogían otras medidas corporales junto con la ficha policial de la personas.

Esto no significa, sin embargo, que cualquier dato biométrico pueda cumplir una función de identificador universal único. Es más, en algunos casos, ni siquiera podrían cumplir la función de identificadores únicos dentro de un sistema. Piénsese, por ejemplo, en un sistema de verificación que asocia la posesión legitima de una tarjeta con dos Biometrías: una obtenida de la Biometría del rostro y otra de las huellas dactilares; estadísticamente el nivel de singularidad que necesitamos para cada uno de esos dos patrones no ha de ser excesivamente elevado y podría darse un caso como el de los dos *Will West*[18] en la geometría del rostro o en el patrón de las huellas. Más difícil será, sin embargo, una coincidencia en los tres elementos que este sistema tiene de referencia: posesión de la tarjeta, coincidencia de la geometría del rostro y coincidencia de la huella.

2. LAS *CUALIDADES* QUE DEBEN REUNIR LAS CARACTERÍSTICAS BIOMÉTRICAS PARA PODER SERVIR DE SOPORTE A UN SISTEMA DE RECONOCIMIENTO MEDIANTE BIOMETRÍA.

Al genoma humano se le calculan más de 10 millones de polimorfismos, lo cual lleva a presumir que entre dos seres humanos no emparentados cabría encontrar millones de diferencias genéticas que, junto con la interacción con otros factores, les hacen tener una apariencia física y comportarse de formas diferentes[19]. Sobre cualquiera de esas diferencias genéticas o en las manifestaciones estáticas o dinámicas de las mismas cabe plantearse la localización de

[17] Más detalles sobre este sistema en el capítulo 3 de la PARTE II, Capítulo 3, Epígrafe 4. La Biometría en las relaciones entre los Estados y sus nacionales y residentes.
[18] Véase en la parte primera, 1.2.3.2. El caso del os dos Will West.
[19] GOLDSTEIN, D.B./ CAVALLERI, G.L. "Understanding human diversity", *Nature*, vol 437, 27 de octubre de 2005, pp1241-1242.

información biométrica con potencial singularizante. Adentrarse, sin embargo, en diseñar y construir un sistema de reconocimiento basado en información biométrica requiere tener en cuenta más consideraciones que el potencial singularizante de la información en sí misma. Las características estáticas o dinámicas que se escojan como referencia deben *de forma suficiente* una serie de cualidades que garanticen que el esfuerzo de crear y establecer el sistema de identificación se verá compensado con un rendimiento razonable en su funcionamiento a corto, medio y largo plazo.

Decimos que estas cualidades deben reunirse de forma suficiente porque, como se verá, puede que no todas las características lleguen reunir de igual forma (o en el mismo nivel) las cualidades que aquí van a reseñarse. Esa circunstancia hará que no todos los sistemas ofrezcan el mismo nivel de eficiencia y seguridad en su funcionamiento, como analizaremos de forma comparativa al final de este capítulo. Es comprensible, en coherencia, que no pueda predecirse los resultados que dará un sistema de reconocimiento mediante Biometría "estudiando otro", o un conjunto de éstos. Cada característica presenta una potencialidad y la eficiencia del sistema dependerá tanto de la potencialidad singularizante de la característica en sí, como del modo en que su diseño haya tenido en cuenta elementos tan relevantes como los perfiles de la población diana o el escenario operativo en que se aplicará.

Para precisar y desarrollar qué cualidades son imprescindibles en una característica biométrica de cara a construir sobre ella un sistema de reconocimiento, la literatura recurre a la formulación de listados más o menos extensos. Vamos a realizar un repaso crítico de dichos listados, procediendo a proponer argumentadamente el nuestro. Una de las propuestas más conocidas es la que describe estas cualidades con la los *Siete pilares del Saber Biométrico* (Seven Pillars of Biometrics Wisdom)[20]. WAYMAN, por su parte, se refiere a las *Cinco cualidades ideales de las características biométricas*[21], y el Grupo de Trabajo del artículo 29 (GT WP 29) indica de forma más sintética los *tres requisitos* que deben reunir los datos biométricos[22]. El listado más amplio de los que hemos encontrado es el de CLARKE, que procede a señalar 12 requisitos[23] de referencia.

---

[20] Vid. JAIN, A. K. / BOLLE, R./ PANKANTI, S. *Personal Identification in Networked Society*, 1999, pp22 y ss; IPTS, *Biometrics at the Frontiers*, 2005, pp32-34: MARTÍNEZ JARRETA, M. B. voz "*Biometría* ", en *Enciclopedia de Bioderecho y Bioética*, 2011, pp257-26.

[21] WAYMAN, J./ JAIN, A./ MALTONI, D./ MAIO, D. (eds), *Biometric Systems*, 2005, p3-4.

[22]Página 4 del Informe elaborado para la Comisión Europea por el *GT-WP 29*: universal, captable como única y permante; IPTS, *Biometrics at the Frontier* (informe para la Comisión LIBE del Parlamento Europeo), p.37; MORDINI, E./ MASSARI, S. "Body, Biometrics and Identity", *Bioethics J.*, 2008, p489.

[23] CLARKE, R. "Human Identification in Information Systems", ITP 1994/4, pp7-8.

Si comparamos los listados, encontramos que muchas de las cualidades que se describen en los listados más extensos son subcategorías de cualidades que pueden expresarse de forma más sintética o cualidades que no es imprescindible recoger, en tanto no son sólo necesarias para los sistemas biométricos automatizados sino que podrían predicarse de todos los sistemas de reconocimiento (incluso los que no tienen que ver, en sentido estricto, con los métodos biométricos).

Conforme a los *Siete pilares del Saber biométrico*, los datos biométricos que sirven de soporte a un sistema de reconocimiento deben reunir los requisitos de: *universalidad, potencial singularizante, permanencia del rasgo, posibilidad de captura, factibilidad, aceptación social y su potencialidad para resistir o esquivar los intentos de fraude o suplantación de identidad*. La universalidad implica que el dato empleado es una característica empleada en todos los seres humanos, el potencial distintivo se refiere al hecho de que cada persona sea portadora de atributos únicos en relación con la característica de que se trate y la permanencia del rasgo destaca la necesidad de que tanto la característica en sí como los atributos singularizantes se mantengan estables en la persona a pesar del paso del tiempo. La posibilidad de captura, su factibilidad en relación con el funcionamiento del sistema y su aceptación social no tienen ya tanto que ver con la característica en sí, sino con las implicaciones operativas y ético-sociales de un sistema de identificación basado en ella. WAYMAN, por su parte, nos dice que la característica biométrica debe ser: *robusta, distintiva, disponible, accesible y aceptable*; y el GT-WP del artículo 29 destaca que la característica biométrica de referencia debe reunir las cualidades de: universal, captable como única y permanente. Este es, por último, el listado de CLARKE:

Universitat d'Alacant
Universidad de Alicante

***LISTADO DE CARACTERÍSTICAS QUE DEBEN REUNIR LOS DATOS BIOMÉTRICOS QUE SIRVEN DE BASE A UN SISTEMA DE IDENTIFICACIÓN, POR R. CLARKE* (1994)**	
1) Universal	*1) Exclusivo*
2) Único[24]	*2) Preciso*
3) Permanente[25]	*3) Simple*
4) Esencial (inherente)	*4) De coste razonable*
5) Susceptible de recolección[26]	*5) De uso proporcionado*
6) *Almacenable*	*6) Aceptable socialmente*

Como se avanzaba ya, en la lista de CLARKE aparecen cualidades que ya no son, en sentido estricto, cualidades de la característica biométrica sino que se refieren al diseño y la arquitectura

[24] Que no sea idéntico en dos personas distintas.

[25] Que permanezca invariable en el tiempo

[26]En el sentido de susceptible de mesuramiento cuantitativo.

del sistema y a los dispositivos de software y hardware que se vayan a emplear para captar o medir aquella. Nosotros, en una propuesta que se acerca a la del GT WP 29, hemos agrupado en tres conjuntos las cualidades que creemos que son necesarias en una características biométrica que desea emplearse como base de un sistema de reconocimiento, y los desarrollaremos a continuación: 1) Cualidades que tienen que ver con la entidad de los rasgos y con el conocimiento científico que se tiene sobre ellos: *Universalidad, singularidad y permanencia*; 2) Cualidades que tienen que ver con la capacidad de los dispositivos y las aplicaciones informáticas: *Colectividad, capacidad de rendimiento y fiabilidad*; y 3) Cualidades que tienen que ver con la interacción entre los sistemas y las personas o el conjunto de la sociedad: la *aceptabilidad*.

2.1. Cualidades que tienen que ver con la entidad de los rasgos y con el conocimiento científico que se tiene sobre ellos. *Universalidad, singularidad y permanencia.*

La observación de que en algunos rasgos biológicos están presentes las cualidades de universalidad, singularidad (o univocidad) y permanencia es lo que, como se ha visto ya[27] dio a pie a formular estudios destinados a contribuir al conocimiento biológico a través, entre otras cosas, del estudio de variables continuas. De la mano de esta línea de trabajo vino también la posibilidad de plantear sistemas de reconocimiento de las personas basados en el potencial singularizante de los datos biométricos (como el *Bertillonage*)[28]. Comparten los seres humanos una serie de elementos anatómico-físico y rasgos comportamentales –de ahí que se hable de *universalidad*-; y en dichos elementos es potencialmente posible detectar tal variabilidad inter-personal que tal información tiene la potencialidad de servir para distinguir a las personas (singularidad o univocidad).

Pero el esfuerzo de construir un sistema de reconocimiento social con base en esas características universales y singulares sólo parece razonable, claro está, si son características que *permanecen* en las personas a pesar del paso del tiempo. Sólo así podremos garantizar un uso prolongado de los sistemas que justifique el despliegue de medios necesarios para implantarlos. Esa *permanencia* implica que la variabilidad intra-personal de la característica o características escogidas sea la mínima posible y no se vea afectada por condiciones ambientales o temporales. Veamos con algo más de detalle estos tres grupos de cualidades.

---

[27] PARTE PRIMERA, 1.2 *Biometría, antropometría e identificación biométrica: precisiones históricas y primeras delimitaciones conceptuales.*

[28] PARTE PRIMERA, 1.2.3 *La primera experiencia biométrica en el sentido actual del concepto: el sistema antropométrico de identificación diseñado por Alphonse Bertillon (el Bertillonage o signalement anthropométrique).*

2.1.1. *Universal, disponible*

Aplicada esa reflexión al objetivo de este apartado, la exigencia de que un dato biométrico sea *universal* hace referencia a la necesidad de que se tome de un rasgo físico o biológico presente o latente, *en principio*, en todo ser humano[29]. Se dice "en principio", en tanto es posible detectar un deterioro grave o la ausencia total de alguno de los rasgos de referencia en una persona concreta. Ello puede deberse a alguna deformidad congénita o a un accidente o proceso de enfermedad; pero la construcción de un sistema sobre la base de una característica biométrica requiere que estos casos sean los mínimos posibles.

WAYMAN y JAIN se refieren a la *disponibilidad* de esta característica en el conjunto –o en la mayoría- de la población. Si bien determinadas manchas características, cicatrices o tintados en la piel, o la peculiaridad del cabello pueden resultar de utilidad en la identificación de una persona, esos elementos no pueden servir de soporte –al menos no de soporte único[30] - a un sistema de reconocimiento mediante biometría. Nótese que ello impediría enrolar a las personas en cuya piel no hubiera manchas, tatuajes o cicatrices suficientemente singularizantes, o –en el caso del pelo- a las personas sin éste (vid. IMÁGENES 49 y 50).

Puede decirse que las características que sirven de base a las Biometrías dinámicas que se emplean en la actualidad como base de algunos sistemas de reconocimiento son las más universales (las señales electrofisiológicas o la respiración, por ejemplo, están presentes en todo ser humano vivo), aunque se considera que algunas características estáticas también reúnen de forma suficiente la cualidad de la universalidad. Así, por ejemplo, si bien las huellas dactilares, el patrón del iris o la geometría del rostro pueden verse afectados o estar ausentes en una persona consecuencia de una enfermedad, accidente u otra circunstancia, se aceptan como universales porque, en principio, se entiende que son captables en la gran mayoría de los seres humanos. Esta afirmación, con todo, será revisada desde otra óptica en el capítulo 2 de esta exposición de resultados.

2.1.2. *Singularidad o, al menos, cualidad para una diferenciación suficiente* (variabilidad interpersonal)

---

[29] IPTS, *Biometrics at the Frontiers*, p.37; MORDINI, E./ MASSARI, S. "Body, Biometrics and Identity", *loc cit;* ZHANG, D./ LU, G. *3D Biometrics. Systems and Applications,* Springer, 2013.

[30] JAIN, A. K./ JIN, R. están desarrollando un proyecto sobre reconocimiento automatizado con base en cicatrices, marcas y tatuajes como herramienta de apoyo al FBI (Project-Tatoo): el proyecto *Automatic Matching and Retrieval of Scars, Marks and Tatoos.* Vid. HAN, H./ JAIN, A. K. "Tattoo based identification: Sketch to image matching", *Proceedings of the International Conference on Biometrics Compendium*, pp. 1-8, 2013 (http://www.cse.msu.edu/biometrics/Publications/SoftBiometrics/HanJain_TattooBasedIdentification_Sketch2ImageMatching_ICB13.pdf) y DUANGPHASUK, A./KURUTACH, W. "Tattoo skin detection and segmentation using image negative method," *Proceedings of the 13th International Symposium on Communications and Information Technologies*, pp. 354-359, 2013.

La característica que se emplea como base de un sistema de reconocimiento biométrico debe tener, además, la potencialidad de ofrecernos *un dato singular,* característico una persona; una información según la cual en dicha característica, por su composición, caracteres y dimensiones, existe algún atributo que es diferente en cada persona[31]. Unido a esto, claro está, necesitamos un método que sea capaz de captar de forma suficiente ese carácter distintivo. A este respecto veremos que hay rasgos de los que se presume un potencial distintivo elevado, pero con base en los cuáles a día de hoy el conocimiento científico disponible o las tecnologías existentes no permiten configurar un sistema de identificación sólido[32].

¿Cuándo podemos decir que en una característica biométrica concurre esta cualidad? En nuestra opinión son varias las claves que hay que tener en cuenta para dar respuesta a esta pregunta. De una parte, ha de tenerse en cuenta el potencial singularizante de la característica en sí misma; es decir, la tasa de variabilidad que existen en términos absolutos. Esto tiene que ver con la característica en sí, pero también el estado del arte. En algunos casos, como por ejemplo el iris, veremos que la comunidad científica expresó su convencimiento de que era posible diseñar sistemas de reconocimiento sobre su base mucho tiempo antes de que tecnológicamente dispusiéramos de sistemas capaces de captar y procesar su singularidad. Pero, de otra parte, valorar si el nivel de captación de la singularidad es suficiente es algo que sólo cabe hacer juzgando cada sistema en el contexto del escenario operativo en el que se desea aplicar. Es decir, que un mismo dispositivo de identificación de las personas a través de sus huellas dactilares y que concentre su atención en determinados atributos (como por ejemplo, un numero concreto de minucias) puede ser suficientemente capaz de distinguir en una población y ofrecer, sin embargo, resultados insuficientes en otros grupos diana. Por ello, la singularidad de un característica – o su potencialidad para una diferenciación suficiente- se evalúa también atendiendo a la tasa de falsa aceptación que ofrece en cada uno de los sistemas de reconocimiento; esto es, en el número de veces que, por error, acepta a un tercero no-enrolado considerando que se trata de un usuario enrolado. Esto no depende (o no solo) de la variabilidad que en términos absolutos exista para esa característica biométrica o comportamental en el conjunto de sujetos diana, sino que guarda también relación con la capacidad que el sistema automatizado tiene de captar la variabilidad inter-personal.

Cuando una aplicación de reconocimiento mediante Biometría va a emplearse en un grupo reducido de personas entre las que, además, hay notables diferencias antropométricas, es posible

[31] MORDINI, E./ S. MASSARI, S. "Body, Biometrics and Identity", *Bioethics J.*, 2008, p489.

[32] Algún autor, como C.M. ROMEO CASABONA, se refiere a esta característica en el sentido de que el dato debe estar "individualizado" y ser irrepetible, vid. *Los perfiles de ADN en el proceso penal*, pp430-431.

que muchos rasgos reúnan este carácter de singularidad suficiente. Quizá no sea necesario que la característica permita un nivel elevado de diferenciación. Sí lo es, en cambio, cuando el objetivo es implementar los sistemas de reconocimiento en grandes grupos de población, como es el caso de su uso en los documentos nacionales de identidad o los pasaportes.

¿Cuándo puede decirse que el potencial singularizante es tal que la característica puede darse por única? El concepto de *unicidad* es un concepto resbaladizo, que requiere una cierta puntualización ya desde este momento. Sin perjuicio de que más adelante profundicemos en esta cuestión[33], que tiene gran trascendencia, ha de tenerse en cuenta que en puridad sólo podríamos aceptar como único un atributo (o un conjunto de ellos) cuando la posibilidad de hallar otro igual fuera de *cero.* Parece así que, de algún modo, la propia idea de la universalidad (o existencia de algo común en la característica) nos excluye estadísticamente la posibilidad de una unicidad en términos absolutos. Sin embargo, en el estudio de los sistemas de reconocimiento biométrico se emplea el concepto de unicidad en una forma similar a la que tradicionalmente maneja la ciencia forense. Esto es, cuando la posibilidad de hallar otro patrón biométrico igual (por ejemplo, un set de minucias dactilares, o una geometría del rostro iguales) se considera muy inferior al grupo de población de referencia en el sistema, entonces tiende a aceptarse que el patrón es único[34].

El modo en que cada sistema trata de captar y maximizar este potencial singularizante es algo muy relevante. De hecho, uno de los elementos en los que se evalúa la fiabilidad de un sistema es en el nivel de diferenciación de los patrones almacenados[35] y en la probabilidad de que aparezcan *gemelos biométricos*; esto es, personas para las cuáles el sistema ha almacenado patrones excesivamente similares y, en consecuencia, hace probable que se confundan entre sí.

2.1.3 *Permanente, invariable o suficientemente estable (respecto del sujeto fuente)*

Un sistema de reconocimiento necesita garantizar que todas aquellas veces en que el sujeto fuente se presenta ante el dispositivo de identificación (ofreciendo nuevos datos en fresco), el sistema será capaz de reconocer a esta persona, comparando los nuevos datos con los patrones, y determinando que se está ante *la misma persona*[36], ante la persona de la que el sistema obtuvo

[33] Véase en el capítulo 2 de esta PARTE II, los epígrafes 6.1.1 y 6.1.2.

[34] Vid. JAIN, A./ PRABHAKAR, S./ PANKANTI, S. 'On the similarity of identical twin fingerprints', *Pattern Recognition*, 2002, pp. 2653–2663 y, en relación con las diferencias de patrón obtenido del iris en los gemelos monocigóticos, DAUGMAN, J. ,"Interview. Pattern recognition", en *BioSocieties* 2008, p. 82.

[35] ZHANG, D./ LU, G. *3 D Biometrics. Systems and Applications*, Springer, 2013.

[36] VIELHAUER, C. *Biometric User Authentication*, 2006, p22-24.

en su día el patrón almacenado[37] (IMAGEN 69). Verificamos que alguien es quien alega ser o reconocemos en alguien aquellos elementos con los que hemos configurado –construido- *determinada identidad* en nuestro sistema. En consecuencia, necesitamos que la característica biométrica singularizante que se ha escogido como referencia permanezca invariable en el sujeto, y que a pesar de que pase el tiempo o concurran otras circunstancias ambientales, cada vez que el sujeto muestre sus rasgos al dispositivo el sistema sea capaz de asociarlos correctamente al patrón almacenado. Es decir, que el sistema tiene que *darse cuenta* de que dos muestras o patrones que se le remiten, *provienen del mismo sujeto*. Si envejece el patrón y ya no sirve, es como si no tuviéramos enrolado al sujeto.

Para expresar esta idea de estabilidad se emplea el término permanente, aunque hemos de hacer algunas reflexiones al respecto. Conforme al diccionario de la RAE, permanente es aquello que se mantiene "*sin mutación en un mismo lugar, estado o calidad*". En ese sentido estricto, no parece posible aplicar este adjetivo a ningún atributo biológico o comportamental. Advertía KIRK en el manual *Crime Investigation* (1974) que "no hay dos objetos iguales". Si al comparar dos objetos biológicos encontramos propiedades que dificultan la distinción entre ambos y, además, consideramos que tales propiedades son "suficientes", podemos llegar a establecer que ambos objetos; por ejemplo, que dos muestras biológicas proceden de una única fuente (un mismo cuerpo humano). Así, una huella dactilar recogida en la escena de un crimen y la que se ha tomado de una persona sospechosa no serán totalmente idénticas (porque el nivel de roce entre el dedo y el objeto, y la presión que se realiza generan diferencias), pero es posible que las propiedades que en la comparación son aceptadas como idénticas sirvan para determinar que las huellas pertenecen a una misma persona.

Tampoco *serán nunca idénticos* dos patrones biométricos (WEIR dice que *no pueden serlo)*, pero su comparación podrá llevar a demostrar que existen evidencias suficientes como para considerar que han sido originados por la misma fuente[38]. Esto explica que algunos autores, como WAYMAN/ JAIN/MAIO, en lugar de permanente, indiquen que la característica haya de ser *robusta*[39]. De hecho, en el contexto de los sistemas de reconocimiento biométrico *permanente* se emplea para referirse a aquellos atributos biométricos respecto de los cuales la variabilidad intrapersonal es muy pequeña o para casos en los que, al menos, es posible gestionar esa variabilidad de forma que no interfiera con el adecuado funcionamiento del sistema de reconocimiento. La medida en que dicha gestión se realiza o no de forma adecuada quedará reflejada, como veremos, en la tasa de falso

[37] PARTE PRIMERA, epígrafe 1.1.2
[38] WEIR, B. S., *Are DNA Profiles Unique ?* 114-117.
[39] WAYMAN, J./ JAIN, A./ MALTONI, D./ MAIO, D. (eds), *Biometric Systems*, cit., p3.

rechazo (o tasa que indica cuántas veces rechaza el sistema a un sujeto que fue debidamente enrolado)[40].

La permanencia se refiere, en principio, al ciclo vital del individuo, desde el nacimiento hasta su muerte, aunque hay algunos rasgos que se conservan *post mortem* (como las huellas dactilares, durante un breve periodo de tiempo y especialmente toda información contenida en el ADN, que se conserva mientras quede algún tipo de vestigio biológico). No obstante, una fórmula que muchos sistemas de reconocimiento biométrico introducen para afrontar el envejecimiento de los patrones consiste, precisamente, en re-enrolar periódicamente a los sujetos, exactamente igual que se hace con los plazos de vigencia y fechas de expiración de documentos identificativos como el DNI o los pasaportes. En términos relativos, por tanto, la permanencia o estabilidad será deseable durante al menos el tiempo que deberá transcurrir entre el primer enrolamiento y los enrolamientos periódicos que sigan a éste.

Algunos autores interpretan que la imposibilidad de modificar voluntariamente el rasgo ha de entenderse como una cualidad vinculada a la permanencia, aunque otros como CLARKE consideran que dicha imposibilidad expresa una cualidad diferente; esto es, la cualidad de *inherencia* de la característica biométrica[41]. Ello es visto como garantía frente a la manipulación y/o la suplantación de identidades. Los patrones dentales o la Biometría del esmalte dental o el cabello ofrecen una tasa muy baja de cumplimiento de este requisito, como sucedería si empleamos como referencia el cabello de las personas. En relación con el resto de las características, en cualquier caso, pueden ser modificadas de forma temporal o definitiva y con diferentes niveles de precisión mediante intervenciones biomédicas, pero es difícil que lleguen hasta posibilitar la suplantación. Operaciones de cirugía estética del rostro, trasplantes de huellas dactilares[42], cambios de la coloración de la piel, implantes, etc. pueden hacer que una persona se libere de los rasgos que lo dan por enrolado (y le den una nueva identidad en el sistema), pero es poco previsible –por la precisión que requeriría la intervención- que se puedan generar en alguien rasgos idénticos a los de otra persona.

[40] PARTE SEGUNDA, Capítulo 2, apartado 4.3.

[41] MARTÍNEZ JARRETA, M. B. Voz "Biometría ", cit; JAIN, A. K./ ROSS, A./ PRABHAKAR, S., "An Introduction to Biometric Recognition", *IEEE Transactions*, 2004, pp4-5.

[42] SZAJERKA, T./ JUREK, B./ JABLECKI, J. "Transplanted fingerprints: a preliminary case report 40 months posttransplant", *Transplant Proc 2010*, Nov 42 (9), 3553-55.

2.2. Cualidades que tienen que ver con la capacidad de los dispositivos y las aplicaciones informáticas. *Colectividad, capacidad de rendimiento y fiabilidad.*

Para servir de base a un sistema de reconocimiento automatizado mediante biometría, es necesario que la característica biométrica de referencia se pueda captar métricamente y que ofrezca a los sistemas un nivel suficiente de calidad de reconocimiento.

2.2.1. *Colectividad, accesibilidad*

La colectividad no se refiere únicamente a la posibilidad de una única captación; es necesario que de la característica de que se trate pueda obtenerse información en todas las ocasiones y situaciones en que haya de emplearse el sistema. Es decir, que si las condiciones ambientales en las que una persona es enrolada diferirán de aquellas en las que se realizará, a futuro, la verificación o reconocimiento, la característica deberá ser captable en ambos contextos. Imagínese que el enrolamiento se produce en unas condiciones controladas de iluminación, de temperatura o de pureza ambiental, pero que el reconocimiento a futuro deba realizarse en unas condiciones no controladas (por ejemplo mediante un dispositivo de captación que está situado al aire libre en una instalación militar en un desierto de arena, que se ve cotidianamente afectado por el polvo, además de expuesto a altas variaciones de luz y temperatura entre el día y la noche).

No todas las características singularizantes son fáciles de captar. Por ejemplo, en la actualidad, no hay duda de que el ADN de las personas es una fuente potencial de información biométrica, pero, presenta dificultades para su recolección y procesamiento con la agilidad y eficiencia que se espera de los sistemas de reconocimiento automatizado[43]; de hecho, como se verá, algunos autores excluyen la Biometría del ADN de la tipología de datos biométricos que pueden servir de base a sistemas de reconocimiento automatizado, a pesar de que es previsible que en el futuro contemos con una tecnología adecuada para ello.

También presentan problemas de colectividad algunos de los datos biométricos dinámicos. La Biometría de habilidades motoras como la escritura, la forma de tecleado o la marcha, la Biometría vocal o la captación métrica de señales y parámetros corporales implican la obtención de información secuencial o cíclica. Esto es, requieren que tanto en el enrolamiento (en crudo) como en la verificación (o comprobación en fresco) esté expuesto al dispositivo de captación durante un lapso más o menos largo de tiempo. Metodológicamente, además, la cantidad de información secuenciada que puede ser necesaria registrar para extraer un patrón singularizante puede ser, en términos comparativos, bastante elevada.

[43] OCDE, Biometric based technologies, Paris, 30 de junio de 2004, p. 11.

1.2.2.2. *Rendimiento y fiabilidad*

La característica biométrica de referencia debe ofrecer un adecuado nivel de rendimiento en lo que se refiere a la identificación, y ha de presentar una cierta resistencia al fraude, en el sentido de que no pueda copiarse o imitarse con facilidad. Como hemos visto, algunos autores expresan esta cualidad como parte de la cualidad de permanencia o, al menos, como cualidad vinculable a ésta, pero otros autores consideran que la resistencia al fraude va más allá de la permanencia o inherencia de la característica biométrica de referencia. Dentro del rendimiento se evalúan las tasas de falsa aceptación y falso rechazo[44], y otro factor a tener en cuenta es el lapso de tiempo que el sistema necesita en el enrolamiento, en la captación del dato en fresco y/o en la realización de la comparación; ese tiempo, ha de ser *razonable*[45].

2.3. Cualidades que tienen que ver con la interacción entre los sistemas y las personas o el conjunto de la sociedad. La *aceptabilidad*.

Al describir las cualidades que debe reunir la característica biométrica que sirve de referencia al sistema, algunos autores indican que los sistemas de reconocimiento biométrico deberían ser *socialmente aceptables* o, al menos, *user-friendly*[46] en dos sentidos. En primer lugar, en el sentido de ser fáciles para el manejo de usuarios no adiestrados; y, en segundo lugar, de no generar problemas de aceptación por parte de los usuarios. Se considera que reúnen esta cualidad aquellas características que sirven de referencia a sistemas de reconocimiento a los que las personas se acostumbran con facilidad[47], con independencia de la razón por la que las personas muestren esa capacidad de adaptación. Por ejemplo, el hecho de que prestemos nuestras huellas para el DNI puede hacer que no nos sintamos incómodos si se nos pide colocar la huella digital en un lector de acceso a un parque temático o en un mecanismo de control horario de empleados, mientras que en algunos países –en los que las huellas sólo se usan con fines de persecución criminal- es posible que los ciudadanos sientan que un control biométrico de este tipo de algún modo *les estigmatizaría*. Difiere también la percepción de las personas en lo que se refiere a qué sistemas invaden más su intimidad corporal o su privacidad.

Son varios los proyectos europeos que, por parte de las corporaciones empresariales, las instituciones o las universidades, han abordado la aceptabilidad de los sistemas de reconocimiento biométrico y las características biométricas que sirven de base a estos sistemas

---

[44] ZHANG, D./ LU, G. *3 D Biometrics. Systems and Applications*, Springer. 2013.

[45] VIELHAUER, C. *Biometric User Authentication for IT Security*, 2006, p22-24.

[46] ZHANG, D./ LU, G. 3 D *Biometrics. Systems and Applications*, Springer, 2013.

[47] ITU-T, 2009, pp6-7.

son uno de los factores clave en esa aceptabilidad[48]. Las características biométricas tomadas del ojo, por ejemplo, son vistas con recelo (al menos en relación con dispositivos de captación que no pueden usarse a distancia) por un miedo -a veces injustificado- a sufrir lesiones, y en algunas culturas las personas se muestran reacias a ser fotografiadas.

3. CRITERIOS DE CLASIFICACIÓN DE LAS BIOMETRÍAS QUE SIRVEN DE BASE A LOS SISTEMAS DE RECONOCIMIENTO

Para presentar las características biométricas que pueden servir de base a una obtención suficientemente universal, singularizante y permanente de patrones biométricos, la literatura suele proceder a enumerarlas y describirlas una a una comenzando por aquellas respecto de las cuáles contamos con métodos de captación métrica más asentados o, al menos, de mayor tradición (como es el caso de los dermatoglifos, patrones de iris, o la geometría del rostro y de la mano), dando paso después a características que sirven de base a sistemas que están aún en fases más o menos avanzadas de desarrollo. En tanto la lista ha ido creciendo en la última década, es frecuente proceder, antes del listado, a ofrecer alguna fórmula de clasificación que permita al lector hacerse una idea del panorama completo. Este tipo de clasificaciones atienden, entre otros, a la naturaleza de las fuentes de información biométrica de referencia (normalmente ofreciendo una clasificación bipartita[49] o tripartita), al momento histórico en el que han ido desarrollándose los métodos que permiten obtener patrones a partir de las características (señalando, por tanto, décadas o generaciones de sistemas de reconocimiento mediante biometría) [50] o a una distinción entre métodos uni-, bi- o tridimensionales.

Universitat d'Alacant
Universidad de Alicante

En este epígrafe prestaremos atención a dos clasificaciones que, aunque no son la que hemos escogido para presentar las características biométricas que se emplean en la actualidad como base de los sistemas de reconocimiento, son clasificaciones que nos parece interesante tener en cuenta para completar la presentación del conjunto. Se trata de las clasificaciones que tienen una base cronológica (o histórica), distinguiendo generaciones de tecnologías de reconocimiento biométrico, y de clasificaciones que atienden al número de dimensiones con que son captados los datos. Por otra parte, y de cara a comprender el funcionamiento los sistemas multimodales, esto es, sistemas de reconocimiento mediante Biometría que combinan una o más Biometrías –como

---

[48] El proyecto BioSec (2003-2005): ESCHENBURG, F./ BENTE, G. / TRITZSCH, H. / POWIERSKI, R. / FISCHER, O. "The Biosec Mobile Usability lab for biometric security systems", *Third Cost 275 Workshop*, pp63-7.K; UNYSIS, *Global Acceptance of Biometrics among Consumers*, 2009.

[49] PARTE PRIMERA. 1.2.2.2. Clasificación bipartita de los datos biométricos atendiendo a la tipología de las características humanas de las que son tomados: estáticos y dinámicos.

[50] Es el caso, por ejemplo, de JAIN/ KUMAR, o de MORDINI/TZOVARAS.

es el caso del que da soporte al pasaporte biométrico europeo, que combina Biometría dactilar y Biometría del rostro- se realizarán aquí algunas consideraciones sobre el sentido en el que se emplea la clasificación o distinción entre *soft*, *weak* y *robust biometrics.*

Tras este apartado introductorio, y de cara ya a ordenar los resultados de la investigación realizada, la clasificación que nos ha parecido más útil es la que agrupa las características biométricas de referencia distinguiendo entre Biometrías estáticas y Biometrías dinámicas. Se presentará a continuación, y será objeto de aplicación a partir del epígrafe número 4 de este capítulo.

3.1. Clasificación de los métodos biométricos que sirven de base a los sistemas de identificación, atendiendo a la naturaleza dinámica o estática de la información que les sirve de referencia.

Cercanas a la clasificación entre Biometrías dinámicas y estáticas son, se dijo ya en la introducción, las de los autores que distinguen entre: Biometrías físicas y comportamentales[51]; Biometrías activas o pasivas; o Biometrías basadas en características anatómico-físicas y Biometrías comportamentales. Por las razones ya justificadas el apartado 1.2.2.2. de la PARTE PRIMERA (entre ellas el hecho de que Biometrías comportamentales no es un término que acoge a todas las Biometrías dinámicas, ni todas las Biometrías dinámicas pueden entenderse de captación activa) en el presente trabajo se ha procedido a distinguir entre Biometrías dinámicas y Biometrías estáticas.

Universitat d'Alacant
Universidad de Alicante

Son datos biométricos estáticos los que son obtenidos en un momento puntual a partir de las características anatómico-físicas de una persona, y son datos biométricos dinámicos aquellos que son obtenidos de fuentes dinámicas, esto es, de cualquier expresión secuencial o cíclica que expresa la actividad externa o interna del cuerpo de la persona. Aplicando esa clasificación y conforme al estado actual de desarrollo científico y tecnológico, describimos a continuación dos grandes bloques de Biometrías que obtienen, de una parte, de características estáticas y, de otra, de características dinámicas información que es susceptible de servir de base a sistemas de reconocimiento e identificación de las personas.

PROPUESTA de clasificación de los métodos de obtención de información

[51] POLEMI, D. Informe E*TS Biometrics para la Comisión Europea: Biometricc techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the áreas where they are most applicable*, Institute of Communcation and Computer Systems. National Technical University of Athens, 1997.

biométrica según la naturaleza de la característica corporal de la que se obtienen.

1. BIOMETRÍAS ESTÁTICAS. Métodos que captan información métrica puntual a partir de las características anatómico-físicas de una persona.

1.1. Biometría de los dermatoglifos (dedos y huellas palmares).
1.2. Biometría del rostro.
1.3. Geometría de la mano.
1.4. Biometría ocular (iris y retina).
1.5. Biometría auricular.
1.6. Biometría del ADN.
1.7. Otras Biometrías estáticas.

2. BIOMETRÍAS DINÁMICAS Métodos mensurativos que se aplican a las habilidades motoras y las señales y parámetros corporales y comportamentales, y captan por lo general información secuencial o cíclica que expresa la actividad interna o externa, voluntaria o involuntaria, del cuerpo de una persona.

2.1 Biometría de la escritura o la firma dinámica.
2.2. Biometría de las pulsaciones en teclado.
2.3. Biometría del movimiento labial.
2.4. Biometría de la marcha.
2.5. Biometría vocal.
2.6. Biometría del comportamiento.
2.7. La captación métrica de señales y parámetros corporales.

Universitat d'Alacant
Universidad de Alicante

3.2. La clasificación cronológica o la explicación de las *generaciones* de sistemas de reconocimiento mediante biometría

En la narración de la evolución de las tecnologías biométricas desde sus orígenes hasta el momento actual suele describirse una línea temporal en la que determinados hitos parecen separar, entre los sistemas de reconocimiento automatizado, Biometrías de primera y Biometrías de segunda generación. Esta forma de narrar la evolución guarda cierto paralelismo con lo que, por lo general, se suele hacer al describir complejos *fenómenos multifactoriales*, que acontecen a lo largo del tiempo; marcar unos hitos destacados permite hallar fórmulas más simples para sintetizar lo acontecido y agrupar los acontecimientos permite visualizarlos mejor. Pero tiene, como es sabido, algunas desventajas. Y es que, con frecuencia –sobre todo cuando se trata de abordar la historia más reciente-, no suele haber acuerdo en lo que se refiere a los hitos que son

suficientemente significativos para distinguir las fases de una evolución, o no hay consenso sobre cuáles de los acontecimientos pueden agruparse y por qué razones. Así, en las narrativas que recogen la evolución científica y tecnológica del reconocimiento biométrico en un plazo de aproximadamente tres o cuatro décadas y con acontecimientos que se han dado en países muy diferentes, tampoco debe extrañarnos que no haya consenso a la hora de establecer y delimitar cada una de las generaciones.

MCCARTHY, por ejemplo, emplea la expresión primera generación de tecnologías biométricas para referirse a las que emplean características que son *visibles para el ojo desnudo o el oído*, y recoge en ese conjunto: la Biometría del iris, el rostro, la geometría manual, la voz o el reconocimiento que tiene su base en la forma de la oreja. Considera, por el contrario, Biometrías de segunda generación aquellas que emplean como referencia los patrones de comportamiento y tienen la intención de perfilar a las personas sobre la base de la predicción de sus acciones y comportamientos[52].

Consideramos que está más extendida, sin embargo, la distinción entre una primera y la segunda generación atendiendo a los siguientes elementos o hitos[53]: la emergencia de nuevas características biométricas, junto con las Biometrías basadas en señales corporales; y los avances en ingeniería informática que darán lugar a sistemas biométricos integrados, sensores a distancia o tecnologías de captación pasiva de la Biometría dinámica.

Universitat d'Alacant
Universidad de Alicante

3.2.1 *La generación cero (o los antecedentes de los sistemas automatizados de reconocimiento biométrico)*

Siguiendo esta línea, Anil K. JAIN[54], uno de más destacados expertos mundiales en el ámbito de las tecnologías de reconocimiento biométrico, afirma que existió una *generación cero* de tecnologías biométricas automatizadas en los años 70, que dio lugar a la primera generación de sistemas AFIS. Esto es, sistemas automatizados de reconocimiento mediante huellas dactilares. Claramente vinculados a los sistemas que desde principios del siglo XX venían empleando las agencias del orden público en multitud de países, los primeros AFIS ofrecían un rendimiento muy limitado y no tenían interconectividad alguna. Funcionaban de forma aislada. En opinión de JAIN/KUMAR, los sistemas de geometría manual que en aquella época se emplearon en algunos controles de acceso,

---

[52] MCCARTHY, P. voz *Biometric Technologies*, en *Encyclopedia of applied ethics*, 2ªed, 2102, Elsevier; vid. también SUTROP. M./ LASS-MIKKO, K. "From Identity Verification to Behavior Prediction", *Review of Policy Research*, vol. 29, nº 1, pp21 y ss.

[53] DE HERT, P. "Biometrics and the Challenge to Human Rights in Europe", en CAMPISI, P. (ed), *Security and Privacy in Biometrics,* 2013, pp406-408.

[54] Departamento de Ciencia e Ingeniería de la Computación de la Universidad de Michigan.

como el servicio acelerado de inmigración y naturalización en los EEUU (INSPASS[55]), también deben entenderse recogidos en esa generación cero[56]. El sistema INSPASS se instaló en algunos de los principales aeropuertos Estadounidenses a mediados de los 90, pero se terminó abandonando por las bajas tasas de enrolamiento y su escaso rendimiento.

3.2.2 *La primera generación de sistemas de reconocimiento automatizado mediante biometría*

La primera generación de sistemas biométricos en el sentido contemporáneo de la expresión se desarrolló e implementó fundamentalmente en la primera década del siglo XXI. En diferentes países y contextos de aplicación se extendieron multitud de sistemas de reconocimiento basados en la Biometría de los dermatoglifos, la Biometría del iris y la Biometría (geometría) del rostro, algunos de los cuáles llegaron a enrolar a millones de seres humanos. Pertenecen a esta primera generación, en primer lugar, una serie de sistemas establecidos para el control de los movimientos transfronterizos como: el pasaporte biométrico Europeo (con Biometría dactilar y del rostro), el sistema *US-Visit* (basado en las huellas dactilares), el sistema Privium del aeropuerto holandés de Schiphol (con escaneado de iris) –imágenes 1.4 y 1.5.- [57], el Sistema de Información Schengen (SIS y SIS II) o la base EURODAC, y el sistema *SmartGate* del aeropuerto de Sídney basado en la Biometría del rostro (Gobierno de Australia[58]). Es el caso también, en segundo lugar, de sistemas como: el sistema de control de acceso con escaneado de huellas dactilares a algunas zonas de la Expo de Sevilla en 1992[59]; el de acceso al *Walt Disney Park* en Orlando (IMAGEN 1.12) [60]y el *Magic Kingdom*; o el sistema japonés Luxe X2 que *PROnetworks* desarrolló para implementar en las máquinas expendedoras[61]. Pertenecen también a este conjunto los sistemas de reconocimiento cotidianos que incluyen lectores de huellas en ordenadores personales o teléfonos móviles, entre otros. Entre los sistemas con mayores tasas de

---

[55] INSPASS US Department of Homeland Security 2010. US Department of Homeland Security. New biometric technology improves security and facilitates U.S. entry process for international travelers. https://www.dhs.gov/xlibrary/assets/

usvisit/usvisit_edu_10-fi ngerprint_consumer_friendly_content_1400_words.pdf. Accessed

30 Jan 2010

[56] JAIN, A. K./ KUMAR, A. *"Biometric Recognition",* en Second Generation, p55-58; MICHAEL, K. *Innovative Automatic Identification and Location-Based services,* IG Global, 2009, pp220-221.

[57] SCHIPHOL, *Fast border passage with iris scan*, 2009.

[58] AUSTRALIAN GOVERNMENT. *Introducing SmartGate*. http://www.customs.gov.au/webdata/resources/files/BR_introSmrtGt0409.pdf. Accessed 30 Jan 2010

[59] Los abonos de temporada se asociaban a una tarjeta inteligente y se empleó Biometría de los dermatoglifos para acceder a varios edificios y exhibiciones. El sistema fue producido por *Bull subsidiary*, Telesincr. Datos tomados de M. CHADWICK, 1992, p253 y ZPREDA/ OTON, 1994, p172.

[60] Se estima que el sistema comercial más importante de los estados unidos de américa es el que da acceso a los cuatro parques temáticos de Disney en Orlando, con aproximadamente diez millones de usuarios.

[61] PROnetworks*. Face recognition cigarette vending machines*.

enrolamiento de esta primera generación está el IAFIS del FBI, que en 2010 se estimaba contaba con 80 millones de registros de 10 huellas (CJIS 2010[62]). Como veremos, algunas tecnologías más recientes han superado con creces dicha cifra.

3.2.3 La segunda generación de tecnologías biométricas

La segunda generación de tecnologías biométricas suele describirse en torno a la introducción de una serie de mejoras científicas y tecnológicas de los sistemas, aunque existe cierta discrepancia sobre la fecha en la que en concreto puede darse por comenzada esta generación. Desde el punto de vista de la ingeniería informática, la nueva generación se caracteriza: por esfuerzos por superar las limitaciones de interoperabilidad; por mejoras en las técnicas de captación, representación digital y comparación de los patrones; y por diferencias cualitativas en lo que se refiere a la seguridad de los sistemas y la calidad de los servicios que pueden prestarse en grandes grupos sociales, que incluyen el desarrollo de variantes multimodales de los sistemas (esto es, modalidades que tienen su base en dos o más características biométricas). De forma incipiente estos sistemas introducen, asimismo, mecanismos destinados a dar respuesta a preocupaciones tales como la protección de privacidad[63].

En este tiempo se han realizado además notables esfuerzos por extraer nuevas características anatómicas, fisiológicas o comportamentales a partir de las cuáles construir futuros sistemas de reconocimiento biométrico. Entre las líneas abiertas pueden citarse: el movimiento corporal al caminar[64], la Biometría auricular[65], las huellas de las pisadas[66], la Biometría periocular[67] (IMAGEN 41), la geometría de los nudillos de la mano[68]), dinámica del tecleado (BENDER/ POSTLEY 2007[69]) o la silueta nasal (DRIRA et al. 2009[70]; SONG et al. 2009[71]), así como el pulso arterial (JOSHI et al.

---

[62] CJIS. *Integrated automated fingerprint identification system* or IAFIS.

[63] JAIN, A. K./ KUMAR, A. "Biometrics of Next Generation".

[64] KELLOKUMPU, V./ ZHAO, G./ LI, S.Z. et alt. "Dynamic texture based gait recognition", *Proceedings of the ICB 2009*, p1000–1009; TAO, D./ LI, X. /WU, X./ ET ALT. "Analysis and gabor features for gait recognition", *IEEE Transactions* 2007, 29(10): 1700–1715.

[65] YAN, P./ BOWYER, K. W. "Biometric recognition using 3D ear shape", *IEEE Transactions on Pattern Analysis* 2007, 29(8): 1297–1308; BHANU, B./ CHEN,H. *Human ear recognition by computer*, 2008.

[66] NAKAJIMA, K./ MIZUKAMI, Y./ TANKA, K./TAMURA, T. "Footprint-based personal recognition", *IEEE Transactions* 2000, 47(11): 1534–1537; UHL, A./ WILD, P. "Footprint-based biometric verification", *Journal of Electronic Imaging*, 2008, 17: 11016..

[67] PARK, U./ ROSS, A./ JAIN, A. "Periocular biometrics in the visible spectrum", *Proceedings of the BTAS*, 2009.

[68] KUMAR, A./ RAVIKANTH, CH. "Personal authentication using finger knuckle surface", *IEEE Transactions* 2009, 4(1): 98–110; WOODARD, D.L./ FLYNN, P.J. "Finger surface as a biometric identifier", *Computer Vision* 2005, 100(3): 357–384; KUMAR, A./ ZHOU, Y. "Human identification using knucklecodes", *Proceeding of BTAS* 2009.

[69] BENDER, S./ POSTLEY, H. *Key sequence rhythm recognition system and method*. US Patent No. 7206938, 2007.

[70] DRIRA H./ AMOR, B.B./ DAOUDI, M./ SRIVASTAVA, A. "Nasal region contribution in 3D face biometrics using shape

2008[72]; IRVINE et al. 2008[73]), las uñas de los dedos (TOPPING et al. 1998[74]), el olor corporal (RAMUS/ EICHENBAUM 2000[75]), el potencial bioeléctrico (HIROBAYASHI et al. 2007[76]), radiografías de las rodillas (SHAMIR et al. 2009[77]), de los senos paranasales (FALGUERA et al. 2008[78]; Tabor et al. 2009[79]), y emisiones otacústicas (SWABEY et al. 2004[80]).

3.3. Strong-weak, hard-soft biometrics

Se emplea la expresión modalidades biométricas tradicionales o robustas (*hard*) para referirse a aquellos métodos de reconocimiento que funcionan sobre la base de atributos biométricos primarios, en el sentido de atributos que en sí mismos reúnen de forma suficiente las cualidades de singularidad y permanencia que se han descrito en el epígrafe anterior. Pero cuando los atributos, por alguna razón no reúnen de forma suficiente tales cualidades se habla de *soft* biometrics, aunque este término no tiene una acepción única.

JAIN (ET ALT.) y KINDT definen como *soft biometrics* aquellas características que no son muy distintivas y/o permanentes pero que, por el contrario, ofrecen una información que puede servir para completar o agilizar la gestión de la que se obtiene de características que si son distintivas y/o permanentes[81]. ZHANG/ ET ALT[82], por su parte, emplean esta expresión para referirse a las

---

analysis framework", *Proceedings of the 3rd IAPR/IEEE* 2009, pp357–366.

[71] SONG, S./ OHNUMA, K./ LIU, Z./ MEI, L./ A. KAWADA/ MONMA, T. "Novel biometrics based on nose pore recognition", *Optical Engineering* 2009, 48(5): 57204.

[72] JOSHI, A.J./ CHANDRAN, S./ ET ALT. "Arterial pulse rate variability analysis for diagnoses", *Proceedings of ICPR*, 2008, Tampa, FL, 1–4.

[73] IRVINE, J.M./ ISRAEL, S. A./ ET ALT. "Eigenpulse: Robust human identification from cardiovascular function", *Pattern Recognition* 2008, 41(11): 3427–3435.

[74] TOPPING, A./ KUPERSCHMIDT, V./ GORMLEY, A. *Method and apparatus for the automated identification of individuals by their beds of their fingernails*, U.S. Patent No. 5751835, 1998.

[75] RAMUS, S.J./ EICHENBAUM, H. "Neural correlates of olfactory recognition memory in rat orbitofrontal cortex", *Journal of Neuroscience* 2000, 20: 8199–8208.

[76] HIROBAYASHI, S./ TAMURA, Y/ ET ALT. "Verification of individual identification method using bioelectric potential of plant during human walking", *Japanese Journal of Applied Physics* 2007, 46(4A): 1768–1773.

[77] SHAMIR, L./ LING, S./ ET ALT. "Biometric identification using knee X-rays", *International Journal of Biometrics* 2009, 1(3): 36 ET ALT. 5–370.

[78] FALGUERA, J.R./ ET ALT. "Frontal sinus recognition for human identification", 2008, *Proceedings of SPIE*, vol. 6944, Orlando, FL, 69440S.

[79] TABOR, Z./ KARPISZ, D./ ET ALT. "An automatic recognition of the frontal sinus in x-ray images of skull", *IEEE Transactions on Biomedical Engineering* 2009, 56(2): 361–368.

[80] SWABEY, M.A./ BEEBY, S.P./ ET ALT. "Using Otoacoustic emission as biometric", Proceedings of ICBA, Hong Kong 2004, LNCS, vol. 3072, pp. 600–606.

[81] KINDT, E. *Privacy and Data*, cit., p35.

[82] PHILLIPS, P.J./ BEVERIDGE, J. R. / DRAPER, B.A., "An introduction to the good, the bad, and the ugly face recognition challenge problem", en *Proceedings Ninth IEEE International Conference on Automatic Face and Gesture Recognition*, 2011.

características que dividen a la personas en grupos que no se solapan (género, edad, color de los ojos) y hay autores que incluyen las expresiones de ánimos (captadas mediante Biometrías dinámicas) u otros atributos como la forma de vestir (IMÁGENES 90 Y 91). Estas modalidades biométricas *débiles* o *blandas* se emplean, por ejemplo: 1) en ausencia de atributos biométricos primarios suficientemente singularizantes; 2) para mejorar la agilidad de bases de datos excesivamente grandes; o, 3) como complemento y refuerzo de las modalidades tradicionales (en sistemas multimodales, por ejemplo)[83].

Ya WAYMAN[84] propuso el uso de indicadores demográficos tradicionales, como el género, la población (a la que en la literatura biométrica es frecuente referirse con expresiones como *raza* o *etnia*) o la edad para ayudar al filtrado de bases de datos excesivamente grandes. Además de la posibilidad de registrar dicha información en el enrolamiento, y algunos investigadores han presentado, con mayor o menor éxito, sistemas automatizado destinados a reconocer tal información. Es el caso del que se conoce como SexNet (que clasifica los rostros por géneros, IMAGEN 21) o sistemas que clasifican por género las huellas dactilares (como el propuesto por GNASIVAM y MUTTAN, atendiendo al movimiento al simular el boxeo[85], o el de KRISHAM, con base en las huellas palmares)[86]. Por su parte, el *Luce X2* de PRONetworks puede programarse para evitar que los niños compren tabaco o que los pacientes de los hospitales acudan a la cafetería a adquirir alimentos salados o azucarados (IMAGEN 81). Estos sistemas abordan el reconocimiento de la identidad no en el sentido de *ser uno mismo*, sino en el sentido de pertenecer (o no) a una determinada categoría de personas con las que se comparte una cierta identidad[87].

Existen asimismo sensores que se instalan en pantallas digitales colocadas en espacios públicos y que tienen como finalidad la detección y captación de las características de las personas que atienden a este tipo de publicidad. Sobre su uso en España se pronunció en 2012 la Agencia Española de Protección de Datos[88]. El sensor detecta los rostros y procede a clasificar a las personas según su sexo biológico y edad, almacenando datos anónimos sobre qué tipos de personas han prestado atención a la pantalla y durante cuánto tiempo, en qué franja horaria, etc.

---

[83] AILISTO, H./VILDJIOUNAITE, E./ ET ALT., J. 'Soft biometrics-combining body weight and fat measurements with fingerprint biometrics', *Pattern Recognition Letters* 2006, pp. 325–334.

[84] WAYMAN, J.L.,"Large-scale civilian biometric systems - issues and feasibility", *Proceedings of the CardTech/SecureTech Government*, 1997, Washington DC.

[85] WANG, J./ HU, W./ WANG, Z./ CHEN, Z. "Human Identification and Gender Recognition from Bozing", en SUN/ LAI/ ET ALT (eds.), *Biometric Recognition*, 2011, p1952;

[86] PRABHU, G./ POORNIMA, S. "*Minimize Search Time through Gender Classification from Multimodal Biometrics*", *Procedia Computer Science* 50 (2015), 289-294. Los resultados publicados del sistema de determinación de género mediante las huellas dactilares tienen una tasa de acierto de un 88% y en el caso de las huellas palmares, la tasa de acierto es de en torno a un 70%.

[87] Vid. PRIMERA PARTE, 1.1.2.

[88] AGPD, Informe 0328/ 2012.

Se ha calculado que las Biometrías débiles tienen un gran potencial como apoyo de las Biometrías robustas (en sistemas multimodales, por ejemplo) así como en sistemas de identificación o re-identificación que no pretenden una identificación indubitada, sino una identificación razonable dentro de un contexto. En relación con su posible apoyo a Biometrías robustas, JAIN (ET ALT.) calcularon en 2004[89] la tasa en la que mejora el funcionamiento de un sistema de huellas dactilares (en torno a un 5%) incorporando informaciones como la edad, el género, el color de la piel o la altura de los usuarios. Pequeñas marcas faciales o tatuajes y cicatrices pueden también ser útiles en este sentido[90], [91].

Guardan relación con esta línea de trabajo la investigación en la Biometría de la región periocular (la piel, las cejas y la forma del ojo), que está avanzando como posibilidad intermedia entre usar el rostro completo o sólo el iris. Cuando se capta el rostro desde cierta distancia, la información del iris suele ser (dependiendo de la cámara) de una resolución baja y, al su vez, cuando se capta sólo el iris no se tiene información del entorno del ojo (es decir, información parcial del rostro de la persona) que puede ayudar a un primer cribado entre sujetos enrolados[92] (IMAGEN 41).

GONG (et alt.) [93], por su parte, describen otro interesante uso potencial de estas tecnologías. Los operadores que están en un puesto de control y deben atender la información que les muestran, al mismo tiempo, varias cámaras de vigilancia no pueden prestar atención a todos los detalles. Ni siquiera los más adiestrados. Colocar más operadores supone un coste muy relevante y opciones como las de las tecnologías de reconocimiento robusto no tienen sentido cuando, por ejemplo, estamos controlando a las personas que circulan por en el área de las tiendas de la terminal de un gran aeropuerto. (IMÁGENES 87, 88 y 89) Algunos sistemas captar determinados atributos en las persona, ya sean físicos o comportamentales, y los señalan como "idénticos" permitiendo su seguimiento mientras transitan del espacio de una cámara a otra (con independencia de que puedan, por ejemplo, cambiar radicalmente su peinado o su forma de vestir).

---

[89] JAIN, A.K./ DASS, S. C./NANDAKUMAR, K. "Soft biometric traits", *Proceedings of International Conference on Biometric Authentication*, 2004, 731–738.

[90] JAIN, A.K./ PARK, U. "Facial marks", *Proceedings of the International Conference on Image Process*, 2009.

[91] LEE, J.-E./ JAIN, A. K./ JIN, R. "Scars, marks and tattoos (SMT): Soft biometric for suspect and victim identification", *Proceedings of the Biometric Symposium, Biometric Consort Conference*, Tampa, Florida 2008.

[92] JAIN, A. K. *Introduction to Biometrics*,, pp190-191.

[93] GONG, S./ CRISTANI, M./ YAN, S./ CHANGE LOY, C. (eds.), *Person Re-identification*, Springer, 2014, p2.

3.4. Sistemas 1D, 2D y 3D

Según ZHANG, D. / LU, G.[94], atendiendo a las dimensiones de la señal captada cabe distinguir tres categorías de sistemas de identificación biométrico: de una, dos y tres dimensiones respectivamente. Son sistemas 1D los de reconocimiento de voz y algunos sistemas de reconocimiento mediante la firma. Son sistemas 2D muchos de los sistemas de reconocimiento mediante, por ejemplo, Biometría del iris, geometría de la mano o del rostro y huellas dactilares de primera generación. Y recientemente, gracias al desarrollo de distintos tipos de dispositivos, han surgido sistemas de captación de las características biométricas en tres dimensiones que obtienen datos del rostro, las orejas, las huellas dactilares o la geometría de las manos[95].

En las evaluaciones los sistemas 3D aparecen como modalidades biométricas más robustas que las 2D por la cantidad de información adicional que ofrecen. Algunos dispositivos comerciales son: la cámara *Konica Minolta Vivid* 9i/910[96] y el escáner de cuerpo completo en color y 3D conocido como *Cyberware* 2003[97]. (IMAGEN 51, la firma en 2D y en 3D, IMÁGENES 35 y 39, la biometría de la oreja en 2D y en 3d)

4. BIOMETRÍAS ESTÁTICAS

4.1. Biometría de los dermatoglifos (crestas y surcos dérmicos de las manos, plantas de los pies y dedos).

4.1.1. El concepto de dermatoglifo.

Dermatoglifo –del griego, grabado en la piel- *es el nombre que se da a los dibujos que los pliegues cutáneos, las crestas y los surcos dérmicos forman sobre las palmas de las manos, las plantas de los pies y los pulpejos de los dedos.* Los dermatoglifos son un sistema de desarrollo puramente embrionario y terminan de formarse totalmente hacia el tercer o cuarto mes del desarrollo fetal. Dice la *Enciclopedia histórica de Antropología Física* que esas formas han generado desde siempre fascinación[98] y se vienen trazando desde hace décadas estudios sobre grupos de población, ya sea etnias ya personas afectadas por una enfermedad o un síndrome en

---

[94] ZHANG, D./ LU, G. *3 D Biometrics. Systems and Applications*. Springer. 2013, pp7-8.

[95] WOODARD, DL, "A comparison of 3D biometric modalities*", Comput Vis Pattern Recogn Workshop*, 2006 57–60.

[96] ZHANG, D, *Automated biometrics: technologies and systems,* Hardbound, Boston, 2000; ZHANG, D. "Biometrics technologies", en *Proceedings of 1st international conference on image and graphics*. 2000, pp 42–49.

[97] MEXICAN GOVERNMENT (2003) Face recognition technology to eliminate duplicate voter registrations in upcoming presidential elections. http://www.shareholder.com/identix/ReleaseDetail.c fm?ReleaseID=53264.

[98] F. SPENCER (ed.), *History of Biological Anthropology: an Enciclopedia*, p340.

concreto, con la intención de hallar criterios que puedan ayudar bien en la identificación de las personas, bien en el diagnóstico precoz de las enfermedades[99],[100]. Las personas con Síndrome de Down, por ejemplo, presentan en más de un 90% de los casos 10 asas cubitales en las huellas dactilares, así como un pliegue palmar único y otras características en su geometría manual.

4.1.2. La Biometría de los dermatoglifos dactilares

Hace siglos que conocemos que las crestas o surcos que presentan las superficies de la piel de las falanges tienen un diseño único[101], con lo cual el estudio de sus minucias o puntos característicos (morfología, ramificación, dirección e interrupciones) puede emplearse potencialmente para diferenciar a unas personas de otras[102] o para identificar quién es una persona. El contacto de las crestas papilares con otro objeto produce una impresión latente y la forma más frecuente de obtener la muestra biométrica para el estudio consiste en reproducir el dibujo papilar impregnando el dedo en tinta y presionándolo sobre cartulina o papel. Los relieves lineales que existen en la epidermis de distintas zonas (las crestas) alternan con valles o surcos y ello hace que al cubrir con tinta el dedo las crestas dejen sobre el papel unas rayas oscuras en las que se ven una serie de elementos. Así, los deltas o núcleos (zonas en las que hay triangulaciones o divisiones de las líneas) o las llamadas minucias (terminaciones de líneas, bifurcaciones, horquillas y otros puntos característicos). Véase la IMAGEN 22.

Se tiene constancia de que Marcelo MALPHIGI estudiaba en Bolonia los relieves papilares en el siglo XVII, aunque el inicio de las ciencia que estudia los dermatoglifos se sitúa en los trabajos de Nehemiah GREW (1641-1712)[103], que publicó uno de los primeros estudios europeos sobre las impresiones dactilares. Tiempo después publicó Jan Evangelista PURKHINE[104] la obra *Comentation de examine physiologico organi visus et systematis cutanei* (1823). Alphonse BERTILLON, William HERSCHELL[105] y Henry FAULDS[106] también son señalados como investigadores que realizaron importantes aportaciones a este campo[107], junto con Francis GALTON. Se afirma que fue este último

---

[99] CUMMINS, H./ KENNEDY, R. "Purkinji's observations (1823) on fingerprints and other skin features", *Am. J. Police Sci.,* 31(3), 1940.

[100] WOODWARD, J. D. "Biometrics: privacy's foe or privacy's friend?" *Proc. IEEE*, 85(9), 1480–1492, 1997.

[101] Vid. en la PARTE PRIMERA las referencias a la antigua Babilonia y a Persia.

[102] L. DE DIEGO DÍEZ, *La Prueba Dactiloscópica*, 2001, pág. 30.

[103] KINDT, E. 2013, p17.

[104] CUMMINS, H./ KENNEDY, R. "Purkinji's observations (1823) on fingerprints", 1940.

[105] HERSCHEL W. "Skin furrows of the hand", *Nature*, 23, 76, 25de noviembre, 1880.

[106] Faulds, H. "On the skin furrows of the hand", *Nature*, 22, 605, 28 de octubre, 1880.

[107] B. Kaufer, History of the finger-printing system, 1912, Smithsonian Institution Annual Report – consultado en su reimpresión en The Print, vol 16 (2), 2000, pp1-13.

quien aportó una base más solida para afirmar que las huellas dactilares permanecen toda la vida[108] y que la posibilidad de hallar dos individuos con las mismas huellas dactilares es estadísticamente tan remota que puede afirmarse que es casi nula[109]. En su libro *Fingerprints* (1892) GALTON abordó la herencia del patrón dermatoglífico y comparó estadísticamente las frecuencias de los patrones entre poblaciones, determinando para ello un conjunto de características o rasgos de las huellas que permitían clasificar las impresiones dactilares[110].

Tanto en el uso forense como en el campo de las tecnologías biométricas, las huellas dactilares constituyen uno de los sistemas de reconocimiento más consolidados y de los que cuentan con mayor confianza por parte de las fuerzas del orden[111]. Los primeros sistemas de reconocimiento mediante huellas dactilares se implementaron en el cambio del siglo XIX al XX en grandes áreas metropolitanas. Se considera que fue Iván Vučetić (Croacia 1858 – Buenos Aires, 1925) quien desarrolló y patentó en Argentina el primer sistema de identificación que empleaba las huellas dactilares de ambas manos, es decir, *la ficha decadactilar* (1891). Conocido también como Juan VUCETICH, este investigador amplió la descripción de rasgos de GALTON hasta un centenar, pero ideó un sistema simplificado de consulta basado en la clasificación propuesta por Henri FAULDS. Es decir, un sistema de consulta basado en los cinco tipos de: arco, presilla externa e interna y verticilo o bucle. Conforme a este sistema, los análisis de las huellas se realizan comenzando por los rasgos más gruesos, procediendo a clasificar la huella atendiendo a la estructura global de sus anillos. Los tipos de minucia más comunes son las terminaciones, bifurcaciones, lagunas, bordes independientes, puntos o islas, aguijones y cruces. A continuación, se procede a un estudio más detallado, en el que se comprueba si las minucias de una huella (o una selección de las más características de ésta) coincide con las minucias de una huella almacenada (*Fingerprint matching*).

La validez del sistema de VUCETICH para la identificación fue reforzada con la resolución de un asesinato en 1892 en ciudad de *Necochea*[112] y un estudio realizado en 645 reclusos de la cárcel de la Plata. Como advierten los forenses, el hallazgo de huellas en la escena de un crimen tiene la doble virtualidad no sólo de contribuir a la identificación del presunto responsable sino, además, de situarlo en la escena del crimen y demostrar que ha estado, en su caso, en contacto manual

---

108 GALTON, F, "Personal identification and description", *Nature*, 21 y 28 de junio de 1888, pp. 173–177, 201–202.

109 ALLEN, R./ SANKAR, P./ PRABHAKAR, S. "Fingerprint Identification Technology", en *Biometric Systems*, p21.

110 BREITENSTEIN, en NOLDE/ LEGER (eds), *Biometrische Verfahren*, 2002, p35; GRUNER, A. *Biometrie und informationelle Selbstbestimmung,* 2004/ 2005, pp242-25.

111 ALLEN, R./ SANKAR, P./ PRABHAKAR, S. "Fingerprint Identification Technology", cit., p21..

112 Francisca Rojas fue la primera asesina identificada mediante esta técnica, una mujer que culpaba a su marido del asesinato de los dos hijos del matrimonio, y cuyos dedos ensangrentados dejaron huellas en la escena del crimen.

directo con objetos que pueden tener gran relevancia penal (como el arma homicida o los bienes sustraídos)[113]. En 1894 la policía de Buenos Aires adoptó oficialmente su sistema dactiloscópico (inicialmente denominado *icnofalangometría*). Destacan entre los escritos de VUCETICH las *Instrucciones Generales para el sistema antropométrico e impresiones digitales*, *Idea de la identificación antropométrica* (1894) y su trabajo *Dactiloscopia comparada* presentado en el Segundo Congreso Médico de Buenos Aires (1904). Este trabajo recibió premios y distinciones internacionales, siendo objeto de traducción a varias lenguas. Brasil, Chile, Rumania, Uruguay, Francia y China adoptaron poco después el sistema, que en 1907 la Academia de Ciencias de París señaló como el más exacto de los conocidos en ese momento. Al médico Federico OLÓRIZ AGUILERA (1855-1912)[114] se atribuye la creación del sistema de identificación dactilar usado en España y Portugal y conocido como *método Oloriz* o *sistema Dactiloscópico español* (1903). Y Edward HENRY contribuyó, por su parte, al sistema que adoptaría Scotland Yard (1901)[115]. En los Estados Unidos el primer sistema se implementó en la ciudad de Nueva York con uso civil (1902) y poco después en el sistema de prisiones de dicho estado (1903). En 1924 el Congreso de los Estados Unidos aprobó el establecimiento de una División de Identificación en el FBI que durante casi 50 años se calcula que gestionó manualmente 200 millones de impresiones dactilares empleando el sistema de clasificación de HENRY[116].

Desde mediados de los años 60 se vienen realizando en los países occidentales esfuerzos por automatizar las bases de datos de impresiones dactilares para facilitar y agilizar la consulta y la búsqueda de coincidencias. El NIST (Instituto Nacional de Estándares y Tecnologías) estadounidense, la Policía Montada del Canadá y la Home Office del Reino Unido impulsaron varios proyectos cuyos primeros sistemas piloto se implementaron a comienzos de los años 70[117]. Esa primera generación de sistemas se vio mejorada en los años 90, en la que se implementó definitivamente el IAFIS (Integrated Automated Fingerprint Identification System). En ese periodo entre 1970 y 1990 el desarrollo de los escáneres y los ordenadores personales contribuyó a que la Biometría de las impresiones dactilares se extendiera también a usos que nada tenían que ver con la persecución criminal.

Para el escaneado se usan sensores ópticos, térmicos o de ultrasonidos que obtienen una imagen de los dedos en gamas de grises y muestran las líneas papilares. Véase en el anexo, IMAGEN 26, diferentes sensores de captación. Se aplican a la imagen una serie de filtros, para optimizar la

---

[113] LORENTE ACOSTA, J. A. "Identificación genética criminal", cit., 2002, pp1-2

[114] SÁNCHEZ VIGIL, J. M./FERNÁNDEZ FUENTES, " B. La fotografía como documento de identidad", 2005, pp189-195.

[115] HENRY, E. R. *Classification and Uses of Fingerprints*. 1900.

[116] ALLEN, A./ SANKAR, P./ PRABHAKAR, S: *Fingerprint identificaction technology*, cit, pp21 y 23.

[117] ZHANG, *3D Biometrics*, 2013, p11.

imagen, y a continuación se señala la posición de una serie de puntos característicos o minucias[118] (que son los atributos que, en conjunto, darán lugar al patrón biométrico de la huella dactilar). Normalmente, por cuestión de capacidad, no se conserva la huella en formato de imagen, sino que se binariza la imagen original (resaltando más la impresión de las crestas), se aligera para eliminar el ruido causado por la presión excesiva del dedo y a partir de la imagen adelgazada se obtienen las minucias. Cada patrón de una huella ofrece una media de entre 15 y 50 minucias[119], y con una coincidencia en más de 14 puntos, se considera que dos huellas pertenecen a la misma persona, aunque en el resto no coincidan al 100%. Véanse la IMAGEN 25 y la IMAGEN 66 (en esta última, problemas de captación de las huellas por diferentes factores).

Ha de insistirse, con todo, en la notable diferencia que puede haber entre el dato en crudo y la expresión métrica digital de un dermatoglifo. No existen dos huellas dactilares idénticas ni, por ello, dos posibles impresiones idénticas de dos huellas distintas; pero en los sistemas automatizados, sin embargo, como sólo se procesan algunos elementos de las huellas sí es posible que aparezcan dos *patrones digitales idénticos* para dos huellas diferentes[120].

En la emisión del pasaporte Europeo la normativa requiere la captación, entre otros, de elementos biométricos obtenidos de las huellas dactilares. En tanto estos elementos se almacenarán en el CHIP de radiofrecuencia que incluye el pasaporte y serán objeto de control por las autoridades aduaneras de diferentes países, la forma de conversión de los datos en crudo en patrones biométricos obedece a una serie de estándares que han sido fijados por el ICAO y las normas ISO, teniendo en cuenta otros como los del ANSI y del FBI[121]. Se obtienen las impresiones planas del dedo índice de ambas manos, y en el caso de que la calidad de las huellas de éstos no fuera adecuada o se presentase lesión en los índices, se registrará impresión de los dedos medio, anular o pulgar. Los datos se almacenan como imágenes conforme al estándar *ISO/ IEC FCD 19794-4*[122], que fija también determinados estándares de calidad, aunque dichas imágenes son comprimidas usando un algoritmo WSQ para que su tamaño sea de apenas unos KBs.

---

[118] HEUMANN, B. *Whitepaper Biometrie*, www.biometrie-online.de, 2006, p8; KUHN, M., „Security-Biometric identification“, University of Cambridge, 2003.

[119] En *The Use of Technology to Combat Identity Theft,* 2005, p37-38.

[120] DE ANTON Y BARBERÁ, F., “Las Huellas Dactilares a Examen”, 2009, 020-026.

[121] ICAO NTWG, *Biometrics Deployment of Machine Readable Travel Documents,* 2004; ISO/ IEC FCD 19794-4 *Biometric Data Interchange Formats – Part 4: Finger Image Data*, y *Part 2: Finger Minutiae Data*; ANSI/NIST-ITL 1-2000 Standard “Data Format for the Interchange of Fingerpring, Facial, Scarmark & Tatoo (SMY) Information”; *FBI: Wavelet Scalar Quantization* (WSQ).

[122] ISO/ IEC FCD 19794-4 *Biometric Data Interchange Formats – Part 4: Finger Image Data*.

En el año 2004 más del 50% de las tecnologías de reconocimiento biométrico tenían su base en las huellas dactilares[123], que captaban las huellas con escáneres ópticos, sensores del estado sólido o sensores acústicos. Los patrones biométricos obtenidos de las huellas necesitan muy poco espacio digital para su almacenamiento. Además, los dispositivos de captación son relativamente fáciles de usar (sólo requieren colocar el dedo sobre un escáner), y la proporción entre el precio de los escáneres y la calidad de reconocimiento que ofrecen es alta[124]; quizá por ello, son una de las tecnologías más extendidas[125]. IMÁGENES 82, 83 y 1.17.

También se considera que obtienen un buen resultado en las evaluaciones que tienen como referencia las cualidades requeridas a los sistemas de identificación biométrica. Existen Biometrías más singularizantes (como la del iris) o más universales (como la Biometría facial o la del ADN), pero es una Biometría cuya singularidad es bastante fácil de capturar y ofrece buenos rendimientos[126]. Su uso a gran escala es muy notable. El sistema EURODAC de apoyo al sistema europeo de visados tiene en torno a 200.000 enrolamientos al año y 900.000 personas están enroladas en el sistema de ayudas sociales de Nueva York. Se emplea también en los pasaportes biométricos de los países que –como la mayoría de los miembros de la UE- están asociados al programa US-Waiver.

4.1.3 La impresión de los dermatoglifos de la palma de la mano

La superficie interna de la mano tiene una serie de patrones y formas que se estiman también con un gran potencial singularizante. Históricamente no se les ha prestado tanta atención como a los dermatoglifos de los dedos, ni hay por tanto sistemas de clasificación de sus elementos que estén tan asentados como los de las impresiones dactilares, pero sí que se han desarrollado tecnologías automatizadas de reconocimiento biométrico con base en ellos.

Compañías como NEC y PRINTRAK desarrollaron muy temprano sistemas con aplicaciones criminales[127], que extraían características y minucias en una forma similar a la que se empleaba para el estudio de las impresiones dactilares. ZHANG [128]refiere como en la Universidad Politécnica de Hong Kong se desarrolló en 1997 un sistema automatizado que captaba las imágenes de los

---

[123] Informe IBG – International Biometric Group, The Biometric Market and Industry Report, 2004-2008.

[124] BROWNSTEIN, R."E-Commerce Becomes Mainstream", *Electronic Design*, 52 (13), 2004, pp75-76; BOLLE/ RUUD / ET ALT, "Biometric perils and patches", *Pattern Recognition* 35 (2002) 2727 – 2738.

[125] LANGENDERFER; J./ LINNHOFF, S. "The Emergence of Biometrics", 2005, pp. 317-318.

[126] IPTS, p136.

[127] JAIN A.K./ HONG, L./ BOLLE, R. "On-line fingerprint verification", *IEEE Trans Pattern Anal Mach* 1997.Intell 19:302–314. doi:10.1109/34.587996; MILLER B, "Vital signs of identity", *IEEE Spectr 1994*, 31:22–30.

[128] ZHANG, *3D Biometrics*, 2013, p12.

dermatoglifos palmares en 2D y cumplía los requisitos de velocidad, precisión y fiabilidad que se esperan de un sistema de reconocimiento con aplicaciones civiles.

4.2. Biometría facial.

La cabeza es la estructura más compleja en todos los animales. En el caso de los humanos aloja al sistema nervioso central, los ojos y las estructuras auditivas internas y contiene las vías de acceso de los sistemas digestivo y respiratorio; además está caracterizada por el rostro[129]. Es discutible si comparativamente el rostro es o no la parte del cuerpo que más elementos singularizantes contiene, pero sí hay consenso científico al afirmar que es en el rostro donde están ubicados muchos de los rasgos en que los humanos nos fijamos para reconocer a otro[130]; juega además un papel clave en la comunicación e interacción con los demás[131], en la transmisión de la identidad y de la emoción[132]. De hecho, la especial habilidad que tiene el cerebro humano para procesar los rostros humanos, ya desde edades tempranas[133], ha sido motivo de fascinación para los científicos y los filósofos (incluyendo a personalidades tan destacadas como ARISTÓTELES o Charles DARWIN)[134].

4.2.1 El estudio de los rostros en la historia: diferentes utilidades

La forma del rostro (tamaño, forma y peculiaridades de cada una de sus partes) guarda estrecha relación por un modelo de desarrollo compuesto y coordinado de elementos cartilaginosos, óseos, dentales y de tejido blando. Detallan SFORZA/ FERRARIO cómo artistas y científicos han venido diseñando métodos similares en sus estudios de los rostros humanos, aunque con distintos objetivos. Así por ejemplo, Leonardo DA VINCI (1452-1519) y Alberto DURERO[135] (IMAGEN 9) desarrollaron métodos gráficos para describir las variaciones en la morfología facial con objetivos de expresión artística y a comienzos del siglo veinte D'Arcy

[129] SFORZA, C./ FERRARIO, V. F. "Soft-tissue facial anthropometry in three dimensions", JASS 2006, pp97-98.

[130] VALENCIA CABALLERO, L. *Metodología para elaborar reconstrucciones faciales*, 2007, pp 194-199; TISTERELLI, M./ BICEGO, M./GROSSO, E. "Dynamic face recognition: from human to machine vision", *Image Vision Comput*. 27 (3) (2009) 222–232."

[131] HENNESSY, R.J./ MCLEARIE S./ ET ALT 2006. "Facial shape and asymmetry by three dimensional laser surface scanning", *J Neuropsychiatry Cli Neurosci*, 18: 73-80.

[132] TURK, M./ PENTLAND, A. "Eigenfaces", *Journal of Cognitive Neuroscience*, Vol. 3, nº 1, 1991, pp71-72.

[133] VALENCIA CABALLERO, L. *Metodología para elaborar reconstrucciones faciales empleando gráficos computarizados trimensionales*, Tesis doctoral, Universidad de Granada, 2007, pp60-61.

[134] TURK, M./ PENTLAND, A. "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience*, 1991, pp71-72.

[135] *Vier Bücher von menschlicher Proportion*, 1528 – Véase Fig. 1.

Wentworth THOMPSON (1860-1948) retomó esos estudios con lo que se conoce como "Transformaciones Cartesianas" del rostro.

Desde el punto de vista histórico-científico, se atribuye al holandés Petrus CAMPER (1722-1789) el primer método de medición angular del rostro con fines de realizar estudios comparativos del cráneo humano. A lo largo de la historia se han suscitado no pocas polémicas en torno a este rasgo. Ya Aristóteles se refirió al ángulo facial como un supuesto indicador de la inteligencia y, como recoge John S. HALLER, este rasgo –el ángulo facial- es uno de los criterios de los que más se ha abusado en la somatología racial[136], en muchas ocasiones para manifestar una *inferioridad implícita*. Su recuperación por CAMPER en el siglo XVIII y otras teorías estadísticas que pretendían demostrar que el ángulo facial mostraba una relación directa con la inteligencia humana, se asocian también con la pretensión de dar preeminencia a los caucásicos. Los objetivos sociales y políticos de las citadas investigaciones merecen un rotundo rechazo, como también han sido revisadas las propuestas de LAVATER (y los fisonomistas) o las tesis del *uomo delinquentis* de LOMBROSO y sus discípulos[137]. No obstante, algunas de sus aportaciones metodológicas han servido de base a nuevas hipótesis de trabajo biométrico[138]. CAMPER determinó que el ángulo formado por dichas líneas variaba según el grado de prognatismo y fue a partir de los ángulos faciales desde dónde trató de establecer las diferencias entre las etnias humanas[139].

El ángulo facial de CAMPER lo formaba la intersección entre dos líneas imaginarias: 1) una línea imaginaria desde la base de la nariz al *orificio de la oreja (auditory meatus)*; y 2) otra tangencial al perfil de la cara (desde la frente hasta la mandíbula superior). En la actualidad, la identificación por geometría del rostro sigue un planteamiento similar, aunque se trazan numerosas líneas imaginarias, destacando aquellos puntos focales sobre los que se encuentran. En comparación con la base científica para otros métodos de reconocimiento mediante biometría, ha de advertirse que la captación de patrones suficientemente singularizantes y con garantía de permanencia en los rostros humanos es algo en lo que aún queda mucho margen para investigar[140].

---

[136] HALLER, J.S. *Outcasts from evolution*, 1859-1900, SIU Press, 1995, págs. 9-10.

[137] WECHSLER, H. "Biometric Security and Privacy Using Smart Identity", Review of Policy Research, vol 29, 1/ 2012, pp78-79; STRASSER, P.: "Biometrie – ein Schritt in die Überwachungsdemokratie?", SCHAAR, P. (ed), *Biometrie Und Datenschutz – Die vermessene Mensch*, 2007, pp14-15.

[138] GOULD, S. J. *Der falsch vermessene Mensch*, Franfurt a. M. 1988; STRASSER,P. *Verbrechermenschen. Zur kriminalwissenschaftlichen Erzeugung des Bösen*, 2005 (original de 1948), pp41ss

[139] MEIJER, M. C. *Race and Aesthetics in the Anthropology of Petrus Camper* (1722-1789), 1999, p56-57.

[140] WECHSLER, H. "Biometric Security and Privacy", Review of Policy Research, vol 29, 1/ 2012, pp78-79.

4.2.2 La utilización de fotografías con fines de identificación: algunas notas históricas

La utilidad de la fotografía en la identificación y persecución de los criminales se reconoció ya en el siglo XIX[141]. Las fotografías de los rostros humanos, decía BARTHES, son *documentos de presencia*[142] y nos ofrecen importante información sobre las personas. Las representan tal y como se muestran o no se muestran ante un espejo. Se atribuye a DISDERI (1853) la aplicación de la fotografía a la identificación y reconocimiento de las personas mediante la divulgación de las *cartes de visite*. En Francia Ernest LACAN propuso un sistema fotográfico policial en 1854, aunque no fue establecido definitivamente hasta 1872[143]. A partir de esa fecha en numerosas comisarías de policía europeas se crearon secciones fotográficas destinadas a identificar los delincuentes, en paralelo a las cuáles otros investigadores desarrollaron técnicas antropométricas. Así, el método de BERTILLON[144], que combinó antropometría y fotografía para aumentar la fiabilidad de los sistemas de identificación. Entre los antecedentes del reconocimiento biométrico contemporáneo se citan también los carteles de "se busca"[145](IMÁGENES 56) y 57 y los sistemas manuales de elaboración de *retratos robot* (IMAGEN 16). Por ejemplo, aquellos que consistían en láminas transparentes en las que había dibujado un rasgo físico y que se iban superponiendo hasta elaborar el posible rostro del autor de los hechos investigados. Se han ido sucediendo otros sistemas de retrato robot, desde el método directo en el que el agente dibuja directamente en el papel según lo que describe el testigo, pasando por los identity-kit o foto-kit, hasta los actuales sistemas informáticos. Fue en 1992 cuando la Policía Nacional de España realizó el primer retrato robot mediante el uso de la informática. Los programas actuales, como el *Facette*, poseen una base de datos con segmentos faciales y una opción de dibujo con el que poder hacer modificaciones.

4.2.3 Los sistemas automatizados de captura del rostro

La captación, segmentación y localización de un rostro en una base de datos previamente creada es un método biométrico que se viene empleando a partir de los años 60[146]. Fue entonces cuando comenzaron a desarrollarse métodos de captación, segmentación y localización de un

---

141 NORRIS, C./ ET ALT. "The Growth of CCTV: A Global Perspective", *Surveillance & Society*, 2004, 110.

142 SÁNCHEZ VIGIL/, ET ALT, "La fotografía como documento de identidad", 2005, pp189-195.

143 Detalles en SÁNCHEZ VIGIL/,ET ALT, "La fotografía como documento de identidad", 2005, p191.

144 Parte Primera, apartado 1.2.3. *La primera experiencia biométrica, en el sentido estricto del concepto: el sistema antropométrico de identificación diseñado por Alphonse Bertillon*.

145 Según los historiadores, el primero que se empleó en el Reino Unido buscaba a *Percy Leproy Mapleton* (1881), pero estos carteles se emplearon muchos años antes en los Estados Unidos de América.

146 KLINK, A. "Die Anforderungen der ICAO an Reisedokumente mit Biometrie", Seminar *Biometrische Systeme*, 2005, pp17-18.

rostro sobre imágenes bidimensionales. Debe destacarse, además, que desde los años 80, la tomografía computerizada (un sistema basado en los rayos x) y la imagen por resonancia magnética, que permite analizar el comportamiento de los tejidos vivos introducidos en campos magnéticos, han proporcionado reconstrucciones tridimensionales del esqueleto craneofacial en conjunto con los tejidos blandos[147]. Las dos técnicas analizan virtualmente la estructura y la reconstrucción tridimensional, empleando para ello una serie de ejes y coordenadas, pero económicamente esta tecnología resulta muy costosa.

En lo que se refiere a la *captura de la muestra*, las tecnologías de reconocimiento facial son comparativamente más simples que las de otras Biometrías, pero los retos técnicos de la captura de atributos biométricos singularizantes y los de creación de los patrones son mucho mayores[148]. El rostro es considerado universal[149], pero la capacidad de los sistemas automatizados de detectar en él atributos singularizantes varía mucho de un sistema a otro. Se calcula que en entorno a un 90% de la información que ofrece el rostro no es singularizante, y ello lleva a que los sistemas se concentren en la información contenida en aproximadamente el 5 o 10% del rostro. Además, la fotografía tiene limitaciones dependiendo del ángulo con la que ésta se haya tomado. Los sistemas más extendidos emplean clasificadores basados en la apariencia o que tratan de medir determinados puntos nodales en el rostro, como la distancia entre los ojos o la longitud de la línea mandibular. Son aspectos importantes a tener en cuenta: la iluminación del rostro y la reducción de sombras, la orientación común o la postura de un rostro, así como la posibilidad de variar las expresiones faciales (IMAGEN 68). Todos ellos pueden determinar la calidad de los patrones.

Los patrones biométricos del rostro se extraen en la mayoría de los sistemas partiendo de una de estas dos aproximaciones: la geometría del rostro –que expresa las reacciones entre determinados puntos del rostro- o las características fotométricas del rostro –que tratan el rostro como un patrón general (IMÁGENES 27 y 28). A partir de ese punto: a) algunos sistemas convierten las imágenes bidimensionales en un vector unidimensional; es el caso de la técnica PCA o Principal Components Analysis o LDA Linear Discriminant Analysis, aunque la primera de estas técnicas parte de una sola foto y la segunda de un set de imágenes en las que se ha pedido al sujeto enrolado que muestre diferentes expresiones; b) el EBGM (Electric Bunch Graph Matching, en cambio, tiene en cuenta que en los rostros hay muchas características no lineares y lo que hace es aplicar pequeños bloques de números (filtros de Gabor) en pequeñas áreas de la imagen, en las que optimiza la extracción de atributos. En el reconocimiento forense los expertos complementan estas Biometrías con análisis de la morfología facial, superponen imágenes para identificar las

[147] SFORZA, C./ FERRARIO, V. F. "Soft-tissue facial anthropometry", *JASS* 2006, p99.

[148] ALTERMANN, A. "A Piece of your Self", *Ethics and Information Technology* 5, 2003, 139-150, p139.

[149] IPTS, p124.

potenciales similitudes y diferencias y tienen en cuenta unos índices de proporcionalidad normalizados para gestionar las potenciales diferencias que pueden producirse dada la distancia respecto a la cámara[150]. La experiencia y la pericia del forense son claves a la hora de valorar ese conjunto de información.

Los primeros prototipos de reconocimiento automatizado de rostros se desarrollaron en la década de los años 90. El Departamento de Defensa de los EEUU creó el programa FERET (Face Recognition Technology, 1993-1997) y para principios del siglo XXI existían ya más de veinte sistemas comerciales disponibles[151]. Sobre varios de ellos, seis departamentos gubernamentales de los EEUU realizaron en 2002 el FRVT (Face Recognition Vendor Test), un test independiente de evaluación de los sistemas comerciales. El sistema con mejores resultados tenía, en entorno controlado, una tasa de error del 10%, con una tasa de falsa aceptación del 1%; en entornos no controlados, sin embargo, la tasa ascendía la 50%, con un 1% de tasa de falsa aceptación.

4.2.4. Gestión de las variaciones inter e intra clase. En especial, las expresiones faciales.

En la década de los 90 muchos de los trabajos se concentraron en un reconocimiento basado en la detección de características individuales en los ojos, nariz, la línea del cabello, en la definición de la forma facial, medidas y/o relaciones entre algunas de las citadas características[152]. Otros enfoques se han concentrado en un conjunto de parámetros geométricos y el desarrollo de un sistema de "reconocimiento de patrones" con base en dichos parámetros, manteniéndose un importante debate sobre qué aspectos del conjunto del rostro han de ser considerados los más relevantes para la identificación. El conocido como enfoque "EIGENFACE" destaca una serie de características locales y globales de cada rostro, a partir de un set de imágenes faciales (conocido como training set)[153]. El rostro de un individuo viene básicamente a representarse en un "rostro promedio", fruto de un mapeado de las variaciones entre diferentes imágenes de su rostro, aunque resulta difícil entrenarlo para poblaciones muy distintas (caucásicos, asiáticos, aborígenes australianos,..).

JAIN y BOLLE fijaron en 1999 seis expresiones universales que debían adoptarse en el enrolamiento, para garantizar una mayor precisión de los sistemas de reconocimiento. La alegría y la tristeza, el disgusto, el enfado, la sorpresa y el miedo eran las expresiones en las que había que

---

150 GHARAIBEG, W. "Correcting for the Effect of Orientation in Geometric Morphometric Studies of Side-View Images of Human Heads," en *Modern morphometrics*, 2005, pp117-142.

151 IPTS, Biometrics, 2005, p123.

152 TURK, M./ PENTLAND, A. "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience*, 1991, pp76, 84.

153 OCDE, *Biometric based technologies*, 2004, p26.

captar un rostro (IMAGEN 29). Así, algunos sistemas de reconocimiento tienen en cuenta un abanico de imágenes del mismo sujeto en el que se reflejan diferentes expresiones de emoción (como la alegría, la tristeza o el enfado). O bien teniendo en cuenta un conjunto de fotografías tomadas al mismo sujeto y desde el mismo ángulo pero recogiendo varias expresiones distintas (alegría, tristeza, enfado,…). Nótese que una fotografía puede ser empleada en la identificación forense, o cuando un testigo comprueba la identidad de un sospechoso, pero propiamente es una *fuente de datos biométricos*, más que un dato biométrico en sí[154].

4.2.5 El reconocimiento facial en ambientes no controlados (videovigilancia)

Dado el nivel de implantación de sistemas de videovigilancia y su previsible expansión[155], sumado al hecho de que existen numerosas bases de datos de fotografías ya creadas[156], las tecnologías de reconocimiento facial (FRT, Facial Recognition Technology) aparecen como una solución atractiva para las necesidades de identificación y verificación contemporáneas. Por ejemplo, el Aurora Imaging Recognition es capaz de confirmar la identidad del pasajero medio en 5 segundos[157]; establecido este sistema como complemento de los controles de tarjetas de embarque primero en la entrada de las terminales y después en el embarque al vuelo, se pretende garantizar que los viajeros no pueden intercambiar sus tarjetas de embarque con otros[158]. La literatura recoge también las referencias del sistema de reconocimiento que se empleó en la *Superbowl* de 2011, en el aeropuerto Keflavik de Reykjavic, el Aeropuerto Logan de Boston (2003) o el Aeropuerto Internacional de Palm Beach en Florida (2002), así como el *ZN-Face-Engine* que se instaló en el Zoo de Hannover (Alemania), elabora un modelo geométrico flexible del rostro empleando una referencia de aproximadamente 1700 puntos de referencia[159].

Universitat d'Alacant
Universidad de Alicante

No obstante, si bien el reconocimiento facial automatizado en ambientes controlados está relativamente maduro, no cabe afirmar lo mismo del reconocimiento facial en ambientes no controlados o sólo controlados moderadamente[160]. Véase la IMAGEN 30. Las tecnologías de reconocimiento de patrones emplean técnicas estadísticas para detectar y extraer patrones a

---

[154] Los estándares a los que atiende el identificador biométrico obtenido del rostro y contenido en el pasaporte europeo son: ICAO NTWG, *Biometrics Deployment of Machine Readable Travel Documents*, Technical Report, 2.0, de 5 de mayo de 2004 y ISO/TEC FCD 19794-5: *Biometric Data Interchange Formats – Part 5: Face Image Data*. La imagen facial (frontal) se almacena como un documento comprimido de imagen (se recomienda JEPG 2000).

[155] INTRONA, L. D. / NISSENBAUM, H. *Facial Recognition Technology*, 2009, pp3-4.

[156] DEPARMENT OF TREASURY, *The Use of Technology*, 2005, pp38-39; *Biometric Comparison Chart*, SJI, National Centre for State Court, USA (2002).

[157] ZHANG/ ET ALT, *3D Biometrics*, 2013, pp10-11.

[158] London Heathrow set to roll-out facial recognition security checks (2011).

[159] ZIEGLER, *Adlerauge*, cit., *C`t*, 9/03.

[160] WECHSLER, H./ LI, F. "Biometrics and Robust Face Recognition", *Biometrics and Forensics*, 2014, p193.

partir de muestras de datos, como por ejemplo una fotografía[161]. Cuando esa muestra reúne las características óptimas para el funcionamiento del sistema, la fiabilidad es elevada. Pero la fiabilidad es todo un reto cuando necesitamos que el sistema de reconocimiento localice rostros dentro de un amplio campo de visión (por ejemplo, en una imagen en la que se pueden ver 40 o 50 metros cuadrados de la calle de una gran ciudad, una terminal de aeropuerto o un centro comercial). El sistema automatizado debe tener capacidad para localizar rostros en un campo de visión (saber qué píxeles de la imagen son partes de un rostro y cuáles no) y normalizar ese rostro (separándolo del resto) para después poder proceder a la extracción de los atributos; con ellos configurará patrones que podrá comparar bien con los almacenados en su base de datos, bien con los que vaya incorporando con posterioridad. La localización y la normalización de los rostros, algo instintivo para el cerebro humano, es algo en lo que resulta difícil adiestrar a los sistemas. Una vez que en esa fase ha localizado un rostro y generado la muestra de análisis se encontrará con algunas dificultades que no se dan en las fotografías controladas. La forma de lidiar con la información incompleta (por oclusiones) o alterada (por ocultación o enmascaramiento), la iluminación, los cambios de expresión o los cambios temporales son aspectos en los que se trabaja con intensidad.

4.3. Biometría (geometría) de la mano.

A partir de la sexta semana de gestación es posible distinguir las áreas de los pies y de las manos en las extremidades. En ese momento pies y manos cuentan ya con dedos, si bien éstos están con frecuencia adheridos aún mediante membranas. Los sistemas de reconocimiento automatizado que emplean como referencia las características de las manos registran su anchura, altura y longitud, así como las de los dedos; y captan también las distancias existentes entre diferentes puntos de articulación o características singulares de los nudillos[162]. Dichos atributos, en conjunto, generan un patrón, de forma que lo que se hace en el proceso de comparación no es confrontar una o dos de dichas medidas, sino el conjunto de éstas; por eso es frecuente emplear la expresión reconocimiento mediante *geometría manual*[163].

---

[161] INTRONA, L./ NISSENBAUM, H. *Facial Recognition Technology*, 2009, p16-17.

[162] SÁNCHEZ-REILLO, R./ ET ALT.: "Biometric identification through Hand Geometry", *IEEE Transactions* 2000, 1168ss, 1169; FACT, 2005, pp38-39; PIECHULECK, A. "Empfehlung für Unternehmen, 2008, p6-7.

[163] BREITENSTEIN, en NOLDE/ LEGER (eds.), *Biometrischer Verfahren*, 2002, p40.

Los dispositivos suelen contener una cámara óptica que normalmente captura imágenes bidimensionales ortogonales de la palma y de ambos lados o bordes de la mano[164]. De ellas se extraen, de media, unas 90 medidas dimensionales relacionadas con la longitud y grosor de los dedos, así como dos siluetas de la mano. Véanse las IMÁGENES 31 y 32. Algunos sistemas escanean uno o más dedos, y existen también sistemas multimodales que combinan la captación de la geometría de la mano con otro tipo de reconocimiento biométrico (de los dermatoglifos o , por ejemplo, de los patrones vasculares de la mano)[165]. Vid. IMAGEN 33.

La captación de la imagen requiere que la persona coloque la mano en una posición fija, en una plataforma, aunque existen sistemas que no requieren contacto[166]. La imagen capturada en color se pre-procesa, transformándola en una imagen en blanco y negro sin fondo, en la que pueden corregirse algunas desviaciones en la mano. Esta imagen es la muestra biométrica o dato en crudo de la que se extraen una serie de medidas, en píxeles o en ángulos, y a partir de dichos atributos se procede a la creación del patrón[167]. Hace años que vienen demostrando su potencialidad en sistemas de reconocimiento diseñados para su uso en un periodo limitado de tiempo o respecto de grupos reducidos de población (acceso a zonas de seguridad de aeropuertos, acceso a depósitos de seguridad en los bancos o en las penitenciarías)[168]. Son los sistemas de Biometría contemporánea más antiguos, en el año 1971 se reconoció la primera patente[169]. La calidad del reconocimiento en los casos en los que las personas realizan trabajos en los que las manos sufren un deterioro importante o su capacidad de captar la permanencia de los rasgos a medida que la persona envejece están todavía en entredicho en el estado actual del desarrollo tecnológico[170].

Universitat d'Alacant
Universidad de Alicante

4.4. Biometría ocular (datos obtenidos de la retina y el iris).

El ojo humano tiene una arquitectura muy compleja; en esencia es un globo opaco, relleno de un fluido y con una membrana que tiene el doble objetivo de proteger el ojo y refractar la luz que entra en él. Los patrones vasculares de la retina y la estructura anular del iris son

---

164 KUMAR, A/ ET ALT : "Personal verification using Palmprint and Hand Geometry", en J. *Proceedings of the 4th International Conference on Audio- and Video-Based Biometric Personal Authentication*, 2003, pp1-8.

165 National Science and Technology Council (NSTC), *Palm Print Recognition*, 2006, p10.

166 JAIN, A. K./ ET ALT, *Introduction to Biometrics*, 2011, p186-187.

167 SANCHEZ-RAILLO/ ET ALTERE, 2000.

168 ALSTER, N.: "A Touchy Object", *CFO* 21 (5), 2005, pp39-42; WILLIAMS, S.: "'Big Brother' Biometrics?", *Credit Union Management*, 28 (4) 2005, pp44-46.

169 ZHANG/ ET ALT. *3D Biometrics*, p12; ASHBOURN, *Guide to Biometrics*, 2012, p19.

170 SHONIREGUN, C./ CROSIER, S.: *Securing Biometrics Applications*, 2007, p12; SANCHEZ-REILLO/ ET ALT. 2000; KUMAR/ZHANG, 2006.

características de las que se obtienen muestras biométricas[171]. Se calcula que el patrón del ojo se desarrolla a partir del tercer mes de gestación y su estructura persiste aproximadamente desde el octavo mes[172] con muy pocas alteraciones[173] y resulta difícil modificarlo sin afectar a la visión[174].

4.4.1. Biometría del iris.

El iris es un órgano interno protegido por una membrana sensible y altamente transparente (la cornea). Esta membrana coloreada y circular del ojo cumple para el ojo la función que el diafragma realiza en una cámara fotográfica. La dilatación de la pupila, que comunica la cámara anterior y la cámara posterior del ojo, se controla mediante los músculos del iris. Éste es, además, el responsable del color del ojo. Los bebés tienen inicialmente ojos color azul-grisáceo, color que puede modificarse en los primeros meses de vida, pero el color definitivo lo determinarán el número y la distribución de unas células que contienen el pigmento melanina (melanocitos). Existe un elevado componente genético en esta determinación. Si hay poca cantidad de melanina, los ojos se mantienen de color azul (es decir, como si no tuvieran color); si ésta se distribuye por todo el espesor del iris, el ojo pasa a ser de color marrón. La textura del iris es de gran utilidad para la identificación debido a su carácter *permanente e inalterable*[175] y al hecho de que presenta una alta variación entre en los humanos[176], se considera que de un solo patrón pueden obtenerse más de 250 puntos diferenciales y digitalizables[177]. Su modificación resulta difícil sin riesgo de afectar gravemente a la visión y se considera prácticamente imposible encontrar a dos personas con un patrón idéntico (con una estructura geométrica similar) del iris[178],[179].

Universitat d'Alacant
Universidad de Alicante

La idea de usar patrones de iris como método de identificación fue propuesta ya en 1936 por el oftalmólogo Frank BUSCH[180] –aunque tiempo antes BERTILLON había señalado el potencial

---

171 RATHGEB, C./ UHL, A./ WILD, P. *Iris Biometrics. From Segmentation to Template Security*, Springer, 2013, p6.

172 KROENFELD, P. "Gross anatomy and embryology of the eye", en H. DAVIDSON (ed.) *The Eye*, 1962.

173 FENKER, S. P./ BOWYER, K. W. "Experimental evidence of a template aging effect in iris biometrics", C. RATHGEB (ed.) Iris Biometrics, 2011, p149.

174 ROSS, A. "Iris recognition: the path forward", *Computer* 43, 2010, pp30-35.

175 A. PIECHULECK, "Empfehlung für Unternehmen", *Workshhop IT-Sicherheitsmanagement*, 2008, p4.

176 R. WINSTON, *What makes me me?,* 2004, pp28-29; LÓPEZ CARVAJAL, J./ LÓPEZ PATIÑO, J. "Estado del arte: reconocimiento automático del iris humano", *Scientia et Technica* 2005, p77-80.

177 US GAO, *Using Biometrics for Boder Security*.

178 DAUGHMAN, J.G.: "How iris recognition works", *IEEE Transactions*, 2004.

179 DAUGHMAN, J./ DOWNING, C. "Epigenetic randomness, complexity and singularty of human iris patterns", en *Proceedings of the Royal Society*, 2001, vol 268, pp1737-1740.

180 DAUGHMAN, J. "Iris Recognition", *Am Sci* 89 (4), 2001, 326-333.

del color del iris para el reconocimiento[181] -. De la propuesta de Busch se hicieron eco obras de ciencia ficción, como la saga de James Bond de Ian Fleming[182]. Pero los sistemas que permiten este tipo de reconocimiento son mucho más recientes. Se conoce como Eye Identify una de las primeras y más destacadas unidades de investigación y desarrollo en esta materia, fundada en 1976. La investigación de los doctores Leonard FLOM y Aran SAFIR fructificó en la primera aplicación patentada en 1985 (US PATENT 4641349)[183], aunque su implementación quedó pendiente de hallar un algoritmo. En 1989 FLOM y SAFIR recurrieron a John DAUGMAN para crear algoritmos para el reconocimiento de iris y estos algoritmos, patentados por DAUGMAN en 1994[184] y que son propiedad de *Iridian Technologies*, son la base para todos los productos de reconocimiento de iris que existen en el mercado[185]. Los sistemas de reconocimiento de iris toman la imagen del iris y la pre-procesan tomando como referencia la pupila; para obtener los atributos se aplican filtros de Gabor de dos dimensiones y a partir del set de atributos se crea un patrón que será almacenado y utilizado en el futuro para la comparación. Veanse las IMÁGENES 40 y 41.

DAUGHMAN desarrolló, además, un test de independencia estadística que compara cada nuevo patrón de iris obtenido con patrones ya los almacenados[186]. A este experto recurrió la revista National Geographic en el año 2002 para determinar cuál de las mujeres que así lo alegaban era realmente la niña pastún que fue fotografiada por Steve McCurry en junio de 1984 en un campo de refugiados de Afganistán y hoy sabemos que se llamaba Sharbat Gula. Véase la IMAGEN 34.

El iris destaca por sus altas tasas de universalidad –mayores que las de las huellas, aunque menores que las del rostro-, su elevado poder singularizante y su permanencia respecto de otros datos biométricos[187]. Hay que advertir, no obstante, que a la hora de diseñar sistemas biométricos basados en rasgos del iris algunas de sus características resultan desventajosas[188]. Comenzando ya por la captura misma, el reconocimiento mediante el iris es altamente complejo. Su pequeño tamaño dificulta la adquisición a ciertas distancias y la necesidad de contar con la colaboración

---

181 BERTILLON, A. "La coleur de l'iris", en *Annales de demographie internationale*, 1886, pp226-246.

182 ITU-T Technology Watch Reports, 2009, p4.

183 KISKU ET ALTERE, *Advances in Biometrics for Human Secure Authentication*, 2013, pp42-65; DEHGHANI, A./ ET ALTERE, 2013.

184 DAUGMAN, J. G. "High confidence visual recognition of persons", *IEEE Trans. Pattern,* Vol. 15, No. 11, 1148-1161.

185A. PIECHULECK, "Empfehlung für Unternehmen", *Workshhop IT-Sicherheitsmanagement*, 2008, pp1-3.

186 DAUGMAN, J. G. "High confidence visual recognition of persons", I*EEE Trans. Pattern,* Vol. 15, No. 11, 1148-1161; DEL MISMO, How iris recognition Works, IEEE TRans Circ Sys Video Tech 4 (1), 21-30, 2004.

187 WAYMANN, J. L. "Technical testing and evaluation of biometric identification devices", en *Biometrics Personal Identification in a Networked Society*, 1999, pp343-368; ZHANG/ ET ALT, *3D Biometrics*, 2013, pp10-11; IPTS, p.142.

188 MURON, A y J. POSPISIL, "The human iris structure and its usages", *Physica*, Elsevier,2000, 39:89-95.

del usuario[189], por cuanto se trata de un objetivo móvil y que está ubicado en una superficie curva, húmeda y reflexiva. A ello se añade el hecho de que, en no pocas ocasiones, la imagen del iris suele verse estar afectada por pestañas, párpados y reflejos de luz, y sus deformaciones no son elásticas cuando la pupila cambia de tamaño. Muchos de los sistemas requieren la cooperación del sujeto dirigiendo su pupila hacia un punto concreto[190], aunque se han desarrollado también métodos de captación a distancia o sin cooperación específica del sujeto[191]. La tecnología de reconocimiento mediante el patrón del iris es, a día de hoy, una de las más seguras, rápidas y precisas –funcionan incluso con gafas o lentillas[192]- y menos invasivas, como es el caso del *IrisAccess*™ (2012) de Iridian technologies, pero su aceptación por parte de los usuarios no es buena en casos en que ha de hacerse un uso frecuente (como por ejemplo para acceder cotidianamente a un puesto de trabajo o al ordenador personal).

En 1993 la *Agencia Nuclear de Defensa* empezó a trabajar con *IriScan, Inc.* para desarrollar y probar un prototipo. Dieciocho meses después el primer prototipo se completó y desde entonces está disponible comercialmente en diferentes calidades de resolución[193]. Las agencias gubernamentales comenzaron a emplear esta tecnología en 1994 para identificar a los reclusos en la Prisión de Lancaster (Pensilvania). Posteriormente se empleó en la de Berkshire, esta vez para control de seguridad de los empleados[194] y en algunos aeropuertos europeos (Schiphol, Heathrow, Frankfurt a. M.) permiten a usuarios habituales enrolar el iris para simplificar los procedimientos de embarque[195]. Véanse las IMÁGENES 1.4. y 73. En diecisiete puntos de acceso a los Emiratos Árabes se establecieron sistemas de enrolamiento de los viajeros que llegaban, así como en los Programas de viajeros frecuentes de los aeropuertos de Schiphol, Frankfurt Internacional o en algunos aeropuertos de Canadá o Estados Unidos (2004). El Informe IPTS menciona además el uso por parte del ACNUR en el control del retorno de los refugiados afganos en la frontera entre Pakistán y Afganistán[196] (IMAGEN 75), y aunque no se han publicado datos es sabido que los ejércitos occidentales –especialmente el estadounidense- han venido recogiendo datos del iris de muchos varones en Irak y otras zonas conflictivas de África y Oriente medio y próximo. Véanse las IMÁGENES 1.2 y 75.5.

---

189 VIELHAUER, C. *Biometric ser Authentication*, Springer, 2006, p60-61.

190 KINDT, E. *Privacy and Data*, 2013, p27.

191 MALEY, J. R./ ET ALT, "Iris on the move", *Proceedings of the IEEE*, 2006, pp1936-1947.

192MASEK, L. *Recognition of Human Iris Patterns*, *2003*, pp13-16.

193MASEK, L. *Recognition of Human Iris Patterns*, *2003*, pp13-16.

194 EUROPEAN COMMISSION (ED), *Biometrics in Europe*, 2007, pp22-23.

195 ALONSO-ZALDIVAR, R.: "Airports Test Express Security Lane", *Los Angeles Times*, 8 de julio de 2004; LANGENDERFER, J. / LINNHOFF, S. "The Emergence of Biometrics", 2005, págs. 315ss.

196 IPTS, pp143-144.

Algunas empresas de finanzas, fundamentalmente bancos, estudian el escáner de iris y hay expertos que advierten que algún día llegarán a ser una rutina en las transacciones ATM[197]. Sin duda, la aplicación de tecnología de iris más relevante hasta el momento es el proyecto Aadhaar de la Autoridad de Identificación Única de la India. Este sistema emplea el iris y las huellas dactilares en una configuración multimodal con el objetivo de otorgar un único número de identificación a todos los residentes en la India. Sus tasa de falsos positivos se fijó en un 0,057% en 2012 y la tasa de falsos negativos en un 0,035%[198].

En los próximos años se estima que seguirá desarrollándose el potencial de estas tecnologías. Existen en la actualidad importantes bases de datos disponibles para el reconocimiento mediante la Biometría del iris, muchas de las cuáles permiten el acceso público de investigadores. Es el caso de la base de datos CASIA V1.0 del Laboratorio Nacional de Reconocimiento de Patrones (National Laboratory of Pattern Recognition), el Institute of Automation y la Academia China de las Ciencias (CAS). La literatura clasifica estas bases atendiendo al número de muestras intra-clase, a su tamaño, a su representatividad poblacional, a la captación en periodos de tiempo más o menos extensos. Los tipos de algoritmos que emplean, la forma en que se enfrentan a los problemas de oclusiones, falta de iluminación etc. son diversos (vid. IMAGENES 21 y 66).

4.4.2. Biometría de la retina.

Universitat d'Alacant
Universidad de Alicante

El escáner de retina es, entre los sistemas automatizados, uno de los sistemas de reconocimiento biométrico que se consideran más antiguos; las primeras patentes son de mediados de los años 70 (Texas Instruments, 1976)[199]. En los años 30 algunas investigaciones sugirieron las posibilidades de los patrones vasculares de la parte posterior del ojo como posible fuente de datos biométricos y se considera que los patrones vasculares de la retina no sólo son distintos para cada individuo, sino para cada ojo, resultando además imposibles de replicar[200]. No obstante, el proceso de desarrollo tecnológico ha sido bastante más lento. Se conoce como *EyeDentify* una unidad fundada en 1976 con estos fines y que desarrollo la primera aplicación a mediados de los años 80. El escáner computerizado de retina tiene hoy día un uso bastante extendido en lo que se refiere a los estudios diagnósticos[201], pero su uso como base de un

---

[197] FACT, 2005, p39-40.

[198] UNIQUE IDENTIFICATION AUTHORITY INDIA, *Role of Biometric Technology in Aadhaar enrollment*, 2012.

[199] DUNSTONE, T./ YAGER, N. *Biometric System and Data Analysis*, 2009, p8.

[200] JAIN, A. K./ET ALT, *Introduction to Biometrics*, 2011, p34.

[201] Es el caso del *Optomap Computerized Retinal Scan*.

procedimiento de reconocimiento mediante Biometría veremos que ha suscitado bastantes recelos.

La tecnología capta los patrones vasculares del fondo del ojo dirigiendo a éste una luz infrarroja de baja intensidad, algo para lo que se necesita la cooperación y el adiestramiento de los sujetos. Los atributos captados se digitalizan y con ellos se construye el patrón[202].

4.5 Biometría auricular (datos biométricos obtenidos de la oreja) y el otograma o la llamada *huella de la oreja*.

4.5.1. Biometría auricular

La oreja humana se compone de tres partes, el oído externo (pabellón auricular), el oído medio (cavidad timpánica) y el oído interno (laberinto) y desde el punto de vista forense su examen se estima de utilidad con diferentes fines. Entre ellos[203]: la búsqueda de anormalidades genéticas y congénitas[204], la identificación, el diagnóstico de procesos patológicos o la estimación del intervalo posmortem. El pabellón auricular está constituido por un esqueleto cartilaginoso revestido por tegumentos[205]. Esa lámina de cartílago se pliega sobre sí misma y forma relieves y depresiones que dan a cada oreja una forma característica y única. Existen variaciones por enfermedad, modificaciones debidas al envejecimiento y variaciones por grupos de población que han sido descritas en la literatura. Además, los restos de descamación, sudor y grasa de la oreja hacen que el contacto de ésta con algunos objetos (como la puerta detrás de la que se escucha o el auricular de un teléfono por el que se conversa) deje una huella que se puede rastrear (el otograma). La permanencia de los rasgos de la oreja es también notable. La literatura médica refiere cómo el crecimiento de la oreja durante los cuatro meses posteriores al nacimiento es proporcional, y posteriormente la gravedad puede hacer que se produzca mayor crecimiento vertical (algo más pronunciado en el lóbulo). La tasa de expansión es cinco veces mayor de lo normal entre los cuatro meses y los ocho años de edad y a partir de entonces se mantiene constante hasta aproximadamente los 70 años, cuando comienza de nuevo a crecer[206].

---

202 KIZZA, J. M., "Ethical, and Social Issues in the Information Age", *Texts in Computer Science*, 2010, p287.

203 SWIFT, B./ RUTTY, G. N. : " The Human Ear", *J. Forensic Sci*, 2003, vol. 48, nº 1, pp153 y ss.

204 Así, el síndrome de *Goldenhar* (microsomía hemifacial), el síndrome *Treacher-Collins* (Distosis mandibulofacial), *X Frágil* o Sindrome de *Martin-Bell*. Vid: FARKAS, L. G. "Ear Morpology in Treacher Collins', Apert's, and Crouzon's síndromes", *Arch Otorhinolaryngol* 1978: 220 (1-2), pp153-157; BUTLER, M. G./ ET ALT, "Standards for selected anthropometric measurements in males with the fragile X syndrome", *Paediatrics* 1992, 89 (6ª parte), 1059-1062; LOESCH, D. Z./ ET ALT, "Anthropometry in Martin-Bell Syndrome", *American Journal of Medical Genetics* 1988, 30 (1-2), 149-64.

205 CURIEL LOPEZ DE ARCAUTE/ GRANELL NAVARRO, "La huella de la oreja", *Act Otorrinolaringológica* 2006, 57: 329-332.

206 BURGE, M. / BURGER, W. / KEPLER, J. *Ear Biometrics*, Universidad de Linz, p5-6.

El reconocimiento de su potencial como elemento de identificación es antiguo[207]. En su famoso libro *La Photographie judiciaire* **(**1890**),** advertía BERTILLON de que la oreja humana, "*gracias a sus múltiples valles y a las colinas que los atraviesan, es el más significativo de los factores desde el punto de vista de la identificación*". Probablemente fue uno de los primeros científicos que utilizó la oreja como medio de identificación, junto con Johan Casper LAVATER (1741-1801) o posteriormente Haken JORGENSEN en Dinamarca (1879-1927)[208]. Un siglo después, tras 38 años estudiando orejas y con una base documentada de más de 10.000, IANNARELLI llegó a la conclusión de que no existían dos orejas iguales[209]. Véase la IMAGEN 35. Ni siquiera son iguales entre sí las dos que pertenecen a una misma persona o las de los gemelos monocigóticos. También estableció que la estructura de la oreja no cambia sustancialmente con la edad[210] (véase la IMAGEN 35) y participó como perito en varios juicios, aunque no todos los tribunales admitieron este tipo de pruebas[211].

Aún hoy día, y a pesar de los avances en el conocimiento científico (en antropometría auricular, así como en variaciones congénitas y genéticas en la morfología auricular[212] ha permitido desarrollar de forma importante el campo de la identificación auricular), y en el desarrollo metodológico[213], en algunos países se discute si estas técnicas tienen la madurez suficiente como para ser empleadas en los procedimientos de enjuiciamiento criminal[214]. Todo hace pensar, sin embargo, que esto cambiará en un futuro no muy lejano. En febrero de 2002 se puso en marcha el proyecto FEARID ("Forensic EAR Identification"), aprobado por la Unión Europea, como respuesta a la necesidad de una investigación científica estricta y un estudio sistemático de las huellas de orejas y el desarrollo de herramientas de apoyo automatizado para su cotejo. El objetivo es establecer un proceso estándar de detección, recuperación, almacenamiento e identificación de las huellas de oreja y el establecimiento mediante programas informáticos de una base de datos paneuropea de huellas de oreja que permita un cálculo estadístico y aumente la potencia de la

---

[207] CURIEL LOPEZ DE ARCAUTE/ GRANELL NAVARRO, "La huella de la oreja", *Acta Otorr* 2006, 57: 329-332.

[208] SWIFT, B./ RUTTY, G. N. "The Human Ear", *J. Forensic Sci*, 2003, pp153 y ss, p160 con más referencias; B. BHANU/ ET ALT, *Human ear Recognition by Computer*, 2008, 20-22.

[209] IANNARELLI, A. *Ear Identification*, 1989; vid. sobre este autor, detalladamente Mark Burge/ Wilhelm Burger, "Ear Biometrics", en JAIN, A. K./ BOLLE, R./ET ALT, *Biometrics – Personal Identification*, 1999, cap. XIII, pp276 y ss.

[210] IANARELLI, A. *Ear Identification*, 1989.

[211] *State v. David Wayne Kunze*, Corte de Apelación de Washington, 1999. Más referencias de casos, BHANU, B./ ET ALT, *Human ear Recognition by Computer*, 2008, pp20-21.

[212] PEEPLES, E. F./ DIXON, L. K./ BUSS, W. R. "Genetic analysis of the pina of the human ear: sex differences in collage age adults", *J. Heredity*, 1985: 76 (5), 390-2; FARKAS, L. G. : "Anthropometry of normal and anomalous ears", *Clinics in Plastic Surgery*, 1987, 5 (3), 401-12.

[213] HOOGSTRATE, A. J./ ET ALT, "Ear identification based on surveillance camera images", *Sci Justice* 2001, pp167-172.

[214] CHAMPOD, C./ EVERTT, J. W./ KUCHLER, B. "Earmark as evidence", *Journal of Forensic Science*, 2001, 1275-84.

prueba dando una validez científica y judicial a la identificación por huellas de oreja. El proyecto FEARID ya ha dado los primeros resultados con los trabajos publicados[215].

En comparación con la Biometría del rostro o de las huellas dactilares, la oreja ofrece una gran riqueza de caracteres[216] aunque existe una gran variedad de formas de obtención de una muestra biométrica de la oreja para su tratamiento biométrico automatizado[217]. En algún caso se transforma la imagen en un campo de fuerza para extraer de ahí el patrón, o se aplica una técnica similar a la del análisis de huellas dactilares captando los surcos y los valles. Las imágenes de referencia pueden ser en 2D y 3D (véanse las IMÁGENES 35, 38 y 39). BURGE/ BURGER desarrollaron un sistema en 2D con un algoritmo de 4 componentes (que extraía vértices y curvas y construía un modelo gráfico a partir del diagrama de Voronoi[218] de los vértices). HURLEY ET ALT., por su parte, transformaron las imágenes de la oreja completa en campos de fuerza, extrayendo después las ondas y canales. Aunque hay más técnicas. Para el tratamiento de la Biometría de la oreja en tres dimensiones (3D), se emplean métodos que se focalizan, entre otros, en las hélices y anti-hélices o en determinadas peculiaridades de las superficies locales.

4.5.2. El otograma (huella de la oreja) en los procesos judiciales

Define el diccionario de la RAE como "otograma" la huella del que escucha. Son también muy pocos los casos documentados en que se han aceptado identificaciones judiciales por este tipo de huellas. (véanse las IMÁGENES 36 y 37). El primer proceso del que se tiene noticia es un caso registrado en Suiza en 1965[219], y en Holanda hay ya más de 200 casos documentados, pero en países como los Estados Unidos los jueces tienden a rechazar la identificación por otograma, con el argumento de que la generalidad de la comunidad científica no respalda este tipo de identificaciones. [220]

El Tribunal de Apelaciones del Estado de Washington en 1999 señalaba que "la novedad científica, el conocimiento técnico u otro conocimiento especializado puede ser admitido o se puede confiar en él sólo si es, en general, aceptado como fiable por la comunidad científica, especializada o

---

[215] MEIJERMAN, L./ ET ALT. "Exploratory study on classification and individualisation of earprints", *Forensic Science International* 2004;140:91-99; y KIECKHOEFER, H./ INGLEBY, M./ LUCAS, G. *The physical formation of ear-prints: optical and pressure mapping evidence*, 2003.

[216] BAHNU/ CHEEN, *Human Ear*, Springer, 2008.

[217] RUTTY, G. N./ ABBAS, A./ CROSSING, D. "Could earprint identification be compterised", *International Journal of Legal Medicine*, vol 119, nº6, 2005, pp335-343; MEIJERMANA, L./ SHOLLB, S./ DE CANTIC, D. "Exploratory study on classification and individualisation of earprints", *Forensic Science Int*, vol 140, pp91-99, 2004.

[218] El diagrama de Voronoi un tipo de estructura empleado dentro de la Geometría computacional.

[219] CURIEL LOPEZ DE ARCAUTE/ GRANELL NAVARRO, "La huella de la oreja", *Acta Otor Esp* 2006, 57: 329-332.

[220] CURIEL LOPEZ DE ARCAUTE/ GRANELL NAVARRO, "La huella de la oreja", *Acta Otor Esp* 2006, 57: 329-332.

técnica. La aceptación general puede ser encontrada en el testimonio de quien lo afirma, en artículos y publicaciones, en su uso extendido entre la comunidad o en otros tribunales. La aceptación general no se puede encontrar si hay una disputa significativa entre expertos cualificados en torno a la validez de la evidencia científica". En este caso doce miembros reconocidos de la comunidad de la ciencia forense declararon que la identificación a través de las huellas de oreja no está aceptada en su generalidad por la comunidad de dicha ciencia. La falta de apoyo en la literatura científica es la gran debilidad del estado actual de la identificación por la huella de oreja, a pesar del progreso habido en los últimos años[221].

En España la primera sentencia firme en la que se empleó el otograma fue de 2002 (Sentencia de la Audiencia Provincial de Palencia 2/ 2002, de 22 de enero)[222]. La sentencia, que se hizo pública, ratificó la condena de 2,5 años de cárcel impuesta en el año 2000 por el Juzgado de lo penal, en la que se castigaba a un ciudadano colombiano por la comisión de un robo siendo determinante "*la prueba de cargo consistente en la práctica de otogramas mediante el contraste de la oreja indubitada del recurrente con las huellas dubitadas halladas en el lugar en el que el robo fue perpetrado*"[223].

4.6 La Biometría del ADN y el debate sobre si debe o no considerarse entre las características que pueden servir de base a los sistemas automatizados.

Las muestras de biológicas humanas y, en especial, algunos de sus componentes o de sus características (grupo ABO o los antígenos de histocompatibilidad), son empleados cotidianamente en la identificación forense[224].. De entre esos componentes, el ADN humano presenta unas cualidades muy interesantes como base potencial para los sistemas de identificación de las personas. Cumple el requisito de la universalidad; además se le estiman millones de polimorfismos que pueden ser captados de forma singularizante (patrones de moléculas, en especial del ADN no codificante[225]) y se considera diferente de un individuo a otro, con la única excepción de los gemelos monocigóticos. Si en algo destaca sobre otras fuentes potenciales de datos biométricos es, sin embargo, en su estabilidad; a día de hoy es la única fuente de datos biométricos que se afirma con rotundidad que cumple el requisito de *permanente*. Véanse las IMÁGENES 43 y 44.

---

221 CHAMPOD, I. C./ EVETT, I.W./ KUCHLER, B. "Earmarks as evidence", *J Forensic Sci* 2001;46:1275-1284.

222 LÓPEZ GOBERNADO, C. J. *Los otogramas como prueba en el proceso penal español*, cit.

223 En expresión del Auto nº 499/ 2004 del TC, en respuesta al recurso de amparo interpuesto por el letrado del reo.

224 GAINOTI, S./ SPAGNOLO, A. G. "Test-genetici: a che punto siamo in Europa?", *Medizina e Morale*, 2004, pp750-751; LORENTE ACOSTA, J. A/ LORENTE ACOSTA, M.: *El ADN y la identificación en la investigación criminal*, 1995, 3 y ss.

225 SUÁREZ ESPINO, M. L. *El derecho a la intimidad genética*, Madrid, 2008, pp124 a 153.

Los datos biométricos que pueden obtenerse de este tipo de muestras presentan, sin embargo, una importante limitación a la hora de servir de base a sistemas de reconocimiento automatizado[226]. Y es que el acceso a esta información no se puede aún realizar a la misma velocidad que, por ejemplo, el reconocimiento mediante datos biométricos obtenidos de la huella dactilar[227]. Ello explica porqué en la literatura no hay consenso a la hora de considerar (o no) el ADN humano como una característica de las que pueden servir de base a los sistemas automatizados de reconocimiento mediante biometría[228]. Algunas definiciones y listado incluyen expresamente al ADN humano como fuente de datos biométricos[229] y otras lo excluyen.

En nuestra opinión la clave del debate está en cómo debemos interpretar, en conjunto, las siguientes circunstancias. En primer lugar, hemos constatado que no hay duda de que el ADN es una fuente de información biológica de los individuos y, unido a ello, tampoco se discute que dicha información ofrece en forma suficiente las cualidades de universalidad, singularidad y permanencia. Es más; con la única excepción de los gemelos idénticos, se insiste con frecuencia en la literatura en que el ADN es, a día de hoy, el elemento más singularizante de cuantos pueden hallarse en el cuerpo del ser humano y, se ha dicho ya, es el elemento identificador más permanente que se ha captado hasta el momento. De hecho, y como es sabido, existen bases de datos de ADN que son empleadas, entre otros, con una finalidad criminal o judicial. Se trata de colecciones de perfiles registrados o codificados estructuralmente sobre un soporte informático y, con las herramientas necesarias, pueden proporcionar información en el curso de diferentes tipos de investigaciones.[230].

Unido a esto, y en segundo lugar, tampoco se discute que dicha información sea susceptible de *estudios mensurativos* y que el objetivo de tales estudios biométricos puede ser, entre muchos otros, la captación del potencial singularizante del ADN. ¿Cuál es, pues, el problema? La clave de la discusión se concentra en el hecho de que conforme al actual estado científico y tecnológico no es posible obtener datos biométricos del ADN con la agilidad suficiente como para servir de soporte a un sistema de reconocimiento *automatizado*. Es decir: se retoma aquí la cuestión de la acepción

---

[226] LANGENDERFER, J./ LINNHOFF, S. "The Emergence of Biometrics", 2005, pp322.

[227] Así, con más referencias, GIROTTO, S.: "Il tratamento dei Dati Biometrici", en *Tratatto di Biodiritto.* 2011, p1238, y el Documento WP 80 del GT-WP 29 (2003).

[228] VIELHAUER, C.: *Biometric User Authentication for IT Security*, 2006, p. 34.

[229] Por ejemplo la definición de biometrics que aparece en el *Computer Science and Communication Dictionary*, 2001, p122.

[230] MORA SÁNCHEZ explica con detalle cómo los problemas que plantean estas bases de datos difieren según la finalidad con la que se crean, así como en función de su ámbito subjetivo (bases de datos a nivel general de una población, bases de datos de personas que comenten cualquier tipo de delito, bases de datos específicamente orientadas a la persecución de determinados delitos), en MORA SÁNCHEZ, J. M.: *Aspectos sustantivos y procesales de la tecnología del ADN*, 2001, pp301 a 308.

amplia y la acepción estricta de biometría, y el modo en que se emplea el binomio *biometry-biometrics*. Extraer secuencias de ADN implica un proceso bioquímico que no está totalmente automatizado y, además, requiere aún lapsos de tiempo considerables.

Algún autor expresa un segundo argumento, que expondremos a continuación, pero que en nuestra opinión resulta muy débil en relación a lo que aquí se pregunta. Afirman que el ADN *no debería ser empleado como fuente de datos biométricos* dado el fácil acceso que terceros pueden tener a las muestras biológicas con ADN que cotidianamente se desprenden del cuerpo de las personas -como cabellos, saliva en los vasos o cigarrillos, etc.-[231]. En nuestra opinión considerar que *no debería* emplearse no justifica la exclusión del ADN del listado de fuentes potenciales de datos biométricos. Más aún; la afirmación de que no debería emplearse de hecho implica aceptar que, en puridad, sí que lo es.

Las dos primeras circunstancias –el indudable potencial singularizante y la posibilidad de su estudio mensurativo- son suficientes como para considerar al ADN una fuente de datos biométricos[232], máxime teniendo en cuenta que los avances científicos y tecnológicos probablemente permitan superar a futuro los obstáculos que en la actualidad dificultan el diseño de sistemas de reconocimiento automatizado con base en el ADN. Bromba advierte, no obstante, de la distancia entre el potencial singularizante del ADN y su rendimiento actual; en su opinión, la precisión del reconocimiento mediante el ADN no codificante es en promedio menor que la que ofrece las tecnologías mediante el iris, porque los patrones que se obtienen de las muestra son siempre son comparables (es necesaria una cantidad de ADN), y existe riesgo de contaminación o de degradación que afecte a la calidad de las muestras [233].Otras desventajas: que el ADN no diferencia entre gemelos idénticos y existe un notable rechazo social a su utilización con fines de reconocimiento civil, por su vinculación con información sobre el origen y la salud de las personas[234]..

De una muestra biológica que contiene suficiente se aísla el ADN y esa muestra se transforma en un perfil que expresa las regiones no codificantes del ADN que se caracterizan por un elevado grado de polimorfismo. Existen ya, de hecho, sistemas semi-automatizados para el análisis de la

---

[231] VIELHAUER, C.: *Biometric User Authentication for IT Security*, 2006, p. 34.

[232] NOLDE, N.: "Grundlegende Aspekte biometrischer Verfahren", en *Biometrische Verfahren*, 2002, 20 (21).

[233] BROMBA, 2004.

[234] Informe IPTS, p155.

sangre y la saliva sobre tarjetas FTA[235]. Se emplea, entre otros, por el IPDIS (Israel Police DNA Index System), porque permite un procesamiento rápido de las muestras de ADN con poco personal de laboratorio. Lo mismo podrá suceder con técnicas de laboratorio forense –como las de las huellas latentes, el análisis de cabello o fibras – que en la actualidad no se consideran parte de este campo.

4.7. Otras Biometrías estáticas

4.7.1. Biometría del olor corporal

Los seres humanos, al igual que otros animales, emiten olores en varias de las partes de su cuerpo. La composición bioquímica de esas secreciones depende de su genética, hormonas, metabolismo, dieta, así como de su entorno social y ambiental[236] y se considera que, por tal motivo, una tecnología adecuada podría servir para identificar a los individuos mediante la Biometría del *olor corporal*[237]. Los dispositivos capaces de captar el olor corporal y hallar atributos en su composición química son del tipo de los que se conoce como *nariz electrónica*[238] (ENose; IMAGEN 45). Se trata de dispositivos que tienen ya una trayectoria asentada en la interpretación de olores procedentes de otras fuentes en campos como la detección de riesgos ambientales, la inspección de la calidad alimentaria[239] o en el diagnóstico médico. En este último campo se estima que pueden contribuir al diagnóstico de problemas gastrointestinales o sinusales, así como infecciones, diabetes o problemas de hígado).

El estado del arte en esta cuestión no hace previsible que vayan a comercializarse en breve sistemas de reconocimiento humano basados en el olor corporal, aunque en la literatura hay referencia de dos sistemas que se desarrollaron con dicho objetivo. El *Scentinel*, de la compañía británica *Mastiff Electronic Systems*[240] y otro sistema desarrollado por el Pentágono[241]. La estructura básica de estos sistemas se compone de un cromatógrafo o un espectrómetro realizan

---

235 JAFFREDO, F./ FREUND, F./ ET ALT, "Complete automated DNA procedure to facilitate DNA database collection", *Forensic Science International: Genetic Supplement Series*, 3 (2011), e228-e229; ZAMIR, A./ DELL'ARICCIA-CARMON, A./ ET ALT "The Israel DNA database", *Forensic Science International: Genetics*, 6, 2012, 286-289.

236 GUTIÉRREZ, F.J./ HORRILLO, M. C./ SAYAGO, I/ ET ALT, *Electronic olfactory nano-microsystems for recognition in biometrics*, 2008.

237 KOROTKAYA, Z.: "Biometrics Person Authentication: Odor", http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf, 2003; LAWSON, W. J.; *Enhancing Assistive Technologies: Throught the Theoretical Adaptation of Biometric Technologies to People of Variable Abilities*, 2003.

238 WYLIE, M. "An Artificial Nose that Can Sniff out Terrorists? It May Not Be Sci-Fi", *Newhouse News Service*, 2003.

239 DI NATALE, C./ MACAGNANO, A./ MARTINELLI, E./ PAOLESSE, R./ PROIETTI, E./ D'AMICO, A."The evaluation of quality of post-harvest oranges and apples by means of an electronic nose" *Sens. Actuators B* 78, pp. 26–31, 2001.

240 Citado por DAVIS, A."The Body as Password", Wired News. 1997.

241 Wylie, M. "An artificial Nose that Can Sniff Out Terrorists? It May Not Be Sci-Fi"-*Newhouse News Service*, 2003.

un análisis y ofrecen un desglose de las medidas que corresponden a cada uno de los componentes presentes en un olor.

4.7.2. Biometría del esmalte dental y la huella de la lengua

En la mayoría de las especies mamíferos el esmalte dental está caracterizado por la presencia de capas de primas en direcciones que se alternan. Se conocen como capas de Hunter-Schreger y algunos estudios apuntan a sus posibilidades biométricas[242], aunque se trata de investigaciones que están aún en una fase inicial. Véase la IMAGEN 46.

Hemos encontrado también una propuesta de reconocimiento automatizado basado en la huella de la lengua (tongue-print images). Diwakar/ Marhashi[243] destacan entre las particularidades de este tipo de reconocimiento el hecho de que la lengua es un órgano que para ser captado requiere interacción del sujeto (demostrando una prueba de vida), ofrece información tantoe geométrica como de la textura y no está tan expuesto a terceros como la geometría del rostro o la de las huellas, por lo que resulta difícil su captación sin el consentimiento de la persona. Véase la IMAGEN 47.

4.7.3 Biometría del lecho ungueal (*nail bed*)

La medición de características del lecho ungueal o de los patrones vasculares son otros ámbitos de trabajo de las investigaciones biométricas. La uña es una estructura anexa a la piel y está formada principalmente por células muertas que contienen queratina, y se conoce como lecho ungueal el tejido conectivo adherente situado entre la uña y el dedo. Esta estructura tiene una cifra importante de surcos que van en paralelo desde la matriz de la uña (el lugar de donde crece) hasta donde termina el dedo. Mediante interferometría se estima posible obtener patrones de las uñas y se ha documentado un prototipo AIMS[244]. Vease la imagen 48.

4.7.4 Patrones vasculares de la mano

Las venas forman un dibujo único en cada ser humano y ese patrón vascular es fácil de captar en aquellas partes del cuerpo que normalmente están visibles (como las manos)[245]. El grosor, la ubicación y el trazo de las venas son diferentes incluso entre los gemelos monocigóticos

---

[242] LRAMENZONI, L. L. / LINE, S. R. P.„Automated biometrics-based personal identification of the Hunter-Schreger bands of dental enamel", *Proceedings of the Royal Society B* (2006), 273, p1155-1158.

[243] DIWAKAR, M./ MAHARSHI, M. "Extraction and Recognition of Tongue-Print Images for Biometrics Authentication System", *Journal of Computer Applications*, vol. 61, nº 3, 2013, pp36-42.

[244] AMBERG, FISCHER, RÖßLER: *Biometrische Verfahren* (2003), p31-32.

[245] MARINO, T. M. *Tecnologías biométricas aplicadas a la seguridad*, Alfaomega, 2005; SUÁREZ RUIZ/ FAJARDO PITO/ TIBADUIZA, "Autentificación de Personas a partir de la Biometría de las Venas de la parte posterior de la manos", *Revista Colombiana de Tecnologías Avanzadas*, nº 12, 2008, pp62ss.

y aunque su tamaño varía con el paso del tiempo, su estructura singular se mantiene durante toda la vida del individuo[246]. Se comenzó a prestar atención a su potencial como base para sistemas de reconocimiento biométrico en los años 90 y en 1997 surgió en Korea el modelo BK-100 del cual se establecieron más de 200 unidades en Korea y Japón. A él les siguieron los modelos BK-200 y BK-300 (vid imagen del BK 100)[247]. Véase la imagen 33.

Entre las ventajas potenciales de este tipo de identificación se dice que se emplea el mismo sistema para estudiar las venas de cualquier parte del cuerpo[248], con lo que sirve también para identificar personas con alguna discapacidad. Los laboratorios Fujitsu desarrollaron el sistema de reconocimiento PalmSecure™ en el año 2002[249].Obtiene los patrones vasculares mediante un rayo infrarrojo cercano. Una de las ventajas respecto de otros sistemas es que no es necesario el contacto físico entre la persona y el escáner[250]. La imagen capturada de la mano mediante infrarrojos o cerca del infrarrojo se digitaliza y se extraen las regiones de interés; S. LAJEVARDI/ A. MEHDI/ ET ALT[251] emplean un algoritmo BGM (biometric graph matching) que sitúa las conexiones vasculares, las bifurcaciones y las terminaciones y da lugar a un patrón biométrico significativamente más pequeño que el resultante de métodos anteriores.

Entre enero y junio de 2011 Fujitsu puso en marcha un proyecto piloto en Boca Ciego High School en el sistema de pago en la cafetería. La tasa de éxito en el primer escaneado fue de un 98% y redujo de 15 a 7 minutos las colas en las horas punta. Entre otoño de 2011 y 2012 se puso en marcha un sistema similar en las escuelas de Pinellas County, con la intención de gestionar el cobro en las cafeterías de decenas de miles de estudiantes de enseñanzas medias y superiores. Según J. REGER once millones de personas utilizan cotidianamente este sistema de pago en el mundo[252]. Vñeanse las imágenes 84 y 85.

---

[246] AMBERG/FISCHER/ RÖßLER: *Biometrische Verfahren* (2003), p35-3; KALLIES, *Biometrische Erkennungssysteme*, 2007, p13; HWANSOO CHOI, A. „Back-fo-Hand Vascular Recognition," en LI (ed.) *Enciclopedia of Biometrics*, Springer, pp55-57.

[247] HWANSOO CHOI, A. „Back-fo-Hand Vascular Recognition," en LI (ed.) *Enciclopedia of Biometrics* ,p56.

[248] FACT, 2005, p42.

[249] FUJITSU LABORATORIES LIMITED (2011) Fujitsu PalmSecure selected as a "world changing idea" for2011 by scientific American magazine. http://www.fujitsu.com/us/services/biometrics/palmvein/SA_news.html.

[250] ZHANG, 2013, p13.

[251] "Hand vein authentication using biometric graph matching", *IET Biometrics*; 2014, Vol. 3 Issue 4, p302-313.

[252] FUJITSU: *The future of biometrics* – Dr Joseph Reger, en Future Banking.

5. SISTEMAS BIOMÉTRICOS CON BASE EN CARACTERÍSTICAS DINÁMICAS. (I) BIOMETRÍA DE LAS HABILIDADES MOTORAS.

Aunque en algunas obras se hace referencia a estos sistemas de reconocimiento como sistemas biométricos de segunda generación, sistemas activos o sistemas biométricos comportamentales, se ha explicado ya que en este trabajo se ha optado por emplear la expresión Biometrías dinámicas[253] para hacer referencia a: los métodos que captan información a partir de un conjunto de características biométricas que tienen la particularidad de que sólo pueden ser captadas mediante un seguimiento del cuerpo humano y su funcionamiento *a lo largo de un lapso de tiempo* más o menos amplio[254]. Es cierto que muchas de las tecnologías disponibles corresponden a la segunda generación de sistemas biométricos, y que varias de ellas requieren la colaboración activa de los sujetos fuente, pero también hay sistemas estáticos de segunda generación y Biometrías dinámicas que se captan sin la colaboración del sujeto.

Algunos autores, como G. SCHÜMACHER[255] advierten que a primera vista este tipo de informaciones parece ser menos sensible que la información que se obtiene de la Biometría tradicional (en referencia a la estática), pero profundizando en la naturaleza de los datos que se obtienen, pronto nos damos cuenta de que ello no es así. Sí que se diferencian de los sistemas de reconocimiento basados en Biometrías estáticas en el sentido de que se estiman menos susceptibles de falseamiento o suplantación (toda vez que los movimientos corporales que se registran son por lo general movimientos involuntarios). Pero no es cierto que la información que captan no sea sensible.

La tendencia a considerar que son menos sensibles o invaden en menor medida la intimidad de las personas nace, en buena medida, del hecho de que respecto de algunas características (como el movimiento del cuerpo en la marcha) no disponemos aún de sistemas que nos ofrezcan un nivel de precisión y fiabilidad equivalente al de una Biometría basada, por ejemplo, en el iris. Pero ha de notarse que, al margen de la capacidad para establecer la identidad con mayor o menor precisión, el nivel de intromisión de un sistema de reconocimiento en la intimidad de las personas ha de medirse también en relación con el tipo de información que colateralmente se puede llegar a obtener. Así, por seguir el ejemplo, si bien estimamos que puede haber una correlación entre determinada conformación del iris y algunos datos de salud, esa es una información que hoy día no se conoce, mientras que sí se dan por establecidas correlaciones entre algunos parámetros corporales, señales electrofisiológicas o comportamiento y la salud. De

---

[253] Véase la PARTE PRIMERA.

[254] Glossary of Terms for Voice Biometrics, Biometric Security Ltd. 2009. http://www.voicebiogroup.com/glossary.html.

[255] SCHÜMACHER, G. "Behavioural Biometrics, en *Second Generation*, 2013, p216.

hecho, algunos de los antecedentes de determinados sistemas de reconocimiento mediante Biometría dinámica son, precisamente, herramientas que en su día se desarrollaron para el diagnóstico de enfermedades. Así, el proyecto FIDIS recogió detalladamente la peculiaridad de los riesgos que plantean las tecnologías de reconocimiento mediante Biometrías dinámicas[256]: riesgos de que la información obtenida sea empleada para discriminar a las personas que, por ejemplo, puedan entenderse como "*personas con un perfil de riesgo*" de cara al acceso a determinados empleos ; riesgos de estigmatización para personas inocentes que puedan ser etiquetadas como terroristas potenciales[257]; y riesgo de que no se respete el derecho de las personas a no conocer la información relativa a su salud[258].

5.1. Biometría de la escritura

La escritura es internacionalmente reconocida como elemento que permite la identificación de las personas, especialmente la firma[259]. Tenemos noticia de que ya en la Antigüedad se empleaban sellos o cuñas en relieve, confeccionados en piedra o en metal, para personalizar la correspondencia y en la confección de documentos. Además de esa firma manuscrita, algunos países reconocen efectos jurídicos a la *firma digital*, realizada mediante mecanismos criptográficos[260]. ¿En que consisten los sistemas de identificación biométrica basados en la firma? Tradicionalmente las firmas nos han servido para identificar que un documento es (o no) autoría de una persona, algo que se realiza mediante un análisis visual entre la firma contenida en el documento y otra que podamos tener de muestra. Sólo un experto grafólogo, no obstante, es capaz de comprobar si la representación de los trazos en dos firmas aparentemente iguales es coincidente o no[261].

En sus modalidades antiguas, el análisis de la firma era un análisis dinámico, en el sentido de que observando el resultado de la firma los grafólogos establecían con más o menos aproximación cuál era el modo en que dicha firma se había realizado[262]. Ese tipo de sistemas, en versión automatizada, son conocidos como sistemas de reconocimiento de firma *off-line,* que obtienen

---

256 FIDIS PROJECT, Behavioural biometric profi ling and transparency enhancing tools, FIDIS Project (Future of Identity in the Information Society), 2009.

257 The Boston Globe:

258 SHERLOCK, R./ MORREY., J. D. *Ethical issues in biotechnology*, 2002, p44.

259 ZHANG, *3D Biometrics,* 2013, pp9-10.

260 PÜHRINGER, S.: *Biometrische Daten im Datenschutzrecht*, 2008, p4; BJÖRN, H., *Whitepaper biometrie*, p9-10; LANGENDERFER, J./ LINNHOFF, S."The Emergence of Biometrics", 2005, pp320.

261 POLEMI, D. *Biometric techniques: review*, 1997, pp74-75.

262 HEUMANN, B. *Whitepaper Biometrie*, 2006; BOLLE, R. M./ CONNEL, J. H/ ET ALTERE, *Guide To Biometrics*, Springer, New York, 2004; FICHES, M. "BioMetrics: The Future is Today", *Access Control & Security Systems*, 2003, pp20-26; BREITENSTEIN, "Überblik Über biometrische Verfahren", en NOLDE/ LEGER (ed.), *Biometrische Verfahren*, p35, 55.

toda la información interpretando las imágenes estáticas a las que ha dado lugar la firma. Pero existen también los sistemas *on*-line; es decir, sistemas en los que se registra todo el proceso de firmado, como es el caso del sistema con el que Berrin Yanikoglu y A. Kholmatov obtuvieron el primer premio en el Primer Concurso Internacional de Verificación Mediante Firma (SVC 2004)[263]. El sistema de Li/ Zhang (véase IMAGEN 51) extrae segmentos estables de las firmas, y a partir de ellos obtiene los atributos con los que configurará el patrón.

Es decir, que los sistemas biométricos contemporáneos no sólo atienden al resultado de la firma sino que son capaces de captar de forma secuencial el modo en que la persona realiza la firma. Existen sistemas en los que el dispositivo de captación es el bolígrafo y otros en los que la captación se realiza desde la tableta o el soporte en el que se firma (o con una combinación de ambas fuentes de información)[264]. Muchos son los parámetros que pueden tenerse en cuenta, como por ejemplo: el tiempo de realización de la firma, las medidas de determinados puntos, la fuerza, los trazos, los toques sucesivos de la superficie de la escritura, el ángulo que se forma entre la tableta y el bolígrafo que firma.

5.2. Biometría de las pulsaciones en teclado

Entre las líneas de investigación y desarrollo abiertas han de mencionarse también los sistemas que tratan de captar digitalmente la singularidad del movimiento del cuerpo humano al escribir en un teclado (*Keystroke scanning*)[265]. Los usuarios de los teclados de ordenador desarrollan patrones de tecleado específicos, que se diferencian en el ritmo, en la precisión, en la velocidad[266], así como en el tiempo en que cada tecla es presionada de forma individual o, por ejemplo, cuando ha de combinarse con otra (como la presión conjunta de una tecla con mayúsculas, *alt* o *ctrl* o combinaciones de letras que habitualmente van seguidas[267]), y en muchas otras características[268].

Los sistemas en desarrollo se concentran en aquellos rasgos especialmente característicos que, a su vez, pueden ser objeto de captación mediante estudios mensurativos. No obstante, entre sus debilidades está el hecho de que importantes aspectos de la forma de teclear resultan más fáciles

---

263 ZHANG, 3D, p10.

264 POLEMI, D. *Biometric techniques: review*, 1997, p27.

265 BARTMANN, D. "PSYLOCK - Identifikation eines Tastaturbenutzers durch Analyse des Tippverhaltens"; LANGENDERFER, J./ LINNHOFF, S. "The Emergence of Biometrics and Its Effect on Consumers", 2005, pp320.

266 DUNSTONE, T./ YAGER, N. *Biometric Systems and Data Analysis*., 2009,pp67-68.

267 En español, por ejemplo: qu, mp, mb, o la articulación de las tíldes.

268 ITU-T, *Biometrics and Standards,* 2009, p5.

de falsear que otros rasgos[269]. En principio se trata de sistemas que requieren un equipamiento mínimo (un teclado y un sistema de registro), pero las complicaciones comienzan cuando se trata de establecer al modo en que las características captadas serán escogidas como atributos a partir de los cuáles construir patrones fiables. Uno de los sistemas desarrollados es el Psylock (Universidad de Regensburg, Alemania).

La fiabilidad de estos sistemas depende de muchos factores. Cuanto más largo es el texto que las personas deben teclear, más información se obtiene; pero la fórmula de captación debe tener en cuenta que el cansancio o la distracción pueden afectar de forma importante al ritmo de tecleado[270]. El desarrollo de estos sistemas, con todo, no está pensado tanto para identificaciones puntuales como en relación con aquellos casos en los que ha personas que están manejando un teclado dentro de un espacio necesitado de seguridad y se desea monitorizar su identidad de forma[271].

5.3. Biometría del movimiento labial

El movimiento labial comenzó a abordarse en las tecnologías de reconocimiento biométrico como un complemento de la Biometría vocal, en la que existe una correlación estadística entre determinados tipos de señales de audio y la vocalización, (o en estudios que tratan de comprender el modo en que el cerebro humano es capaz de interpretar lo que una persona dice aún sin emitir sonidos). Sin embargo, existen también investigaciones que tratan de determinar la identidad de las personas a partir del movimiento de los labios, con el objetivo de ser empleados en tecnologías multimodales.

Universitat d'Alacant
Universidad de Alicante

5.4. Biometría de la marcha (movimiento del cuerpo al caminar)

La marcha humana viene siendo objeto de estudio desde hace décadas en campos como la biomecánica la medicina física o la psicofísica[272] con el objetivo de detectar patologías de la marcha, rehabilitar a las personas o mejorar su rendimiento deportivo e incluso de cara al diseño del equipamiento de determinados puestos de trabajo. Las trayectorias de determinados puntos

---

[269] LANGENDERFER, J./ LINNHOFF, S. "The Emergence of Biometrics and Its Effect on Consumers", 2005,pp322; US GAO, *Using Biometrics for Border Security*, 2002, p50; TEIXEIRA, T./ JUNG, D./ DUBLON, G./ SAVVIDES, A. *PEM-ID: Identifying People by Gait-Matching using Cameras and Wearable Accelerometers*, 2009, p.3.

[270] BARTMANN, D. "On the design of an authentication system based on keystroke dynamics using a predefined input text", *International Journal of Information Security and Privacy*, 2006.

[271] ISO/IEC: *Information technology – Biometrics tutorial. ISO/IEC TR 24741:2007(E)*. 2007.

[272] JOHANSSON, G. "Visual motion perception", *Scientific American*, 1975, pp75-88; LUTTGENS, K./ WELLS, K. *Kinesiology: Scientific Basis of Human Motion*, 1982; MURRAY, M. "Gait as Total pattern of movement," *American Journal of Physical Medicine*, vol. 46, nº,1, 1967, pp290-332.

del cuerpo, la frecuencia y las fases de los movimientos o las trayectorias son algunas de las fuentes de información que se manejan. Vease la IMAGEN 51b.

Al caminar las diferentes partes del cuerpo (piernas, rodillas, brazos, codos) tienen un patrón de movimiento que puede captarse incluso a distancia[273] y G. JOHANSSON impulsó en 1975 una investigación que trataba de determinar el modo en que las personas somos capaces de reconocer a otras por la forma de caminar. Utilizaba como referencia el movimiento de unos indicadores de luz adheridos al cuerpo de las personas a identificar (*Moving Light Displays*) y se estudiaron las tasas de acierto en el reconocimiento del género[274] y en el reconocimiento de amigos[275]. En aquel caso se trataba de determinar qué es lo que el cerebro humano percibe en el movimiento de alguien y le permite reconocer a esa persona, si la estructura del movimiento –en su conjunto- o el patrón de movimiento de determinadas partes del cuerpo. Pero existen, asimismo, modalidades biométricas recientes que persiguen la identificación de las personas por su marcha[276]. Una aplicación eficiente de este tipo ofrecería la posibilidad de una identificación de personas en secuencias de video grabadas por las cámaras de video-vigilancia en casos en que la resolución no fuera lo suficientemente buena como para aplicar, por ejemplo, un reconocimiento facial.

5.5. Biometría vocal

Merece también atención la Biometría vocal. Las características que permiten discriminar la voz tienen una doble base, fisiológica y comportamental, pero se considera una característica biométrica dinámica porque para su captación es imprescindible un lapso de tiempo[277]. La voz de una persona cambia con el estado de ánimo, con el tipo de conversación o incluso con la edad, pero hay una serie de tonos que son distintivos durante toda su vida[278]. Un analizador de voz adecuado, puede reconocer con exactitud estos sonidos[279]. En la articulación y control de la voz tienen incidencia el diseño del tracto vocal de cada individuo (cavidad faríngea, cavidad oral y

---

[273] LU, J./ ZHANG, E, "Gait recognition for human identification based on ICA and fuzzy SVM through multiple views fusion", *Pattern Recognition Letters* 28 (2007), 2401-2411; *Second Generation Biometrics*, 2012, pp9.

[274] BARKLAY, C./ CUTTING, J./ KUZLOZSKI, L. "Temporal and Spatial Factors in Gait Perception that influence Gender Recogniton", *Perception and Psychophysics*, vol. 23, n2, pp145-152 (1978).

[275] CUTTING, J./ KOZLOWKI, L. "Recognizing Friends by their Walk: Gait Perception without Familiarity Cues", *Bulletin Psychodinamic Soc*, vol 9. Nº 5, pp3535-356, 1977.

[276] VIELHAUER, C.: *Biometric User Authentication for IT Security*, 2006, p47-48.

[277] BARBU, T. "Comparing various voice recognition techniques", *IEEE proceedings of the5th conference on speech technology and human-computer dialogue*, 2009, pp 1–6; RASHID, R.A. "Security system using biometric technology: design and implementation of voice recognition system (VRS)", *IEEE Int Conf Comput Commun Eng* 2008, pp898–902.

[278] DE DIEGO DÍAZ, L. A. *Identificación fotográfica y reconocimiento en rueda del inculpado*, 2003, p215.

[279] FACT, 2005, p40.

cavidad nasal), así como la forma en que se produce el movimiento de la boca[280], mandíbulas, lengua, faringe y laringe. Todas esas características pueden un impacto en los patrones acústicos con los que la voz se expresa, y en ellos tienen su base los sistemas que verifican la identidad de las personas mediante la Biometría vocal[281].

En los años 60 comenzaron a vislumbrarse los primeros sistemas de verificación e identificación automatizados gracias al desarrollo de técnicas de elaboración de los patrones de reconocimiento, las propuestas de métodos estadísticos y la exploración de sistemas de selección de los atributos[282]. En la década de los 90 la tecnología TESPAR (Time Encoded Signal Processing and Recognition) era capaz de analizar las instantáneas de una curva de sonido respecto del tiempo y calculaba frecuencias, aunque bastante lejos del rendimiento que ya en aquellas fechas tenía la identificación mediante la Biometría de las impresiones dactilares[283].

El hecho de que desde hace años los ordenadores personales y otros dispositivos electrónicos hayan incorporado dispositivos de captación de la voz –de mayor o menor calidad – fue visto como una oportunidad para el desarrollo de estos sistemas, aunque los retos siguen estando en lo que se refiere a la formulación de sistemas de selección de atributos característicos y en su posterior conversión en patrones biométricos almacenables con garantías de buen rendimiento en las comparaciones a futuro[284], [285]. Desde hace décadas el análisis del llanto y su vocalización ha sido empleado como apoyo en el diagnóstico de determinadas patologías –entre ellas el daño cerebral- en los neonatos[286]. Con un sistema de reconocimiento similar a los del reconocimiento de identidad mediante la voz, el objetivo de los sistemas computerizados es el de captar patrones que permitan detectar patologías[287].

Universitat d'Alacant
Universidad de Alicante

---

280 JONIETZ, E., "Boosting Biometrics", *Technology Review*, 107 (5), 2004, pp20-21

281 PRABHAAKAR, S./ PANKANTI, S./ JAIN, A. K. "Biometric Recognition: Security and Privacy Concerns", *IEEE SECURITY & PRIVACY*, 2003, p32-33.

282 GISH, H. "Elements of Speaker Verification", en WAYMAN, J./ET ALT *Biometric System*, 2005, p125-126.

283 POLEMI, D., *Report* 1997, p26.

284 PIECHULECK, A. "Empfehlung für Unternehmen", *Workshhop IT-Sicherheitsmanagement*, 2008, p8-9; PÜHRINGER, S.: *Biometrische Daten im Datenschutzrecht*, 2008, p6-7.

285 VIELHAUER, C.: *Biometric User Authentication for IT Security*, 2006, p40-41.

286 Ya en la década de los 60, KARELITZ, S./ FISICHELLI, V. R: "The cry thresholds of normal infants and those with brain damage", *J. Pediat*, 61, 1962, 679-685; PARMELEE, A. H.: "Infant crying and neurologic diagnosis", *J. Pediat*, 1962, 801-802; WASZ-HÖCKERT, O./ LIND, J./VUORENKOSKI, V./ PARTANEN, T./ VALANNE, E.: "The infant cry a spectrographic and auditory analysis", *Clinics in Devel Medicine*, 29, 1968.

287 REYES GARCÍA, C. A./ REYES-GALAVIZ, O. F./ ET ALT, "Soft Computing Approaches to the Problem of Infant Cry Classification with Diagnostic Purposes", en P. MELIN/ J. KACOZRZYK/ W. PEDRYCZ (eds.), *Soft Computing for Recognition Based on Biometrics*, Springer, 2010, pp3-10.

Más que captar *lo que el usuario dice* -algo que hacen las tecnologías de transcripción o dispositivos automatizados que funcionan por órdenes dadas con la voz (reconocimiento vocal)-, las tecnologías biométricas basadas en la voz captan una serie de rasgos de *la forma en que una persona habla*[288]. El analizador de voz convierte una frase hablada a un formato digital y permite extraer las características distintivas de una voz (tono, cadencia, etc.).A partir de ahí es posible establecer el patrón que corresponde a un hablante. Esa sería su huella de voz o *voiceprint*[289].

La literatura distingue entre métodos dependientes e independientes de un texto[290]. Los textos dependientes del texto discriminan la voz por determinadas particularidades en el modo en que las personas emiten determinadas palabras, números o frases, mientras que en aquellos casos en que el sistema no depende de un texto el patrón de la voz se ha creado con independencia de la forma de las palabras o los nombres que el hablante ha emitido. Se han desarrollado sistemas para controlar viviendas inteligentes y dar en ellas órdenes para encender luces, bajar persianas, etc.[291] y sistemas que tienen su aplicación en las comunicaciones telefónicas de la banca o el comercio a distancia[292].

5.6. Biometría de los patrones del comportamiento

Este tipo de Biometrías persigue perfilar –e incluso llegar a singularizar- a las personas sobre la base de predecir sus acciones y comportamientos[293]. A día de hoy los sistemas de reconocimiento con base en este tipo de Biometrías están aún en fase de desarrollo y más que un objetivo de singularizar a los individuos persiguen detectar, en masas de personas, comportamientos que pueden resultar predictivos de algún riesgo para la colectividad. Dos proyectos destacados en la investigación de su potencial son el proyecto FAST (Future Attribute Screening Technology) del Departamento de Interior de los EEUU (DHS – Departament of Homeland Security) y el proyecto europeo ADABTS (Automatic Detection of Abnormal Behaviour and Threats in crowded spaces)[294]. Véase la imagen 53. Ni siquiera los documentos de identidad *mejorados* con Biometrías estáticas robustas pueden prevenir de las "malas intenciones" y ello

---

[288] EISENBERG, A.: "Is That You, Son? Voice Authentication Trips Up the Experts", *New York Times*, 13 de noviembre de 2003; ROCKWELL, M.: "Can Voice Recognition Answer the Call?", *Wireless Week*, 10 (10), 2004, págs 21-23.

[289] SHONIREGUN, C./ CROSIER, S.: *Securing Biometrics Applications*, 2007, p12.

[290] COLE R.A./MARIANI, J./ USZKORET, H./ ZAENEN, A./ ZUE, A. *Survey of the state of the art in human language technology*, Cambridge University Press, 1997; SAMMUT, C./ SQUIRES, B. "Automatic speaker recognition: anapplication of machine learning", en *Proceeding of the 12th international conference on machine learning*,1995.

[291] BAYGIN, M. "Real time voice recognition based smart home application", *IEEE 20th,* 2012, pp 1–4.

[292] YANG, W. "Application of voice recognition for mobile E-commerce security", *IEEE 3rd Pacific-Asia,* 2011, pp 1–4.

[293] MCCARTHY, P. *Biometric Technologies*, cit, 2012.

[294] SUTROP, M./ LASS-MIKKO, L. "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics", *Review of Policy Research*, vol 29, nº 1, 2012, pp21 y ss.

llevó a las instituciones a interesarse por sistemas de reconocimiento que pudieran identificar no ya tanto a una persona (en el sentido de captar *quién es*), sino una serie de atributos conscientes o inconscientes en los que de algún modo pretende verse *qué tipo de persona se es*[295], permitiendo aplicar clasificaciones social basadas en esa categorización[296].

El referente de estas Biometrías son informaciones que en la biomedicina se emplean para detectar anomalías en la fisiología o en los procesos perceptivos, motores, emocionales o cognitivos[297]. Sobre la base de que el cuerpo reacciona de forma involuntaria y en ello pueden revelarse nuestras emociones[298] –y según algunos expertos, incluso las intenciones-, se buscan parámetros de comportamiento en los que poder captar métricamente la expresión de dichas intenciones[299]. Ni siquiera las personas entrenadas son capaces de controlar algunas de sus reacciones porque incluso una ausencia total de señales puede llevar a sospechar de la persona[300].

FAST (2008) es un proyecto que concentra su atención en la mejora de los procesos de cribado de las personas que utilizan los transportes o transitan por una serie de puntos de control que se consideran críticos. El objetivo es detectar comportamientos que aporten a los controladores informaciones adicionales sobre las personas, en el sentido de informaciones que permitan identificar y validar indicadores de malas intenciones[301]. Sobre la base de esa detección se desarrollaron unos prototipos de sensor que fueron testados en grupos de voluntarios[302]. La fiabilidad del sistema, en septiembre de 2009, se fijó en un 89%, lo cuál dejaba un espacio excesivo como para causar falsas alarmas en países que, como es el caso de los miembros de la UE, ven cruzar anualmente sus fronteras a cientos de millones de personas[303].

Universitat d'Alacant
Universidad de Alicante

El proyecto ADABTS, por su parte, concentró su atención en grandes aglomeraciones de gente, escogiendo, en concreto, tres escenarios para los estudios piloto: los aeropuertos, los estadios de

---

295 European Network and Information Security Agency, ENISA Briefing: Behavioral Biomettrics, 2010, en en www.enisa,europa.eu.

296 LYON, D. "Surveillance as social sorting: computer codes and mobile bodies", en *Surveillance as social sorting: privacy, risk and automated discrimination*, Routledge, 2003, pp13-31.

297 ACTIBIO (sin indicación de fecha), *Unobstrusive authentication using activity related and soft biometrics*..

298POLZEHL, T./ SCHMITT, A./ METZE, F./ ET ALT, "Anger recognition in speech using acoustic and linguistic cues", *Speech Communication*, 2011; DHALL, A./ R GOECKE, R./ ET ALT, "Emotion Recognition in the will challenge," *Proceedings of the 15th ACM on International conference on multimodal interaction*, 2013, pp509-516.

299 THORPE, J./ VAN OORSCHOT, P.C./ SOMAYAJI, A. "Pass-thoughts: authenticating with our minds", *Proceedings of the 2005 Workshop on New Security Paradigms*, doi.acm.org/10-1145/1146269.1146282:14

300 CHERRY, S./ CORLEY, A. M. "Loser: Bad vibes", *IEEE Spectrum*, enero de 2010.

301 ROSENBLATT, *Brain-fingerprinting technologies*, CCN 2008.

302 MESSMER, E. "Can behavioral biometrics help detect terrorists entering the US?", *Networked World*, 22 de sept de 2010, en www.networkedworld.com.

303 SUTROP, M./ LASS-MIKKO, K., pp28-29,

fútbol y los centros de las grandes ciudades. Se analizaban tres grandes grupos de comportamiento: comportamiento terrorista; comportamientos de las masas de personas; y comportamientos de individuos o pequeños grupos de individuo. El proyecto buscaba elementos, atributos que pudieran llevar a detectar los comportamientos diana (p.ej anomalías[304], comportamientos infrecuentes; infracciones; comportamientos sorpresa) y situar aquellos que pudieran considerarse como típicos del estrés, el cansancio o determinados estados de ánimo. Por razones de seguridad no se han hecho públicas todas las conclusiones de este proyecto.

En comparación con otras Biometrías estáticas y dinámicas, las Biometrías del comportamiento –salvedad de aquellas que algunos autores sitúan en el siguiente grupo que se analizará- pueden ser captadas a distancia, sin conocimiento de las personas. Tratando de expresar la ventaja potencial, algunas voces indican que se los sistemas de reconocimiento basados en ellas no hacen que las personas pierdan el tiempo y que, además, no se molestará a los *no sospechosos*. El hecho de que, además, las personas estén actuando en un espacio público, en el que por lo general pueden ser vistas por otros, hace que en muchos ordenamientos jurídicos no sea imprescindible el consentimiento y queden bajo lo que a grandes rasgos establece la normativa sobre video-vigilancia. Pero difícilmente puede obviarse la complejidad y la trascendencia de atribuir a las personas *intenciones* antes de que actúen, máxime cuando las base científica que sostiene tales atribuciones tiene tal margen de incertidumbre. ¿Cómo diseñamos, esto es, qué criterios le damos a un sistema para que interprete la identidad moral de alguien y prediga su comportamiento?[305].

SUTROP/ LASS-MIKKO advierten que sobre la base de informaciones predictivas, con márgenes de fiabilidad por determinar, un sistema de estas características colocaría a algunas de las personas que transitan en el espacio público etiquetas como terrorista, criminal, poco fiable o, al menos, sospechoso[306]. Ha detenerse, además, cierta cautela ante el riesgo de que resurjan –con otros perfiles- explicaciones biológicas del comportamiento humano (en especial de la criminalidad) que en el pasado llevaron a prácticas sociales que hoy día resultarían de todo punto inaceptables.

5.7. Biometría de las señales electrofisiológicas y parámetros corporales.

Muchos de los sistemas biométricos que van a presentarse a continuación se han desarrollado en paralelo o como consecuencia de sistemas biométricos creados con fines de

---

[304] Correr en contra de la muchedumbre o emplear una salida de emergencia sin necesidad, por ejemplo.

[305] MANDERS-HUITS/ VAN DER HAREN, "Moral identification in identity management systems", en IFIP – International Federation for Information Processing, *The Future of Identity in the Information Society*, 262, 2009, pp77-91.

[306] SUTROP, M./ LASS-MIKKO, K., p32.

diagnóstico biomédico. En el campo de la biomedicina la conjunción entre la biología, la medicina, la computación y la bioestadística está propiciando un cada vez mayor uso de los datos de los atributos personales obtenidos en imágenes, señales y otras fuentes. Dichos datos contribuyen de forma significativa a mejorar la detección precoz de las patologías y a realizar seguimientos más exhaustivos de los pacientes que están recibiendo distintas tipos de terapias. Los mismos dispositivos de captación de señales electrofisiológicas y otros parámetros son empleados para captar muestras biométricas con el objetivo de obtener atributos o conjuntos de atributos con los que generar patrones biométricos permanentes y singularizantes.

Las bioseñales o señales fisiológicas se originan como cambios electroquímicos en las neuronas, músculos o glándulas y pueden ser detectadas en la superficie de la piel mediante la colocación de electrodos en determinados puntos del cuerpo[307]. La electrofisiología estudia estas señales a diferentes escalas[308]. La actividad de los músculos puede registrarse mediante electromiogramas, la del corazón mediante electrocardiogramas, el funcionamiento cerebral mediante los encefalogramas o sistemas que captan la actividad electrodérmica en glándulas sudoríparas. Se estima que tienen potencial para singularizar a una persona y que es potencialmente posible generar perfiles personales a partir de ellos (vid. MARCEL/MILLÁN 2007 [309]; MOHAMMADI/ ET ALT. 2006 [310]; PARANJAPE/ ET ALT. 2001 [311]; POULOS/ ET ALT. 1998, 1999, 2001, 2002[312]; RIERA /ET ALT. 2008 [313]; BIEL/ ET ALT. 2001 [314]; CHANG 2005 [315]; ISRAEL ET ALT. 2005 [316] ; KYOSO 2001 [317] ; PALANIAPPAN/KRISHNAN 2004 [318]).

Universitat d'Alacant
Universidad de Alicante

---

[307] VAN DEN BROEK, E.L. "Beyond Biometrics", *Procedia Computer Science* 1, 2010, 2511–2519, p2513.

[308] RIERA, A./ DUNNE, S./ ET ALT., "Electrophysiological Biometrics: Opportunities and Risks", en *Second Generation Biometrics*, p154.

[309] MARCEL, S., / MILLÁN., J."Person authentication using brainwaves", *IEEE Transactions on Pattern Analysis* 2007.

[310] MOHAMMADI, G.,/ET ALT. "Person identification by using AR model for EEG signal", *Proceedings of 9th International Conference on Bioengineering Technology*, 2002.

[311] PARANJAPE, R./ET ALT. 2001. "The electroencephalogram as a biometric", *Proceeding of the Canadian Conference on Electrical and Computer Engineering*, 2001.

[312] POULOS, M./ET ALT. "Person identification via the EEG using computational geometry algorithms", en *Proceedings of the Ninth European Signal Processing*, 1998, 2125–2128; POULOS, M./ET ALT. "Parametric person identification from EEG using computational geometry", en *Proceedings of the 6th International Conference on Electron, Circuits and System*, 1999; POULOS, M./ET ALT. "On the use of EEG features towards person identification via neural networks", *Médical Informatics & the Internet in Medicine*, 2001; POULOS, M./ET ALT. "Person identification from the EEG using nonlinear signal classification", *Methods of Information in Medicine* 2002, 41: 64–75.

[313] RIERA, A./ ET ALT. "Unobtrusive biometric system based on electroencephalogram analysis", *Hindawi Journal of Advances in Signal Processing* 2008; RIERA, A./ ET ALT. "STARFAST: A wireless wearable EEG/ECG biometric system based on the ENOBIO sensor", *Proceedings of the 5th International Workshop on Wearable Micro and Nanosystems for Personalised Health*, 2008.

[314] BIEL, L./ ET ALT. "ECG analysis: A new approach in human identification", *IEEE Transactions on Instrumentation and Measurement* 2001, 50: 808–812.

[315] CHANG, C. *Human identification using one lead ECG*, 2005.

[316] ISRAEL, S./ ET ALT. "ECG to identify individuals", *Pattern Recognition*, 2005.

Partiendo del número de neuronas (10^11) y de sus conexiones (10^15), Riera et alt. afirman que es improbable hallar dos cerebros iguales[319]. Existen además investigaciones que tratan de hallar los potenciales asociados a determinados eventos (Event-Related Potentials), mediante la vinculación entre las medidas que se obtienen en los encefalogramas y determinadas estimulaciones; al asociar componentes individuales de esos ERP se abre la vía para determinar estados cognitivos en los sujetos atendiendo únicamente a su corporeidad[320]. Pero el estado del arte no está en estos momentos cerca de ofrecer un sistema comercial de reconocimiento de estas características[321].

De hecho, más que como base para sistemas biométricos unimodales, estas características son estudiadas como posible complemento en sistemas multimodales, en tanto aumentan el conjunto de información disponible sobre una persona[322]. Algunos ejemplos que hemos hallado en la literatura: electromiogramas de la voz que procesan no el sonido sino la forma de emisión de la voz y podrían ser usados potencialmente en entornos de comunicación muy ruidosos (como zonas de combate)[323], y sistemas de reconocimiento de la escritura manual que captan no el movimiento corporal sino el electromiograma de los músculos que participan en la escritura[324]. También existe una tecnología de firma biométrica (*IDesia*) que procede al reconocimiento de identidad de una persona capturando señales electro-fisiológicas que son únicas para cada persona[325]. Funciona simplemente realizando dos contactos con los dedos y no requiere una posición o condición especial en los dedos.

Universitat d'Alacant
Universidad de Alicante

---

317 Kyoso, M. "Development of an ECG identifi cation system", *Proceedings of 23rd Annual International IEEE Conference of Engineering in Medicine and Biology Society*, 2001, 4: 3721–3723.

318 PALANIAPPAN, R./ KRISHNAN, S. M. "Identifying individuals using ECG beats", en *Proceedings of the International Conference Signal Processing Communication*, 2004, 569–572.

319 RIERA, A./ DUNNE, S./ CESTER, I./ RUFFINI, G. "Electrophysiological Biometrics: Opportunities and Risks", en Mordini/ Tzovaras (eds,), *Second Generation*, p154.

320 ARMSTRONG, B. C./ M. V. RUIZ-BLONDET, M. V./ ET ALT, "Brainpint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics", *Neurocomputing*, 166 (2015), pp59-67.

321 BELGACEM, N./ FOURINIER, R./ NATT-ALI, A./ BEREKSI-REGUIG, F. "A novel biometric authentication approach using ECG and EMG signals", *Journal of Medical Engineering & Technology*, 2015, 226-238.

322 AILISTO, H./ VILDJIOUNAITE, E./ LINDHOLM, M./ ET ALT, 'Soft biometrics-combining body weight and fat measurements with fingerprint biometrics', *Pattern Recognition Letters* 2006, pp. 325–334

323 DENBY, B./ SCHULTZ, T./ HONDA, K./ ET ALT, "Silent speech interfaces", Speech Communication 2010l, pp270–287; JORGENSEN, C./ S. DUSAN, S. "Speech interfaces based upon surface electromyography", *Speech Communication,* 2010, p354–366.

324 VAN DER PLOEG, I. *Beyond Biometrics*, cit.

325 HUIJGENS, R. en EUROPEAN COMMISSION (ed), *Biometrics in Europe. Trend Report*, UNISYS – European Biometrics Portal, 2007, pp20-21.

Algunos de los dispositivos de reconocimiento mediante Biometría dinámica que están en investigación presentan como aspecto interesante el poder monitorizar de forma prolongada la presencia de una persona en un espacio continuo. Esto es, más allá del control de acceso con Biometría estáticas, hacer un seguimiento de su presencia y monitorizar, entre otros, el cansancio o el estado de ánimo, y la presencia de parámetros inusuales que puedan ser motivo de alerta. No parece, sin embargo, que pueda pensarse en este tipo de dispositivos para el gran público.

He aquí algunas claves sobre las ventajas y desventajas que se discuten sobre la hipótesis de futuras aplicaciones. Entre las ventajas comparativas se ha dicho que mientras las Biometrías tradicionales pueden manipularse, las Biometrías dinámicas no pueden enmascararse. Si se consiguiera desarrollar sensores no invasivos (que no requirieran contacto)[326] o al menos sensores inalámbricos, podrían tener muchas aplicaciones[327]. Además, combinadas con otras Biometrías –se ha dicho ya- aumentarían el conjunto de información que se tiene sobre el cuerpo de una persona, pudiendo ayudar bien como *soft biometrics* –acelerando el proceso de búsqueda de comparaciones- o reforzando la fiabilidad de otros sistemas.

No se pierden de vista, sin embargo, los puntos débiles de estas tecnologías de reconocimiento tanto desde la perspectiva de su fiabilidad y aplicabilidad, aún por demostrar, como en lo que se refiere a los aspectos éticos y sociales relativos a su uso para la identificación de las personas. A estos últimos nos referiremos más adelante, en el capítulo segundo, junto con cuestiones de la misma naturaleza que plantean el resto de sistemas de reconocimiento biométrico. En lo que se refiere a la base científica de los sistemas de reconocimiento mediante Biometría dinámica ha de tenerse en cuenta que elementos clave en el desarrollo de estos sistemas, especialmente en lo que se refiere a la definición de la muestra biométrica y a la captura de atributos singularizantes, necesitan aún mucha investigación científica básica[328]; y se necesitan asimismo sistemas para depurar el ruido de las bioseñales[329] e interpretarlas. En lo que se refiere ya a la arquitectura de los sistemas los sensores necesitan acomodarse a otros entornos; existen dispositivos como el ENOBIO –de captación de la actividad cerebral- y versiones similares de pulsera, pero sin un claro

---

326 FRADEN, J. *Handbook of Modern Sensors: Physics, Designs, and Applications*, 2004; OUWERKERK, M./ PASVEER, F./ LANGEREIS, G. "Unobtrusive Sensing of Psychophysiological Parameters: Some Examples of Non-Invasive Sensing Technologies", *Philips Research Book Series*, 2008, pp. 163–193.

327 VAN DEN BROEK, E. L./ WESTERINK, J. H. D. M. "Considerations for emotion-aware consumer products", *Applied Ergonomics* 2009, pp1055–1064.; JORGENSEN, C./ S. DUSAN, S. "Speech interfaces based upon surface electromyography", *Speech Communication,* 2010, p354–366.

328 FRADEN, J. *Handbook of Modern Sensors: Physics, Designs, and Applications*, 2004; OUWERKERK, M./ PASVEER, F./ LANGEREIS, G. "Unobtrusive Sensing of Psychophysiological Parameters: Some Examples of Non-Invasive Sensing Technologies", *Philips Research Book Series*, 2008, pp. 163–193; HAO, Y./ FOSTER, R. "Wireless body sensor networks for health-monitoring applications", *Physiological Measurement* 2008, ppR27–R56.

329 VAN DEN BROEK, E. L./ WESTERINK, J. H. D. M. "Considerations for emotion-aware consumer products", *Applied Ergonomics*, 2009, 1055–1064; VAN DEN BROEK, E. L./ SCHUT, M. H./ WESTERINK, J. H. D. M./ TUINENBREIJER, K. "Unobtrusive Sensing of Emotions (USE)", Journal of Ambient Intelligence, 2009, 287–299

desarrollo hacia su utilización con fines de reconocimiento de las personas (en el sentido de individualización). Véase la IMAGEN 52.

6. FORTALEZAS Y SISTEMAS DE LOS SISTEMAS BIOMÉTRICOS, ATENDIENDO A LAS CARACTERÍSTICAS QUE LES SIRVEN DE BASE PARA EL RECONOCIMIENTO Y AL ESTADO DEL ARTE DE LOS MÉTODOS CON QUE SE CAPTAN

No hay unanimidad en la literatura a la hora de valorar hasta qué punto cada una de las características biométricas descritas reúne las cualidades que, en el epígrafe segundo de este capítulo, se han descrito como requisitos para poder emplearlas como base de un sistema de reconocimiento. No habiendo aún sistemas basados en el ADN –que hipotéticamente ofrecerían un mayor rendimiento en términos de universalidad, singularidad y permanencia- se advierte que todos los sistemas de reconocimiento biométrico tienen limitaciones. No existe una Biometría que pueda señalarse como mejor en términos absolutos[330]. Según el uso que se quiera dar al sistema de reconocimiento y en relación con un concreto escenario operativo, *se dará por bueno* un determinado grado de equilibrio entre la satisfacción de las diferentes cualidades. Sobre esa premisa, y dejando para capítulos posteriores la consideración de los sistemas y de los escenarios operativos, van a ofrecerse aquí algunas reflexiones desde la comparativa de las características en su conjunto. Para la realización de esta comparativa se han tenido en cuenta, entre otras cosas, las valoraciones de varios autores[331] y algunos estudios en los que se procede a comparar el nivel de rendimiento de varias características.

6.1. Valoración de las características biométricas desde la perspectiva de las *cualidades* necesarias para servir de base a un sistema de reconocimiento mediante biometría.

Como se ha explicado ya en el apartado 1.2.1 de este capítulo, la universalidad, la singularidad y la permanencia son tres cualidades a valorar a la hora de escoger una característica biométrica de referencia para un sistema de reconocimiento. A grandes rasgos, y sin perjuicio de algunas apreciaciones que se harán en el próximo capítulo desde la perspectiva ya del concreto funcionamiento de los sistemas, vamos a proceder a recoger una serie de reflexiones sobre el conjunto de las características empleando la referencia de las citadas cualidades.

[330] CHIN/ ET ALTERE, 2009, p24.

[331] Se han tenido en cuenta: las conclusiones del test SANDIA, publicado por NEWMAN, E. *The Biometrics Report*, SBJ Services, UK, 1995; las publicadas por Despina POLEMI en su informe de 1997; la comparativa de Jain, A. K./ et alt, *Introduction*; el documento elaborado por encargo de la OCDE en 2003, el informe IPTS de 2005 así como las reflexiones y tablas comparativas publicadas por varios autores en sus trabajos monográficos (vid. las notas al pie de aquí en adelante).

6.1.1 Universalidad

De las Biometrías estáticas, el rostro y el iris se consideran más universales que, por ejemplo, las Biometrías dactilares o las que tienen que ver con las manos o las orejas. JAIN ET ALT (2004) consideran que dedos y manos se ven afectadas como consecuencia de determinadas actividades laborales o la enfermedad, aunque no hemos encontrado ninguna tasa que refleja porcentualmente esa diferencia.

Estos autores, como sucede en buena parte de la literatura, no tienen en cuenta la Biometría del ADN por estimar –como hemos explicado- que el estado actual de la ciencia y la tecnología no puede ofrecer aún un sistema de reconocimiento automatizado basado en él. De las Biometrías dinámicas, la captación métrica de las señales y parámetros corporales son las más universales, y aunque no hemos encontrado estudios que aporten datos a este respecto, es previsible que diferentes factores –como la enfermedad o la discapacidad- afecten y reduzcan la universalidad de característica que tienen que ver con los movimientos corporales voluntarios (la marcha, la escritura, la emisión de la voz, etc).

6.1.2. Potencial singularizante

Las huellas dactilares y palmares son, junto con el iris, las características biométricas que se estima pueden ofrecer mejor servicio en términos de unicidad. JAIN ET ALT. (2004) advierten, con todo, que aunque la geometría manual no resulta tan distintiva, si puede servir de base a sistemas en los que el número de usuarios no es muy elevado.

Universitat d'Alacant
Universidad de Alicante

El potencial singularizante de las tecnologías de reconocimiento dinámico es, signifircativamente, interior al de las Biometrías estáticas (vid. IMAGEN 54). A fecha de hoy no hay ninguna tecnología de reconocimiento dinámico que supere en este potencia a las tecnologías de reconocimiento mediante Biometrías estáticas. Desde el punto de vista de su riesgo para la privacidad de las personas, sin embargo, algunas tecnologías de reconocimiento mediante biometías dinámicas se consideran más invasivas (captación de señales corporales, y programas que mediante entornos gráficos sencillos permiten la interacción entre personas y ordenadores - GIU, Graphical User Interface)

6.1.3 Estabilidad de los rasgos o características

El iris y las huellas dactilares son señaladas por los expertos como características más persistentes, aunque existen otros rasgos que sin ser *permanentes* sí ofrecen una *estabilidad razonable*. Por ejemplo la oreja, aunque está expuesta a posibles alteraciones ocasionadas por la

decoración, las enfermedades[332] o la cirugía[333]), con lo cual la permanencia de estos rasgos como soporte para sistemas a largo plazo no parece estar garantizada[334].

En el caso de otros rasgos, como el rostro, captar el potencial singularizante y al tiempo garantizar la permanencia requiere, entre otras cosas gestionar adecuadamente la variabilidad intrapersonal que implican los cambios de expresión[335]. Mucho menos estables son las Biometrías dinámicas (que captan, entre otras, información de las habilidades motoras o la fisiología de las personas), aunque como contrapartida ofrecen información que tiene más potencialidad que la de servir, en sentido estricto, al reconocimiento de la identidad de las personas.

6.1.4 Colectividad y accesibilidad, y resistencia al fraude

El iris destaca por sus altas tasas de universalidad –mayores que las de las huellas, aunque menores que las del rostro-, su elevado poder singularizante y su permanencia respecto de otros datos biométricos[336], pero no resulta fácil de captar. A la hora de diseñar sistemas biométricos basados en rasgos del iris algunas de sus características resultan desventajosas[337]. Comenzando ya por la captura misma, el reconocimiento mediante el iris es altamente complejo. Como ya hemos dicho su pequeño tamaño dificulta su adquisición a ciertas distancias, y la imagen del iris suele verse con frecuencia afectada por diferentes factores.

Los patrones biométricos obtenidos de las huellas necesitan muy poco espacio digital para su almacenamiento. Además, los dispositivos de captación son relativamente fáciles de usar (sólo requieren colocar el dedo sobre un escáner), y la proporción entre el precio de los escáneres y la calidad de reconocimiento que ofrecen es alta[338]; quizá por ello, son una de las tecnologías más

Universitat d'Alacant
Universidad de Alicante

---

332 Procesos primarios locales (como infecciones o tumores), así como enfermedades sistémicas (depósitos tofáceos en el oido) o el surco en el lóbulo de la oreja característico de la cardiopatía isquémica; vid, sobre esto último A. S. DHARAO/ M. THAN: "Five anthroposcopic traits of the ear in a Malaysian population", *Antropol Anz* 1995, 53 (4), pp359-363; BUCHACA FAXAS, E./ VÁZQUEZ VIGOA,. A./ TORUNCHA CHUCKRAM, A./ RODRÍGUEZ VALDÉS, R./ SEIJAS FARIÑAS, H. "Surco en lóbulo de la oreja y cardiopatía isquémica", *Revista Cubana de Medicina, 1995 (5), 31 (1).*

333 Cirugía destinada a modificar estéticamente la forma del pabellón auricular, así como la que se realiza debido a la etiología de tumores en la piel (carcinomas o melanomas), implantes cocleares, etc.

334 ALTMANN, F. "Malformations of the auricle and external auditory meatus", *Arch Otorynology* 1951, 54, pp115-139; BURGE/ BURGER, "Ear Biometrics", en JAIN, A.K./ BOLLE, R./ PANKANTI, S. (eds.), *Biometrics. Personal identification*, 2002, pp273-285.

335 PATO, J./ MILLET, L. (eds), *Biometric Recognition: Challenges and Opportunities*, 2010, 3.

336 WAYMANN, J. L. "Technical testing and evaluation of biometric identification devices", en *Biometrics Personal Identification in a Networked Society*, 1999, pp343-368; PANKANTI/ ET ALT. 2000; JAIN/ PANKANTI 2001; JAIN, A. K./ ET ALT. 2004; DAUGMAN, J. 1993; DAUGMAN, J. 2003; Zhang/ et alt, *3D Biometrics*, 2013, pp10-11; IPTS, p.142.

337 MURON, A./ POSPISIL, J., "The human iris structure and its usages", *Physica*, 2000, 39:89-95.

338 BROWNSTEIN, R. "E-Commerce", *Electronic Design*, 52 (13), 2004, pp75-76; OLLE, RUUD M./ CONNEL, JONATHAN H./ RATHA, Nalimi. "Biometric perils and patches", *Pattern Recognition* 35 (2002) 2727 – 2738.

extendidas[339]. También se considera que obtienen un buen resultado en las evaluaciones que tienen como referencia las cualidades requeridas a los sistemas de identificación biométrica. Existen Biometrías más singularizantes (como la del iris) o más universales (como la Biometría facial o la del ADN), pero es una Biometría cuya singularidad es bastante fácil de capturar y ofrece buenos rendimientos[340].

Conforme al actual estado de la tecnología, el reconocimiento por medio de la geometría del rostro se considera algo menos preciso que el reconocimiento mediante huellas dactilares[341], porque los rostros son complejos, multidimensionales y capaces de variar de forma notable en las expresiones, pero tiene como principales ventajas que económicamente es la menos costosa[342], resulta menos invasiva que la toma de huellas y que, al no requerir contacto físico, se evita el riesgo de contagio de enfermedades microbianas[343]. Además, su uso es relativamente sencillo y no requiere excesivo control del ambiente. Resultan, además, más económicos que los dispositivos que captan las huellas dactilares[344].

6.1.5. Difusión, madurez tecnológica y aceptabilidad social

Las tecnologías dactilares y las del iris son las que a día de hoy se emplean en los sistemas biométricos con mayor número de usuarios[345]. El sistema EURODAC de apoyo a los visados tenía hasta 2014 una media de doscientos mil enrolamientos al año (fechas aportadas antes de la crisis de los desplazados de Siria, en el verano de 2015), a los que se suman los millones de huellas recabadas en las bases de datos policiales norteamericanas, o los cientos de miles enrolados en los sistemas de ayudas sociales de diversos estados norteamericanos entre otros. El *Aadhaar*, por su parte, que combina las huellas dactilares y la geometría del iris, ambiciona con enrolar a todas las personas (cientos de millones) que habitan en la India, sean o no nacionales de este país.

Las tecnologías que implican contacto físico son vistas como problemáticas por las posibilidades de contagio, por los problemas de mantenimiento de la calidad de las capturas y por la incomodidad o rechazo que pueden generar en algunas personas (grupos culturales o

---

339 LANGENDERFER, J./ LINNHOFF, "The Emergence of Biometrics", 2005, pp. 317-318.

340 IPTS, p136.

341 BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, *BioFAce*, 2006, p9-10.

342 ZHANG/ ET ALT, *3D Biometrics*, Springer 2013, pp10-11

343 HEUMANN, B. *Whitepaper Biometrie*, www.biometrie-online.de, 2006, p9-10.

344 Biometric Comparison Chart, SJI, National Centre for State Court, USA (2002); WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-Based Technologies*, 2003.

345 *Ashbourn Guide to Biometrics for a Large-Scale Systems*, 2012.

religiosos)[346]. Esto ultimo sucede también en algunos casos con las fotografías, aunque en buena parte de los países occidentales los ciudadanos están acostumbrados a colocar fotografías en todo tipo de tarjetas de identificación[347]. En los casos en que el uso de los dispositivos ha de ser frecuente la preocupación (fundada o no) en los posibles riesgos derivados del uso tiende a registrar un rechazo importante de las Biometrías oculares (en especial las que captan los patrones vasculares de la retina).Desde el punto de vista de la privacidad la toma de huellas o el reconocimiento facial, incluso la geometría del rostro, resultan menos intrusivos que la captación de otras Biometrías, como la del iris o la de la retina -que además requieren un alto nivel de colaboración[348]. Y es que suele ser necesario que el sujeto dirija su pupila hacia un punto concreto[349], aunque se han desarrollado también métodos de captación a distancia o sin cooperación específica del sujeto[350].

6.2. Tabla comparativa de fortalezas y debilidades de los sistemas (valoración relativa, desde la perspectiva de la característica que emplean como referencia).

Fortalezas y debilidades de los sistemas biométricos, atendiendo a las características que les sirven de base para el reconocimiento		
Base del sistema	Fortalezas	Debilidades
Huellas dactilares	Es una de las características biométricas más empleadas en el mundo (y con mayor diversidad de fines). Se pueden enrolar varios dedos de una misma persona, y eso aumenta la fiabilidad. Necesita muy poco espacio de almacenamiento. Numerosa tecnología disponible y a muchos precios. Hoy por hoy, en términos comparativos, no es cara. El rasgo tiene un elevado nivel de permanencia en el tiempo.	Posibilidad de hacer *Dummy fingers* (solucionable con un test de vitalidad). Cada huella se estima diferente al 100% pero el patrón no tiene por que ser único. La posibilidad de falsos positivos es remota, muy reducida también la de falsos negativos. Sí es posible, no obstante que haya gemelos biométricos. Necesita un sistema óptico cualificado, que responde mal a la suciedad, al envejecimiento, a la sequedad de la piel. Necesario el contacto físico, es algo más intrusivo que otras técnicas biométricas. No disponible en las personas que tienen afectada la piel de los dedos o en ausencia de éstos. Algunos ciudadanos las perciben negativamente por asociar su uso con las investigaciones criminales y forenses. Se le asocia un cierto estigma.

346 Por ejemplo, a las personas de cultura japonesa no les gusta colocar las manos donde otros colocaron antes las suyas (POLEMI, 1997, cit. p25)

347SHONIREGUN, C./ CROSIER, S.: *Securing Biometrics Applications*, 2007, p14-15; ELLERBROK, A., "Playful biometrics: Controversial Technology through the Lens of Play", The Sociological Quarterly 52, 2011, pp528-547, p529.

348 RENGAMANI, H./ KIMARAGURU, P./ CHARAKRABOIL,R./ RAGHAU RAO, R. "The Unique Identification Number Project", en KUMAR, A./ ZHANG, D. (ed.), *Ethics and policy of Biometrics*, 2010, pp146, ss., pp150-151.

349 KINDT, E. 2013, p27.

350 MALEY, J. R./ NARODITSKY, O./ HANNA, K./ ET ALT, "Iris on the move", *Proceedings of the IEEE*, 2006, pp1936-1947.

Biometrías de la mano	El potencial singularizante de la Biometría manual o de la Biometría de los patrones venosos se estima medio, y las tecnologías no son muy costosas. Puede operar en ambientes muy diversos y muchos dispositivos no requieren contacto físico. No se percibe como una tecnología invasiva y los usuarios no necesitan adiestramiento. En algunas cafeterías escolares de Reino Unido y los Estados Unidos de América se usa con buen rendimiento en niños.	En la identificación 1:1 tiene menos posibilidades, porque la mano no es excesivamente rica en datos biométricos singularizantes. Las lesiones en la mano, los cambios producidos por la edad, enfermedades como la artritis o el envejecimiento reducen la fiabilidad. Es muy difícil un falso positivo (aceptar a un impostor), aunque el riesgo de un falso negativo (rechazo de un usuario legítimo) no es tan difícil. Algunos autores reseñan que su diseño puede ser complicado para determinadas poblaciones
Geometría del rostro	Alta tasa de universalidad. Es un sistema poco invasivo y relativamente aceptado por la mayoría de los ciudadanos (con la excepción de algunos grupos culturales o religiosos). Puede pasar desapercibido cuando no se necesita una gran resolución o cuando se dispone de tecnología muy avanzada, capaz de captar las imágenes de los sujetos a distancia y en entornos no controlados. Los dispositivos no son caros (cámaras digitales), Es una de las pocas tecnologías que (junto con el reconocimiento por la forma de caminar) puede emplearse a distancia, por ejemplo en el cribado biométrico	En los sistemas más básicos es necesario que el sujeto coopere manteniendo el rostro en la misma posición mientras es escaneado (no así en los avanzados). En algunos sistemas la iluminación o los gestos, el peinado, las gafas y otros elementos pueden contribuir a una mayor tasa de error (fundamentalmente falsos negativos). Existen, con todo, tecnologías recientes que superan buena parte de esos inconvenientes. Entre gemelos es difícil distinguir y es más fácil de falsear que otros sistemas (mediante postizos etc).
Patrón del iris y de la retina	Alta tasa de universalidad. En el caso del iris, el rasgo captado tiene un elevado nivel de singularidad y permanencia. En el caso de la retina los niveles son algo menores.	Poca aceptación por parte de los ciudadanos en los casos en que ha de hacerse un uso frecuente del sistema de reconocimiento (piénsese, por ejemplo, en el control cotidiano del acceso al puesto de trabajo). Son sistemas económicamente costosos. En el caso de las tecnologías biométricas con base en patrones de la retina, el hecho de que se empleen sistemas de infrarrojos (o cercano al infrarrojo) es visto como peligroso; por otra parte, la enfermedad y determinadas circunstancias ambientales afectan de forma notable a la estabilidad de estos patrones.
Reconocimiento vocal	Se estima no invasivo. Hardware asequible y muy extendido (micrófonos) No es intrusivo y tiene un elevado nivel de aceptación (se usan hoy día sistemas automatizados que emplean la voz, aunque la identificación es por palabras clave y no de reconocimiento por patrones). Fácil manejo por los usuarios.	El ruido ambiental afecta seriamente al sistema Algunos tipos de patrones ocupan mucho espacio, entre 5 y 10 veces superior a un patrón de huella digital. Se necesita mucho espacio de almacenamiento. Con relativa facilidad puede verse afectado por circunstancias externas (un catarro común, la gripe o afonía, condiciones ambientales) o el estado de ánimo[351]. Su potencial singularizante es menor que el de

[351] MASTALI, N. "Authentication of subjects and devices using biometrics ", *IEEE 5th international conference on broadband and biomedical communications*, 2010, pp 1–6

		otras Biometrías.
Reconocimiento por firma dinámica	Potencial de identificación muy limitado (aunque el rendimiento en verificación se considera suficiente).	La tasa de error es elevada. Muy sencillo el falso negativo (que el usuario legítimo no consiga reproducir la firma con exactitud), algo menor la tasa de falsos positivos Lesiones en la mano, cansancio, etc. pueden influir en la firma y los usuarios cambian con relativa facilidad su tipo de firma, algo que reduce la fiabilidad de estos sistemas.
Reconocimiento mediante tecleado	Hay muy pocos datos, finalidad de verificación. Esta tecnología requiere aún desarrollo.	La tasa de error es elevadísima, sobre todo la de falsos negativos. El cansancio, la enfermedad, las lesiones en la mano, influyen en la forma de teclear.
Reconocimiento por patrones de ADN	Elevadísimo potencial de verificación y de identificación. De cribado, incluso, al permitir localizar a una persona mediante sus parientes biológicos. La tasa de error se estima ínfima.	A día de hoy no existen sistemas totalmente automatizados basados en la Biometría del ADN. La percepción ciudadana es muy negativa y, de hecho, la legislación vigente en muchos países limita este tipo de reconocimiento a las investigaciones criminales y a las de paternidad.
Reconocimiento mediante Biometrías dinámicas	Se consideran más difíciles de falsear que muchas Biometrías estáticas, toda vez que no son alterables ni pueden simularse voluntariamente por las personas.	El perfilado que ofrecen se asocia más a grupos de personas (potencialidad de cribado) que a la singularización de individuos. La captación de estos datos se estima preocupante desde la perspectiva ética, en tanto pueden ofrecer detalles de la persona que afecten a su reputación o a sus relaciones personales.

Universitat d'Alacant
Universidad de Alicante

Universitat d'Alacant
Universidad de Alicante

Capítulo 2

Funcionamiento, utilidades y limitaciones de los sistemas de identificación biométrica. Los riesgos y su tratamiento

1. LAS UTILIDADES SOCIALES QUE OFRECE EL RECONOCIMIENTO MEDIANTE BIOMETRÍA: VERIFICACIÓN, IDENTIFICACIÓN EN SENTIDO ESTRICTO Y CRIBADOS BIOMÉTRICOS.

1.1 Introducción a los usos de los sistemas de reconocimiento mediante biometría

Describiendo a grandes rasgos el conjunto, puede decirse que los sistemas que emplean las sociedades contemporáneas para identificar a las personas tienen su base, fundamentalmente, en: 1) algo que la persona sabe (una información secreta, una contraseña, un PIN); 2) algo que la persona posee extrínsecamente (un objeto, una tarjeta o carnet, un documento); o 3) algo que la persona posee intrínsecamente y que le caracteriza (alguna marca corporal especial o elementos que describen su corporeidad)[1]. Los sistemas de reconocimiento mediante Biometría pertenecen al tercero de los conjuntos. A través de características que son captadas en el cuerpo de una persona[2] se procede a reconocer la identidad de una persona; a establecer *que una persona es ella misma … y no otra*; que es *una persona en particular*[3].

Universitat d'Alacant
Universidad de Alicante

Aunque se profundizará en ello en el siguiente capítulo, los ejemplos que han sido ofrecidos hasta el momento ya permiten entrever que desde el punto de vista operativo las finalidades con que pueden aplicarse las tecnologías de reconocimiento mediante Biometría son tan diversas como las tecnologías en sí. El análisis operativo requerirá, por ello, situar las aplicaciones biométricas en diferentes países y entornos. Pero, antes de entrar en dicho análisis, los resultados de esta investigación nos han permitido concluir que desde el punto de vista técnico es posible realizar una explicación detallada de los usos o utilidades del reconocimiento biométrico y del modo en que los sistemas funcionan, señalando además las limitaciones científico-técnicas y las cuestiones ético-sociales que plantean.

---

[1] JAIN ET ALTERE, *Introduction to Biometrics*, 2011, p2.
[2] BSI, *Biometrie*, Berlin, 2005, p1.
[3] CLARKE, R. "Human Identification", ITP 1994/7, p7-8.

En este primer apartado vamos a describir las utilidades que ofrecen los sistemas de reconocimiento mediante biometría. Estas utilidades, en esencia, puede categorizarse en tres grandes grupos[4]: utilidades de verificación (o comprobación de la identidad alegada) ; utilidades de identificación en sentido estricto (o de determinación de la identidad sin alegación previa de ésta); y utilidades de *cribado biométrico* o de búsqueda y localización de personas.

1.2. Sistemas de verificación: *¿soy quien digo ser?*

1.2.1 Verificación o comprobación de la identidad alegada

Algunos sistemas de reconocimiento mediante Biometría comprueban que la identidad alegada por una persona coincide con la identidad que, asociada a su biometría, ha almacenado un sistema. El hecho de permitir que el sujeto *alegue una identidad* –mediante una información que aporta o un objeto que porta, por ejemplo una tarjeta inteligente- hace que la comparación entre patrones sea mucho más ágil. Una persona alega que, por ejemplo, es la usuaria número X de una biblioteca municipal y el sistema busca en su unidad de almacenamiento la Biometría que fue almacenada para dicho número de usuario. A continuación la compara con los datos en fresco que la persona está mostrando a su dispositivo de captación.

No es relevante el modo en que la persona alega su identidad; puede ser introduciendo mi nombre, alegando una clave o mostrando un carnet o una tarjeta inteligente. Vénse las IMÁGENES 74 y 75.3. Quien adquiere una tarjeta de abono se beneficia normalmente de descuentos respecto al precio que le supondría pagar una entrada completa por cada día de acceso; lo mismo sucede con las tarjetas que se han expedido a un usuario al que su edad, una minusvalía o la pertenencia a una familia numerosa le permiten acceder al servicio de forma más ventajosa. Estos descuentos pretenden fidelizar a los clientes o reconocer la situación de desventaja social y económica de algunos colectivos, animándoles a sacar un abono; el riesgo está, como es sabido, en que personas diferentes a aquellas para las que se expiden estos títulos hagan uso fraudulenta de ellos. Grabar una huella dactilar asociada a un número de abono o a un PIN que se teclea, permite a quien ofrece el servicio proceder a comprobar si quien desea acceder con la ventaja de un abono es la misma persona que se enroló. Otro uso interesante para los dispositivos de este tipo es el de su instalación en teléfonos móviles, PDAs u ordenadores portátiles (en la imagen un USB con escáner dactilar), para garantizar a su propietario mayor seguridad en caso de sustracción o pérdida. Como puede verse, lo característico de estos sistemas es que al alegar una identidad concreta, el sistema busca en su unidad de almacenamiento el patrón que fue almacenado como asociado a dicha identidad y realiza una comparación *1 a 1* entre dicho patrón y el patrón que se muestra en

[4] WAYMAN, J. / JAIN, A. K. / MAIO, D. "An Introduction", 2005, pp4-5.

fresco. Así por ejemplo, en el acceso a la zona de máxima seguridad de un aeropuerto se puede exigir no sólo la presentación de una tarjeta personal, sino que los empleados con derecho a acceso coloquen su huella dactilar[5]. O, como sucede en algunos centros deportivos, puede que los usuarios introduzcan un código numérico o PIN y después coloquen su huella dactilar en un lector.

De esta forma se evitan tanto el falseamiento de identidades, como que un usuario emplee varias identidades o que un usuario no enrolado acceda usurpando la identidad de otro. No debe confundirse esta *utilidad* de verificación que ofrecen algunos sistemas, con la *finalidad concreta* con la que un sistema de estas características es implementado en un escenario operativo en concreto. La verificación puede emplearse con fines muy diversos, que van desde la alta seguridad en instalaciones militares o en altas operaciones financieras, hasta usos más triviales como impedir la picaresca de clientes o usuarios que tratan de beneficiarse de forma abusiva de abonos o ventajas que ofrecen con carácter personal (en el acceso a parques temáticos y zoológicos, en establecimientos para la práctica deportiva, por ejemplo). Aún y cuando en estos últimos casos los gestores del sistema puedan alegar *un objetivo de evitar pérdidas económicas,* lo cierto es que, como veremos, se discute hasta que punto la pérdida económica que supone la picaresca en el uso de un abono justifica la intromisión que, respecto a todos los usuarios, implica el establecimiento de un sistema de verificación biométrica.

Universitat d'Alacant
Universidad de Alicante

1.2.2. *¿Ofrece la verificación, información adicional?*

Con frecuencia se da a entender que la verificación biométrica nos permite saber "*que un individuo es quien dice ser*". Pero, ¿en qué sentido llega a determinarse que es "quien dice ser"? La persona no necesariamente ha tenido que enrolar elementos de su identidad civil. Es posible que, por ejemplo, haya sido enrolada específicamente para un entorno (en el que es empleado o empleada de determinada categoría, o cliente, y con derecho de acceso a determinados recintos virtuales o físicos y no a otros); también es posible que haya sido enrolada como persona que es titular legitima de una tarjeta de crédito o de un pasaporte. Pero la verificación, en puridad, únicamente nos confirma que la persona para la cuál se creó el pasaporte o la tarjeta de crédito, la persona que ha sido registrada como cliente o empleado de tal categoría, es la misma que tenemos ahora mismo ante el dispositivo de escaneado. Si el sistema enroló indebidamente a alguien –

[5] IPTS, *Biometrics at the Frontiers*, 2005, pp46 y ss; A. BIASOTTI, *Le tecnologie*, cit., p30 y ss; G. Preite, *Il riconoscimento biometrico. Sicurezza versus privacy*, Ed Uni Service, Trento, 07, pp 47 yss; GARANTE, *Linee guida per le tecnologie biometriche*, 8 de octubre de 2004, pp13 y ss

porque en el momento de expedirle el pasaporte consiguió hacerse pasar por quien no era-, el sistema de verificación no tiene capacidad alguna de responder ante ese hecho.

En cuanto a la posibilidad de ofrecernos más información, no debemos olvidarnos de que se trata de un sistema informático. En un interrogatorio ante el juez es posible que un ser humano, testigo de un crimen, pueda de pronto recordar información que no haya sido tenido en cuenta en la investigación criminal; pero un sistema informático sólo *recuerda* aquello que hemos almacenado en él. Quiere esto decir que si más allá de la información mínima que necesita el sistema (esto es, el patrón almacenado más la clave para su activación) hemos almacenado alguna otra información adicional (o, por ejemplo, hemos previsto que se registren los datos de cada ocasión en la que el individuo accede al sistema), dicha información reaparecerá al alegar la identidad. Y si no se ha producido tal almacenamiento, pues no habrá más información.

En el caso del *Pasaporte Biométrico Europeo*, IMAGEN 74,el chip con dispositivo de radiofrecuencia que lleva incrustado el documento, sirve para comprobar que su portador es la persona a la que legítimamente se le expidió. Los datos biométricos incorporados al mismo tienen, pues, como finalidad la de verificar la autenticidad del pasaporte, y el Reglamento CE 2252/ 2004 establece una serie de requisitos técnicos destinados a garantizar la integridad, la autenticidad y la confidencialidad de ésos y otros datos que almacena. Ninguna autoridad europea puede almacenar la información que está recogida en el CHIP en sus bases de datos; la normativa lo prohíbe. Aunque el control de fronteras sí permite registrar en las bases de datos de los sistemas aduaneros que la persona titular del pasaporte cruzó determinada frontera tal día y a tal hora.

Universitat d'Alacant
Universidad de Alicante

También en un sistema de control de acceso horario de los trabajadores, se produce de forma asociada un almacenamiento de datos como las fechas, y las horas exactas de entrada y salida, aunque dicho almacenamiento no tiene porqué operar ya con datos biométricos[6]. La persona de recursos humanos que tiene acceso a las tablas de control horario no necesita conocer los patrones biométricos; si tras verificar la identidad, el sistema abre la ficha del trabajador –ya con su nombre y apellidos- puede registrar asociado a estos datos el acceso o la salida de que se trate, de forma totalmente disociada al sistema de almacenamiento de los patrones biométricos. La misma filosofía persigue la propuesta de un *European Entry/Exit System and Registered Traveller*

[6] OCDE – WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, Biometric-based Technologies, cit, pp16-17; Consejo de Europa – Comité del Convenio 108, Progress Report on the Application of the principles of the Convention 108, cit., cap II.

Programme for non-EU citizens[7], que almacena información asociada a la entrada o salida, o el padrón electoral biométrico de la República de Bolivia[8] que tiene como fin último garantizar que sólo se emite un voto por persona y que quien acude a emitir sufragio es la persona legitimada para ello.

1.2.3 *La toma de decisiones y los tipos de error que pueden generarse*

Las decisiones finales que toman estos sistemas de verificación no son, propiamente, de determinación de la identidad de una persona. Lo que hacen, tras la comparación 1 a 1, es decidir si se acepta o no como igual el patrón almacenado y el nuevo patrón obtenido del dato en fresco. Los errores que pueden producirse en esta toma de decisiones son los de falsa aceptación (por considerar erróneamente que la persona que se enroló y la que aporta el dato en fresco son la misma) o falso rechazo (por considerar erróneamente que quien aporta el dato en fresco no es igual a la persona que se enroló).

1.3. Sistemas de identificación: *¿quién soy?*

1.3.1. *Identificar, en sentido estricto*

Un segundo tipo de servicio de reconocimiento mediante Biometría es el de determinación de la identidad de las personas en sentido estricto. Estos sistemas, con base en la información almacenada, tratan de determinar *quién es* una persona. Captada su información biométrica, ésta se compara con los patrones de todas las personas que fueron enroladas en búsqueda de coincidencias (*1* a *n*). El objetivo puede ser el de una identificación positiva (es decir, deseamos saber quién es 1 dentro de ese *grupo n*), pero también existen sistemas que ofrecen una identidad negativa. Esto es, contribuyen a determinar que *1* no pertenece a ese *grupo n*. Esta utilidad tiene interés, por ejemplo, cuando se desea determinar que 1 no está entre las personas que ya han solicitado asilo previamente en otro país (como hace el sistema EURODAC), o que no es una persona a la que por determinado motivo se le denegó ya el asilo o a la que no se le puede reconocer éste.

La identificación negativa también resulta de utilidad para controlar el acceso a lugares que son *sólo para miembros*, y que permiten en acceso sin necesidad de una alegación puntual; o en sistemas en los que se ha establecido un reconocimiento biométrico como parte del ejercicio del

[7] ISARIS, N. Deputy Head of Unit, DG Home Affairs, Unit C3 – Large-scale IT Systems and Biometrics en European Commission (ed.), "Biometrics in EU border controls: The move towards smarter borders", *Biometrics Conference*, 2012.
[8] Ley nº 4021 del Régimen Electoral Transitorio de la República de Bolivia, de 2009. Vid. CNE – Corte Nacional Electoral, *¿Qué es el Padrón Electoral Biométrico?* Documento de Información Pública, nº 1, La Paz, junio de 2009.

derecho de admisión. Así, por ejemplo, en los casinos y salas de juego de algunos países, en cadenas de clubes nocturnos o en el control de los ultras violentos en los estadios de futbol se están extendiendo sistemas que pretenden impedir la entrada a individuos con antecedentes criminales o de mal comportamiento, así como a personas que voluntariamente (por problemas, por ejemplo de ludopatía) han solicitado que se les deniegue tal acceso. En esos casos el sistema de identificación persigue que quien desea acceder demuestre que *no pertenece al conjunto de las personas declaradas "non grata".*

También es posible que el resultado de la identificación lleve a situar al sujeto en una categoría. Por ejemplo, que de cara a la adquisición de alimentos y bebidas en la cafetería de un hospital se distinga entre pacientes, personal sanitario y/o visitas (con objetivos tan diversos como aplicar distintos precios o impedir que los pacientes consuman alimentos que no están indicados para ellos) o que dentro de un recinto escolar o de una prisión se distingan también por categorías a las personas, gestionando con base en ello su acceso a diferentes espacios de los edificios.

En este caso la forma en la que el sistema informático activa la búsqueda en su unidad de almacenamiento no parte de una identidad alegada, sino de alguna peculiaridad que capta como clave en el patrón que se le muestra en fresco. De algún modo habremos ordenado o categorizado los patrones almacenados, enseñando al sistema a buscar similaridades hasta determinar, tras una comparación con todos los patrones almacenados, si existe o no una coincidencia entre el patrón en fresco y alguno de los patrones almacenados. Si el sistema confirma un match (o hallazgo de coincidencia), esa decisión nos dará acceso a la información –más o menos amplia- que hallamos almacenado como asociada al patrón biométrico de que se trate. Esta forma de proceder no dista en exceso de la que realizaba BERTILLON, cuando comparaba los datos recogidos de un sospechoso detenido, con la información recogida en sus fichas, o con el modo en que operaban y operan los sistemas manuales de reconocimiento dactilar. En esos casos, dado que el orden alfabético de nada servía en supuestos en que el sospechoso se negaba a identificarse o trataba de falsear su identidad, la clave de búsqueda de las fichas policiales se hacía sobre la base de un estudio comparativo de los patrones biométricos almacenados. La mayor diferencia entre aquellos sistemas y los sistemas automatizados que se emplean en la actualidad es la precisión y la velocidad con la que las tecnologías son capaces de comparar los patrones biométricos. Así, y conforme a los datos que periódicamente publica, se calcula que el FBI consulta en sus bases de datos aproximadamente 50.000 patrones de huellas dactilares al día.

1.3.2. Complejidad

En comparación con los sistemas de verificación, los de identificación resultan mucho más complejos. No se realiza una comparación *1 a 1*, sino que, como se ha dicho, el sistema está organizado de tal forma que compara el patrón en fresco con todos los almacenados (1 a n). La clave o claves de organización del sistema y de su funcionamiento posterior tienen una gran trascendencia, sobre todo en los casos en los que el número de patrones almacenados (*n)* es muy elevado –sistemas a gran escala o, como se dice del *Aardhaar* de india "extremely large-scale", con una población destinataria de 1200 millones de personas-. En el Aardhaar la identificación se emplea en el enrolamiento, como test de independencia, para evitar que se enrolen dos o más identidades con base patrones biométricos iguales; esta circunstancia, se ha dicho ya en el capítulo anterior, puede producirse porque alguien intenta enrolarse falsamente (con dos o más identidades), pero también porque a partir de muestras biométricas distintas –de sujetos fuente distintos- la reducción de potencial singularizante que implican el hecho de escoger sólo algunos atributos y elaborar con ellos el patrón haya tenido como consecuencia la aparición de *gemelos biométricos*.

También es una base de datos de identificación a gran escala la de EURODAC[9]; esta base de datos central informatizada fue creada en la UE para comparar informáticamente las huellas de los solicitantes de asilo para evitar lo que se conoce como "asylum shopping". En su base se almacenan las huellas de todos los solicitantes de asilo mayores de 14 años, con independencia del país en el que hayan solicitado el asilo, así como de todas aquellas personas que hubieran sido detenidas por tratar de cruzar ilegalmente las fronteras de la UE o por permanecer irregularmente en un Estado miembro de la Unión. Además de las huellas, se almacenan otros datos como el país de la UE por el que accedieron, su sexo, lugar y fecha en que fueron interceptados o solicitaron el asilo, pero no datos como nombre, apellidos o país del que son originarios[10]. Al introducir una nueva Biometría dactilar, EURODAC procede a compararla con todas las almacenadas y nos indica si la persona está o no enrolada y, en el caso de que lo esté, cuál es la información que se tiene de ella. Son datos que se conservan por un período de 10 años, a menos que la persona obtenga el asilo o un permiso de residencia en la Unión.

Existen, con todo, sistemas de identificación que tienen como destinatarios grupos poblacionales más pequeños. Así, los programas de viajeros registrados tanto en los Estados Unidos como en los aeropuertos internacionales de Schiphol, Heathrow o Frankfurt[11]. En estos casos, la Biometría de

[9] Entró en funcionamiento en 2003, con base en el Reglamento CE 2752/ 2000, en aplicación del Convenio de Dublín de 11 de diciembre de 2000, completado el 28 de febrero de 2002.
[10] AUS, J. P. "Eurodac: A Solution Looking for a Problem?", *European Integration online Papers*, 2006; BROUWER, E. R.: "Eurodac: Its Limitations and Templations", en *European Journal of Migration and Law*, vol, 4. pp. 231-247.
[11] Vid WHITE, C. "The TSA Registered Traveler Program", *Biometrics Consortium Conference*,, 2006; M. ROTENBERG, "Database Regulation Key to ID cards and Biometrics. Panel Says", *Washington Internet Daily*, oct 23, 2001, p.3.

su iris (acompañada o no de algún otro elemento identificativos[12]) les permite un embarque ágil, para lo cual es imprescindible que el sistema asocie sus datos biométricos con los datos concretos del viaje que tienen previsto realizar en cada ocasión.

1.3.3 La toma de decisiones y los errores que pueden producirse

En los sistemas de identificación puede producirse un hallazgo de coincidencia o *match* erróneo, esto es, cabe la posibilidad de que se asocie erróneamente un dato en fresco a un patrón ya almacenado (y, por consiguiente, a toda la información vinculada a este patrón), o cabe la posibilidad de que el sistema concluya erróneamente que el sujeto captado no está entre aquellos que han sido enrolados en el sistema, no reconociendo, por tanto, su identidad.

1.4. Sistemas de cribado biométrico: *se busca*

1.4.1 *Sistemas open set y sistemas closed set de verificación e identificación, y sistemas de cribado*

Tanto los sistemas de verificación como los de identificación pueden emplearse open o closed set; esto es, cabe la posibilidad de que todos los usuarios o candidatos al reconocimiento hayan sido previamente enrolados (closed-set) o que, sin embargo, existan usuarios que el sistema no conoce (open-set). Uno de los entornos operativos más claros para un sistema que funciona *closed-set* es el de las prisiones. En un sistema de reconocimiento biométrico implantado en una prisión se enrolará potencialmente a todas las personas que acceden a ella, sean reclusos, personal o visitas. Es posible que dicho sistema ofrezca, cuando sea necesario, la opción de identificación, pero también que –por ejemplo en el control de los accesos a las distintas zonas del recinto- simplemente verifique la pertenencia de un usuario a una determinada categoría, y con base en ello decida si la persona de que se trate está o no autorizada para entrar o salir de la zona correspondiente. En otros casos, sin embargo, es posible que el sistema tenga que enfrentarse con cierta frecuencia a la presencia de usuarios o candidatos no enrolados previamente.

El cribado biométrico, implica –como todo cribado- un proceso de selección rigurosa. En el fondo, se trata de una utilidad más cercana a la identificación que a la verificación, toda vez que no hay personas que alegan identidades a comprobar, sino una necesidad de comprobar patrones en fresco con patrones almacenados. ¿Por qué se subraya la idea de selección rigurosa o tamizaje? Porque la utilidad de cribado, que por lo general opera open-set, implica que el sistema se enfrentará a un número bastante amplio de sujetos no enrolados (es decir, sujetos en cuyos datos en fresco *no hallará ninguna coincidencia* o match). En algunos casos resulta difícil distinguir

[12] El RT INTEROPERABILITY CONSORTIUM (RTIC) se creó en 2005, su TSA *Registered Traveler Program* emplea smart cards y biometría.

entre sistemas de identificación negativos (en los que se persigue determinar que la persona a la que se va a dar acceso no está *entre las personas non grata*, por ejemplo) y sistemas de cribado; por ejemplo, si en la entrada de un estadio de futbol situamos un lector de huellas para acceder a las gradas de los ultra y el objetivo es que no entren personas *a las que se ha prohibido la entrada en el recinto*, ¿estamos ante un sistema de identificación o ante un sistema de cribado? Realmente ambos consisten en lo mismo: en la comparación de patrones. Si porcentualmente el número de personas que serán chequeadas es muy superior al número de hallazgos potenciales, nuestro sistema de identificación probablemente sea clasificado en la literatura como sistema de *screening*, pero la utilidad que ofrecen es prácticamente la misma.

Lo que se espera de un sistema de cribado es, en el fondo, muy similar al sistema que mediante recompensa ha existido históricamente en el rastreo de personas (y aún existe). "*Se busca a Percy LeFroy Mapleton, acusado de homicidio, se recompensará a quien contribuya a su detención con 200 libras esterlinas*". Así rezaba el primer cartel de "se busca" publicado en el Reino Unido por el Director de Investigación Criminal de Scotland Yard (1881). A un dibujo realizado a mano –IMAGEN 56- - se acompañaba una detallada descripción física del que entonces se conocía como "asesino del ferrocarril". Otra imagen, de las Autoridades de Kansas, ofrecía un perfil aproximado de Bob, Emmet y Grattan "Grat" Dalton (1892) con el aliciente de una recompensa de 5000$ de la época. Entre los *se busca* más sonados de la ultima época, los 3,8 millones de dólares USA que ofrece el gobierno mexicano por la captura de "El Chapo" Guzmán, jefe del cartel de Sinaloa, fugado en 2015 de forma espectacular de una prisión de máxima seguridad en la que portaba brazalete electrónico y era vigilado las 24 horas del día (IMAGEN 57).

Universitat d'Alacant
Universidad de Alicante

1.4.2. Los problemas del cribado sin enrolamiento previo

En algunos casos el patrón de la persona buscada fue enrolado: por ejemplo en algunos escenarios de conflicto bélico veremos que se están registrando sistemáticamente todos los rasgos de los varones de cierta edad, o que se controlan los movimientos de los refugiados, del mismo modo que las huellas dactilares o perfiles de ADN de criminales y sospechosos son almacenados por las autoridades de cada vez más países. En esos casos, los sistemas de cribado buscarán, entre una población no sospechosa, a la persona buscada. Más polémicos son, sin duda, aquellos sistemas de cribado que emplean un patrón de referencia que es artificial; esto es, se trata de sistemas que pretenden localizar a una persona que no ha sido enrolada sobre la base de un patrón en el que se ha tratado de representar de la forma más fidedigna posible los rasgos de la persona que es objeto de búsqueda. Esto, como es de imaginar, sucede sobre todo en sistemas con base en la Biometría facial (en los que fotografías de poca calidad o testimonios de testigos

pueden permitir hacer un patrón de referencia), aunque también es posible hacer cribados, por ejemplo, con huellas dactilares parciales.

Si, como veremos, todos los sistemas biométricos se ven afectados por las limitaciones que les generan factores como el envejecimiento de los patrones, en el caso de los cribados suelen ocasionarse algunos problemas añadidos. Sobre todo si en lugar de emplear como referencia patrones reales se emplean patrones artificiales o patrones aproximados o de baja calidad que han sido mejorados artificialmente. Conforme al estado actual de desarrollo científico y tecnológico de las infraestructuras de cribado biométrico, ha de admitirse que esto tiene bastantes más sombras que luces. Quizá se recuerde la polémica de aquel retrato robot de *Bin Laden* en cuya configuración se habían empleado –entre otras cosas- algunos componentes de una fotografía del que entonces era Coordinador General de Izquierda Unida (Gaspar Llamazares). IMAGEN 58. Si siempre hay un margen estadístico a tener en cuenta cuando se compara un patrón almacenado y un nuevo dato en fresco, ¿qué puede esperarse de un patrón biométrico o versión simplificada tomado de un dato en crudo que, ya de partida, no es el real? Más aún, ¿cuál es la posibilidad de que una persona *que hemos enrolado con un patrón aproximado* sea reconocida porque, por casualidad, se le ocurre exponerse a nuestro sistema automatizado de reconocimiento (entrando por la puerta principal de un edificio público, o yendo a tomar un avión a rostro descubierto a uno de los aeropuertos más vigilados del mundo)?

No obstante ha de reconocerse que los sistemas han mejorado exponencialmente. La posibilidad de captar patrones de calidad en 3D y a distancia y la mejora de las herramientas analíticas está dando lugar a procesos de elaboración de patrones que sin ser aun de la calidad de los que se obtienen con la presencia y colaboración del sujeto, sí comienzan a tener un potencial singularizante más que razonable.

Con todo, los debates más encendidos que plantea el cribado biométrico no se deben sólo al modo en que se busca a alguien, sino también al problema que se genera por la *vigilancia colateral* a la que se somete al resto de ciudadanos. Descrito el patrón biométrico de un rostro, por ejemplo, que además puede ser tanto de una persona como de un tipo de personas a las que se asocia con algún colectivo determinado (árabes o coreanos, por ejemplo), se procede a rastrear su posible coincidencia con fotografías almacenadas en bases de datos (como las de obtención de la licencia de conducción en los EE.UU., por ejemplo) o con imágenes obtenidas de los sistemas de video-vigilancia[13]. Existen cámaras fijas instaladas en los aeropuertos, en los cajeros de los bancos, en los accesos a los edificios públicos, que graban constantemente a las personas. También es posible realizar rastreos en Internet o en las redes sociales, especialmente con la ayuda de las

[13] JAIN, A. K./ PANKHATI, S./ ET ALTERE, "Biometrics: a Grand Challenge", *Proceedings,* Cambridge, UK, 2004.

herramientas *facematch*, que permiten etiquetar hasta a 50 de las personas que aparecen en una fotografía colgada en la red[14]. Todas las personas que guarden algún tipo de similitud con la persona o personas que se buscan, corren injustificadamente el riesgo de ser observadas, trazadas o incluso interceptadas o detenidas sólo por ese parecido biométrico. ¿Resulta esto adecuado?

En junio de 2014 se publicó en la prensa estadounidense a referencia del primer caso en el que el autor de un robo con violencia fue detenido empleando un sistema de reconocimiento biométrico a distancia (NeoFace) que genera alertas en tiempo real y emplea una tecnología de reconocimiento facial de alta precisión. La cuestión es que la disponibilidad de las imágenes y su almacenamiento y procesamiento con ese motivo implican almacenar datos de ciudadanos sin antecedentes (ni intenciones) criminales. Aunque la percepción social sobre esta cuestión cambió drásticamente.

> Una de las discusiones más interesantes sobre la utilidad y las limitaciones de estas tecnologías se produjo en torno a la XXXVª Super Bowl (2001). En los accesos al estadio se instaló un sistema de reconocimiento facial que, con la excusa de buscar criminales potenciales vigilaba a los miles de ciudadanos ordinarios que acudían a dicho evento[15]. Laurence WEIN de la Universidad de Stanford, calculó que las posibilidades que un sistema de estas características tiene para captura a un terrorista que tengamos enrolado a partir de sus verdaderos datos en crudo, apenas supera el 50% y eso, además, en el caso de que la persona buscada se ponga ante uno de los dispositivos que están tratando de localizarle.

Pero el tema dejó de discutirse tras los atentados que se cometieron apenas unas semanas después, el 11 de septiembre de 2001. Opinamos, sin embargo, que la valoración de la legitimidad y proporcionalidad de estos sistemas no ha de hacerse al calor de los acontecimientos sino enjuiciando, de forma pausada, sus ventajas y sus costes potenciales. Así se ha procedido en este capítulo –en relación con el funcionamiento en sí- y en el próximo –en relación con la aplicación de los sistemas a escenarios operativos concretos.

2. EL FUNCIONAMIENTO BÁSICO DE LOS SISTEMAS AUTOMATIZADOS DE RECONOCIMIENTO MEDIANTE BIOMETRÍA

Sea con la finalidad de identificación, verificación o activación de un sistema de cribado, encontramos una gran diversidad de tecnologías de reconocimiento biométrico. Existen desde sistemas relativamente sencillos, para grupos de usuarios muy reducidos, hasta otros capaces de comparar en poco tiempo una muestra con los millones de patrones previamente almacenados

[14] *Google* también incluyó un sistema de Facial Recognition, posteriormente sustituido por la herramienta *find my face*.

[15] E. VOLKOH, jurista de la UCLA, defendía que existen situaciones en las que un sistema de cámaras puede ofrecer tanto seguridad como libertad, en *Big Brother is Watching – Be Grateful,* Wall Street Journal, 26 de marzo de 2002, p. A 22. Pero no era una opinión generalizada.

(estableciendo categorías previas que agilizan la comparación de patrones). Algunos sistemas son multimodales, esto es, funcionan sobre varias características biométricas diferentes[16] (IMÁGENES 60 y 61) para mejorar la fiabilidad. No obstante existen una serie de elementos comunes a todos los diseños y la reflexión conjunta sobre sus utilidades, limitaciones riesgos requiere, por ello, un cierto consenso sobre el contenido y el significado de los términos que se emplean para referirse a los elementos comunes de dichos sistemas[17].

2.1 La estructura básica

Los procedimientos biométricos registran una característica biológica mensurable con capacidad potencial para singularizar a un ser humano[18]. Potencialmente es posible construir una infraestructura de reconocimiento basada en dichos procedimientos, pero es imprescindible distinguir en la estructura de los sistemas una serie de pasos clave. Así, mientras algunos procedimientos transforman un dato en crudo en un dato biométrico, otros gestionan y procesan éste, y realizarán comparaciones a futuro. Ello implica que además de elementos de captación de los datos y de gestión singularizante de éstos, habrán de diseñarse dispositivos que procedan al almacenamiento, a la comparación y a la toma de decisiones tras la comparación. Así, y aunque a lo largo de la historia y aún en la actualidad se han manejado y se siguen manejando sistemas manuales con representaciones analógicas de los datos biométricos, la expresión sistema biométrico de reconocimiento se emplea en la actualidad para referirse a una estructura que combina *Hardware* y Software y que opera aplicando un procedimiento biométrico. Es decir, un sistema que registra características mensurables en un formato digital y ofrece además algún tipo de utilidad relacionada con la singularización de los individuos. La Biometría digital se diferencia de aquellos sistemas cuantitativa y cualitativamente[19], especialmente por la calidad y la velocidad a la que es capaz de realizar la comparación entre el nuevo dato que se le presenta y el que tiene almacenado[20].

2.1. *Elementos estructurales (arquitectura de los sistemas)*

Según la *Encyclopedia of Biometrics,* el diseño de un sistema de identificación biométrica es un proceso por el cuál se definen, de una parte, *la arquitectura del sistema de identificación* –

[16] WAYMAN, J. / JAIN, A. K. / MAIO, D. "An Introduction", 2005, pp4-5.
[17] KINDT, E. "Biometric applications and the data protection legislation. The legal review and the proportionality test," *Datenschutz und Datensicherheit, DuD* 2007, 166, p167.
[18] BSI, *Biometrie*, Berlin, 2005, p1.
[19] MORDINI, E./ MASSARI, S., *Bioethics Journal*, 2008, p489; SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008, págs. 2-3.
[20] ALTERMAN, A.: "'A Piece of your self': Ethical issues in biometric identification", *Ethics and Information Technology* 5: 139-150, 2003

seleccionando los componentes de hardware y software adecuados- y, de otra parte, *una política de administración del sistema*[21]. Es decir, una estructura informática y, junto a ello, una serie de normas o reglas que el sistema aplicará para tomar decisiones. En términos estructurales la arquitectura del sistema suele comprender un conjunto de módulos (una media de 7) que operan de forma secuencial: 1) un interfaz que incorpora un lector o sensor; 2) un módulo que chequea si la muestra captada por el lector es de suficiente calidad como para ser procesada; 3) un módulo de mejora de la muestra; 4) un módulo de extracción de atributos; 5) una base de datos de almacenamiento; 6) un comparador de muestras que determina el grado de similitud entre las muestras captadas y las que están almacenadas; 7) y un módulo de toma de decisiones[22]. Vease la IMAGEN 59.

Necesitamos, además, fijar una serie de normas que el sistema aplicará para decidir, por ejemplo: qué calidad de la muestra biométrica es suficiente para ser captada y qué hará cuando no lo sea; en qué modo procederá a *mejorar* las muestras; qué atributos extraerá y cuántos; qué grado de similitud se considera como limite para considerar que dos patrones proceden del mismo sujeto fuente; o que hará el sistema cuando se hallen coincidencias o, por el contrario, se considere que las coincidencias halladas no permiten determinar que un patrón en fresco y uno almacenado proceden del mismo sujeto fuente. La mayor diferencia entre otros métodos de identificación y los sistemas contemporáneos de reconocimiento mediante biometría, lo decíamos en la introducción, es su automatización. Quiere ello decir que en ningún momento del proceso y toma de decisiones interviene un ser humano, aunque haya sistemas cuyo funcionamiento esté *monitorizado* (u observado) por un ser humano. El sistema, por tanto, se gestionará con las órdenes que, con más o menos acierto, abarcando o no el mayor número de hipótesis posibles, hayamos introducido en él en su fase de diseño.

Universitat d'Alacant
Universidad de Alicante

2.2. *Fases de los procesos*

La obtención y almacenamiento de un dato biométrico con fines de utilización del mismo en el seno de un sistema de reconocimiento comprende una serie de procesos o fases en los que intervienen los módulos a los que ya nos hemos referido y que, de forma simplificada, que pueden agruparse en cuatro:

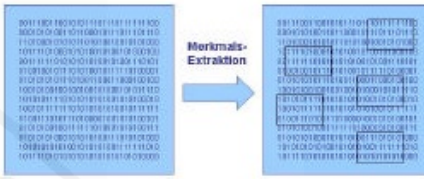
a) una primera fase de obtención de la información biométrica de una persona;
b) una fase de elaboración del patrón (que puede comprender a su vez varias subfases);
c) un tercer momento de captación del patrón en fresco;

[21] JAIN, A. K. / NANDAKUMAR, K., "Biometric System Desing - Overview", S. Z. LI/ A. K. JAIN, *Encyclopedia of Biometrics*, Springer, consultada la edición de 2009, p135.
[22] JAIN, A. K. / NANDAKUMAR, K., "Biometric System Desing - Overview", *ult. loc.cit.*

d) y una última fase de comparación entre el patrón almacenado y el patrón en fresco, procediendo a la toma de decisiones.

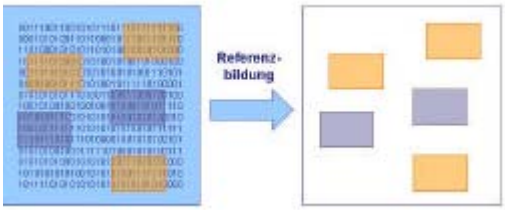
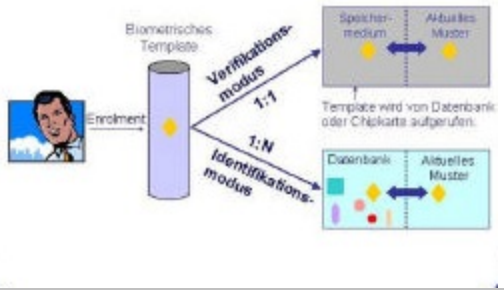
El *enrolamiento*[23] implica obtener del cuerpo de una persona datos biométricos. Como ya se ha dicho, cada sistema tiene como base uno o varios tipos de datos biométricos, obtenidos a partir de determinadas características estáticas o dinámicas de la biología de una persona. Dependiendo del tipo de fuente de datos de la que vaya obtenerse el dato en crudo, serán necesarios distintos mecanismos de enrolamiento.

PROCESO DE ENROLAMIENTO (FASES 1 Y 2)[24]

FASE 1 Obtención de los datos	FASE 2 Elaboración del patrón
 Se **obtienen datos** mediante la toma de medidas de un rasgo biológico o comportamental. Así, por ejemplo, de la geometría de la mano, las minucias de las huellas dactilares, el patrón vascular del fondo del ojo.	 Esos datos **no se almacenan en su totalidad**. Sólo aquellos que son más característicos y que, por consiguiente, diferencian el patrón de un individuo respecto del de los demás.

Obtenido el patrón se pasa a la fase de almacenamiento, que como se verá a continuación admite muy diversas modalidades. El objetivo de este almacenamiento es *permitir comparar patrones obtenidos en vivo* con los ya almacenados, para dar así cumplimiento a la finalidad con la que se ha creado la infraestructura de reconocimiento.

[23] AMBERG, FISCHER, RÖßLER: *Biometrische Verfahren* (2003), p6.
[24] AMBERG, FISCHER, RÖßLER: *Biometrische Verfahren* (2003), p6.

FASE 3 Almacenamiento del patrón	**FASE 4** Comparación del patrón obtenido en vivo, con el almacenado
	
El patrón puede **almacenarse** en una Base de Datos (las hay de diferentes tipos) o en un CHIP integrado en una tarjeta de identificación.	Se obtienen **nuevos patrones en vivo**, que son comparados con los almacenados. Esto difiere según el tipo de sistema biométrico. Es decir, según sea de verificación, de identificación o de cribado.

2.2 El enrolamiento (o reconocimiento primario), la captación de la información biométrica y la creación del patrón.

Un sistema biométrico tiene como actividad más característica la comparación de la información biométrica obtenida en dos momentos: el momento del enrolamiento[25], o de acceso al sistema, y el momento de reconocimiento, o momento en el cual un rasgo es presentado por segunda vez al sistema (o patrón elaborado a partir de la muestra biométrica en fresco). Los patrones, se ha explicado también, hipotéticamente sintetizan la singularidad que para una persona se expresa en una característica biométrica universal y permanente, y con ese fin se elaboran a partir de una serie de atributos singularizantes obtenidos mediante algún tipo de dispositivo de captación[26].

Para ello, tras la captura de una muestra a través de un dispositivo (una cámara, un escáner, un sistema de grabación de sonidos, etc.) se produce con frecuencia un *preprocesado* de la muestra captada, operación ésta que tiene el doble objetivo de permitir mejora la imagen de la muestra y facilitar la selección de las zonas que se consideran más óptimas para la obtención de los atributos (minucias de una huella dactilar, vectores de longitud y anchura en la geometría manual, etc.). Los atributos extraídos se traduce o representan como algoritmos u otras representaciones matemáticas, susceptibles de un procesamiento ágil.

[25] REID , P. 2004:6; NAVATI/ THIEME/NAVATI, 2002, p17.
[26] GIROTTO, S. "Il tratamento dei Dati Biometrici", en *Tratatto di Biodiritto*, cit., 2011, p1239; ICAO, *Biometric Deployment of Machine Readable Documents*, ICAO-MRTD/NWTG, Technical Report, 21 de mayo de 2004; ICAO – Technical Advisory Group of Machine Readable Documents (TAG-MRTDs), *History, interoperability and implementation*, 2007, p16.

El proceso de enrolamiento, advierten muchos autores, es un proceso intrínsecamente *propenso al error*[27]. Los sistemas dependen, en primer lugar, de la veracidad con la que una persona alega la identidad que le da derecho a enrolarse; esa alegación inicial de identidad no depende, en absoluto, del sistema de reconocimiento biométrico. De igual modo, de nada serviría que sea tecnológicamente complicado crear un DNI falso si resultase relativamente sencillo acudir a la oficina del DNI y conseguir que nos emitan un DNI auténtico con el que fingir ser alguien que no somos.

Por otra parte, y en segundo lugar, durante el enrolamiento queda en evidencia que se trata de sistemas inherentemente probabilísticos y esa característica, fundamental y crítica, no debería perderse de vista. La fase de comprobación de patrones, como se verá, es una fase también crítica, pero ya en este primer momento hemos tenido que establecer *cómo escogerá el sistema los atributos que se estiman singularizantes*, cuántos atributos escogerá (por ejemplo cuántas minucias o cuantos puntos de referencia geométricos) captará, con qué precisión los expresará métricamente y en qué forma elaborará con ellos un patrón biométrico. En este sentido, es especialmente interesante un elemento que introducen algunos sistemas de reconocimiento biométrico –aunque no todos. Nos referimos al hecho de que en este momento de enrolamiento activan un *test estadístico*, una comparación 1 a n entre el nuevo patrón que se desea enrolar y los ya enrolados previamente, con el objetivo de evitar el enrolamiento de patrones que, aunque indubitadamente se sepa que pertenecen a sujetos fuente diferentes, en sí mismos no resultan lo suficientemente distintivos respecto de otros ya almacenados en la base de datos.

Universitat d'Alacant
Universidad de Alicante

2.3 El almacenamiento del patrón biométrico

El almacenamiento aglutina, como veremos, buena parte de las preocupaciones relacionadas con las tecnologías biométricas[28]. ¿Quién y cómo podrá acceder a la información biométrica que, con fines de reconocimiento, captan estos sistemas? ¿Cómo se protegerá esa información de accesos no consentidos o de usos abusivos? ¿Qué sucederá si los datos quedan, de algún modo, expuestos? Es importante advertir en este lugar que la decisión del tipo de almacenamiento que se empleará no depende del tipo de información biométrica que sea objeto de almacenamiento. Por sus características, los patrones biométricos se crean con el objetivo de poder ser almacenados en espacios digitales relativamente pequeños y, posteriormente,

[27] NRC, *Biometric Recognition*, 2010, p3.
[28] Así también LUCAS, P. "Biometrics Come into Focus", *Collections & Credit Risk*, 10 (3), 2005, pp18-21; LANGENDERFER, J. / LINNHOFF, S. "The Emergence of Biometrics", *Journal of Consumer affairs*, vol 39, nº 2, 2005, pp324-325.

procesados con agilidad[29]. Se capten huellas dactilares, geometría del rostro, secuencias de información biométrica dinámica o huellas de voz, en todos los casos son posibles tres tipos de almacenamiento: almacenamientos que controla el sujeto fuente (es decir, almacenamiento que implican que el patrón lo conserva, de algún modo, la persona); almacenamientos en una base de datos que controla un tercero, distinto del sujeto fuente, pero que no está comunicada en red con tras bases o con otros usuarios diferentes a ese tercero; y almacenamientos en red. Escoger uno u otro tipo de almacenamiento no dependerá del tipo de información biométrica de que se trate, sino de la organización técnica y de las finalidades que se persigan con cada sistema de reconocimiento en un escenario operativo en concreto.

Si nuestro sistema ofrece una utilidad de verificación y sólo necesitamos garantizar que cada vez que se usa una tarjeta o un pasaporte la persona portadora de éstos es la persona para la cuál se emitió válidamente dicho título, podemos –por ejemplo- almacenar esta información en un CHIP insertado en la tarjeta. No necesitamos que la información este almacenada en ningún lugar. Al captar la presencia del pasaporte el sistema busca en ese chip el patrón almacenado, y lo compara con el captado en fresco. Si el CHIP utiliza un sistema de radiofrecuencia ello permite que los datos sean leídos a distancia, sin necesidad de introducir la tarjeta en ningún lector. El almacenamiento en dispositivos insertados en tarjetas hace que no pueda conocerse la totalidad del patrón biométrico sin disponer, conjuntamente, de la tarjeta que contiene el chip o dispositivo de almacenamiento y de un lector adaptado al mismo[30]; eso sí, si las tarjetas o pasaportes van a emplearse ante diferentes autoridades y en diferentes países, será necesario que la forma en la que se almacene la información en el CHIP esté homologada como para permitir ese acceso. Se establece, asimismo, qué datos deben recogerse y cuáles han de ser la capacidad mínima y la estructura lógica del CHIP[31], además de una serie de medidas de seguridad e integridad. El Pasaporte Europeo recoge la huella plana (no rodada) del dedo índice de la mano derecha y de la izquierda; si las huellas de dichos dedos no son de calidad o hay lesiones en los dedos índices, se pueden emplear huellas de calidad de los dedos medio, anular o pulgar. Estas huellas se almacenan como imágenes comprimidas de entre 12 y 15 Kbs en un Chip instalado en el propio documento[32]. Leyendo el chip, el dispositivo nos dice si el pasaporte le pertenece o no a la persona que lo portaba y cuyas huellas hemos escaneado. Más allá del CHIP no hay almacenamiento o, lo

[29] LANGENDERFER, J. / LINNHOFF, S. "The Emergence of Biometrics", *Journal of Consumer affair*s, vol 39, nº 2, 2005, p325.
[30] D. GRAHAM-GROWE, "Secure Signature Means No One Can Steal Your ID. A New Approach to ID Card Biometrics Will Enhance Security and Privacy", *New Scientist*, 182/ 2004, PP22-23.
[31] Los datos alfanuméricos impresos en el MRZ del Pasaporte deben corresponder con los almacenados digitalmente en el CHIP. Los estándares lógicos que se han tenido como referencia son el Doc 9303 del ICAO, parte 1, Machine Readable Passports, 5ª edición, 2003; *Common Consular Instructions*, CCI, Capítulo VI, nº 4 y anexo 10; ICAO NTWG, *Development of a Logical Data Structure (LSD) for optional capacity expansion technologies*, Technical Report, Revisión 1.7., 18 de mayo de 2004.
[32] Más detalles en *Biometrische Daten in EU-Pässen*.

que es lo mismo, desde una hipotética huella encontrada en un crimen y perteneciente a alguien no fichado, la policía no es capaz de determinar a quién pertenece la huella, porque las huellas no se han almacenado en una base centralizada para toda Europa[33]. Los centros de control transfronterizo tanto Europeos como de muchos otros países disponen de lectores capaces de comprobar si los rasgos biométricos del portador de un documento de estas características coinciden con los de la persona para la que se emitió dicho documento, aunque esos lectores no pueden en ningún caso afectar a la información contenida en el CHIP[34].

En otros casos, como por ejemplo el de EURODAC, no nos sirve un almacenamiento así. Se trata, decíamos, de un sistema que trata de evitar que las personas soliciten asilo en más de un país o que personas a las que se les ha denegado el asilo, lo intenten de nuevo bajo una nueva identidad. En este caso, es necesario que los patrones estén almacenados en un tipo de base al que las autoridades de control de la inmigración de cualquier país de la UE puedan acceder en algún momento. Es decir, es necesario un almacenamiento en una base de datos que pueda usarse en red.

2.4. La captación del dato en fresco, la comparación con los patrones almacenados y la toma de decisiones.

A partir de los datos almacenados, el sistema se pone al servicio de su gestor un potencial de reconocimiento. Cuando un usuario ya enrolado se presenta ante el sistema, éste procederá a obtener un nuevo set de atributos biométricos (patrón en fresco) que se comparará con un patrón biométrico ya almacenado o con todos los patrones almacenados, según sea el caso. Tras una comparación, se produce un cálculo del nivel de coincidencia y de divergencia entre el patrón almacenado y el patrón en fresco[35] y sobre ese dato el sistema tomará una decisión. Para ello se le ha fijado un umbral de tolerancia; un umbral que refleja hasta qué punto patrones mínimamente divergentes pueden ser considerados como procedentes del mismo sujeto; y a partir de qué nivel de diferencia se considera que el patrón en fresco no puede ser del mismo sujeto que los almacenados (o el almacenado respecto al cuál se alega una identidad).

[33] Vease el Reglamento modificado por el Reglamento CE 444/ 2009, del Parlamento Europeo y del Consejo, de 28 de mayo de 2009.
[34] ICAO NTWG, *Biometrics Deploument of Machine Readable Travel Documen*, Technical Report, Versión 2.0 de 4 de mayo de 2004; ISO/IC FDIS 14443, *Identification Cards – Contactless integrated circuit(s) cards – Proximity Cards*; ICAO NTW, Use of Contactless Integrated Circuits in Machine Readable Travel Documents, Technical Report, Version 3.1., 16 de abril de 2003.
[35] ALTERMANN, A.: "'A Piece of your self': Ethical issues in biometric identification", *Ethics and Information Technology* 5: 139-150, 2003.

La declaración de resultado tras la comparación, tomada entre otras cosas teniendo en cuenta el criterio del umbral de tolerancia[36]., tendrá una de estas consecuencias. Verificar implica determinar la validez (o no) de la identidad alegada; identificar implica concluir si la referencia biométrica que una persona ha expuesto al sistema es una referencia biométrica previamente contenida en el sistema o, por el contrario, no lo es. Todo sistema de reconocimiento biométrico tiene una *Tasa de Aceptación Errónea* y una *Tasa de Falso Rechazo*. La primera se refiere a los casos en los que un impostor es admitido como individuo autorizado, lo cual supone un grave problema de seguridad. La tasa de falso rechazo, por su parte, calcula los casos en los que un usuario legítimo es considerado por el sistema como impostor, algo que no afecta a la seguridad aunque sí a la adecuación del sistema. El punto de encuentro entre una y otra curva nos señala la tasa de error del sistema en su conjunto.

Nótese que este umbral de tolerancia tiene una gran trascendencia. Si se pide al sistema que el nuevo vector guarde un gran parecido con el patrón almacenado, se corre el riesgo de que el sistema provoque falsos rechazos o no se reconozca a un sujeto cuya identidad está almacenada en la base de datos; un umbral de tolerancia muy bajo, por el contrario, posibilita que un tercero se haga pasar por usuario legítimo y sea falsamente aceptado o falsamente identificado por el sistema. De hecho, para medir el rendimiento de los sistemas se tienen en cuenta una serie de tasas que forman parte de lo que expresa dicho umbral: 1) La tasa de error en la captura de la muestra (Failure to Acquire Rate); 2) la tasa de error de enrolamiento, por ejemplo porque el sistema no puede generar patrones de suficiente calidad; 3) tasas de error que implican no reconocer a un usuario enrolado: el falso non-match (FNM) en el caso de los sistemas de identificación y el falso rechazo (FRR) en los sistemas de verificación; 4) tasas de error por aceptar como enrolados a sujetos que no lo están: el falso match en los sistemas de identificación y la falsa aceptación en los de verificación.

Los dos últimos grupos de tasas se calculan sobre el número total de comparaciones, aunque con matices Según la normativa ISO, las tasas de falsa aceptación y falso rechazo se calculan sobre el número de transacciones de verificación y las de match/ no match sobre el numero total de comparaciones (incluyendo por tanto los casos en que por baja calidad de la nuestra se ha producido un error de captura que impide después una verificación). En ambos casos, las tasas guardan relación con el valor del umbral (alto o bajo) que se haya fijado. Las tasas de las aplicaciones comercialas varían de forma importante; entre un 20% y un 0,1 en las tasas de falso rechazo, y entre un 1% y un 1 entre 10 millones para las tasas de falsa aceptación[37]. ¿Son altas,

[36] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK -BSI, *Biometrie*, RFA, 2005, p4.
[37] CAVOKIAN, A. / STOIANOV, *Biometric Encryption*, 2007, 8.

bajas? Depende. CAVOIAN/ STOIANOV nos invitan a pensar en grupos de usuarios de varios millones de personas, en los que tasas de error que pueden parecer razonables (un 0,01%) pueden implicar identificaciones erróneas en miles de personas. KINDT indica que en el año 2004 el laboratorio nacional de física propuso una tabla de referencia para la evaluación de los errores, dependiendo del uso que se pretendiera dar a los sistemas[38], pero lo cierto es que no hay unos criterios de referencia asentados a este respecto y se han producido relativamente pocos test independientes (especialmente sobre escenarios o a nivel de operatividad real). Sí que se han publicado, en cualquier caso, informes que valoran o comparan las tasas de error bien en la evolución de algunos sistemas, como comparando algunos sistemas entre sí. Así, en el año 2010 se estimaba que un 91% de éxito en un sistema de 20,000 usuarios/ día era el mejor rendimiento que había ofrecido hasta el momento un sistema instalado[39].

Dependiendo del método que se emplee y de la capacidad que el sistema de procesamiento tenga para captar métricamente la singularidad y gestionar la variabilidad encontraremos, y ese es un dato importante, distintos niveles de *precisión* en el servicio que ofrecen los sistemas de reconocimiento. Esto nos recuerda a una expresión del filósofo Ludwig J. J. WITTGENSTEIN (1889-1951), que cuestionaba la existencia de un único tipo de exactitud. "*En cada momento* –afirmaba- *tenemos diferentes ideales de lo que es la exactitud*"[40].

3. LAS LIMITACIONES Y LOS RIESGOS DE LA IDENTIFICACIÓN BIOMÉTRICA CONFORME AL ESTADO ACTUAL DE LA CIENCIA Y LA TECNOLOGÍA (I). LIMITACIONES Y RIESGOS QUE TIENEN RELACIÓN CON LA BASE CIENTÍFICA DE LOS SISTEMAS.

Universidad de Alicante

En las dos últimas décadas se han afirmado con insistencia dos importantes observaciones ante los sistemas de reconocimiento biométrico: primera, que el reconocimiento biométrico podría ofrecer soluciones socialmente aceptables y tecnológicamente viables[41] a las necesidades de identificación de la era contemporánea; segunda, que ello no implica que sea *una tecnología infalible*. Ambas afirmaciones se han reforzado en esta última década, especialmente desde los debates parlamentarios ocasionados por la incorporación de elementos biométricos a los pasaportes europeos, importantes instituciones y organizaciones públicas y privadas han

[38] KINDT, E. *Privacy and Data Protection,* 2013, p53.
[39] CAVOUKIAN, A./ MARINELLI, T. *Privacy-protective Facial Recognition: Biometric Encryption. Proof of Concept*, Information and Privacy Commisioner, Ontario, 2010, p13; GROTHER, P./ QUINN, G. / PHILLIPS, P. "Multiple-Biometric Evaluation (MB) – Report on the Evaluation of 2D Still Image Face Recognition Algorithms", *NIST Interagency Report* 7709, 2010, p34; Busch, C. "Forschung für die Grenzkontrollen der Zukunft", 2009, p10; BOURLOY, T./ ROSS, A. / JAIN, A. "On matching Digital Face Images against Scanned Passport potos", 2009, p9.
[40] Citado por G. GILLET, *Subjectivity and Being somebody. Human identity and neuroethics*, Imprint Academic, Exeter, 2008, p32.
[41] REBERA, A. P. / MORDINI, E.: "Biometrics and Ageing", en M. FAIRHURST (ed.), *Age Factors*, 2013, p54; GELB, A. / DECKER, C.: "Cash at your fingertips: Biometric Technology for transfers in developing countries", *Review of Policy Research*, 29 (1), 2012, pp91-117.

dedicado atención a las tecnologías biométricas, en algunos casos con el apoyo de estudios multidisciplinares de expertos independientes[42]. Hasta el Supervisor Europeo para la protección de datos (SEPD)[43] ha reconocido que estamos ante una *tecnología imperfecta*[44].

Pero, ¿imperfecta, en qué sentido? ¿Cuáles son las limitaciones, riesgos y desventajas que hemos de tener en cuenta a la hora de valorar la implementación de un sistema de reconocimiento de estas características? En esta exposición las limitaciones, riesgos y desventajas de estos sistemas se presentan agrupados en tres conjuntos. En primer lugar, en el presente epígrafe, se presentan aquellas limitaciones y riesgos que tienen que ver con la base científica de los sistemas de reconocimiento biométrico; esto es, con el estado del arte en lo que se refiere a las cualidades de universalidad, permanencia y singularidad que, junto con otras, son requisito para poder construir un sistema de reconocimiento automatizado sobre la base de una característica biométrica. En segundo lugar, en el epígrafe siguiente, se abordan aquellas limitaciones y riesgos que tienen su origen en la arquitectura informática que sirve de soporte a estos sistemas de reconocimiento, y al funcionamiento de esos soportes. Por último se harán una serie de consideraciones en relación con la implicación ética y social del uso de las tecnologías de reconocimiento biométrico.

3.1. Hasta qué punto pueden darse por cumplidos los *Seven Pillars of Biometric Wisdom*

Las cualidades específicas que hemos presentado en el capítulo anterior y hacen esperar un importante rendimiento de las características biométricas en la identificación de las personas, son en nuestra opinión uno de los flancos más débiles de las tecnologías de reconocimiento biométrico. Es cierto que todos los sistemas de este tipo se han creado sobre la base de "una característica a la que se atribuyen un conjunto de cualidades", especialmente los de universalidad, permanencia y singularidad, pero como advertimos ya en el capítulo anterior se reconoce que esas cualidades de universalidad, permanencia y singularidad son interpretadas de una forma *flexible*. A día de hoy no existen sistemas completamente automatizados que tengan como base las biometrías que se consideran más universales, permanentes y singulares de todas: las biometrías del ADN; y aún incluso éstas tienen como punto débil la existencia de gemelos monocigóticos.

---

[42] Proyectos EU RISE Consortium (Rising Pan-European and International Awareness of Biometrics and Security Ethics), BITE (Biometric Identification Technology Ethics) y HIDE (Homeland Security, Biometric Identification & Personal Detection Ethics), subvencionados por la Comisión Europea.

[43] SEPD, Opinión sobre el sistema VIS.

[44] DE HERT, P./ SCHEUERS, W./ BROUWER, E.: "Machine-readable identity documents with biometric data in the EU – part III- Overview of the legal Framework", *Keesing Journal of Documents and Identity*, 2007/ 22, pp23-26; KINDT, E. "Biometric applications and the data protection legislation (the legal review and the proportionality test)", *Datenschutz and Datensicherheit (DuD)*, 31/ 2007, pp166-170; BROUWER, E. R. *Digital Borders and Real Rights,* 2008, p137.

Cuando se habla de "flexibilidad" se reconoce que ninguna Biometría es universal, permanente ni estable al cien por cien[45], y que, al no ser el cuerpo humano *fácilmente metrificable*, los métodos de captación existentes no descartan que de muestras biométricas diferentes (de sujetos diferentes) puedan producirse patrones biométricos idénticos; del sistema de captación y de la metodología que se emplee para extraer datos mensurativos y transformarlos en un patrón biométrico depende, como venimos diciendo que el patrón sea tan singularizante (o casi tanto) como el rasgo biométrico en sí. Ante ello nos hemos preguntado de cuánta flexibilidad estamos hablando y cómo se gestiona, en el caso concreto, ese margen de imprecisión.

3.2. Limitaciones relativas a la *universalidad* de las características biométricas que sirven de soporte a los sistemas de reconocimiento mediante biometría.

Según el GRUPO DE TRABAJO DEL ARTÍCULO 29 (que asesora a la UE en materia de protección de datos) el adjetivo *universal* aplicado a la información biométrica ha de entenderse en el sentido de que para establecer un sistema de reconocimiento sobre la base de una característica, ha de poderse esperar que ésta esté presente en todas las personas, si bien es posible que excepcionalmente, por accidente, enfermedad u otra circunstancia, algunas personas carezcan de ella. No hemos encontrado, sin embargo, propuestas que fijen un umbral de presencia por debajo del cual se considere que una característica no puede servir de base a un sistema.

La cualidad de la universalidad se resiente, en algunos casos, por la ausencia del rasgo de referencia en algunas personas. La Biometría del iris, la geometría del rostro y la geometría dactilar son la base de los sistemas más extendidos y se da tácitamente por universal su presencia. Pero en algunas personas no es posible captar la Biometría del iris; la ausencia de pigmentación en el iris (como consecuencia, por ejemplo, del albinismo), la anoftalamia o aniridia, la microoftalamia, excluyen a las personas del reconocimiento por Biometría ocular, como la anotia y microtia las excluyen del reconocimiento por Biometría auricular. Y por sus condiciones de salud algunas personas quedan excluidas de la mayoría de las biometrías dinámicas (con excepción de las que captan señales electrofisiológicas o parámetros corporales).

Al margen de los casos en los que algunas personas carecen de alguna de las falanges, ha de tenerse en cuenta que existe también una peculiaridad genética que se conoce como adermatoglifia que ocasiona una ausencia de huellas dactilares[46].

---

[45] LANITIS, A. "A survey of the effects of ageingon biometrical identity verification", *International journal of Biometrics*, 2 (1), 2010, pp34-52.
[46] NOWBECK, J. / BURGER, B. / FUCHS-TELEK, D. / PAVLOSKI, M. "Adermatoglyphia", *American Journal of Human Genetics*, 2011, 89 (2), p302;

En otros casos el problema no es tanto la ausencia, como el hecho de que las características que son empleadas con referencia en un sistema biométrico presentan en algunas personas algunos rasgos que, por exceso o defecto, quedan fuera del rango de lo normal. Eso hace que imposible que los sistemas de captación obtengan de estas personas la información biométrica necesaria para el reconocimiento.

La promesa biométrica invitaba a pensar que de algún modo la ciencia biométrica sería capaz de condensar relaciones y conocimientos complejos en un único *mapa digital del cuerpo humano*, pero lo cierto es que todas las tecnologías biométricas se diseñan para un prototipo que se considera *el promedio* o la norma y queda siempre margen para personas que trasciendan dicho estereotipo[47] por razones etnia, género, edad, ocupación o color de los ojos[48]. SURGEON se refiere a mujeres asiáticas con una piel tan fina que algunos escáneres de huellas dactilares no consiguen captar su impresión dactilar[49], un fenómeno que también se produce en otras personas como consecuencia de la raza, el género o la edad tal y como demostró el test comparativo realizado por IBG[50]. Algunos escáneres de iris, por su parte, tienen dificultades para situar adecuadamente el iris en el contraste de tonos de piel oscura alrededor del ojo[51]. Algunos estudios han mostrado cómo la distribución de las tasas de error en diferentes colectivos no se produce de forma linear,[52] sino que discrimina significativamente a las personas de edad avanzada, las de talla muy alta o significativamente baja, y las personas con alguna discapacidad, especialmente en aquellos casos en los que el reconocimiento requiere que las personas mantengan respecto al dispositivo de captación una posición concreta, con un ángulo concreto[53]. Las personas de edad avanzada y los niños tienen una tasa de falsos rechazos muy superior a la media en cualquier tipo de sistema de reconocimiento biométrico[54]; teniendo en cuenta las previsiones de las Naciones Unidas sobre el envejecimiento global[55] es de prever que los sistemas biométricos que no gestionen adecuadamente el envejecimiento encontrarán cada vez más problemas de rendimiento.

La captación de la Biometría del rostro puede presentar dificultades en casos de anormalidades craneofaciales congénitas como la macro- o microcefalia o las craneosinostosis, o anomalías

[47] MAGNET, S. A. *When biometrics fail,* p29.
[48] MORDINI/ ASHTON, "The Transparent Body: Medical Information, Physical Privacy and Respect for the Body Integrity," en MORDINI/ TZOVARAS, *Second Generation*, p269.
[49] SURGEON, 2005; DAS, 2007; FLETCHER, 2006; MAGNET, S. A. *When biometrics*, p26.
[50] NAVANATI/ THIEME/ NAVANATI, *Biometrics: Identity verification in a Networked World*, 2002, p60.
[51] KABLENETT, 2006; estadísticas de Reino Unido recogidas por SAEB, 2005;
[52] BAHNU, *Ear* , 2008, capt. 7.
[53] MAGNET, S. A. When biometrics fail, 2011, p30.
[54] MORDINI/ ASHTON, "The Transparent Body: Medical Information, Physical Privacy and Respect for the Body Integrity," en MORDINI/ TZOVARAS, *Second Generation* p270.
[55] MORDINI/ REBERA, con más referencias, en M. FAIRHURST (ed.), pp37-39.

oculares (como el hiperteolirsmo y el hipotelorismo, la microoftalmia o la anoftalmia[56]; algunas anomalías se asocian a factores genéticos y otras a factores ambientales relacionados con el tiempo de gestación (como la toxoplasmosis, la rubeola, el herpes o la fenilcetonuria, entre otros). Por otra parte, el aspecto de la persona, en muchos casos asociado con su nacionalidad, cultura o religión, genera también algunas limitaciones en el rendimiento de los sistemas de reconocimiento biométrico. Las barbas pobladas, algunos tipos de peinados y, curiosamente, la calvicie (por la falta de la referencia de la línea capilar), las pestañas largas (no necesariamente artificiales) o los tonos de piel muy oscuros generan falsos rechazos muy por encima de la medida[57]. La Biometría de la marcha resulta difícil de captar cuando las personas llevan faldas largas o túnicas al igual que las uñas postizas interfieren en la captación de la Biometría de la forma de teclear. Las biometrías dinámicas son, asimismo, muy sensibles a los tics y movimientos involuntarios, al estrés, la tensión o cualquier tipo de distracciones tanto en el enrolamiento como en la toma secundaria de muestras biométricas. Véanse las IMÁGENES 71 y 72.

3.3. Limitaciones relativas a la *singularidad*. Lobos, ovejas, cabras y corderos.

La segunda de las cualidades que se exige a las características biométricas que sirven de base a un sistema de reconocimiento biométrico es su *potencial singularizante*[58]. Pero no es suficiente con que la característica lo sea; esto es, no es suficiente con que los rostros de las personas cuya Biometría facial se va almacenar sean lo suficientemente distintos. Una de las claves de rendimiento de estos sistemas reside en que la captación métrica de aquello que hace distinto a cada uno de los rostros se realice de modo que los patrones almacenados sean, también, lo suficientemente diferentes.

3.3.1 *Reconocimiento mediante Biometría y unicidad.*

Advertíamos ya, con el compromiso de volver a ello en este lugar, que el concepto de unicidad es un concepto muy resbaladizo. Y no sólo en el campo del reconocimiento biométrico; la identificación o singularización de personas y objetos se cuenta entre las cuestiones más controvertidas de la práctica forense. Un informe de la Academia Nacional de Ciencias del año 2009 afirmaba que aún faltan estudios sobre grandes poblaciones que nos permitan establecer adecuadamente la unicidad de huellas o atributos, uniéndose a otras voces que cuestionan, en

[56] BOYADJIEV BOYD, S. A. "Congenital Craniofacial Abnormalities", en *Mercx Manual - Professional Edition* (Pediatrics), 2014.
[57] MORDINI/ ASHTON, "The Transparent Body: Medical Information," en MORDINI/ TZOVARAS, *Second Generation*, p269-271.
[58] Cap .1 de la II PARTE.

algunos casos, el hecho de que la prueba de individualidad se deposite sobre los forenses dejando a éstos un importante margen de apreciación subjetiva[59]. Como consecuencia de las incertidumbres que inevitablemente acompañan a todo evento forense en la vida real, prácticamente todos los procedimientos de identificación implican algún tipo de matemáticamente aceptable y estrictamente riguroso componente probabilístico[60]. Las conclusiones finales de la identificación no son por tanto, el mero resultado de un proceso científico, sino una toma de decisiones que, desde los conocimientos y la experiencia del forense concreto, implica interpretar la información, a veces incompleta, y las evidencias, a veces imperfectas[61]. Según PAGE (ET ALT) la posibilidad de que la misma serie de marcadores aparezca más de una vez en una población debería ser técnicamente cero para que una característica fuera considerada realmente única, siendo así que una característica que se da por universal no parece posible que en puridad llegue a ser única. La probabilidad de observar esa característica ya sola ya en combinación con otras es siempre superior a cero, lo que implica que siempre existe alguna probabilidad –aunque sea pequeña- de que exista un duplicado.

La identificación forense comienza reconociendo que las características físicas de los objetos y los rastros que dejan pueden variar, incluso para el mismo tipo de objetos, pero todas las ciencias forenses adoptan la premisa de la unicidad: que dos objetos no pueden dejar dos marcas indistinguiblemente similares; o lo que es lo mismo, que si dos huellas no pueden distinguirse, debieron ser originadas por el mismo objeto[62]. Pero de cuando en cuando algunas reflexiones recuerdan, a pesar de esa fe en la unicidad, que los criterios para la identificación absoluta son producto de intuiciones probabilísticas, ya sea en la identificación de huellas dactilares, documentos o armas de fuego entre otros. SACKS detalla como en algunos casos se ha llegado ha hablar de la "*falacia de la individualizació*n". La identificación forense, explica, consiste en dos importantes procesos: primero, determinar si las huellas de lo que se cuestiona y lo que se conoce son indistinguiblemente similares; el segundo paso, no menos importante, es evaluar el significado de esa similitud. En la mayoría de las áreas de la identificación forense distinguir entre diferencias reales (inexplicadas) y diferencias artifíciales es algo en lo que no existen guías estándares, dejando un margen de apreciación para determinar la similitud. Pero aún determinada ésta, debe interpretarse lo que ésta significa. Calcular la frecuencia de las

[59] PAGE, M. / TAYLOR, J. / M BLENKIN, M. "Uniqueness in the forensic identification Sciences- -Fact or fiction?", *Forensic Science International* 206 (2011) 12–18

[60] BIEDERMAN, A./ BOZZA, S. / TARONI, F. "Decision theoretic properties of forensic identification: Underlying logic and argumentative implications", *Forensic Science International* 177 (2008), 120–132; CHAMPOD, C. "Identification/individualisation", en J.H. SIEGEL/ P.J. SAUKKO,/ G.C. KNUPFER (Eds.), *Encyclopedia of Forensic Science*, Academic Press,
San Diego, 2000, pp. 1077–1084..

[61] BIEDERMAN, A./ BOZZA, S. / TARONI, F. "Decision theoretic properties of forensic identification: Underlying logic and argumentative implications", *Forensic Science International* 177 (2008), p130.

[62] SACKS, M. J. "Forensic identification: From a faith-based ''Science'' to a scientific science", *Forensic Science International* 201 (2010) 14–17

coincidencia en la población o subpoblación de que se trate, como se hace por ejemplo con los análisis de ADN en que se evalúa la incidencia del polimorfismo en la población. Algunos consideran que cabe deducir la unicidad si la probabilidad de hallar un duplicado se entiende que supera varias veces la magnitud total de la población (o la suma de la población que ha vivido, vive y nacerá). En puridad, ello no determina que el rasgo sea único, porque no garaniza que no pueda producirse una duplicación. Como argumento para defender la existencia de la unicidad, los expertos suelen afirmar que en la historia de sus disciplinas no se han hallado aún dos objetos idénticos, y por ello hay quien indica que aceptar la unicidad conlleva, hasta ciento punto, un cierto acto de fe[63] porque el forense lo que hace es, desde su experiencia, reforzar o debilitar la probabilidad de la identificación[64].

En el caso del sistema de reconocimiento automatizado se da, sin embargo, la circunstancia de que debemos adiestrar por anticipado al sistema, ofreciéndole aquellas referencias con las que reforzará o debilitará la probabilidad de la identificación y sin margen, por lo tanto, de que de la reflexión sobre la comparación de patrones pueda llegar a nuevas conclusiones y nuevas experiencias.

A día de hoy, advierte JAYAPRAKASH, las comparaciones en algunos tipos de patrones están mucho más desarrolladas y validadas que en otras, y aun incluso en los casos más validados (como los de las huellas dactilares) se han producido algunas identificaciones erróneas. Entre los más clamorosos el caso la identificación errónea de un supuesto terrorista de los atentados de Madrid en el IAFIS[65], también conocido como *el fiasco Mayfield.* Mayfield, ciudadano musulmán asentado en Seattle fue detenido sobre la base de una huella latente encontrada en los atentados del 11-M en Madrid; sus huellas, todo hay que decirlo, estaban en la base del FBI porque sivió durante varios años en el ejército de los Estados Unidos. A veces, advertía Cole, el poder de la identificación de las huellas latentes en el juicio descansa en la mágica habilidad de cautivar a los jurados[66].

3.3.2. *La distribución de la variabilidad y la menagerie biométrica*

[63] PAGE, M. / TAYLOR, J. / BLENKIN, M. "Uniqueness in the forensic identification Sciences- -Fact or fiction?", *Forensic Science International* 206 (2011) 12–18
[64] JAYAPRAKASH, P. T. "Practical relevance of pattern uniqueness in forensic science", *Forensic Science International* 231 (2013), pp403e1 – 403e16.
[65] STACEY, R. B. "Report on the erroneous fingerprint individualization in the Madrid train bombing case", *Forensic Sci. Commun.* 1 (2005) 7.
[66] COLE, S. A. "Witnessing Identification: Latent Fingerprinting Evidence and Expert Knowledge", *Social Studies of Science* 28, nº 5/6, Special Issue on Contested Identities: Science, Law and Forensic Pracice (1998), pp687-712; KERSHAW, S. "Spain and US at Odds on Mistaken Terror Arrest", *New York Times*, 5 de junio de 2004.

Todas las características biológicas están sometidas a la variabilidad y ello afecta a la muestra biométrica, a su transformación analógico-digital y a los procesos de comparación[67]. Por ello, y sin dejar de distinguir entre individuos, el sistema debe ser capaz de reconocer que en las muestras biométricas de un mismo sujeto –aunque no sean idénticas- existe una raíz común que lleva a reconocerlas como muestras que pertenecen a un mismo sujeto. Adiestrar a un sistema automatizado para que sea capaz de gestionar adecuadamente esta variabilidad constituye todo un reto, sobre todo en los casos de comparación de patrones *1 a n*.

En el actual estado del arte, se considera que hay suficientes elementos como para considerar que la mayoría de las dimensiones del cuerpo humano tiene una distribución normal (o gaussiana) y en un conjunto de población más o menos homogéneo encontraremos que los valores más probables son los más cercanos a la media y que los valores que se alejan de la media van decreciendo en probabilidad conforme más lejos están de aquella. Si sobre la base de esta idea categorizásemos a los usuarios de un sistema biométrico, encontraríamos que aquello que permite distinguir entre sí "a los que están en la media" es significativamente menor que lo que distingue a este grupo, que esta en la medida, de aquellas personas a los que su Biometría los ha situado en uno de los dos extremos.

En la literatura se emplea una forma muy gráfica para expresar esta situación. DODDINGTON/ YAGER[68] describieron cuatro categorías dentro de los conjuntos de usuarios, apreciando el potencial singularizante que para ellos tenían los sistemas de reconocimiento mediante Biometría vocal (ovejas, cabras, corderos y lobos). Es común referirse a esta propuesta como la *menagerie* biométrica[69] o el *biometric zoo*[70]. Existe un grupo de usuarios, *las ovejas,* que son aquellos que son reconocidos con facilidad por un sistema y resulta poco probable que sean suplantados o rechazados. Es deseable que constituyan el grupo más numeroso de un sistema de reconocimiento. Otro conjunto de usuarios son señalados como *las cabras*; se trata de un grupo de personas que tiene un patrón de datos que queda fuera del rango óptimamente reconocido por el sistema y, en consecuencia, aunque se enrolen legítimamente sufren elevadas tasas de falsos rechazo.

Los corderos, por su parte, son usuarios que el sistema acepta con facilidad pero que resultan excepcionalmente vulnerables a la suplantación de identidad, porque sufren el impacto de

[67] VIELHAUER, C. *Biometric User Authentication for IT Security*, 2006, pp22-24.
[68] DODDINGTON, G. / LIGGETT, W. / MARTIN, A. / PRZYBOCKI, M. / REYNOLDS, D. "Sheep, Goats, Lambs and Wolves", en *A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation*, Int Conf. Spoken Language Processing (ICSLP), Sydney, vol. 4., pp. 1351 - 1354 (1998).
[69] YAGER, N./ DUNSTON,T. "The biometric menagerie", *IEEE transactions on Pattern Analysis*, 2010, pp220-230.
[70] ADLER, A. / SCHUCKERS, S. "Biometric Vulnerabilities", S. Z. LI/ A. K. JAIN, *Encyclopedia of Biometrics*, 2009, p63.

terceros que son aceptados en su lugar. El cuarto y último grupo es el de los lobos, los individuos que son excepcionalmente exitosos en la suplantación de identidad, porque obtienen elevadas tasas de falsa aceptación[71]. Los sistemas se diseñan empleando como diana óptima a las ovejas, pero teniendo en cuenta que es inevitable la existencia del resto de los grupos. Los corderos, cuya Biometría es relativamente más fácil de suplantar, y los lobos, excepcionalmente exitosos en la suplantación, son los individuos que generan mayor vulnerabilidad en un sistema[72], porque a las cabras lo que les sucede es que sufren el inconveniente de ser sistemáticamente rechazados, de quedar fuera, y ello afecta al rendimiento pero no estrictamente a la seguridad de una tecnología de reconocimiento biométrico.

3.3.3. Pero, ¿qué hacemos con este "*zoo*"?

Esta imagen del zoo biométrico, que resulta muy gráfica para explicar la situación, genera en la realidad contextos muy complejos de gestionar. ¿Cómo saber, antes de enrolar a una persona o conforme las vamos enrolando, si serán lobos, ovejas o corderos? ¿Es posible agruparlos claramente en uno de esos conjuntos y, por ejemplo, gestionar diferentes umbrales de tolerancia para cada uno de los casos? Es decir, flexibilizar la tasa de rechazo de las cabras que son tendentes al falso rechazo, y endurecer los umbrales de los fácilmente suplantables corderos para, al mismo tiempo, dificultar que se nos cuelen los lobos entre la manada. Lo cierto es que, no. Que no es posible, La variabilidad no es, para cada persona, un valor estable[73], o al menos el conocimiento de la Antropología física no ha llegado aun hasta el extremo de poder simplificar hasta ese punto la diversidad humana.

Universitat d'Alacant
Universidad de Alicante

El cuerpo humano no es fácilmente biometrizable, dice MAGNET[74]; se refiere, claro está, en la posibilidad de generar identidades a partir de las biometrías obtenidas del cuerpo. Inversiones multimillonarias, apunta, parten de la asunción de que los cuerpos pueden fácilmente ser transformados en códigos binarios y que los datos métricos obtenidos son estables, que el cuerpo es una fuente de información personal inmutable que puede proporcionar datos precisos sobre la identidad de las personas. De algún modo, se presume que los mapas binarios de los cuerpos expresan "verdades corporales" que reflejan la identidad esencial, nuclear de un ser humano[75]. Pero la eficiencia de los sistemas de reconocimiento biométrico necesita, de algún modo, un soporte científico que la ciencia, a día de hoy, no le puede proporcionar.

---

[71] DUNSTONE, T. /YAGER, N. *Biometric system and Data Analysis*, Springer, 2009, p116.
[72] ADLER, A./ SCHUCKERS, S. "Biometric Vulnerabilities", S. Z. LI/ A. K. JAIN, *Encyclopedia of Biometrics*, 2009, p63.
[73] POPESCU-BODORIN, N./ BALAS, V. E. /MOTOC, I. M. *The Biometric Menagerie – A Fuzzy and Inconsistent Concepto, 5th Int Conf Soft Computing and Applications,* 2012, pp1-9.
[74] MAGNET, S. A. *When Biometrics Fail. Gender, Race and Technology of Identity,* Duke UP; 2011, p2
[75] HARAWAY, 1997, 147; MAGNET, S. *When Biometrics Fail*, 2011, p4.

Empleando únicamente la referencia de las medidas antropométricas, sabemos que factores genéticos, alimenticios y ambientales inciden en las características físicas de los grupos de población y en las diferencias que hay entre unos grupos y otros. Pero no existe una fórmula matemática que recoja o exprese este modelo de interacción. Así, aunque conocer la procedencia y composición de la muestra de población para la que se ha de diseñar el sistema de reconocimiento concreto pueda ayudar a fijar, por ejemplo, los rangos dentro de los cuáles estarán las medidas a tomar, gestionar adecuadamente la variabilidad necesitaría –como punto de partida- un profundo estudio antropológico, pausado, no ya de la variabilidad entre poblaciones sino la diversidad de las personas destinatarias del sistema de reconocimiento respecto de un rasgo concreto.

Los sistemas, sin embargo, no se están creando así. Lo más frecuente es ir enrolando personas y, como mucho, realizar *test de* independencia (1 a n) que, antes de enrolar cada nuevo patrón, nos indican si es suficientemente diferente respecto de los ya almacenados. Siendo valioso este mecanismo, no excluye los problemas que por el parecido de los patrones puedan producirse a futuro. Otra peculiaridad de los sistemas que están en activo, muy criticada, es que muchos de ellos han sido diseñados para funcionar de forma óptima con determinados prototipos de persona. Estos sujetos diana son, a veces, las poblaciones de inmigrantes más frecuentes[76]; los perfiles que se consideran más frecuentes en determinados tipos de terrorismo o delincuencia; o el prototipo de oficial militar o de viajero VIP en las aerolíneas. Como veremos esto tiene, además, implicaciones desde el punto de vista ético social.

Universitat d'Alacant
Universidad de Alicante

3.4. Limitaciones que afectan a la permanencia (o estabilidad) de las características biométricas.

Ninguna característica biológica es permanente en términos absolutos. El modo en que se entiende la permanencia como cualidad de la información que sirve de base a un sistema de reconocimiento biométrico no coincide con el modo en que ese término se interpreta en el lenguaje común: *que se mantiene sin mutación en un mismo lugar, estado o calidad*[77]. Es importante, por ello, hallar formas para flexibilizar los sistemas de reconocimiento y garantizar que a pesar de las variaciones en un conjunto de muestras, sea posible determinar adecuadamente si todas ellas tienen o no una raíz común que permite afirmar que provienen de un mismo sujeto fuente[78].

---

[76] RAZACK, S. *Casting Out: The eviction of Muslims from Western Law and Politics*, 2008, Univ Toronto Press, 2008.
[77] Diccionario de la RAE, 24ª edición, de octubre de 2014. Consultado en www.rae.es
[78] LANITIS, A. "A survey of the effects of aging on biometric identity verification", *International Journal of Biometrics*, 2 (1), 2010, pp34-52.

En algunos casos la estabilidad de una característica biométrica se ve afectada por una enfermedad, y esa afectación puede ser temporal o definitiva. En otros casos, los cambios se deben al impacto que el paso del tiempo tiene en la evolución del cuerpo de una persona (el desarrollo y el envejecimiento), impacto que cabe apreciar tanto en las biometrías dinámicas como en las estáticas.

3.4.1 *Deterioro temporal o definitivo de algunas características biométricas, por enfermedad.*

En algunos puestos de trabajo las manos están expuestas a productos o tareas que afectan a las huellas dactilares[79] y existen además enfermedades de la piel que les afectan temporal o definitivamente[80]. Asimismo algunas enfermedades de la piel tienen influencia en el reconocimiento dactilar. DRAHANSKY/ DOLEZEL/ URBANEK/ ET ALTERE clasifican estas enfermedades en tres grupos y las catalogan fotográficamente[81]: 1) enfermedades comunes (como, por ejemplo) eccemas, herpes simple, tiña, lepra, fenómeno de Raynauds, esclerosis sistémica o reacciones a algunos fármacos); 2) enfermedades decolorantes (como el virus mano-boca-pie, la escarlatina o la sífilis secundaria); y 3) enfermedades que causan histopatologías en la unión entre la epidermis y la dermis (como las formas crónicas de eccemas, verrugas WARTS o epidermolysis bullosa). Vid. en la IMAGEN 72, algunas de esas enfermedades y de sus efectos en las impresiones dactilares.

La ceguera o las limitaciones visuales, incluso las temporales, dificultan ofrecer posiciones optimas a los sistemas de captura, del mismo modo que los resfriados, laringitis y afonías más o menos severas, efectos del alcohol o de la anestesia dental y obstrucciones orales afectan a la voz[82]. También son relativamente frecuentes las contusiones o inflamaciones, por no hablar de vendajes u otro tipo de productos sanitarios que puedan afectar temporalmente al rostro o a las manos. ¿Cuál es la incidencia de este tipo de afectaciones temporales? ¿contamos con índices de impacto que nos permitan corregir los problemas que pueden plantearse en el reconocimiento de las personas? ¿Sabemos, si acaso, cuál sería la incidencia de este tipo de problemas? Por ejemplo, por una circunstancia temporal de estas característcias, ¿cuántas personas podrían ver hipotéticamente restringido su derecho de sufragio por tener dañados sus dermatoglifos el día de la convocatoria electoral?

3.4.2 *Permanencia de la información biométrica y envejecimiento de los patrones*

[79] UK BIOMETRICS WORKING GROUP, 2002; MAGNET, S. *When biometrics fail*, 2011, p30.
[80] Bioidentification 2007.
[81] DRAHANSKY, M./ DOLEZEL, M./ URBANEK, J./ ET ALTERE, "Influence of Skin Diseases on Fingerpring Recognition", *Journal of Biomedicine and Biotechnology*, vol. 2012. ID 626148.
[82] POLEMI, D. 1997, p27.

La expresión envejecimiento se usa en relación con las tecnologías biométricas en dos sentidos. De una parte, en relación con el modo en el que la edad absoluta de los sujetos fuente tiene impacto en el rendimiento de un sistema. De otra, para atender al hecho de que los sistemas de reconocimiento biométrico se enfrentan, inevitablemente, a un factor crítico: el lapso de tiempo –más o menos extenso- que separa el momento del enrolamiento y el momento (o momentos) en los que el sujeto presentará una nueva muestra biométrica en fresco al sistema, solicitando su re-identificación. El impacto de la edad absoluta en el rendimiento de los sistemas es un elemento que ha de tenerse en cuenta cuando el rango de edades comprendidas en el grupo de sujetos diana es muy diverso. Conocer y registrar de algún modo la edad absoluta de los sujetos fuente puede tener, además de importante utilidad práctica, numerosas ventajas de cara a la mejora de la eficiencia del servicio que se presta[83]. Las huellas dactilares se vuelven más finas y la capacidad del iris de adaptarse a diferentes niveles de luz incidental decrece y, en ese sentido, que el sistema disponga de información relativa a la edad absoluta de un sistema incorporaría un elemento más en el proceso de toma de decisiones. Además, la edad también puede afectar a la mayor o menor facilidad que los sujetos tienen para usar los dispositivos[84]. La referencia de la edad absoluta permitiría, por ejemplo, establecer algún tipo de flexibilización para estos sujetos sin necesidad de extenderla para todo el conjunto.

En el segundo de los sentidos, la gestión adecuada del lapso de tiempo que mediará entre el enrolamiento y capturas de la muestra biométrica que se produzcan en el futuro resulta clave para garantizar que un sistema de estas características –en muchos casos de un elevado coste económico- pueda mantenerse en funcionamiento en un periodo de tiempo que justifique la inversión. El modo en que el envejecimiento afecta a las diferentes características biométricas difiere en intensidad, algo que lleva a hablar de sistemas biométricos más o menos sensibles al envejecimiento, aunque el único rasgo del que se predica la permanencia es el ADN. Los sistemas que se han diseñado sobre la base de otro tipo de muestras biométricas han de afrentar, de algún modo, la situación. Algunos sistemas, por ejemplo, han previsto una actualización de los patrones cada cierto tiempo; es decir que, con el objetivo de dar respuesta al amplio lapso de tiempo que puede transcurrir entre el enrolamiento y la nueva obtención en fresco, lo que hacen es evitar que ese lapso de tiempo llegue a ser excesivamente amplio. Pero este mecanismo, nótese, no termina de encarar el impacto del envejecimiento y, además, puede que el enrolamiento reiterado no sea una opción posible –o razonable- para todos los sistemas de reconocimiento biométrico[85]. De ahí que algunas investigaciones concentren su esfuerzo en desentrañar los procesos de

[83] FAIRHURST, M./ ERBILEK, M. "Analysis of physical ageing effects in iris biometrics", *Computer Vision*, vol. 5, 2011, pp358-366.
[84] SASSE/ KROL, *Usable biometrics for an ageing population*, en M. Fairhurst (ed.), *Age Factors in Biometric Processing*, 2014, p303.
[85] MORDINI/ REBERA, "Biometrics and Ageing", 2013, p41.

envejecimiento y formular éstos en un modo que puedan emplearse como *factores de* impacto, de cara a insertarlos entre las variables que los sistemas de reconocimiento mediante Biometría tienen en cuenta en sus tomas de decisiones.

¿Es realmente posible ofrecer una fórmula que recoja el *impacto del envejecimiento*? En comparación con la incidencia de las enfermedades que afectan a las características biométricas de referencia y cuyo impacto concreto en el conjunto de los sujetos diana puede ser muy complejo de calibrar, algunos expertos que sí sería posible formular, de algún modo, el factor (o los factores) de impacto del envejecimiento. Invita a pensar así el hecho de que se trata de un proceso esperable en todos los sujetos y que se traduce en una serie de cambios progresivos y graduales, con un cierto grado de universalidad. Así, y aun cuando aunque las expresiones concretas de este proceso muestren una alta variabilidad según la persona, la hipótesis de muchas investigaciones es que del estudio de la variabilidad en los procesos de envejecimiento será posible expresar, de algún modo, aquellos cambios que se consideran *esperables*[86].

En el campo del reconocimiento mediante Biometría el problema del envejecimiento no había recibido una excesiva atención, al menos en comparación con las dificultades que planteaban otro tipo de variaciones[87]. Téngase en cuenta que en las primeras décadas de desarrollo de estas tecnologías muchos de los esfuerzos se habían venido concentrando en el reto de captar automatizadamente la singularidad –como primer paso imprescindible para poner en marcha un sistema de este tipo. A partir de 2009 encontramos ya los resultados de algunas investigaciones específicamente orientadas, por ejemplo, a: la reducción de los efectos del envejecimiento respecto de los patrones[88]; a la cuantificación de los efectos del envejecimiento en determinados atributos concretos[89] ; o a la simulación de los efectos del envejecimiento, con la finalidad de generar modelos para una adecuada gestión del impacto de la edad[90]. Los datos para dichos estudios se obtuvieron de diferentes fuentes. Existen, de una parte, bases y colecciones de datos creadas con fines biomédicos –entre otros para investigaciones relativas a la cirugía plástica o la investigación forense- y que resultan de utilidad para la realización de investigaciones que persiguen la mejora de la eficiencia de los sistemas de reconocimiento biométrico, aunque –por la

[86] MARCIALIS, G./ RATTANI, A./ ROLI, F. "Biometric template update: An experimental investigacion on the relationship", en N. DA VITORIA/ T. KASPARIS (eds.), *Structural, Syntactic and Statistical Pattern Recognition*, Springer, 2008, pp684-693.
[87] LANITIS, A./ TSAPATSOULIS, N. "Quantitative evaluation of the effects of aging on biometric templates", *IET Computer Vision Journal, Special Issue on Future Trends in Biometric Processing*, vol 5, issue 6, pp228-347.
[88] RATTANI, A./ FRENI, B./ MARCIALIS, G./ ROLI, F. "Template update methods in adaptative biometric systems: A critical review", Advances in Biomerics, vol LNCS 5558, 2009, pp847-858; ULUDAG, U. / ROSS, A. / JAIN, A. K. "Biometric template selection and update: a case study in fingreprints", Pattern Recognition, vol 31, nº 7, 2004, pp1533-1542.
[89] ORTEGA, M. / BRODO, L. / M. BICEGO, M. / TISTARELLI, M. "Measuring changes in face appearance through aging", *Computer Vision and Pattern Recognition Workshops*, Florida, 2009, pp107-113.
[90] El libro colectivo, coordinado por FAIRHURST,M. *Age Factors in Biometric Processing*, 2014; LANITIS, A. "A survey of the effects of aging on biometric identity verification", *International Journal of Biometrics*, 2 (1), 2010, pp34-52.

finalidad con la que fueron concebidas- no pueden servir de soporte a todos los aspectos que necesitan estudiar las investigaciones sobre el impacto del envejecimiento en los sistemas de reconocimiento biométrico. Así, por ejemplo, algunas de estas bases de datos contienen una única muestra de cada sujeto, en el sentido de no hacen seguimientos individualizados de los procesos de envejecimiento, o como mucho los siguen en espacios de seis a dieciocho meses[91]; además, de media suelen tener una distribución que se concentra entre los 18 y los 60 ó 65 años. Faltan, en consecuencia, resultados de investigación que abarquen las franjas de edades no cubiertas y, sobre todo, que hagan un mayor seguimiento individualizado de los procesos de envejecimiento en los diferentes sujetos. De esos enfoques se han ocupado bases de datos como datos MORPH y FG-NET, específicamente creadas en el ámbito de algunas técnicas de reconocimiento biométrico en concreto, y para comparar desde diferentes perspectivas –incluyendo la edad- la solidez de los algoritmos empleados por algunas tecnologías de reconocimiento biométrico. Otros ejemplos de bases de datos son BIOMET, BIOSECURE, BiosecurID o POLYBIO[92].

El iris es considerado una de las fuentes biométricas actuales que mejor resiste el paso del tiempo y, como respaldo, se recuerda en ocasiones el test mediante el que Jonh Daughman determinó en 2002 cuál de las mujeres que alegaban ser la niña afgana que apareció en la portada *National Geographic* lo era realmente. No existen, sin embargo, estudios que aporten criterios suficientes como para abordar los cambios que como consecuencia de la edad se producen en el color del iris. Como es sabido, con el tiempo el iris se va haciendo más difuso en algunas personas y suele aparecer la opacidad anular que se conoce arco senil o geróntoxon. Y tampoco se han determinado posibles soluciones a la dificultad que algunas personas de avanzada tienen para interactuar con los interfaces que captan el iris[93].

Más notables son, en cualquier caso, los efectos del envejecimiento en el rostro de la persona o en biometrías dinámicas como la voz, la marcha o las señales electrofisiológicas. Entre la infancia y el comienzo de la etapa adulta se producen en el rostro numerosos cambios ocasionados por el crecimiento y el desarrollo craneofacial que han sido descritos en diferentes grupos de población[94], señalando además algunas diferencias que entre hombres y mujeres se producen en la adolescencia (especialmente en la nariz y las mandíbula). Al nacer la longitud del cráneo tiene entre un 60% y un 75% del tamaño final, alcanzando a los 5 años un 90%. Durante ese tiempo los huesos de la cara se agrandan de forma relevante, pero ese crecimiento continuará aún después.

[91] FAIRHURST, M. "Review of ageing with respect to biometrics and diverse modalities", en M. FAIRHURST (ed.), *Ageing* 2014, pp19-20.
[92] FAIRHURST, M. *Review*, cit, pp20-21.
[93] LIU-JIMENEZ, J. / R. SANCHEZ-REILLO,R. "Ageing in iris biometrics", *Age Factors*, 2014, p149.
[94] TAYLOR, K. "Age progression: Growth," en K. T. TAYLOR (ED.) *Forensic Art and Illustration*, Boca Raton, pp235-249

La etapa adulta no se caracteriza por un crecimiento en la estructura facial, aunque sí se producen otros cambios concernientes al tejido blando del rostro, así como a la apariencia que este tejido va adoptando conforme avanza la edad del individuo (con la aparición de arrugas, pliegues y demás en las alas nasales, los ángulos de la boca, en la línea de los ojos, etc.). Inciden en ello tanto factores biológicos como factores ambientales que llevan a una degradación de los tejidos (especialmente de la piel)[95].

En el período de la senescencia, los rasgos faciales vuelven a modificarse por procesos tales como la pérdida de tono muscular o la aparición de manchas, y la nariz se puede ver más prominente. RICANEK/ MAHALIGAM ET ALTERE describen también tres tipos de anomalías faciales que aparecen en la edad adulta[96]: asimetrías (causadas, por ejemplo, por plagiocefalia deformante o plagiocefalia sinostósica, atrofia hemifacial o hamartomas o malformaciones vasculares en el rostro)[97]; fotoenvejecimiento extremo; y desviaciones en el aspecto de gemelos idénticos ocasionadas por la exposición al sol, el consumo de tabaco o la depresión, entre otros. Se afirma así que la proporciones del rostro no son características absolutas y los atributos del rostro son dinámicos y mutan con cierta facilidad como consecuencia de factores físicos (edad, peso, lesión, enfermedad) o extrínsecos (iluminación, ángulos, distancias respecto a la cámara)[98].

La voz humana, por su parte, sufre sus más importantes transformaciones en los primeros 20 años de vida, hasta que los tejidos de la laringe y las cuerdas vocales maduran, y a partir de aproximadamente los 60 años de edad (por cambios en el sistema subglotal, menor flexibilidad en el tórax y debilitamiento de la contracción muscular en la respiración)[99].

Universitat d'Alacant
Universidad de Alicante

3.5. ¿Cómo tener en cuenta estas limitaciones?

A la vista de los resultados recogidos en este epígrafe, creemos importante destacar una circunstancia que, con frecuencia –y como veremos especialmente en el capítulo siguiente- se pasa por alto a la hora de enjuiciar la la conveniencia o no de emplear una tecnología de reconocimiento biométrica concreta en determinado escenario operativo. La vinculación del

---

[95] FILLIT, H. M. / ROCKWOOD, K. / WOODHOUSE, K. "Ageing and the skin", *Brocklehurst Textbook of geriatric Medicine and Gerontology*, 7ª ed, Elsevier, 2010, pp133-136.
[96]RICANEK, K. / MAHALIGAM, G. / MIDORI, A. / VORDER, R. W. "Human face ageing: a perspective analysis from anthropometry and biometrics", M. FAIRHURST (ed.), *Age Factors*, pp93ss.
[97] Muy detalladamente SANDOR, G. K./ MCGUIRE, T. P./ YLINKONTIOLA, L. P./ SERLO, W. S./ PIRTTINIEMI, P. M. "Management of facial asymmetry", *Oral and Maxillofaxial Surgery of Clinics of North America*, 2007, 19, pp395-422.

[98] MORETON, R. / MORLEY, J. "Investigation into the use of photoanthropometry in facial image comparison", *Forensic Science International* 212 (2011) 232.
[99] LINVILLE, S. E. "The aging voice", The ASHA Leader, 9 819), 2004, pp12-21.

reconocimiento con el cuerpo de las personas contribuye, sin duda, al aura mítica de las tecnologías de reconocimiento biométrico, alimentando su mito con la afirmación de que, además, se sostienen en apariencia sobre una serie de sólidos pilares. Entre ellos la universalidad, la singularidad y la permanencia.

Se obvia, sin embargo, la principal de las premisas. Y es que lo que los cuerpos de las personas tienen de común y de diverso no es, ni con mucho, tan fácil de captar. En esa expresión de *casi perfecta*, hay un casi incierto al que ha de prestarse una grandísima atención: el *casi.* Aun aceptado que todas estas tecnologías necesitan interpretar de forma *flexible* la universalidad, singularidad y permanencia de las características biométricas, porque no puede ser de otro modo, antes de aceptar el uso social de un sistema de este tipo hemos de preguntar, en detalle, qué es lo que, en concreto, entienden como *flexible* y hasta que punto es flexibilidad afectará a la eficiencia y a la fiabilidad de los sistemas, y con qué consecuencias. Esto es, cuántas serán y qué sucederá con las personas *atípicas* para el sistema (los *outlier*) que circunstancialmente o permanentemente no puedan ser adecuadamente identificadas por quedar en el limbo que no cubren esa casi-universalidad, casi-singularidad y casi-permanencia.

4. LAS LIMITACIONES Y LOS RIESGOS DE LA IDENTIFICACIÓN BIOMÉTRICA CONFORME AL ESTADO ACTUAL DE LA CIENCIA Y LA TECNOLOGÍA (II). LIMITACIONES RELATIVAS A LA ARQUITECTURA DE LOS SISTEMAS AUTOMATIZADOS DE RECONOCIMIENTO MEDIANTE BIOMETRÍA.

La arquitectura de los sistemas de reconocimiento se determina con el objetivo de satisfacer al máximo parámetros como la precisión, el rendimiento y la seguridad[100]. La satisfacción de dichos parámetros, sin embargo, se interpreta también, como en el caso de lo que acabamos de ver en relación con las bases científicas de los sistemas, con un cierto margen de flexibilidad[101]. Como advierten KISKU/ GUPTA (pag. xix), incluso escogiendo los algoritmos más óptimos (esto es, algoritmos que den una respuesta adecuada a la necesidad de captar la singularidad de la muestra) [102], acciones como la mejora de las imágenes, la extracción de los atributos, la comparación y la toma de decisiones constituyen elementos críticos en todos los sistemas de reconocimiento biométrico. Comenzando, por ejemplo, por la precisión, explicábamos al presentar las utilidades que pueden ofrecer que los sistemas de reconocimiento mediante Biometría pueden cometer varios tipos de error; entre ellos, por su trascendencia en el servicio final que prestan los sistemas de reconocimiento, están: los errores de falsa aceptación o falso hallazgo de identidad, y los errores de falso rechazo o falsa declaración de no coincidencia. Desde

[100] JAIN, A. K. / NANDAKUMAR, K., *Biometric System Desing.Overview*, S. Z. Li/ A. K. Jain, *Encyclopedia of Biometrics, Springer*, consultada la edición de 2009, pp135-13.
[101] MALTONI/ MAIO/ JAIN/ PRABHAKAR, *Handbook Fingerprint*, 2009, pp11-22.
[102] PFAFFENBERGER, B. *Que's Computer and Internet Dictionary*, Que, 1995, p15; B. PRENEEL, *An Introduction to Modern Cryptology*, junio de 2007, pp19-25.

el punto de vista de la gestión de la base científica del sistema, si la variabilidad intra-clase de la característica que se ha tomado como referencia es elevada (o lo es, al menos, en relación con los atributos seleccionados y el patrón que se ha configurado), en ese caso cabe la posibilidad de que un usuario no sea adecuadamente re-identificado por el sistema. Y si la variabilidad intra-clase de los patrones almacenados es baja sucederá, por el contrario, que es posible que el sistema acepte como usuario legítimo a uno que no lo es, o confunda a dos usuarios entre sí. Pero claro, habremos de tener también en cuenta qué posibilidades hay de que el sistema no capte una imagen óptima, de que no la encuadre bien a la hora de extraer los atributos, de que no capte la singularidad de la muestra o que, al comparar, tome una decisión claramente inadecuada. Estos y otros riesgos forman parte de los *fallos intrínsecos del sistema*. A ellos añadiremos los problemas que se plantean por la seguridad informática de los sistemas de reconocimiento biométrico, toda vez que la casi perfección en términos de soporte científico de poco podrá servir si nuestro sistema no capta que la huella que se le expone en fresco es de un dedo de silicona, o es posible hackearlo de forma tal que nos reconozca como alguien que no somos.

4.1 Fallos intrínsecos de los sistemas

4.1.1. Seguridad y fiabilidad de los sistemas, ¿versus tiempo y negocio?

La evidencia singularizante que haya podido obtenerse de un individuo no garantiza al 100% un proceso de reconocimiento preciso. Incluso seleccionando los algoritmos adecuados para mejorar la imagen, la extracción de atributos, la clasificación de los patrones, la comparación y la toma de decisiones son críticos[103]. Se trabaja por ello en la mejora de los estándares y paradigmas algorítmicos de los sistemas, en nuevas técnicas de extracción de atributos, en la mejora de los sensores o en la combinación multimodal de sistemas. En contra de este esfuerzo juega también un elemento clave para los gestores de los controles de identidad: el tiempo. Y es que junto con la *fiabilidad* se espera –o al menos se predica- la agilidad de los sistemas de reconocimiento biométrico. Los sistemas deben comparar la muestra en fresco (en unos casos *1 a 1*, en otros *1 a n*) y tomar una decisión a gran velocidad, en ocasiones en apenas unos segundos.

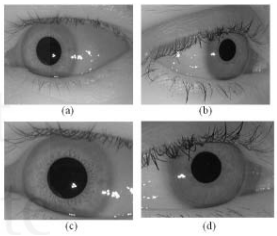
Como consecuencia de ello, se miran con mucho detenimiento aquellas mejoras que, aunque puedan contribuir a la seguridad, puedan también implicar que se necesita más tiempo para proceder a la verificación o identificación de las personas. Criticas también aquellas propuestas que se traducen en que las personas deban ser adiestradas para interactuar adecuadamente con los interfaces para que estos sean eficaces, o que impliquen que los sistemas de captura han de

[103] KISKU, D. R. / GUPTA, P. / SING, J. K. *Advances in Biometrics for Secure Human Authentication*, 2014, pxix.

situarse en entornos controlados[104]; este tipo de mejoras técnicas, nótese, mejoran el rendimiento del sistema en términos de fiabilidad pero reducen sus posibilidades de aplicación en escenarios operativos abiertos y no controlados, esto es, en la mayoría de los escenarios en los que las personas se mueven cotidianamente y sobre los que se calcula el mayor margen para el llamado *negocio biométrico*.

4.1.2. Los fallos intrínsecos en la captación en fresco

Decíamos que el ámbito o umbral de tolerancia puede definirse como aquél margen en el que un sistema biométrico concreto puede reconocer erróneamente que el patrón inicialmente obtenido de la muestra biométrica en crudo y con el que se realizó el enrolamiento, coincide con el patrón obtenido de la muestra en fresco en el proceso de reconocimiento posterior[105]. Este umbral de tolerancia no sólo atiende a la flexibilidad desde una perspectiva de la base científica de los sistemas, sino que también calcula un margen para lo que se conoce como fallo intrínseco. Previsiblemente se producirán falsas aceptaciones y falsos rechazos o, en los sistemas de identificación, falsas coincidencias o falsas no-coincidencias. Véamse las IMÁGENES 64 y 65.



Tales variaciones intra-usuario pueden deberse, por ejemplo, a una inadecuada interacción entre el usuario y el dispositivo de captación por una postura inadecuada. En la IMAGEN de la derecha (además de la IMAGEN 66 del anexo), por ejemplo, puede verse cómo la persona no ofrece al dispositivo de captura un ángulo adecuado y éste no es capaz de obtener el patrón de su iris[106]. ¿Qué hará el sistema? Imaginese la escena en la que una persona muestra el iris a un dispositivo de captación, con la esperanza de que le de acceso aun recinto de un edificio. Un sistema muy básico puede que, simplemente, opte entre abrirle la puerta o mantener ésta cerrada. "*¿Por qué no me abre?* "–pensará la persona usuaria. "No ha leído bien mi iris, está sucia la lente, el técnico no me ha dado acceso a este recinto… ¿qué será?". Obviamente el hecho de que el sistema pueda ofrecer información sobre la fase del reconocimiento en la que se ha producido la circunstancia que da lugar al *non match* permitiría a esta persona solucionar la situación y conseguir que la puerta se abra.

---

[104] JAIN, A. K./ NANDAKUMAR, K. *Biometric System Desing.Overview*, S. Z. LI/ A. K. JAIN, *Encyclopedia of Biometrics, Springer*, consultada la edición de 2009, pp135-136.
[105] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, Biometrie, RFA, 2005, p4.
[106] LI, X. "Modeling Intra-class variation for Nonideal iris recognition", en D. ZHANG/ A. K JAIN, eds, ICB 2006, LNCS 3832, pp419-427, 2005. *Nonideal iris images* es la expresión que se emplea para referirse a las imágenes en las que el ángulo o la posición del iris varia en altura o dirección.

Factores como un usuario mal adiestrado[107] o distorsiones generadas por el "ruido" en el dispositivo de captación (es el caso de una huella residual que ha quedado en el lector de huellas dactilares, por ejemplo)[108] propician los fallos intrínsecos. También las condiciones ambientales adversas, que tienen efectos tanto en los sensores y dispositivos de captación como en la Biometría que se muestra a éstos (manos sudorosas por el calor, ojos hinchados,…). La iluminación, los gestos, el maquillaje, los postizos, las gafas o la falta de colaboración de los sujetos han de sumarse a los parecidos físicos e incluso a los problemas que plantean pequeños cambios en los ángulos o distancia de la captación de las imágenes[109].

4.1.3 Fallos intrínsecos en la digitalización o elaboración de los patrones, ya sea en el enrolamiento ya en la captación en fresco.

La digitalización no es un proceso neutral[110]. Fragmentar los rasgos de identidad, escoger los que se estiman más singularizantes y digitalizarlos es un proceso racional que implica tomar multitud de decisiones. Dichas decisiones, sumadas a la base científica de referencia en el sistema[111], serán determinantes en lo que se conoce como ámbito de tolerancia de un sistema y tasas de error. También es posible que el vector que se ha creado o el patrón elaborado a partir de éste no hayan acertado a captar la individualidad de la característica biométrica de una persona[112] o que sea la infraestructura empleada la que no lo permite[113]. En poblaciones relativamente pequeñas y entornos controlados los estándares de verificación se elevan[114], pero en otro tipo de escenarios la aparición de *dobles* (o gemelos) biométricos aumenta significativamente[115].

---

107 PIECHULECK, A."Empfehlung für Unternehmen zum Schutz personenbezogener biometrischer Daten", *Workshhop IT-Sicherheitsmanagement*, 2008, p8-9; EUROPEAN COMMISSION (ED.), *Biometrics in Europe. Trend Report*, UNISYS – European Biometrics Portal, 2007, pp22-23; MASEK, L. *Recognition of Human Iris Pattenrs for Biometric Identification*, School of Computer Science and Software Engineering, The University of Western Australia, *2003*, pp13-16.

108 KISKU, D. R. / GUPTA, P. / SING, J. K. *Advances in Biometrics for Secure Human Authentication and Recognition*, CRC press, 2014, pp9-10.

109 HEUMANN, B. *Whitepaper Biometrie*, www.biometrie-online.de, 2006, p9-10; LANGENDERFER, J. / LINNHOFF, S. "The Emergence of Biometrics", *Journal of Consumer affairs*, vol 39, nº 2, 2005, págs. 315ss; BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK - BSI, *BioFAce. Comparative Study of Facial Recognition Systems*, 2003.

110 GHILARDI, G. / KELLER, F. "Epistemological Foundations of Biometrics", en E. MORDINI/ D. TZOVARAS (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp23 y ss, 24-25

111 Vid. lo ya dicho en III.1.1. *La base científica del sistema: la fuente de los datos, el método de captación y el grupo de población de referencia.*

112 JAIN, A. K./ BOLLE, R/ PANKANTI, S.: *Personal Identification in Networked Society*, Kluwer, 1999, pp22 y ss; IPTS – Institute for Prospective Technological Studies, *Biometrics at the Frontiers*, cit., 2005, doc EUR 21585, pp32-34; MARTÍNEZ JARRETA, M. B. voz "*Biometría*", C. M. ROMEO CASABONA (dir.), *Enciclopedia de Bioderecho y Bioética*, vol I, Comares, 2011, pp257-261; R. CLARKE, "Human Identification in Information Systems", ITP 1994/4, pp7-8.

113 SHONIREGUN, C./ CROSIER, S. *Securing Biometrics Applications*, 2007, p37.

114 INTRONA, L. D. / NISSENBAUM, H, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, The Centre for Catastrophe Preparedness and Response, 2009; ELLERBROK, A., "Playful biometrics: Controversial Technologt through the Lens of Play", *The Sociological Quarterly* 52 (2011), pp528-547, p529.

115 JAIN, A. K./ NANKUMAR, K. / NAGAR, A. *"Biometric Template Security", EURASIP Journal onf Advances in Signal Processing* 2008, pp1-17; A. K. Jain/ A. Kumar, "Biometrics of Next Generation: an Overview", en E. Mordini/ D. Tzovaras (eds.), *Second Generation Biometrics*, Springer, Heidelberg, 2010; IRWIN, J. O., "Biometric method: past, present, future", *Biometrics*, cit., pp363-365, p363.

Algunas formas de afrontar estos problemas son el empleo de sistemas multimodales (que captan varios rasgos por cada persona) o emplear test de independencia que antes de cada nuevo enrolamiento comprueben que el sistema no ha enrolado ya algún patrón idéntico o excesivamente similar.

A este respecto el umbral de tolerancia a calcular es el margen que expresará la distancia que puede haber entre el patrón inicialmente obtenido y el que se crea en fresco. Inciden –como hemos visto en el apartado anterior- limitaciones en lo que se refiere a la base científica de los sistemas (incidencia de la enfermedad o del envejecimiento), pero también las diferencias en las circunstancias en que se producen, de una parte, el enrolamiento y de otra la captación de la muestra en fresco, o el acierto diseñar una arquitectura de hardware y software capaz de captar la singularidad biométrica de una persona y de traducirla a un patrón digital eficiente.

4.2. Problemas de seguridad de los sistemas

4. 2.1. *Ataques al nivel del sensor (o captación del dato en fresco en la identificación secundaria)*

Como cualquier otro sistema informático, los sistemas de reconocimiento mediante Biometría pueden ser objeto de ataques externos en diferentes puntos de su infraestructura o en diferentes momentos de su funcionamiento; son sistemas vulnerables. Además de las vulnerabilidades que tienen otros sistemas automatizados con funciones similares –esto es, con funciones de identificación o de verificación- estos sistemas tienen unas vulnerabilidades propias, especialmente en el ámbito de un reconocimiento incorrecto o del fallo en el reconocimiento correcto de un individuo[116].

A nivel de sensor es posible un ataque mostrando una *Biometría falsa*. Por ejemplo, tratando de suplantar las huellas de alguien mediante una simulación en silicona de su dedo; o, también se ha dado el caso, mostrando al dispositivo de captación una fotografía del iris de alguien. Véase la IMAGEN 63, con algunos ejemplos. Esta posibilidad de que un tercero capte información corporal de la que inevitablemente llevamos expuesta es señalada, de hecho, como una de las mayores debilidades de los sistemas de reconocimiento biométrico. Piénsese, por ejemplo, que nuestras huellas quedan en todo los objetos que tocamos a lo largo del día. Como muestra de esta vulnerabilidad, el *Chaos Computer Club* generó en Alemania un debate sobre la idoneidad de los datos biométricos para garantizar los niveles de seguridad que se les asocian. Y lo hizo de forma muy provocativa. Ofreció un álbum para "coleccionar huellas dactilares de famosos", y en la

[116] ADLER, A. / SCHUCKERS, S. "Biometric Vulnerabilities", *Encylopedia of Biometrics*, 2009, pp160-161.

primera entrega publicó, entre otras, las huellas del entonces ministro alemán de interior, Wolfgang Shäube[117]. Con ello quiso llamar la atención sobre el riesgo de emplear un tipo de identificación, la biométrica, cuyo *password* podemos ir dejando en todo lo que tocamos (vid. IMAGEN 67).

Si los sistemas no cuentan con elementos para detectar este tipo de fraudes, procesarán estas muestras en fresco como muestras originales y, previsiblemente, serán incapaces de darse cuenta de la suplantación de identidad. La expansión de los sistemas de control biométrico, especialmente en el control de los movimientos transfronterizos de las personas, está propiciando que las personas busquen alternativas para sortearlos, dañándose las huellas o trasplantándose éstas (cambiando, por ejemplo, las de una mano a otra) pagando en muchos casos elevadísimas cantidades a las mafias que se enriquecen con todo tipo de fórmulas de fomento del tráfico ilegal de las personas. Las tecnologías biométricas de segunda generación han desarrollado algunos dispositivos complementarios que tratan de captar este tipo de circunstancias e incluyen no sólo la simulación y/o fabricación de rasgos biométricos, sino también las modificaciones por cirugía. DAUGHMAN ha desarrollado varias propuestas para detectar el falseamiento de las muestras de iris –por ejemplo, con base en la longitud de las ondas que ofrecen los tejidos vivos a la iluminación infrarroja, y frente a la falsificación de huellas dactilares se han desarrollado también diferentes propuestas, como la medicin de las tasas de oxigeno en sangre o el análisis de distorsiones en la piel[118].

Universitat d'Alacant
Universidad de Alicante

4.2.2. *Ataques a nivel de los módulos de procesamiento y ataques en los módulos no biométricos*

Más complejos de atajar son los ataques que replican datos antiguos. Es decir que sin mostrar una nueva Biometría al sistema, saltándose al sensor, se consiguen cargar o simplemente activar en el sistema datos antiguos (haciéndole creer que tiene ante sí, en fresco, un patrón idéntico a uno ya almacenado), o los casos en que se ataca al dispositivo que extrae atributos de la muestra haciendo que genere el conjunto de atributos deseados. En un nivel posterior, también es posible incidir en la creación del vector, en el proceso de comparación o en el módulo de toma de decisiones. Véase la IMAGEN 62, que refleja esquemáticamente todos los puntos de ataque posibles.

[117] *Das Biometrische Sammelalbum*, en su revista *Die Datenschleuder*.
[118] Las propuestas de John DAUGMAN pueden verse en su página web, de la Universidad de Cambridge; sobre las huellas, véase REDDY, P.V./ KUMAR, A. / RAHMAN,S. M. K. / T.S. MUNDRA, T.S.. "A new antispoofing approach for biometric devices", *IEEE Transactions on Biomedical Circuits and Systems* 2008, 2(4): 284–293.; ANTONELLI, A., R. /CAPPELLI, D. /MAIO,/ ET AL. 2006, "Fake finger detection by skin distortion analysis, *IEEE Transactions on Information Forensics and Security*, 2006, 1: 360–373.

Nótese que no se trata ya de un ataque específico de los sistemas de reconocimiento biométrico, sino que la situación se produce *después del sistema de captación* y viene a ser un muy similar al que puede producirse en un sistema de reconocimiento de otro tipo.

Para limitar esta vulnerabilidad existen algunas posibilidades. Cabe establecer una seguridad en relación con la verificación pasiva, esto es, un tipo de seguridad que demuestra que los datos contenidos son auténticos y no se han alterado. En relación con la verificación activa, cabe introducir algún tipo de mecanismo que verifique que lo que se le muestra no es una copia, sino que es información en fresco. Existen también medidas de seguridad de control básico de acceso, que previenen el *skimming* o *eavesdropping*, pero no una sustitución del chip o una sustitución total, y medidas de control avanzado de acceso, que protegen frente al acceso no autorizado a las huellas dactilares y a los datos biométricos de la huella[119]. El pasaporte biométrico europeo, para asegurar la integridad y autenticidad de los datos digitales almacenados en el CHIP incorpora como complemento un certificado de infraestructura de clave pública (de los que se conocen como PKI)[120].

4.2.3 *Fallos en los módulos no-biométricos: la política de administración del sistema*

El sistema de reconocimiento puede también verse atacado más allá de sus módulos biométricos o de la gestión en sentido estricto. COHN[121] describe un sistema de acceso a una escuela en New Jersey en el que en más de una ocasión la puerta quedaba abierta tras el acceso de un usuario, permitiendo al siguiente entrar sin ningún control; también es posible que un fallo eléctrico inhabilite temporal o definitivamente un sensor. A esas y otras circunstancias también se refiere la literatura como "vulnerabilidades" de un sistema de reconocimiento mediante Biometría aunque, en justicia, no creemos que deban atribuirse –al menos no en exclusiva- a la tecnología de reconocimiento biométrico en sentido estricto.

Sí que le corresponderán, en cualquier caso, las vulnerabilidades que se deban a la política de administración del sistema de reconocimiento. Ésta cubre aspectos muy importantes para dar un servicio adecuado en el entorno del que se trate. Entre ellos está la garantía de la integridad del enrolamiento; si es posible enrolarse con una falsa identidad o empleando varias identidades, la efectividad del sistema queda comprometida ab initio. Además, se ha tenido que programar al

[119] Véase EU-Passport-Specification.
[120] PÉREZ HERRERO, D. A. / CORTIJO, P. "Pasaporte electrónico de segunda generación: España en la autopista de los documentos de viaje", REVISTA DINTEL, octubre/noviembre 2010, pp132.
[121] COHN, J.P.: "Keeping an eye on school security: The iris recognition project in New Jersey Schools", *National Institute of Justice J*, 2006, No. 254. http://www.ojp.usdoj.gov/nij/journals/254/ iris_recognition.html.

sistema para la toma de decisiones en varias de sus fases lo que implica precisar, entre otros: el modo de gestión del umbral –o umbrales- de tolerancia, el número de intentos fallidos que se permitirá antes de cancelar una cuenta o hacer saltar la alarma, el tiempo de vigencia de los patrones (antes de requerir su actualización) o la forma en la que excepcionalmente se procederá en los casos en los que un usuario presente una dificultad que impide capturar su biometría[122]. Otra decisión importante, nótese, se refiere al hecho de que vaya o no a haber una supervisión humana de los procesos de funcionamiento del sistema, ya en el enrolamiento, ya en la monitorización.

4.3. Las consecuencias de los fallos del sistema y las propuestas de solución

Las consecuencias de los fallos pueden ser de diversos tipos. De un parte la *denegación de acceso* o *servicio* a personas que están legitimadas. El no reconocimiento de la identidad alegada puede hacer: que se deniegue a una persona el acceso a un club deportivo o a un casino en el que está enrolado como socio, o que no pueda recibir una llamada en su móvil o acceder a su portátil. Son inconvenientes sin duda. Pero nótese la importante diferencia respecto de una situación en la que aterriza a 10,000 kilómetros del país del que es nacional y en el control transfronterizo correspondiente consideran que no es legítimo titular del pasaporte que porta.

Del mismo modo, atribuir a alguien una identidad que no le corresponde puede quedar en algo trivial, fácil de solucionar, o dar lugar, por el contrario, a una situación realmente complicada. Un Informe publicado en el año 2011 denunciaba que la aplicación de un sistema de reconocimiento facial que trataba de localizar la identidad de violadores comparando sus imágenes con las almacenadas en la emisión de las licencias de conducción de automóviles en los Estados Unidos produjo una incómoda tasa de falsos positivos[123]. Es decir, una tasa de personas que, por el mero hecho de que el sistema los reconocía como *físicamente parecidos* a las personas que estaban en búsqueda y captura, se veían ante la incomodidad de ser investigados como presuntos sospechosos de un delito de violación. Interesantes también los casos recogidos por WEISER y KERSHAW en la prensa por presuntas coincidencias de huellas dactilares; en uno de ellos, un abogado fue detenido por la presunta coincidencia de la versión biométrica de sus huellas dactilares con unas halladas en el escenario de los atentados del 11-M en Madrid (2004)[124].

[122] JAIN, A. K. / NANDAKUMAR, K. "Biometric System Desing.Overview" EN S. Z. LI/ A. K. JAIN, *Encyclopedia of Biometrics*, Springer, consultada la edición de 2009, p139.
[123] R. CHARETTE, "Here´s looking at you, and you, and you", IEEE Spectrum, 2011.
[124] WEISER, B. *Can Fingerprints Lie? Yes*, New York times, 31 de mayo de 2004 (caso René Ramón Sánchez); KERSHAW, *Lawyer Linked to Bombing is Released*, New York Times, 20 de mayo de 2004 (por presunta coincidencia de las huellas de Brandon Mayfield con unas halladas en Madrid, en los atentados de 2004).

Puede producirse, asimismo, una intrusión en el sistema[125]. Las consecuencias pueden ser múltiples. De cara al escenario operativo en el que funciona el sistema de reconocimiento biométrico, puede darse el caso de que un impostor acceda de forma fraudulenta y obtenga los servicios cuyo acceso se deseaba gestionar mediante Biometría –acceso a un parque temático o a los servicios de un hospital, por ejemplo-, o que se acceda de forma no autorizada a la información personal de los usuarios legítimamente enrolados. CAMPISI considera que el acceso no autorizado a los patrones es una de las mayores amenazas[126]. Ese fue uno de los motivos que llevó a rechazar la base de datos biométricos de ciudadanos en ISRAEL.

En la literatura se discute si es o no posible reconstruir la Biometría original a partir del patrón. Lo cierto es que depende del sistema[127]; la literatura más reciente considera que en algunos casos de reconstrucción facial o en relación con las huellas dactilares, algunos autores consideran que sí es posible obtener un patrón parcial lo suficientemente bueno[128]. Una vía para dar respuesta a este problema puede pasar por elaborarlos en una forma que *de una misma Biometría* – y garantizando la estabilidad y la singularidad- pudieran obtenerse multitud de patrones diversos, que permitieran una renovación periódica[129] con cancelación de los antiguos. La preocupación por la privacidad ha llevado a tratar la seguridad de los sistemas biométricos en varios proyectos subvencionados que CAMPISI describe, advirtiendo que quedan aún muchos retos a los que dar respuesta[130]; entre otros proyectos destacan: BITE (Biometric Identification Technology Ethics), HIDE (Homeland Security, Biometric Identification & Personal Detection Ethics), PRIME (Privacy and Identity Management in Europe), IRISS (Increasing Resilience in Surveillance Societies), TURBINE (Trusted Revocable Biometric Identities), BEAT (Biometric Evaluation and Testing) o TABULA RASSA (Trusted Biomerics under Spoofing Attacks).

En relación con la posibilidad de intrusiones, se ha debatido y se debate la conveniencia o no de que los sistemas interoperen y de que empleen estándares que lo faciliten. Si el sistema interoperase con otros, podría darse la circunstancia de que un robo de datos biométricos tuviera impacto también en los escenarios operativos en los que funciona los sistemas con los que interopera. Pero, al tiempo, la acumulación de datos biométricos por parte de las autoridades, especialmente con motivo de la emisión de documentos nacionales de identidad o documentos de

---

125 KISKU ET ALTERE, *Security assesment for Biometric systems*, 2014, p14-15; ADLER, A. "Biometric system security", en A. K. JAIN/ P. FLYNN/ A. A. ROSS, *Handbook of Biometrics*, Springer, 2008; P. Campisi, p16-17.

126 CAMPISI, P. Security and Privacy in Biometrics: Towards a Holistic Approach,en P. Campisi (ed.), *Security and Privacy in Biometrics*, 2013, p11.

127 ADLER, A"Can images be regenerated from biometric templates?", en *Proc Biometrics Consortium Conference*, 2003.

128 ROSS, A./ SHAH, J./ JAIN, A.K. "From template to image: reconstructing fingerprints from minutiae points", *IEEE Transactions on Pattern Analysis and Machine Intelligence* 2007, 29(4):544–560.

129 JAIN A.K./ NANDAKUMAR, K./ NAGAR, A. Biometric template security. EURASIP Journal onAdvances in Signal Processing 2008

130 CAMPISI, P. *Security and Privacy in Biometrics* ,pp16-17.

viaje (pasaportes, visados, salvoconductos), ha generado la preocupación de que un acceso inadecuado pueda generar una suerte de *Pearl Harbour Digital*[131]. Durante bastante años el hecho de que cada infraestructura emplease sus propios métodos de captación y encriptación de los datos mantuvo una suerte de balcanización de los sistemas, que impedía a éstos interoperar con otros[132]. Existía, con todo, una cierta preocupación por la posibilidad de que junto con la información biométrica o asociada a ésta quedase recogida información de carácter sensible[133].

La tendencia, con todo, es hacia la estandarización. Los EE.UU. y la OACI[134], con el impulso de otras instituciones como las de la UE[135] o la ISO, se han mostrado partidarias de promover una estandarización de los datos biométricos y de los dispositivos de almacenamiento que conservan estos, para garantizar que en cualquier puesto fronterizo pueda comprobarse al instante la legitimidad de quien porta un documento de estas características. Es importante advertir, en cualquier caso, que la normativa vigente limita muy drásticamente la posibilidad de que almacenamientos de datos con otros fines (sobre todo los privados) puedan realizarse en formas que se permita la interoperatividad de los sistemas. La suma de muchos datos aparentemente insignificantes puede llegar a configurar un perfil virtual de la persona (lo que se ha dado en llamar efecto mosaico)[136].

4.4. Sobre la lectura que se hace de los fallos tecnológicos

Retomando la idea que cerraba las limitaciones desde la perspectiva de la base científica, ¿qué nivel de *flexibilidad aceptaremos dentro del rango de "éxito tecnológico"*? Cuantos outlier y con que consecuencias serán aceptados como "normales" dentro de un buen funcionamieno, o de un funcionamiento "razonable" de un sistema? No hemos encontrado pronunciamiento precisos a este respecto, aunque sí algunas aportaciones interesantes.

En la literatura se recogen ejemplos como un sistema de reconocimiento facial en espacio abierto, dotado de 35 camaras, e implantado en Ybor City, Florida[137]. La American Civil Liberties Union (ACLU) denunció que en su primer año de funcionamiento no había identificado a un solo criminal. El primer sistema de acceso de empleados establecido en el Logan Airport Boston, falló

---

131 CLARKE, R. "Human Identification in Information Systems", ITP 1994/4, pp7-8.
132 WAYMAN, J. L. "Biometric Identification and the Financial Services Industry", Congressional testimony of May 20, 1998, en *National Biometric Center: Collected Works*, p. 263ss, 269.
133Esta cuestión se abordará detenidamente esta cuestión en el capítulo V.
134 BROUWER, E. R. en *Digital Borders and Real Rights*: *Effective Remedies for Third-Country Nationals in the Schengen Information System,* Brill, 2008, p137.
135 Así en el *Programa de La Haya* de 2004, detallamente DIETRICH PLAZA, C. "El Tratado de Prüm en el marco de la regulación de protección de datos personales en la Unión Europea", en *Revista de Derecho Constitucinal Europeo*, año 4, nº 7 (2007).
136 BIZER, J. "Sieben Goldene Regeln des Datenschutzes", *DuD*, 2007; PÜHRINGER, S.: *Biometrische Daten im Datenschutzrecht,* 2008, p6-7.
137 TRIGAUX, R.: Cameras scanned fans for criminals. St. Petersburg Times, 31.1.2001

un 39% de las veces, con las consiguientes consecuencias para quienes cotidianamente trataban de acceder a su trabajo.

Al igual que en muchos otros tipos de tecnologías, los fallos en las tecnologías de reconocimiento biométrico muestran un alto grado de flexibilidad interpretativa. Gooday (1998)[138] explicaba que existe una tendencia a narrar las técnicas exitosas como el resultado de muchos modelos y prototipos sin éxito, como tratando de convencer de que fallar es algo imprescindible para llegar a una tecnología beneficiosa y en la que poder confiar. Se preguntaba, sin embargo, cuántas veces debe fallar un sistema para que, definitivamente, podamos considerarlo como no beneficioso o, al menos, *no digno de nuestra confianza*. Al igual que hemos expresado como reflexión personal a la luz de las limitaciones de la base científica de los sistemas, el número de personas afectadas –en este caso por los fallos técnicos- y las consecuencias que estos fallos tienen para sus derechos y libertades son en nuestra opinión la referencia desde la que han de ser evaluados estos sistemas de reconocimiento.

5. PROBLEMAS QUE PLANTEA EL RECONOCIMIENTO BIOMÉTRICO PLANTEA DESDE LA PERSPECTIVA ÉTICO-SOCIAL.

El articulo *Touching Big Brother: how biometrics will fuse flesh and Machine*, de Simon DAVIES (1994), es considerado una de las primeras y más exhaustivas referencias a las cuestiones ético-sociales que plantean las tecnologías biométricas[139]. A la lista de cuestiones que este autor proporciona se han ido añadiendo en la literatura aportaciones de muchos otros autores, en muchos casos a la luz de las experiencias de aplicación de las tecnologías y los nuevos desarrollos, pero manteniendo en esencia un mismo listado. El miedo de que se produzcan desviaciones en su uso, la deshumanización que puede implicar el hecho de reducir las personas a bytes o, entre otros, el hecho de esa *unicidad* que supuestamente dicen captar quede muy lejos de la identidad que una persona ofrece en los numerosos entornos en los que se mueve, son algunas de las cuestiones que planteó DAVIES. Señaló también las consecuencias de otorgar autoridad y poder de vigilancia a un sistema *supuestamente perfecto*, que en cierto modo recuerda al Gran Hermano de la novela *1984* de Orwell, y el miedo a que en vez de la democracia gobierne la tecnocracia. Apunta también al temor de que, una vez más, sea éste un campo en el que las personas poderosas se beneficien de excepciones y exenciones, de privilegios rente al resto, evocando otra novela de Orwell: *Rebelión en la Granja*. En ella, como es sabido, se recogió aquello de "*todos somos iguales, pero unos mas iguales que otros*" (en inglés en la novela original: "*all animals are equal, but some animals are more equal than others*").

[138] GOODAY, G. "Rewriting the Book of Blots: Critical Reflections on Histories of Technological Failure", *History and Technology* 14, nº 4/ 1998, pp265-291.
[139] DAVIES, S. "Touching Big Brother: how biometric technology will fuse flesh and machine", *Information Technology and People,* 7 (4), 1994.

Tras analizar las diferentes aportaciones y realizar nuestra propia reflexión, vamos a exponer los resultados de esta parcela de la investigación en dos bloques diferenciados, con una importante advertencia. Muchas de las reflexiones y estudios que hemos empleado como referencia emplean un enfoque que atiende, al mismo tiempo y de forma indiferenciada, a dos tipos de implicaciones ético-sociales de las biometrías que en este trabajo se ha decidido tratar de forma interrelacionada pero por separado. Nos referimos :

1) de una parte, a lo que implica, en sí mismo, emplear este tipo de tecnologías para reconocer a las personas. Esta perspectiva es objeto de tratamiento en este epígrafe.

y, 2) de otra parte, a las implicaciones que en concreto emergen del uso que se está dando a determinadas tecnologías de reconocimiento biométrico en diferentes escenarios operativos. Consideramos que un análisis de las implicaciones ético-sociales del uso de estas tecnologías en los diferentes escenarios operativos no puede hacerse en profundidad sin atender debidamente la entidad de cada uno de los escenarios, algo que se hace en detalle en el siguiente capítulo.

En el presente apartado se abordan las implicaciones de las tecnologías biométricas desde la perspectiva que aquí se describe:

1) En primer lugar se atiende a la trascendencia que desde el punto de vista ético y social tiene emplear la referencia del cuerpo de una persona, de sus elementos "singularizantes" en la identificación. Y es que estos sistemas juegan con un peligroso binomio, que tiende a simplificar lo que cada ser humano *tiene de único,* al tiempo que de forma encubierta parece darse buena una vigilancia *colateral* sin precedentes en ninguna democracia del mundo.

2) En segundo lugar nos detendremos a analizar si emplear información biométrica afecta de algún modo a la privacidad de las personas y en qué sentido.

5.1. Cuerpo, identidad y privacidad, ante los sistemas automatizados de reconocimiento mediante Biometría.

La relación entre el cuerpo y la mente o la construcción de las identidades personales albergan aún grandes misterior por descubrir. No obstante, sabemos lo suficiente como para detectar que en la narrativa de los sistemas automatizados de reconocimiento hay algunas explicaciones que no terminan de encajar. El cerebro humanos es capaz de reconocer de forma singular a las personas con las que nos topamos; es capaz de captar e*so que hace que la voz de un conocido nos resulte familiar*, capaz de enfocar en aquello que es peculiar de un rostro o en una forma de

caminar. Un sistema de reconocimiento biométrico, dicen algunos discursos, viene a ser básicamente *lo mismo*. Esto es, se nos presentan las tecnologías biométricas como sistemas a los que hemos enseñado a hacer *algo que ya hace* el cerebro humano, y no resultan ni más ni menos invasivas que éste. Simplemente reconocen quién es alguien prestando atención a algo que estática o dinámicamente se expresa en su corporeidad.

Esa explicación recoge magistralmente un ejemplo de la que se ha dadao en llamar *la madre de todas las* falacias: la *ignoratio elenchi* o elusión del asunto. Por concepto todas las falacias pretenden desviar la atención del diálogo *hacia otro asunto*, pero ésta se caracteriza por no dar, si quiera, la oportunidad de entrar en éste. Ya no se trata de exagerar tanto la necesidad como para no ver el coste de las tecnologías biométricas, sino que se presenta la función que estas realizan como si fuera "algo natural"; se pretende dar a entender estas tecnologías no incorporan nada nuevo a un escenario en el que cotidianamente los cerebros de las personas con las que interactuamos nos reconocen (más o menos) de forma *similar*.

¿De forma similar? Estamos hablando de que un sistema: almacene información sobre los cuerpos de las personas; y, posteriormente, la ponga a disposición de lo que *los cerebros que accedan* consideren que quieren hacer con dicha información. Estos procesos de enrolamiento, además, depositan en la corporeidad –captada además con limitaciones- todas las posibilidades que una persona tiene de expresar *quién es.* De ahí que se haya dicho que las tecnologías de reconocimiento biométrico practican cierto *fetichismo corporal*[140]; aunque vivimos en una época en la que cotidianamente se nos reduce a números, pines y nombres de usuario, involucrar aquí el cuerpo implica un salto cualtitativo. Algunas voces hablan de *códigos de barras*[141] o de *tatuajes biopolíticos*[142] que amenazan la dignidad de la persona como en otra época sucedió con las prácticas de los campos de concentración nazis o el enrolamiento obligatorio de los trabajadores inmigrantes en las colonias británicas (como el impuesto por la Black Act en Transval, Sudáfrica, al que opuso GHANDI su resistencia pacífica). Las Biometría, hay quien advierte, "*autoriza la inscripción y el registro del elemento más privado y más incomunicable de la subjetividad*" (Giorgio AMBGABEN)[143]. "¿Por el mero hecho de que no empleemos contraseña, va el cuerpo humano a dejar de ser el cuerpo de una persona?", se pregunta B. J. MILLER[144].

---

[140] MAGNET, S. *When Biometrics Fail: Gender, Race and the Technology of Identity*, 2011.
[141] CREWS jr., C. W."Human Bar Code. Monitoring Biometric Technologies in a Free Society", *Policy Analysis*, nº 452, 2002, pp1 y ss.
[142] AMGABEN, G. "Bio-political tatooing", Le Monde, 11 de enero de 2004.
[143] AMGABEN, G. "Bio-political tatooing", Le Monde, 11 de enero de 2004.
[144] MILLER, B. J. "If the body becomes password, does it cease to be the body?" en *Security, risk, and the biometric state: Governing borders and bodies*, Routledge, NY, 2010, p109; DEL MISMO, "(Dis)qualified bodies: securitization, citizenship, and 'identity management'", en P. NYERS (ED.), *Securitizations of Citizenship*, 2010, Routledge, NY, 2010, pp77-93.

A estas reflexiones quisiéramos realizar dos modestas aportaciones. Una, en relación con la perspectiva para valorar los sistemas de reconocimiento biométrico en relación con la tutela de la vida privada; dos, sobre el hecho de que con algunos de estos sistemas el cuerpo se convierta, también, en un espacio vigilado.

5.1.1 *El enrolamiento biométrico, en esencia, ante la tutela de la vida privada*

Aunque la afirmación que vamos a recoger a continuación no sea unánime ni a veces se exprese en el mismo sentido en todos los pronunciamientos institucionales –ni judiciales- de los países Europeos, queremos subrayar que se trata de un extracto de una sentencia del Tribunal Europeo de Derechos Humanos de Estrasburgo. Además de fuerza moral, su opinión es vinculante para todos los Estados Adheridos al Convenio Europeo de Derechos Humanos, impulsado por el Consejo de Europa en 1950 y con entrada en vigor en 1953. Cuarenta y siete países están adheridos al mismo, entre ellos los 27 miembros de la Unión.

Toda obtención y conservación de información de las personas, dice el Tribunal Europeo de Estrasburgo, *supone un atentado contra el derecho a la protección de la vida privada*. No distingue, nótese, entre información banal o información que consideremos especialmente íntima; no distingue formas de obtención ni formas de conservación, tiempos, y, lo más importante, tampoco es relevante *quién* (un estado, una autoridad pública, un particular) sea el que obtiene y conserva la información. *Toda obtención y conservación de información de las personas*, incluida la por tanto la información biométrica (sea esta estática o dinámica), *supone un atentado contra el derecho a la protección de la vida privada*. A *sensu contrario*, las personas tienen un derecho a que los demás, con independencia de quiénes sean o el poder que tengan, *no obtengan ni conserven* información que les concierne.

En nuestra cultura jurídica el derecho a la tutela de la vida privada no es interpretado como un derecho "*a ser dejado solo*" ni es visto como un valor a proteger de forma absoluta; vivir en sociedad implica, necesariamente, interactuar en muchos sentidos. El cerebro de la persona que regenta el kiosco de los periódicos, el de la persona que conduce el autobús o chequea los tickets al entrar en el cine, así como el de alguien con quien hayamos coincidido en una ocasión en la sala de espera del centro de salud, puede que guarden datos de haberse cruzado con nosotros. Y, además, explica el TEDH, *valores colectivos* que hacen que como sociedad necesitemos realizar injerencias en la vida privada de los demás (motivos de seguridad nacional o de orden público, de

salud pública, o de protección de otras personas). Incluso, en ocasiones, es posible que necesitemos interferir en la vida privada de alguien para darle protección a su vida o a su salud[145].

Pues bien. Aunque existan razones de las ya citadas que *justifiquen la* injerencia, no por ello deja ésta de ser *una injerencia*, del mismo modo que encarcelar a alguien para cumplir una condena no hace que esa privación de libertad sea *menos privación de libertad*. Quiere ello decir que en ningún momento, aunque se actúe de forma justificada, debemos olvidar que estamos atentando contra la privacidad de alguien y que hemos de ser muy cuidadosos de no interferir en esa privacidad más allá de lo estrictamente necesario.

El modo en que nuestras sociedades gestionan el equilibrio entre privacidad y necesidad de intromisión se expresa en la llamada normativa *de protección de datos de carácter personal.* El nombre, ha de decirse, no es muy afortunado; porque el objeto de la protección no son *los datos de las personas*. sino el derecho que las personas tienen a que nadie se entrometa en su privacidad. Cuando se estima legítimo que una autoridad pública realice injerencias en la privacidad, el parlamento la autoriza por ley y detalla en qué circunstancias y dentro de qué requisitos podrá realizarse esta intervención (en las investigaciones por la comisión de un delito, en la gestión de alertas sanitarias, en el cobro de los impuestos..). Establece, además, que una vez se ha cumplido la finalidad, los datos deben cancelarse, como sucede por ejemplo con los antecedentes criminales que caducan.

Universitat d'Alacant
Universidad de Alicante

En ausencia de esa autorización legal, lo que hace la normativa es recordarle a la persona titular de la información de que se trate, que es libre para decidir *quién, cuándo y qué es lo que un tercero sabrá de ella*[146]. Es decir, que a menos que el parlamento haya dicho otra cosa, sólo podrán adentrarse en nuestra privacidad aquellas personas a los que les damos nuestro consentimiento. Es más, y para prevenir abusos, si alguien quiere hacer una base de datos o un fichero con datos, aun en el caso de que las personas consientan, hemos nombrado unas autoridades (las autoridades de protección de datos) que velan porque la finalidad del fichero en sí y su modo de gestión sean legítimos y proporcionados.

¿Por qué se protege la privacidad? ¿Se protege en sí misma? Esto es también algo importante. La privacidad, para cada persona, es una garantía; una garantía de que dispone de una esfera de libertad, una esfera muy amplia y con multiples dimensiones que *le permite ser libre frente a*

[145] SUTROP, M./ LASS-MIKKO, K. "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics", *Review of Policy Research*, vol. 29, nº 1/2012, pp21ss, p26.
[146] BVerfG 65, 1, Sentencia del TC alemán de 15 de diciembre de 1983; WESTIN, A. F. "Social and Political Dimensions of Privacy", *Journal of Social Issues*, vol. 59, nº 2, 2003, pp.431-453; PENNOCK, J. R./ CHAPMAN, J. W. (eds.), *Privacy*, Atherton Press, New York, 1972; SLOVE, D. J.: "Conceptualizing privacy", *Californian Law Review*, 90 (4), 2002, págs. 1087-1156.

cualquier limite irracional que pueda impedir que construyamos nuestra identidad y nos desarrollemos como personas[147] (el derecho al libre desarrollo de la personalidad). Nuestra corporeidad, la privacidad de nuestro domicilio, la privacidad de nuestros sentimientos y pensamientos, de nuestro comportamiento y acción (preferencias, hábitos, actividades políticas o prácticas religiosas), la privacidad de nuestras comunicaciones, de nuestra localización espacio-temporal, de nuestras interacciones con otros, todas esas esferas resultan importantes para nuestro proyecto vital[148],[149]. Si el panadero de mi barrio desease tomar notas para prestar mejor servicio a los clientes –algo que no parece tan invasivo como colocar una escucha en mi línea de teléfono-, necesitaría mi autorización para incluirme en ese fichero; no hacerlo, según la legislación vigente, puede conllevar una sanción de entre cuarenta mil y trescientos mil euros. Del mismo modo, no tengo porqué aceptar –ni se me debe imponer de forma directa o indirecta- ningún tipo de enrolamiento, sea con mi Biometría o con otros datos, en más bases de datos que las que, en sentido estricto, tienen el amparo de las leyes.

¿Por qué destacamos todo esto? Porque los gobiernos occidentales, incluyendo a los de la UE y a la propia Comisión Europea, no están tomando ninguna medida para que los ciudadanos sean conscientes de la amenaza que suponen estas tecnologías y cuenten con herramientas para proteger adecuadamente su privacidad. Contemplamos con perplejidad cómo se ha permitido extender sistemas de reconocimiento mediante Biometría a situaciones tan triviales como adquirir una bebida isotónica en una máquina expendedora.

Universitat d'Alacant
Universidad de Alicante

5.1.2. *El riesgo de vigilancia excesiva*

El *Comité Consultatif National d'Éthique pour les Sciences de la vie et de la santé (CCNE)* francés advirtió en 2007 *ante la biometrización del ser humano*[150] o informatización de éste[151], destacando especialmente el riesgo de hipervigilancia. Aunque la vigilancia, a primera vista, pueda parecer una modalidad más de injerencia en la vida privada, lo cierto es que se trata de una conducta que va más allá, por cuanto que tiene un mayor potencial de cara a condicionar la libertad de las personas. Esta vigilancia no se produce con todos los sistemas biométricos, sino que es característico de los sistemas que funcionan en red o interoperan con otros[152], [153] y de los

[147] AGREE/ ROTENBERG, *Technology and Privacy: The New Landcape*, MIT Press, Cambridge 2001, p7.
[148] ALTERMAN, A. "A Piece of Yourself: Ethical Issues in biometric identification", *Ethics & Information Technology* 5/ 2003, pp139-150.
[149] HALLINAN, D./ SCHÜLZ, P./ FRIEDEWALD, M. "Neurodata-Based Devices and Data Protection", 5ª Conferencia sobre Vigilancia y Sociedad, Sheffiedl, abril de 2012.
[150] CCNE, *Biométrie, dones identifiants et droits de de l'homme*, 2007, cit., p3.
[151] VAN DER PLOEG, I. *The Machine Readable Body. Essay on Biometrics and the Informatization of the Body*, Shaker, 2005, p8.
[152] MORDINI, E./ PETRINI, C. (eds.), *Ethical and Social Implications of Biometric Identification Technology*, Annali dell'ISSS, 2007, 43, p1; muy crítico: Giorgio AMGABEN, "Bio-political tatooing", *Le Monde*, 11 de enero de 2004.

llamados sistemas de de cribado biométrico, en los que porcentualmente son muchas más las personas controladas que las *enroladas*. Entre estos últimos se cuentan algunas modalidades de reconocimiento mediante Biometría dinámica, que emplean como referencia patrones que se consideran expresión de *comportamientos sospechosos* y proyectan su vigilancia sobre todo tipo de personas, con independencia de que existan o no razones objetivas para vigilarlas.

Desde la década de los años 90 el principal usuario de las tecnologías de reconocimiento mediante Biometría había sido el Gobierno de los Estados Unidos de América, especialmente sus Departamentos de Seguridad Interior y Defensa y el Departamento de Estado[154]. Así lo recoge en detalle un informe hecho público por el Departamento estadounidense del Tesoro en el año 2005[155]. Aunque algunas corporaciones del sector de las Tecnologías de la Comunicación y de la Información presionaba por extender estas tecnologías más allá de los usos gubernamentales estratégicos o de la alta seguridad en operaciones financieras[156], el uso civil de estas tecnologías era visto por el gobierno estadounidense con mucho recelo[157]. Se temían los abusos en el control de los ciudadanos de a pie, tanto por parte de las autoridades públicas[158], como por parte del sector privado. Entre la novedad que aportan los sistemas en red o los que interoperan, está además una peculiaridad de esta nueva forma de vigilancia, y es el hecho de que pueden facilitar el rastreo de los movimientos de las personas (y su trazabilidad), e incluso propiciar geolocalizaciones a tiempo real[159] (una identificación ubicua[160]), como si las personas tuvieran insertado un sistema de localización GPS.

El hecho de autorizar *aunque sólo fuera un uso civil* era visto ya como un peligro, porque el escenario del *Gran Hermano biométrico* no llegaría de repente, sino de forma progresiva. Llegarían primero sistemas aparentemente razonables, con fines bien delimitados, pero después terminarían por extenderse de forma abusiva.

---

153 ALTERMANN, A. "'A Piece of yourself': Ethical issues in biometric identification", *Ethics and Information Technology,* 5/2, 2003, pp139s.

154 TUREK, J."An Industry Group Viewpoint: Biometrics", SIA News, agosto de 2004, pp20-21.

155 *The Use of Technology to Combat Identity Theft, Report on the Study Conducted to Section 157 of the Fair and Accurate Credit Transactions Act of 2003*, Departamento del Tesoro –EEUU, febrero de 2005, p42ss.

156 POLEMI, D., "Biometric techniques: review and evaluation of biometric techniques for identification and authentication, including and appraisal of the areas where they are most applicable", ETS: Biometrics, 1997.

157 SPROKEREEF, A./ DE HERT,P.: "Biometrics, Privacy and Agency", E. MORDINI/ D. TZOVARAS (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context,* Springer, 2012, pp81 y ss, 86.

158 THIERER, A. / CREWS, W. (ed.), *Who Rules the Net. Internet Governance and Jurisdiction*, Cato Institute, 2003, xxiii-xviii.

159 LYON, D. *La societá sorvegliata. Tecnologie di controllo della vita cuotidiana*, Feltrinelli, Milan, 2002, p96.

160 CLARKE, R. "Chip-Based ID:Promise and Peril, Invited Address to a Workshop on 'Identity cards, with or without microprocessors: Efficiency versus confidentiality'", *International Conference on Privacy,* Montreal, 1997.

> Así lo advertia WOODWARD en 1997[161], citando una advertencia del juez BRANDEIS su famoso voto particular a la Sentencia del caso *Olmstead contra los Estos Unidos*[162]"*la experiencia debería enseñarnos que precisamente cuando los propósitos del Gobierno son beneficiosos es cuando más debemos esforzarnos por proteger la libertad. Los seres humanos que nacen libres están normalmente alerta ante los intentos de las mentes-malignas por invadir su libertad. Los riesgos más grandes para la libertad provienen de las insidiosas agresiones de hombres celosos, bien intencionados pero que no comprenden*". Si permitimos un solo uso civil, con el tiempo el reconocimiento biométrico, afirmaba Woodward hace casi veinte años, terminará extendiéndose a situaciones y propósitos de identificación que no se pretendieron inicialmente, como ha sucedido en los EEUU con el número de la seguridad social.

La profecía se cumplió al calor de los pasaportes biométricos expedidos en regiones como la UE o Australia, que dieron paso a muchos otros tipos de usos. Se da la circunstancia, además, de que los ciudadanos se están acostumbrando a que se comentan abusos en lo que a identificación se refiere. No tenemos muy claro cuándo y hasta qué punto nos pueden exigir que nos identifiquemos y en qué términos. Por ejemplo, todos los ciudadanos españoles adultos deben tener, por exigencia legal, un DNI, y el RD 1553/ 2010 que regula la expedición del DNI recoge la obligación de mostrar éste cuando se es requerida por la autoridad o sus agentes. Ahora bien, ¿el hecho de que yo tenga un DNI da ocasión, a cualquiera y en cualquier situación, a requerir que yo lo muestre o incluso a guardarse una copia escaneada del mismo?

Dados los abusos que se producen a este respecto, Noruega, en su normativa de protección de datos, ha establecido con claridad que los números de identidad nacional y otros medios "*claramente identificativos*", como considera su Inspector Nacional de protección de datos que lo son algunos tipos de datos biométricos, sólo deben emplearse cuando existe una "*necesidad objetiva de identificación*" y sobre esa base prohibió algunos usos, como el control horario de los empleados. Mucho menor es, a este respecto, la sensibilidad que hay en nuestro país a pesar de que la ley sólo exige mostrar el DNI en casos como los de la protección de la seguridad ciudadana o la prevención del blanqueo de capitales.

Por ejemplo la ley dice que los hosteleros deben llevar un *registro de viajeros* y comprobar que la información que incluyen en el registro "*coincide con los datos que figuran en el pasaporte o DNI exhibido por el viajero*". Nada se dice, sin embargo, de que haya de escanearse ni almacenarse el DNI –cosa que sí se establece, en cambio, la normativa que lucha contra el blanqueo de capitales. Tampoco es exigible que nos identifiquemos en las compras corrientes, a menos que paguemos con tarjeta, ni pueden emplearse nuestros datos con más fines que los de asegurar dicho pago. Si el vendedor quiere obtener más datos, necesita nuestra autorización; lamentablemente, con cada vez más frecuencia, las personas ceden irresponsablemente sus datos a cambio de los atractivos

[161] WOODWARD, J. 1997, p1485-1486.
[162] Sentencia del caso *Olmstead v. United States*, 277 U.S. 439, 479 (1927).

descuentos y premios que se asocian a tarjetas de fidelización. Tales tarjetas, anunciadas muchas veces como *premios a la fidelidad*, no son sino señuelos para acumular y comerciar con información de carácter personal.

5.2. ¿Cómo de "privada" es la información biométrica?

Después de lo ya dicho, salta a la vista que la pregunta con la que abrimos este apartado es una pregunta *trampa*. Toda información personal, no importa de qué tipo sea, es información que si se obtiene y almacena asociada a una persona identificada o identificable supone una intromisión en la vida privada de alguien. La pregunta, sin embargo, la hemos planteado así, porque en algunas narrativas sobre los sistemas de reconocimiento biométrico se pretende hacer ver que no se trata de información "*excesivamente relevante*" o con trascendencia alguna; que sólo sirven para la identificación "*neutra*" de las personas. En la década de 2000 algunas instituciones llegaron a decir que ni siquiera son datos de carácter personal (o no siempre lo son[163]) , aunque queremos pensar que en los últimos cinco años se está extendiendo otra opinión.

Creemos que, conforme al conocimiento científico que actualmente se tiene de las biometrías estáticas y dinámicas, existen argumentos para sostener que no solo son datos de carácter personal sino que, en muchos casos, han de ser tratados como datos sensibles. A continuación se exponen dichos argumentos.

5.2.1. ¿Son datos sensibles, en en sentido de la Ley orgánica de Protección de Datos de Carácter Personal (LOPD)?

Cuando la información biométrica concierne a una persona identificada o identificable, aplicando la LOPD estamos ante un dato de carácter personal. La injerencia en esa información es, por tanto, una afectación de la privacidad y precisa bien autorización legal, bien consentimiento de la persona titular del dato[164]. Así lo sentencia el Tribunal Supremo Austriaco, en relación con un caso de control de acceso de los trabajadores en un hospital)[165], y se pronuncian en el mismo

[163]El GT WP 29 en su opinión 193, de 2012 decía que son datos de carácter personal *en la mayoría de los casos*, aunque no precisaba en cuáles no lo eran.

[164] LODGE, J. en E. MORDINI/ D. TZOVARAS (eds.), *Second Generation Biometrics*, Springer, 2012, p321; DE HERT, P./ SCHEUERS, W./ BROUWER, E.: "Machine-readable identity documents with biometric data in the EU – part III- Overview of the legal Framework", *Keesing Journal of Documents and Identity*, 2007/ 22, pp23-26; KINDT, E. "Biometric applications ", *DuD*, 31/ 2007, pp166-170.,

[165] OGH, Urteil vom 20. Dezember 2006, 9 ObA 109/06d - ArbVG § 96, ABGB § 16, DSG 2000 § 4, *Fingerscanning in Betrieben*.

sentido, entre otros, la CNIL francesa, el GT-WP 29, el Comité del Convenio 108 y el *Garante Italiano*[166].

Ahora bien, en el conjunto de los datos de una persona, ¿cabe entender que los datos biométricos son *datos sensibles*? La ley distingue una serie de datos a los que, por su sensbilidad, se les ofrece una especial protección. En concreto limita la posibilidad de obtener, conservar y emplear este tipo de datos y, además, que para el responsable de los ficheros unas elevadas exigencias de seguridad (especialmente en relación con los dos primeros grupos, aunque con algunas excepciones[167]). Cuando no haya ley que obligue a prestar datos de este tipo y, por tanto, vayan a obtenerse mediando el consentimiento de las personas, la normativa indica que el consentimiento debe ser *explícito*, especialmente en los casos en los que vayamos a tratar datos sobre: 1) el origen racial o étnico; 2) la opinión política; 3) las creencias religiosas o políticas; 4) los datos de salud o la vida sexual de las personas; o 5) la comisión de infracciones penales o administrativas.

En diciembre de 2008 el Tribunal Europeo de Derechos Humanos de Estrasburgo (TEDH) dictó la Sentencia del caso *S. y Marper contra Reino Unido*, en respuesta a la demanda planteada por dos ciudadanos que, habiendo sido absueltos de los delitos que se les acusaban, reclamaban al Reino Unido la destrucción de las huellas dactilares, muestras biológicas y perfiles de ADN que se les habían tomado en el proceso de investigación criminal. En coherencia con lo ya dicho sobre la interpretación que el TEDH hace de este derecho, consideraban que esa conservación vulneraba su derecho a la vida privada. Pero, además, destacaban *la sensibilidad* de los datos obtenidos de las muestras biológicas o de los perfiles de ADN *que pueden contribuir* a que se establezcan vínculos con posibles familiares, el origen étnico o la salud. ¿Por qué se destaca la sensibilidad de los datos que pueden obtenerse de las muestras biológicas y de los perfiles de ADN, y no en relación con las huellas dactilares? Implica esto que los patrones biométricos que en su diferente tipología hemos visto en el Capítulo primero de la exposición de resultados, *¿que pueden contribuir* a que se establezcan vínculos con posibles familiares, el origen étnico o la salud?

En la primera década del siglo XXI ha habido una cierta tendencia a minusvalorar el tipo de información que cabe obtener de las huellas. El TS español ha dicho, por ejemplo, que la versión digital de una huella dactilar "*no expresa ningún aspecto concreto de la personalidad*" [168] y que los

[166] GT-WP 29, párrafo 3.1. del Documento de 1 de Agosto de 2003, WP 80; parrafo 107 del I*nforme del Comité 108 sobre Biometría*, cit; parrafo 4.1. de las *Linee guida per le tecnologie biometriche*, 8 de octubre de 2004 del GARANTE.
[167] Vid. artículo 81 del Reglamento que desarrolla la Ley 15/ 1999, el RD 1720/ 2007.
[168] Véanse, asimismo Resolución del Expediente E/ 01126/ 2010, sobre instalación de un sistema de fichaje biométrico para el personal de rampa de la empresa *Spanair*; Resolución del expediente E/ 02635/ 2009, contra la empresa *Servicios Logísticos Integrados, S. A.*, por la instalación de un sistema de fichaje mediante huella digital; Resolución del procedimiento PS/ 00272/ 2005. Por la instalación de un sistema de control horario mediante huella digital en la empresa *Rótulos Ayllón*.; Resolución del Procedimiento nº TF/ 01755/ 2009, por ejercer un

datos biométricos *no tienen mayor trascendencia* que los "datos relativos a un número de identificación personal", o de una ficha personal[169]. Se mantienen en esa línea, con matices, otros pronunciamientos. El GT-WP 29, en su documento 4/ 2007 sobre el concepto de dato de carácter personal, se refiere a los datos biométricos inclinándose hacia su consideración como datos sensibles[170] pero no para todos los casos y el Auto del Tribunal Constitucional español 57/ 2007[171] afirma, en referencia a la geometría manual, que no estamos ante datos de los que "*el art. 7 LOPD considera como especialmente protegidos*"; en el mismo sentido recoge el Dictamen de 21 de diciembre de 2011 del Comisionado Irlandés para la Protección de datos, que los datos biométricos no quedan claramente abarcados por la categoría de datos "*sujetos a especial protección*" en la Ley Irlandesa de protección de Datos de carácter personal ni en la Directiva UE de Protección de Datos de Carácter personal.

Pero otras voces han ido abriendo paso a una visión muy diferente de los datos biométricos. El Consejo de Europa, en el año 2005, reconocía que la información biométrica puede revelar *otro tipo de información personal,* como información *sobre la salud de una persona, su origen étnico o racial o sus convicciones religiosas*[172] y el Supervisor Europeo para la protección de datos (SEPD) ha llevado a advertir que debemos tener en cuenta, además, que se trata de datos que pueden ser recogidos sin el conocimiento de la persona y, además, permitir rastrear sus movimientos en la vida diaria[173]. MORDINI/ MASSARI consideran, por su parte, que el hecho de que con los datos biométricos (u otros datos) pueda almacenarse más información de la necesaria o que pueda darse a éstos un uso diferente al inicialmente previsto, no es algo que deba valorarse como característica propia de los datos biométricos en sí, sino como un elemento a testar en relación con el fichero de datos que se desea dar de alta[174]. En la misma línea ANDRADE[175] previene sobre la necesidad de ampliar el concepto actual de dato sensible, atendiendo a aquellos datos que –perteneciendo o no al listado de datos de especial protección- se caracterizan por tener "*intrínseca relevancia en términos de la privacidad de las personas*"[176], en una línea similar a la que emplea el TEDH para distinguir entre datos de carácter personal que quedan abarcados en el ámbito de protección del artículo 8º CEDH, y el resto de datos de carácter personal.

---

trabajador el derecho de oposición a sus datos biométricos en el control de jornada laboral del personal funcionario por parte del *Ayuntamiento de Andújar*.

[169] Procedimiento nº AAPP/00020/ 2007, fundamento 2º.

[170] GP artículo 29, Opinión 4/ 2007, sobre el Concepto de dato de carácter personal, de 20 de junio de 2007.

[171] Fj. 6º.

[172] CoE, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*, Estrasburgo, 2005.

[173] Así por ejemplo los apartados 8 y 17 del Dictamen 2006/C 313/13, sobre el Reglamento de Salvoconductos.

[174] E. MORDINI/ S. MASSARI, "Body Biometrics and Identity", *Bioethics* Journal vol. 22, nº 9/ 2008, p492.

[175] ANDRADE, N.N.G.d.: "The Right to Privacy and the Right to Identity in the Age of Ubiquitous Computing: Friends or Foes? A Proposal towards a Legal Articulation", en AKRIVOPOULOU, C./ PSYGKAS, A. (eds.), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, Information Science Reference, New York, 2011, pp. 19ss,30-31.

[176] Una idea expuesta ya por DE HERT, P./ GURTWIRTH, S.: "Data Protection in the case law of Strasbourgh and Luxembourg: Constitutionalisation in action", en GURTWIRTH, S./ POULLET, Y./ DE HERT, P/ TERWAGNE, C/ NOUWT, S. (eds.), *Reinventing Data Protection*, 2009, p25.

En nuestra opinión, hay pruebas fehacientes de que de los datos biométricos pueden obtenerse de forma directa o indirecta datos relativos a la salud y al origen de las personas, así como informaciones relativas –entre otros- a algunos aspectos de la identidad sexual. Esta idea se desarrollará en el apartado 5.3. Al ser el resultado de la compleja y continua interacción entre los factores genéticos y los ambientales, la información biométrica –piénsese por ejemplo en la obtenida del complejo craneofacial, en cuyo potencial se ha fijado la somatología forense- puede aludir a la entidad de un individuo y a su pertenencia a un determinado grupo racial o ayudarnos a determinar el parentesco entre dos personas.

También se emplean técnicas antropométricas en el Consejo Genético, proceso en el que las personas con riesgo de padecer enfermedades de carácter hereditario, genético o en relación con alguna alteración cromosómica son advertidas de las consecuencias de la misma, de la probabilidad de padecerla o transmitirla y de los medios posibles para evitarlas, mejorarlas o paliarlas. La posibilidad de que un sistema de identificación por Biometría almacene voluntaria o involuntariamente y con o sin el consentimiento de las personas este tipo de información, es algo que dependerá del tipo de dato que se maneja en crudo, del modo en el que se procesa y/o del sistema de almacenamiento que se emplee. Si tomamos como referencia la aplicación de la normativa de protección de datos a otras facetas de la actividad social en las que se emplean datos biológicos de las personas (por ejemplo en la investigación científica), es el dato en crudo la referencia para aplicar la normativa, con independencia de que la información almacenada sea mucho más limitada o de que, por ejemplo, la información posteriormente se anonomice y deje de estar directamente vinculada a una persona.

Universitat d'Alacant
Universidad de Alicante

Creemos que en relación con las tecnologías biométricas, lo coherente es mantener esa referencia. Se da la circunstancia, además, de que esa información no siempre requiere complejos análisis de laboratorio (como puede suceder con algunos estudios genéticos), sino que puede quedar comprometida por algo tan simple como el hecho de que una persona le resulte atípica o *outlier* a un sistema.

5.2.2 ¿Son sensibles en algún otro sentido?

Michiel VAN DER VEEN previene sobre el hecho de que, de comprometerse la información biométrica, ésta quedaría comprometida para siempre. En su opinión, la injerencia de esta información impide asignar una nueva identidad numérica al titular de los datos[177]. Esto sucede

[177] En el debate CESAGEN *2nd Focus Group on Privacy Enhancing Technologies*, HIDE PROJECT, febrero de 2008.

en los casos en los que de los patrones biométricos se obtienen *identificadores* únicos. Si la información ha sido expuesta, ello resultará un inconveniente cuando la persona desee modificar su identidad civil, bien en ejercicio de su derechos a la identidad personal, bien como parte de un programa de protección de su seguridad personal (como los programas de protección de testigos). Entre las propuestas para corregir estos riesgos está la de Ann CAVOUKIAN, Comisionada de Protección de la Privacidad en Ontario, quien entiende que es posible generar claves aleatorias de encriptación. Tales encriptaciones, advierte la alta Comisionada para la información de Ontario, son tan variadas como las contraseñas alfanuméricas y no se retendría la Biometría del dato en crudo, sino un patrón encriptado de forma aleatoria.

Pero estos mecanismos no siempre son infalibles. Quizá por ello, algunos expertos entienden que la mejor garantía es no emplear las biometrías como password o claves de acceso[178], porque son más bien login o definidores de la identidad del usuario. Se basan, además, en datos sobre cuya difusión las personas titulares no tienen ningún control[179]. A su juicio esto constituye un problema de seguridad mucho mayor que el de los umbrales de tolerancia y posibles tasas de error. Los datos biométricos pueden contribuir a completar la identificación, pero, en su opinión, no sirven como métodos de autentificación segura en escenarios en los que un tercero puede tener interés en suplantar nuestra identidad.[180].

5.3. Cuestiones que plantea la información personal directa o indirectamente expuesta ante los sistemas y procesos de reconocimiento mediante biometría.

La cuestión de la información personal que puede quedar directa o indirectamente en los procesos de reconocimiento biométrico ha sido un tema recurrente en los debates sobre la aceptabilidad de estas tecnologías, aunque en la documentación que hemos analizado no hemos encontrado estudios detallados, de conjunto, sobre la magnitud de este problema. En muchos documentos se *alude* a la cuestión, con carácter general, o a lo sumo se da algún ejemplo. Reflexionando sobre base de lo que en estos dos primeros capítulos hemos establecido como *la información biológica* (estática o dinámica) que sirve de soporte a estos sistemas, y atendiendo también a las limitaciones o dificultades que esa base biológica plantea al funcionamiento de los sistemas, hemos concluido que de forma colateral pueden quedar expuestas las siguientes informaciones personales:

---

178 WOLF, P.: "De l'authentification biométrique", *Securité des system d'information*, nº 46, octubre de 2003.

179 LANGENDERFER, J./ LINNHOFF, S.: "The Emergence of Biometrics", *The Journal of Consumer Affairs*, vol. 39, nº 2 2005, pp314 y ss.

180 Vid. también AUGER, D. *Biometrie: l'equilibre entre "liberté individuelle" et promesse sécuritaire serait-il impossible?*, Univ Paris 1, Pantheon-Sorbonne, 2005.

1) Informaciones que expresan por qué una persona es *atípica* para un sistema o, por el contrario, porqué su perfil le adscribe –injustamente- en el grupo de los *sospechosos.*

2) Informaciones relativas a la identidad sexual, especialmente en sistemas de reconocimiento que contienen filtros de género.

3) Datos de salud asociados a características biométricas estáticas o dinámicas.

5.3.1 *El estigma de los outliers* y de los que tienen *perfiles "buscados"*

Aunque hipotéticamente los sistemas de reconocimiento biométrico toman como base una característcia que es aceptada como *universal*, lo cierto es que su arquitectura se diseña, específicamente, para captar rasgos singularizantes y permanentes dentro de esa universalidad. Pero, como se ha dicho, esta hipótesis no tiene en cuenta las limitaciones de la universalidad, singularidad y permanencia, ni las carencias de las tecnologías que se han desarrollado hasta el momento. Ello explica que algunos sistemas de reconocimiento biométrico ofrezcan un mayor rendimiento si la mayoría de los usuarios a los que están destinados reúnen una serie de características que pueden asociarse, por ejemplo, a la etnia, el género, la ocupación laboral, la edad o el color de los ojos.[181] Ese mismo dato puede contemplarse también, claro está, desde otro enfoque: las personas que no encajan en el prototipo de sujetos diana, o los que resulta fácil confundir entre sí, están destinados a sufrir más dificultades de enrolamiento y unas tasas de error muy superiores a la media. Repasando algunas cuestiones ya mencionadas en las limitaciones:

> hay escáneres de huellas dactilares que estadísticamente presentan mayor dificultad para captar las huellas de mujeres asiáticas[182]; algunos escáneres faciales o de iris necesitan la cooperación del usuario manteniéndose en pie o manteniendo fijamente la mirada desde un ángulo concreto –excluyendo a quienes no pueden atender ese requerimiento[183] (véase la IMAGEN 70); y existen numerosos dispositivos que, aún basados en características biológicas aceptadas como razonablemente universales, no han sido diseñados para acoger, sin distinción y en condiciones de igualdad a cualquier ser humano.

Además de personas que resultan atípicas en el sentido de *estadísticamente discriminadas por la distribución de las tasas de error*, encontramos personas que resultan atípicas para el sistema en términos absolutos: los outliers. Personas que por el azar de la naturaleza o acontecimientos

[181] MORDINI, E. / ASHTON, H. "The Transparent Body: Medical Information", en MORDINI/TZOVARAS, p269-270
[182] STURGEON, 2004; NAVARTI/ THIEME/ NANAVATI, *Biometrics. Identity verification*, 2002.
[183] MAGNET, S. *When Biometrics fail*, p30.

posteriores al nacimiento carecen de los rasgos supuestamente universales que dan soporte al sistema, o que temporalmente -por una enfermedad, por ejemplo, se ven en esta situación. Aunque los patrones biométricos almacenados se guarden a buen recaudo, para estas personas enfrentarse a un dispositivo de reconocimiento supone exponerse a que esa circunstancia, esa singularidad, quede expuesta. El hecho mismo de *ser señalado como fuera del promedio humano* es una información altamente sensible y estigmatizante que hace que estas personas sean tratadas de forma diferente por una característica física. Ello genera daños en los grupos y personas vulnerables, en esa convivencia entre cuerpos e identidades diferentes que en teoría las sociedades democráticas dicen defender[184]. Piénsese que aún en los casos en que en el enrolamiento para obtener el DNI necesitemos ofrecer a alguien una alternativa –por ausencia de huellas dactilares, por ejemplo- una vez emitido ese documento, ese objeto, la persona puede acreditar su identidad cuantas veces sea necesario y del mismo modo que la acreditan cotidianamente el resto de los ciudadanos. Si exigimos que las personas muestran sus huellas cada vez que tomen un avión, hagan una transferencia bancaria o acudan a su puesto de trabajo, esta persona se verá enfrentada a su singularidad constantemente.

Imagínese la traslación de esa circunstancia a cualquier escenario de identificación. Si el sistema sólo tiene dos posibilidades de respuesta (MATCH/ NON MATCH), un usuario enrolado pero atípico se arriesga a los inconvenientes que constantemente tendrá ese NON MATCH; aun en el caso de que el NON MATCH aparezca con un asterisco (*), el individuo deberá explicar a la persona que gestiona en ese momento el dispositivo, porqué este sistema de reconocimiento tan infalible que se ha establecido lo deja, sistemáticamente, fuera. Tengo unas huellas muy finas, necesité cirugía facial, un problema en el nervio óptico me impide dirigir bien el ojo, el espectro de mi voz es demasiado grave…Con lo cómodo y "democrático" que resulta un carnet o un documento de identidad, idéntico para todas las personas; un documento que nace, sí, de la universalidad de que todos tenemos *un nombre*, pero que nótese: no reclama comprobar el nombre cada vez que se necesita alegar la identidad, sino sólo mostrar ese documento que, quitando las tres o cuatro lineas con los elementos singularizantes, es universal e idéntico para todos los usuarios.

Otro grupo de personas en alto riesgo de estigmatización son las que tienen patrones biométricos cercanos a lo que se hubiera determinado como *perfiles sospechosos.* Tener nuestro nombre o nuestro rostro guarden un gran parecido con un criminal buscado pueden resultar, sin duda, una importante fuente de problemas. Es probable que en alguna ocasión la policia nos intercepte o alguien denuncie habernos visto, incluso que se nos detenga y necesitemos aclarar el asunto con

[184] MAGNET, S. A. *When Biometrics Fail. Gender, Race and Technology of Identity*, Duke UP; 2011, p2.

algún abogado de por medio para que no vuelva a producirse esta situación. A veces a algunas personas se les llega a expedir un documento que terminan llevando adjunto al DNI para las veces en que se da el caso. Poco más puede hacerse. Ahora bien, imaginese la diferencia cuando estamos constantemente expuestos a sistemas de vigilancia automatizados que rastrean los grupos de población en busca de perfiles sospechosos. Es llamativo que de algunas tecnologías biométricas se predique que son *menos discriminatorias* que los controladores humanos; se ha dicho de ellos que la forma de vestir, la clase social, el aspecto físico no les influyen porque concentran su atención en la Biometría de que se trate. Esto, sin embargo, no es del todo cierto; no es cierto en los sistemas de verificación y de identificación porque, como se ha dicho, se diseñan siempre con la referencia de grupos diana y generan outliers relativos y absolutos; y lo es menos aún en relación con los sistemas de cribado. Los sistemas de cribado, por concepto, buscan perfiles que han sido enrolados como referencias para la búsqueda. En los sistemas de cribado con fines de seguridad, esos perfiles enrolados son *perfiles sospechosos.*

No es dificil imaginar cómo se multiplicarán estas situaciones si constantemente estamos expuestos a sistemas de vigilancia en los que se han registrado *perfiles sospechosos*. Algo así debió pensar Gaspar Llamazares cuando, com ya se ha dicho, se realizó un retrato robot de Bin Laden partiendo de una instantánea suya. En relación con esta idea se abordará un poco más adelante la cuestión del llamado perfilado racial.

Universitat d'Alacant
Universidad de Alicante

5.3.2. *Datos relativos al genero, la identidad sexual y la orientación sexual*

Aunque a diferencia de los escáneres corporales los sensores biométricos no detectan el género genital, algunos de los sensores pueden detectar características secundarias, por ejemplo en la geometría del rostro[185], y los sensores de huellas dactilares o de iris pueden permitir detectar detalles tales como la longitud de las uñas o las pestañas[186]. El concimiento científico en relación con las expresiones de la intersexualidad es cada vez más detallado, con lo que previsiblemente la capacidad para detectar estas peculiaridades en los patrones biométricos aumentará en el futuro. Más controvertidas son, sin embargo, tesis que tratan de vincular

[185] BURTON, A.M./ BRUCE, V. /DENCH, N. "What is the difference between men and women? Evidence from facial measurement", Perception 1993,22: 153–176.; GOLOMB, B.A./ LAWRENCE, D. T./ T.J. SEJNOWSKI. T. "SEXNET: A neural network identifies sex from human faces", en *Advances in neural information processing systems*, 1993, 572–577.; Brunelli, R./ Poggio, T. "HyperBF networks for gender classification". Proceedings of DARPA Image Understanding Workshop, 1992,, 311–314; MOGHADDAM, B./ YANG, M."Gender classification with support vector machines". *IEEE International Conference on Automatic Face and Gesture Recognition*, 2000, 306–311; BAUDOIN, J. Y./ TIBERGHIEN, G.. "Gender is a dimension of face recognition, *Journal of Experimental Psychology*, vol. 28 (2), 2002, pp362-3651; MOGHADDAM, Y., Learning gender with support faces", *Pattern Analysis and Machine*, 2002.

[186] MORDINI, E. / ASHTON, H., en E. MORDINI/ D. TZOVARAS (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p273-274.

patrones biométricos y preferencias sexuales, como por ejemplo las que vinculaban algunas tasas de asimetría con la homosexualidad en los varones[187].

En cualquier caso, respecto de cualquier sistema de reconocimiento en el que directa o indirectamente pueda quedar expuesta información relativa a la identidad sexual o a la vida sexual de las personas, ha de tenerse en cuenta que la exposición de esa información –y más aún la obtención y conservación de ésta- afecta al derecho a la vida privada. Esta información, además, puede generar consecuencias muy negativas en aquellas personas cuya identidad sexual u opciones de vida sexual estén expuestas a la discriminación, rechazo o incluso persecución.

Según los datos de AMNISTÍA INTERNACIONAL (2014) cerca de 80 países del mundo castigan la homosexualidad como delito y en diez de ellos puede llegarse a imponer la pena de muerte por mantener relaciones –adultas y consentidas- entre personas del mismo sexo. Entre las personas más vulnerables están las personas en las que el sexo genital y las características secundarias (o algunas de éstas) no coinciden. En sí misma, esa no coincidencia constituye una información lo suficientemente sensible, a lo ha de unirse que la no coincidencia entre sexo genético, género genital, genero biológico y género social puede revelar otros datos asociados como enfermedades genéticas, operaciones de reasignación de sexo, mutilaciones culturales o religiosas u orientación sexual, entre otras[188]. Nótese que la revelación de esta información no sólo puede generar discriminación o estigmatización; lamentablemente en algunos países estas personas sufren persecución y son objeto de prácticas inhumanas y crímenes de odio sin ser protegidas por las autoridades[189]. Incluso en los países occidentales, se ven obligadas a mantenerse asignadas a uno de los dos generos oficiales (hombre o mujer), y sólo se les permite modificar esa asignación si se someten a esterilizaciones obligatorias y a otros tratamientos como requisito legal previo para autorizar el proceso de cambio de sexo. No desear o no poder permitirse acceder a los procedimientos de reasignación supone que las personas no puedan actualizar su documentación[190].

Recientemente, en el año 2015, el Consejo de Europa se ha pronunciado sobre el hecho de que los padres de las personas que nacen con un sexo que no es claramente categorizable como hombre o mujer se vean forzados a escoger a favor de uno de los dos sexos y la conveniencia de reflexionar

[187] LEVAY, S. *Queer Science: the use and Abuse of Research in to Homosexuality*, MIT Press, Cambridge, 1996.
[188] HAMMARBERB, T. (Comisario de Derechos Humanos del Coe), *Informe Temático sobre Derechos Humanos e Identidad de Género*, Ed TvT,, Berlin, 2010. Acceso en www.transinterqueer.org
[189] HAMMARBERB, T. *Informe*, 2010.
[190] UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, *Discrimination and violence against individuals based on their sexual orientation and gender identity*, 4 de mayo de 2015.

sobre una identificación legal que no sea estrictamente binaria[191]. Los pocos países del mundo que tienen leyes que protegen la identidad sexual articulan, entre otros, mecanismos para modificaciones registrales u operaciones de reasignación, de forma que tampoco permiten una tercera opción. Sólo algunos países como Nepal, Nueva Zelanda o Bangladesh tienen formas de censo que incluyen tres casillas optativas para el género y emiten documentos nacionales de identidad o incluso pasaportes. En Europa Alemania ofrece la opción de emitir los certificados de nacimiento indicando género indeterminado, aunque a la espera de su asignación futura. Si estas dificultades documentales suponen para estas personas no pocos problemas, qué decir de sistemas de reconocimiento automatizados que, como parte de su funcionamiento, procedan a una categorización binaria de las personas según su sexo.

5.3.3 *Datos sobre el origen de las personas*

La información relativa al origen de las personas, sea a su origen familiar, sea en relación con la nación, cultura, etnia o cualquier tipo de vinculación similar, es considerada información sensible, en tanto respecto de algunas personas puede producir estigma y discriminación. La posibilidad de que los sistemas de reconocimiento mediante Biometría dejen directa o indirectamente expuesta esta información muestra un interesante abanico de posibilidades.

Lo mismo que los perfiles de ADN pueden servir para determinar que existe *o que no existe* vinculo genético entre dos personas, determinados tipos de reconocimiento biométrico pueden –aunque obviamente no con la misma precisión- dejar en evidencia la existencia o no de dicha proximidad, o mostrar proximidades llamativas. Que alguien descubra que su parentesco biológico es diferente de lo que pensaba o que lo lleguen a conocer terceros puede dar lugar a situaciones con relevantes implicaciones sociales, e incluso jurídicas.

También nos ha parecido interesante otra grupo de preocupaciones que, sobre todo los antropológos fisicos expresan en relación con algunas formas de diseño de los sistemas de reconocimiento biométrico. Y es el frecuente empleo que se hace de expresiones como etnia o raza en relación con dichos sistemas. Al igual que con el género, algunos sistemas emplean filtros *raciales* diseñados para pre-clasificar a los usuarios y agilizar así los procesos de identificación *1:n*. Por ejemplo, sistemas que aplican una clasificación binaria (asiático, no asiático[192]) o que detectan el color de la piel o del iris y emplean ese dato para sub-clasificar a los usuarios[193].

---

[191] COUNCIL OF EUROPE - Commissioner for Human Rights, *Human rights and intersex people, Issue Paper*, abril de 2015.
[192] OU, Y./ WU, X./ QIAN,H. / XU., Y. "A real time race classification system", *Proceedings of the2005 IEEE International Conference on Information Acquisition*, 2005.
[193] K. Harvati/ T. D. Weaver, "Human cranial anatomy and the Differential Preservations of Population", *History and Climate Signature*, 2006.

El concepto de raza es un concepto muy controvertido tanto en las ciencias sociales como en las ciencias naturales, aunque se coincide en emplearlo con la intención de destacar conjuntos de características que de algún modo expresan la cercanía entre algunos grupos de personas y, al mismo tiempo, sus diferencias respecto de otros. Pero aun siendo cierto que existen diferencias más o menos notables entre grupos de población, también son constatables las diferencias entre individuos que han sido designados como pertenecientes a un mismo grupo[194].

Se considera, por ello, preocupante que se estén recuperando acepciones de raza que se creían ya superados en los enfoques actuales de los estudios de poblaciones[195]. De hecho, hay sistemas de reconocimiento que subclasifican a los grupos de usuarios y se refieren a ellos con etiquetas que tienen esa alusión racial o étnica, lo mismo que los subdividen también a veces en grupos de edad o de genero, con el objetivo de que esas categorías grupales mejoren la eficiencia (sobre todo la agilidad) de los procesos de reconocimiento. Se corre el riesgo, sin embargo, de que se haga un mal uso de este tipo de clasificaciones, extrapolándolas o aplicándolas más allá de la arquitectura del sistema, algo que debería censurarse.

Esa tendencia a asociar determinados rasgos físicos con la pertenencia a países, etnias o culturas concretos queda en especial evidencia en algunos sistemas de cribado que han sido diseñados, específicamente, para perseguir *perfiles sospechosos*. El llamado *perfilado racial* no es nuevo. De hecho de algunos sistemas de reconocimiento biométrico se ha alegado, precisamente, una supuesta *neutralidad*, en el sentido de que los controladores humanos se ven influenciados por prejuicios que consciente o inconscientemente se expresan ante el aspecto de otras personas, sus formas de vestir o sus formas de comportarse. Esa supuesta neutralidad queda, sin embargo, en entredicho cuando hemos enrolado en un sistema de cribado una serie de *perfiles sospechosos* y todos ellos tienden a la búsqueda de varones, adultos jóvenes o personas de mediana edad, con rasgos físicos o comportamentales que se asocian con los países árabes o del medio oriente.

5.3.4 *Datos relativos a la salud de las personas*

La literatura distingue entre implicaciones médicas *directas* e *indirectas* de las tecnologías de reconocimiento biométrico, agrupando en el primer conjunto las consecuencias que para la salud de la persona puede conllevar el uso de estos sistemas y recogiendo en el segundo de los grupos las posibilidades de que junto con la Biometría (o como consecuencia de ésta) pueda ser

[194] LEWONTIN, R.C., S. ROSE,/ ET ALT. "Not in our genes", 1984; DOBZHANSKY, T. *Genetic diversity and human equality. Facts and fallacies in the explosive genetics and education controversies*, 1973

[195] WILKINSON, T. / STRKALJK, G. "The use of race concept in Anthropometry", *Applied Ergonomics* 36 (2005), 121-122; J. MARKS, *Human Biodversoty: Genes, RAce, and History*, Aldine de Gruyter, N. Y.

captada información médica de carácter personal. A esta segundo conjunto nos referiremos en el siguiente apartado, junto con otros tipos de información que puede obtenerse de forma colateral.

Se señalan dos tipos de posibles implicaciones directas, en el sentido de daños a la salud que pueden producirse con ocasión del uso de los componentes de un sistema biométrico. De una parte el riesgo de transmisión de enfermedades en sistemas en los que se produce un contacto físico, especialmente elevado en entornos en los que el riesgo para la bioseguridad es relativamente mayor (laboratorios de investigación biocientífica u hospitales, por ejemplo). El segundo grupo de implicaciones se refiere a los sistemas en los que se produce una exposición prolongada a radiaciones infrarrojas o cercanas al infrarrojo, aunque según el informe de IPTS no hay evidencias de riesgos significativos porque incluso en el caso del iris, en que el enrolamiento puede llevar entre treinta segundos y dos o tres minutos, se absorbe poca radiación[196].

No obstante, las mayores preocupaciones *médicas* en relación con el reconocimiento Biometría se han concentrado en las llamadas implicaciones indirectas. Es decir, en la posibilidad de que sea captada o se vea expuesta información médica de carácter personal.

Los sensores biométricos pueden captar características que ayuden a establecer, con más o menos precisión, la edad biológica que se estima en una persona, que no tiene por qué coincidir con su edad cronológica[197]. Por ejemplo, el grosor de la piel y las capas subcutáneas se ven afectados por el envejecimiento y estas circunstancias pueden apreciarse, por ejemplo, en la luminiscencia de la piel del rostro o en la calidad de los dermatoglifos. Al igual que talla o el peso, el color de la piel o del cabello, la edad (al menos la edad aproximada) es una información que los seres humanos ofrecen constantemente a las personas con las que interactúan; pero el hecho de ser una información que compartimos no implica que damos nuestra autorización para que esa información sea captada y almacenada con una finalidad y por un tiempo indeterminados. Las tallas bajas y el sobrepeso son condiciones que, en general, pueden discriminar a las personas (sea consciente o inconscientemente)[198], e implicar la captación colateral de información médica (como es el caso de anomalías genéticas que tienen expresión en la talla [199] o el haber sido sometido a una operación de cirugía estética[200]).

---

[196] JRC, *Biometrics at the Frontiers,* 2005, pp44-45
[197] MORDINI, E. / ASHTON, H. en E. MORDINI/ D. TZOVARAS/ H. ASHTON, en E. MORDINI/ D. TZOVARAS (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, p273-274.
[198] PUHLL, R.M./ C.A. HEUERL, "The stigma of obesity: A review and update", *Obesity,* 2009; BROWNELL, K./ PUHL, R. "Stigma and discrimination in weight management and obesity", *The Permanente Journal* 2003, 7(3): 21–23.
[199] CHUECA, ET ALTERE, *Anales del Sistema Sanitario de Navarra*, 2008.
[200] OLOGUNDE, R. "Plastic Surgery and the biometric ePassport: implications for facial recognition", *Journal of Plastic Surgery and Hand Surgery*, 2014.

Determinados patrones biométricos pueden, además, dejar expuesta información relativa a la salud toda vez que en las ultimas décadas ha aumentado significativamente nuestro conocimiento sobre las expresiones secundarias de algunas enfermedades. Al igual que algunos biomarcadores genéticos, determinadas biometrías estáticas o dinámicas resultan clave para detectar de forma precoz la presencia o predisposición a padecer a algunas enfermedades.

La ausencia de los dermatoglifos o su dificultad de lectura puntual o definitiva son, en sí mismos, datos médicos. También lo son las expresiones que algunos síndromes genéticos tienen en ellos (Síndrome de Down, o Sindromes de Turner y Klinefelder)[201], y existen estudios que abordan el impacto que en las impresiones dactilares tienen las las pseudo-obstrucciones intestinales crónicas[202], la leucemia y otros tipos de cáncer y el síndrome Rubella[203]. También hemos encontrado un estudio que asocian la asimetría en determinados patrones dactilares con la esquizofrenia o el trastorno bipolar[204] y algunas pecularidades faciales con la enfermedad poliquística renal[205].

Ha de tenerse en cuenta también que suele ser alguna peculiaridad captada en el rostro la que lleva a diagnósticos preliminares que son confirmados después con estudios clínicos más exhaustivos[206]. La forma de los labios, la nariz o los ojos son característicos en el Síndrome Prader Will o el Síndrome de Williams –Beuren, También el color de la piel puede aportar información sobre la población a la que una persona está vinculada así como poner de manifiesto que la persona padece enfermedades cuya expresión afecta al color de la piel (albinismo oculocutáneo; síndrome de Angelman; enfermedad de Addison; vitíligo o hiperpigmentación post-inflamatoria o causada por eccemas o acné), además de los efectos de implantes u operaciones de cirugía estética. También la forma de las orejas es una fuente de información en relación con algunos estereotipos de población[207].

---

[201] SKULER, M. "Finger and Palm Prints: A Window on Your Health", Glamour, 1984; Chen, H. *Medical Genetics Handbook*, W. H. Green, 1988, pp221-226.
[202] Estudio de M.M SCHUSTER del Centro John Hopkins, *Gastroenterology: Fingerpinting GI disease*, John Hopkins Physician Update, Abril de 1996, p5.
[203] WOODWARDS, *Biometrics: Identifying law and policy concerns*, 1999, p9.
[204] YOUSEFI-NOORAIE, R./ MORTAZ-HEDJRI, S., 'Dermatoglyphic asymmetry and hair whorl patterns in schizophrenic and bipolar patients', Psychiatry Research 2008, pp. 247–250.
[205] KHONSARI, R. H. / OHAZAMA, A./ RAOUF, R, / KAWASAKI, M, / KAWASAKI, K,/ PORNTAVEETUS, T./ GHAFOOR, S., "Multiple postnatal craniofacial anomalies are characterized by conditional loos of polycystic kidney disease (Pkd2)", *Human Molecular Genetics*, vol22, iss. 9, pp1873-1885.
[206] BOEHRINGER, S./ ET ALTERE, Genetic determination of human facila morphology, European Journal of Human Genetics, 2011, 19, 1192-1197; LIU, F. / VAN DER LIJN, F. / SCHURMAN, C./ ET ALT, "A Genome-wide Association study Identifies Five Loci influencing Facial Morphology in Europeans", *PLOS Genetics*, 2012, 8(9); JONES, K. L. / JONES, M.C. / DEL CAMPO, M. *Smith's Recognizable Paterns of Human Malformation*, 7ª ed, ELSEVIER, 2013.
[207] KAPIL ET ALTERE, *Morphological Variation of Ear for Individual Identification in Forensic Case*s, 2013.

Algunos sensores biométricos son también capaces de captar información relativo al cabello de una persona (especialmente las tecnologías de reconocimiento facial). El cabello tiene relación con la edad, el sexo o el origen genético de una persona, al tiempo que su forma, así como su presencia o ausencia puede proporcionar información sobre la identidad cultural o religiosa o la salud (hirsutismo, hipertricosis, alopecia areata, psoriasis o tratamientos con quimioterapia)[208].

Los ojos son también una fuente de información importante sobre la salud de las personas. En algún debate parlamentario, por ejemplo en el debate alemán previo a la adopción del pasaporte biométrico europeo, se mencionó la iridiologia y las corrientes que consideran que cabe relacionar diferentes sectores del iris con partes separadas del cuerpo, aunque no se han encontrado evidencias científicas de dicha atribución[209]. Sí que se ha establecido, en cambio, que determinadas condiciones médicas dificultan el reconocimiento mediante el iris[210]: keratoconus, degeneración retinal, retinitis pigmentosa., amaurosis congénita de Leber, degeneración macular o retinoblastoma, entre otros.

Pero la posibilidad de una captación colateral de información sobre la salud de las personas aparece de forma más pronunciada, si cabe, en la captación de las llamadas biometrías dinámicas. Se trata de patrones que, conforme al estado actual del conocimiento, resultan menos singularizantes, pero que sin embargo ofrecen mucha más información asociada que determinadas biometrías estáticas (véase la IMAGEN 54). De hecho en muchos de los casos los sistemas de captación emplean sensores similares –o idénticos- a los que se emplean en el diagnóstico médico y se consideran más invasivos para la privacidad que los sistemas de reconocimiento biométrico de primera generación. Según P. DE HERT, en el desarrollo de estas tecnologías ha jugado y juega un papel clave el deseo de monitorizar los comportamientos, de leer las mentes sin necesidad de conocer exactamente ante quién estamos realmente. Una identificación de la persona, pero llamativamente *despersonalizada*[211]. Desde el punto de vista de la privacidad, la falta de interés que algunos de estos sistemas muestran hacia la individualidad –incluso la dignidad de la persona- lleva incluso a afirmar que, precisamente por esa despersonalización, no afectan a la privacidad de nadie. Esto no es real. Cualquier dato que captamos de una persona es un dato de carácter personal y pertenece a su esfera privada. Es preocupante, en nuestra opinión, que las personas puedan verse confrontadas con información propia que a veces no conocen (ni desean conocer), o que sean caracterizadas y discriminadas por información dispersa con la que no se sienten identificadas.

---

[208] MORDINI, E. / ASHTON, H. pp277-27.
[209] BERGGEN, L. "Iridiology: a critical review", *Acta Ophtalm* 63 (1), 1985, 1-8.
[210] BORGEN, H. "Simulationg the influence of Aging and Ocular Disease on Biometric Recognition Performance", *IEEE Advances in Biometrics, Lecture Notes in Computer Science*, vol. 5558, 2009, pp857-867-
[211] DE HERT, P. "Biometric and the Challenge to Human Rights in Europe", en CAMPISI, 2013, pp496-508.

5.4 Los datos biométricos en relación con las prácticas de perfilado y la explotación de los *big data.*

La abundancia de datos digitales que son recogidos, almacenados y procesados en contextos públicos y privados de todo tipo está adquiriendo proporciones impresionantes. Se ha llegado a un punto en el que lo que marca la diferencia ya no es la cantidad de datos que se poseen, sino la capacidad para discriminar entre tanta información, separando lo valioso de lo que sólo es ruido y al tiempo asegurándose de conservar datos que quizás hoy parezcan ruido pero mañana se conviertan en información valiosa[212].

La expresión big data proviene de "explotación de los big data"; proviene del procesamiento de vastas cantidades de datos en diversos modos, con la finalidad de extraer o ingerir más información. Se emplea sobre todo en la identificación de las transacciones (con objetivos de marketing y comerciales); y con fines de seguridad, en relación con la gestión de identidades y transacciones asociadas a éstas[213]. El perfilado o profiling, por su parte, es la expresión que se emplea para referirse al descubrimiento de conocimiento en las base de datos (process of knowledge discovery in data bases, KDD). A la búsqueda de cuáles de las informaciones almacenadas resultan valiosas no se procede analizando los datos en categorías pre-definidas, porque ello no ofrecería nada que no se conozca ya; el perfilado implica emplear algoritmos que permitan hallar patrones y correlaciones inesperados; patrones válidos, nuevos y potencialmente útiles que estén de algún modo comprendidos en los datos que ya tenemos[214].

Universitat d'Alacant
Universidad de Alicante

Es una técnica aplicable a un individuo o a grupos de personas, pero también a animales, objetos o a las relaciones entre todos ellos; puede emplearse para clasificar, analizar o describir "algo ya sabido", pero también para inferir información sobre algo no sabido, algo deducido, algo predicho o algo esperable[215]. Los usuarios de los servicios en línea revelan grandes cantidades de información sobre si mismos y el volumen y la variedad de los datos generados no puede gestionarse a través de las tecnologías tradicionales de extracción y análisis de los datos; el control se realiza a través del desarrollo de los big data o datos masivos. No todos los datos masivos son personales; pero en muchas ofertas que se perciben como gratuitos la moneda de

---

[212] HILDEBRANT, M. "Who is Profiling Who? Invisible visibility", en S. GUTWIRTH/ Y POULLET/ P. DE HERT/ C. DE TERWAGNE,/ S. NOUEW (eds.), *Reinventing Data Protection?* , Springer, 2009, pp239s, 240-241.
[213] ASHBOURN, J. *Biometrics in the New World. The Cloud, Mobile Technology and Pervasive Identity,* Springer, 2014, p215-217.
[214] FAYYAD, U. M/ PIATETSKY-SHAPIRO, G (EDS.), *Advances in Knowledge Discovery and Data Mining,* AAAI Press- MIT Press, 1996, p6.
[215] GUTWIRTH, S. / HILDEBRANDT, M. "Some Caveats on Profiling", en S. GUTWIRTH/ Y. POULLET/ P. DE HERT (eds.), *Data Protection in a Profiled Wold*, SPRINGER, 2010.

pago es la información personal que se da[216]. Ello hace, advierte el SEPD, que además de ventajas estos mercados impliquen riesgos para el bienestar de los consumidores y de sus derechos a la privacidad y a la protección de datos.

La presencia de datos biométricos en ese conjunto de información masiva aumenta las posiblidades de injerencia en la vida privada de las personas, por las especiales características (la inherencia, la circunstancia de los datos sensibles que quedan directa o indirectamente expuestos, los riesgos de discriminación etc.) que hemos visto concurren en los casos en que se emplean con fines de reconocimiento[217].

Universitat d'Alacant
Universidad de Alicante

[216] Resumen ejecutivo del *Dictamen preliminar del SEPD sobre Intimidad y Competitividad en la era de la obtención de datos masivos*, 2015/ C 225/ 07.
[217] KNIGHT, A./ SAXBY, S. "Identity crisis: Global Challenges of identity prtection in a networked society*", Computer Law and Security Review* 30 (2014), pp617-632.

Capítulo 3

Análisis del funcionamiento de los sistemas biométricos contemporáneos en diferentes escenarios operativos. Estudio de casos.

1. ANÁLISIS DEL FUNCIONAMIENTO DE LOS SISTEMAS BIOMÉTRICOS EN DIFERENTES ESCENARIOS OPERATIVOS: PLANTEAMIENTO Y METODOLOGÍA.

1.1. ¿Cómo se juzga la aceptabilidad de una tecnología biométrica? La pregunta.

Con el objetivo de determinar el nivel de calidad y eficiencia que los sistemas biométricos ofrecen en el reconocimiento de las personas, y de valorar los beneficios y el coste de su aplicación, se han analizado anteriormente: las bases científicas de los sistemas (CAPITULO 1 de los resultados); y la arquitectura y funcionamiento de los mismos (CAPITULO 2). En el apartado 5 de este último se analizaron las implicaciones éticas y sociales de las tecnologías de reconocimiento biométrico, en conjunto, situando como referencia la protección de la privacidad de las personas. Corresponde así presentar en este capítulo los resultados que se han obtenido al investigar la calidad y eficiencia, así como las implicaciones éticas y sociales de estos sistemas desde la perspectiva de su aplicación a diferentes escenarios operativos. ¿Cómo se ha abordado esta parte de la investigación?

Universitat d'Alacant
Universidad de Alicante

Requerido por la Comisión de Libertades del Parlamento Europeo para evaluar el estado del arte y la aceptabilidad del uso del reconocimiento biométrico, el IPTS se vió en el año 2005 ante una tarea muy similar, aunque con una particularidad. Y es que como paso previo al análisis tuvo que idear una serie de escenarios, que casualmente situó en 2015, en los que los sistemas de reconocimiento biométricoa aparecían como elementos cotidianos de la vida familiar, los centros de trabajo o, entre otros, los servicios sanitarios. He aquí un extracto de esos casos[1]:

> *Año 2015 en una familia europea de clase media, con un hijo adolescente y un bebé (Louise). Constantin, el hijo adolescente, ha tenido problemas en la escuela por falsear el sistema de pago biométrico de la cafetería de la escuela con intención de ayudar a un amigo. La madre arranca su coche con la huella dactilar y acude a reunirse con el director, mientras la abuela, que ha sido reconocida como pensionista en el sistema de pago del autobús, discute con la encargada de la guardería porque el sistema de control no la reconoce como persona autorizada para recoger a Louise. Una puerta de acceso al hogar con Biometría del iris, fogones de seguridad que reclaman la*

[1] IPTS Biometrics, 2005, Ejercicios sobre escenarios, pp122ss.

geometría de la mano en la cocina y videojuegos que sólo entran en funcionamiento si el usuario es identificado como adulto forman parte de la escena.

En otro lugar de la misma ciudad dos médicos comentan las diferentes aplicaciones de que disponen: historias clínicas asociadas a la Biometría del paciente, chequeos de identidad en las zonas de maternidad o una puerta de acceso a la farmacia del hospital controlada mediante Biometría. En la sala de espera un hombre comenta con un conocido que el pasado verano, en las vacaciones, el control de iris del aeropuerto de Bangkok no le reconoció por el problema de glaucoma que sufre.

En la realización del presente trabajo, a diferencia de lo que le sucedió al IPTS, no hemos necesitado *imaginar* los escenarios, porque algunas de las aplicaciones biométricas que recogía esa simulación están, junto con otras, presentes ya en diferentes facetas de la vida de millones de personas a lo largo y ancho del planeta (IMAGEN 1). La tarea ha consistido, por lo tanto, en analizar los sistemas que están implementados, y en algún caso también los que están en fases de estudio piloto. Pero sí se nos ha planteado la segunda, y no menos importante cuestión a la que se enfrentó el IPTS. ¿Cuál va a ser el parámetro para realizar el enjuiciamiento? ¿Cuál es la medida de lo aceptable o no aceptable, de lo adecuado o lo no adecuado? Una vez recabados todos los datos relativos a estos sistemas, al modo en que operan y a las situaciones que se plantean en su aplicación en diferentes escenarios operativos, ¿cómo procederemos a enjuiciar su aceptabilidad?

1.2. Nuestra respuesta: con la misma referencia que juzgamos, en la actualidad, sistemas que con otros elementos ofrecen servicios similares.

La obtención y conservación de cualquier información personal implica una intromisión en la privacidad de las personas (y potencialmente limita el libre desarrollo de la personalidad); por ello, sólo es aceptable cuando: 1) mediando un interés colectivo se ha autorizado por ley su obtención; 2) o cuando, habiendo consentido las personas que se obtenga y almacene dicha información, la sociedad estime *que es adecuado y proporcionado* dicho uso.

Además de esa legitimidad de la aplicación de los sistemas en los diferentes escenarios operativos, la evaluación empleará como referencia estos criterios:

1.2.1. *Los principios de finalidad y proporcionalidad. Y la exigencia de que la información recabada sea adecuada, pertinente y no excesiva*

La obtención y conservación de datos de carácter personal sólo se estima legítima cuando responde a una finalidad adecuada y, además, respeta los principios de finalidad y de propocionalidad. Esto se aplica tanto en los casos en que son las autoridades las que desean recabar los datos, como en los que las personas consienten libremente dicha recolección. Aunque

medie consentimiento si la sociedad estima inadecuada una colección de datos, ésta no podrá realizarse. El principio de finalidad implica que los datos de carácter personal "*sólo deberán ser recogidos con fines determinados, explícitos y legítimos",* y que una vez se da cumplimiento a dicha finalidad, sólo excepcionalmente y bajo estrictas condiciones podría autorizarse su utilización con otros fines[2]. El principio de proporcionalidad, por su parte, se traduce que los tratamientos de datos sólo se autorizarán en la medida en que sea necesario y siempre y cuando no haya otro medio de la misma eficacia que afecte menos a la vida privada[3] (por resultar menos invasivo o por no emplear datos sensibles)[4].

1.22. *El consentimiento libre, requiere alternativas a la prestación de datos biométricos*

En la evaluación de la aplicación de un sistema de reconocimiento biométrico a un escenario operativo en el que los sujetos prestan su consentimiento de forma libre, ha de observarse si concurre algún factor que hace que la persona preste un consentimiento *viciado* al uso de sus datos. Por ejemplo: cuando se le invita a ceder los datos *por mayor comodidad*, restando importancia al riesgo que implica que ceda sus datos de carácter personal[5]; o cuando, existiendo éstas, no se le ofrecen alternativas menos invasivas para su identificación o las que se le ofrecen son más gravosas sin que exista una justificación para ello. Como garantía de *respeto a la autonomía del titular de los datos*, tanto el GT-WP como otras instituciones se refieren a la importancia de que en la relación con empresas que ofrecen bienes y servicios a los consumidores la cesión de patrones biométricos no quede *de facto* establecida como una *condición ineludible* del contrato[6].

Universitat d'Alacant
Universidad de Alicante

En ese sentido, se considera una garantía para la autonomía que los usuarios tengan la posibilidad de escoger medios menos intrusivos de su privacidad como alternativa al reconocimiento mediante Biometría. En aquellos casos en los que una persona no desee adherirse a la obtención de datos biométricos, debe dársele una alternativa de identificación, como un PIN o un documento de identidad tradicional, que son menos gravosos[7]. El GARANTE italiano (Supervisor de la

[2] SEPD, Dictamen de 2006, C 313/ 39, 18
[3] El hecho de que, (en definición del SEPD, Dictamen de 2006, C 313/ 39, 18). Así también el artículo 4.1.c) del Reglamento CE 45/ 2001 dispone que los datos tienen que ser adecuados, pertinentes y noe excesivos en relación a los fines para los que se recaben y para los que se traten posteriormente.
[4] SIMITIS,D: "Zur Internationalisierung des Arbeitsnehmerdatenschutzes", en HANAU, P./ HEITHER, F./ KÜHLING, J. (ed), *Richterliches*, 1999; DÄUBLER, W.: "Das neue Bundesdatenschutzgesetz und Seine Auswirkungen im Arbeitsrecht", *NZA*, 2001, pp874-881.
[5] RULE, J. B. *Privacy in Peril*, cit., 2007, p.87-88.
[6] Lo recuerda en la Opinion 3/ 2012, pp10-11.
[7] GARANTE, *Trattamento di dati personali biometrici per l'acceso a un complesso polifunzionale*, 1 feb 2007, doc 1381983, párr. 3.3.

Protección de datos en dicho país) afirma que sólo así puede garantizarse la libertad de elección y el compromiso de respetar el cuerpo humano en la utilización de las nuevas tecnologías[8].

Ayudaría mucho, no obstante, contar a nivel europeo con un precepto similar al que hemos visto que en Noruega limita el uso que se puede dar al DNI en las relaciones entre particulares. Dada la sensibilidad de los patrones biométricos y de las informaciones de la persona que, como se ha visto en el capítulo anterior, directa o indirectamente pueden quedar comprometidas en los procesos de reconocimiento sería deseable una previsión de este tipo en relación con la Biometría. Ello evitaría tener que esperar a que las agencias de protección de datos y los tribunales vayan depurando, caso por caso, criterios de interpretación en atención a las demandas que se les presenten.

Algun autor, como DE HERT, apunta más allá, indicando que quizá necesitemos sistemas para proteger a las personas de su propia inclinación a comerciar con su propia privacidad[9]. Se considera que en algunos casos es tan difícil apreciar si es legitimo y proporcionado usar una tecnología de reconocimiento biométrico que el consentimiento, aunque sea imprescindible, ya no puede ser considerado como un mecanismo "suficiente" en la protección de la privacidad de las personas[10],[11].

1.23. *El derecho al olvido*

Este derecho, el derecho al olvido, es expresado por algún autor como *el derecho a ser diferente de uno mismo*, o, más precisamente, el derecho a ser diferente –a tener una identidad diferente- de aquella persona que en algún momento fuimos en algún contexto social. Volviendo a la idea de Alain DAMASIO que citábamos en la parte introductoria, la identidad social es un artefacto, un constructo de los fragmentos que vamos dejando a nuestro paso; pero las personas tenemos *derecho al libre desarrollo de nuestra personalidad* (algo que recoge, entre otros textos jurídicos, la Constitución Española de 1978). La privacidad, decíamos, es la garantía de que tendremos un espacio libre, sin intromisiones, para ese desarrollo, y el derecho al olvido viene a ser la herramienta para recuperar esa parcela de privacidad que en un contexto concreto y con un fin concreto, temporalmente, nos vimos obligados o consentimos compartir.

El derecho al olvido abarca la cancelación de datos cuando resulta desproporcionado mantener una información personal que se captó legítimamente en su día, pero también el

[8] GARANTE, *Il decalogo su corpor é libertá*, Comunicado de 9 de mayo de 2006.
[9] DE HERT, P. Biometrics: legal issues and implications, Background paper for the IPTS, 2005, p38.
[10] HERRANZ, J. *La Biometría y su repercusión en los datos de carácter personal*, 2010.
[11] En el mismo sentido Nataša Pirc MUSAR, en AA. VV., "Workshop report. Restrictions on the Implementation of the EU Data Protection Directive", en *HIDE Newsletter*, vol. 2 (7), 2009, p2 y ss; HARB, B./ SCHMID, D. "Der Einsatz biometrischer Systeme", 2005, pp158-161.

derecho a eliminar información que ya no se corresponde con la identidad de la persona. El nombre, la nacionalidad, las relaciones paterno-filiales, la apariencia física, el género… las personas tienen derecho a realizar los cambios que consideren oportunos para poder vivir conforme a su verdad personal. Las posibilidades de mejora del ser humano, incluyendo los avances científicos y tecnológicos, abren un debate importante sobre los limites que ha de tener el ejercicio de este derecho pero, por lo que aquí respecta, queremos subrayar que la doctrina del Tribunal Europeo de Derechos Humanos reconoce esta interpretación del derecho a la identidad personal. Ningún *set de datos* que hayan captado de nosotros –aunque sea con fines legítimos- debería ser obstáculo para vivir conforme a nuestra verdad; y el derecho al olvido es la garantía del borrado de aquellos datos que, simplemente, han dejado de ser verdad, como debería suceder en los casos de reasignación del género. En ausencia, sin embargo, de una normativa que claramente establezca el modo en que ha de garantizarse este *olvido*, la única posibilidad que tienen las personas es la de acudir a las instituciones de protección de datos o a los tribunales a solicitar el borrado de los mismos.

Como ya se advirtió en otro lugar, el derecho al olvido resulta altamente difícil de ejercer en relación con los datos biométricos que hayan podido quedar expuestos a terceros. Nótese que cuando ha dado lugar a identificadores únicos basados en datos inherentes, aunque la persona cambie de nombre, nacionalidad o transforme su apariencia física es posible que sigan vinculándole. Habiéndose rechazado –al menos por el momento- el establecimiento de documentos de identidad vinculados a los perfiles de ADN, no tendría sentido que se aceptasen vinculaciones a captaciones biométricas que pudieran generar riesgos equiparables.

Universitat d'Alacant
Universidad de Alicante

2. TIPOLOGÍA DE LOS SISTEMAS DE RECONOCIMIENTO, ATENDIENDO A SU OPERATIVIDAD EN ESCENARIOS CONCRETOS.

2.1. Clasificaciones basadas en las *generaciones* tecnológicas y clasificaciones basadas en el tipo de entornos en los que se aplican, o las funciones que satisfacen.

Una forma de presentar y analizar los escenarios operativos en los que operan sistemas de reconocimiento que han operado u operan en la actualidad es agruparlos en generaciones. Como se vió anteriormente, este tipo de presentación se emplea también para describir o agrupar la tipología de tecnologías. Vimos que se distingue una primera generación de tecnologías, implementada fundamentalmente en los años 90 y comienzos del siglo XXI, y una segunda generación que afronta retos como la mejora de los rendimientos, la garantía de la privacidad o el desarrollo de nuevos tipos de sensores, representaciones de patrones y formas de comparación[12].

[12] JAIN , A. K. / ET ALT, en MORDINI/ TZOVARAS (eds.) *Second Generation*, 2010.

De cara al estudio de los escenarios operativos, esa clasificación bipartita nos ha parecido muy poco eficaz, en primer lugar porque, aunque se incorporan nuevos, los primeros escenarios operativos (instalaciones militares, control de zonas de seguridad o proyectos piloto para viajeros de bajo riesgo) se mantienen en la segunda generación. La clasificación, además, no permite expresar con eficacia los matices que diferencian a los entornos en los que tiene lugar la aplicación, la peculiaridad de los usos y los tipos de relaciones que en ellos se generan entre controladores y usuarios.

2.2. Clasificaciones que atienden al tipo de espacios o entornos en que tiene lugar la aplicación

Las tecnologías biométricas asumen roles en ámbitos operativos y cabe emplear la expresión *aplicación biométrica* para referirse a la conjunción de funcionalidades utilizaciones y roles que desempeñan. En opinión de David DAY La gran mayoría de las aplicaciones encajan en una de estas categorías:[13]

- aplicaciones de orden público o uso forense;
- chequeos de antecedentes; aplicaciones de vigilancia (localización, seguimiento e identificación de las personas en un área);
- control de las fronteras;
- reducción de los fraudes de identidad;
- programas de viajeros frecuentes; controles de acceso físico en puntos fijos;
- controles horarios;
- reconocimiento de consumidores;
- autentificación a distancia; protección de activos (información confidencial o material sensible);
- acceso a bases de datos.

Universitat d'Alacant
Universidad de Alicante

Puede decirse que cada aplicación emplea el reconocimiento biométrico para dar solución aun problema específico de reconocimiento.

Otras clasificaciones concentran su atención en las características de los entornos operativos. WAYMAN (ET ALT.) por ejemplo, tienen encuenta seis elementos para proceder a esta clasificación[14]. Así, los sistemas pueden ser:

- abiertos/ patentes o encubiertos (dependiendo, como hemos visto ya, de si el usuario conoce o no que se está captando su Biometría);
- requerir habituación o no (dependiendo de si necesitan o no que las personas estén familiarizadas con su uso);
- estar supervisados o no supervisados (según si hay un seguimiento del uso del dispositivo durante las operaciones);
- funcionar en ambiente estándar o no estándar;
- ser públicos o privados (dependiendo de quien administre el sistema)

[13] DAY, D. "Biometric Applications – Overview", *Encyclopedia of Biometrics*, Springer, 2009, pp76ss.
[14] WAYMAN, J. / JAIN, A. K. / MALTONI, D. / MAIO, D. en *Biometric Systems. Technology, Design and Performance Evaluation*, Springer, 2005, p7-9.

- y considerarse abiertos o cerrados, según se produzca o no intercambio de datos con otros administradores.

Así, por ejemplo, no es lo mismo dar a los usuarios oportunidad de que conozcan la existencia del sistema de reconocimiento, que diseñar un sistema para que funcione de modo encubierto; tampoco es intrascendente que los usuarios necesiten o no adiestramiento, si un gestor humano supervisará en tiempo real el funcionamiento del sistema o, entre otros, cuáles vayan a ser las condiciones ambientales en que se procederá a aplicar cotidianamente el sistema de reconocimiento (ambientes con o si control y, por ejemplo, variaciones en la temperatura, presión atmosférica, iluminación, etc.).

Un ejemplo de cómo se emplea esta clasificación puede verse aplicándola al *INSPASS (Immigration and Naturalization Service's Passenger Accelerated Service System)* que operaba entre los años 90 y principios de la década de los 2000 en varios aeropuertos norteamericanos (JFK de Nueva York, Newark, Los Angeles, Miami, Washington, Vancouver y Toronto). En el año 2002 fue sustituido por el Global Entry. INSPASS tenía como objetivo agilizar el acceso a los EE.UU. de los viajeros frecuentes. Es un sistema cooperativo (en el sentido de que require la cooperación del usuario), abierto y no-controlado (sin supervision humana directa); es un sistema público (cualquier viajero frecuente puede accede a el), es cerrado (porque no cede datos), no require un especial adiestramiento de los usuarios y puede emplearse en una serie de ambientes estándares con esa finalidad concreta.

Universitat d'Alacant
Universidad de Alicante

2. 3. Atendiendo a sus objetivos operativos

Los objetivos operativos de las tecnologías biométricas son tan diversos como las razones por las cuáles deseamos identificar a las personas o tratamos de encontrar a algunas de ellas[15]. Algunos sistemas buscan a personas cuya Biometría conocemos (enroladas) y otros a personas cuya Biometría –incluso cuya identidad- desconocemos. Algunos sistemas funcionan ante identidades alegadas, y otros verifican la presencia de una identidad no alegada, o puede que en sentido estricto no les importe tanto la identidad de un individuo como su pertenencia a un grupo.

La diversidad también se extiende al modo en que proceden; algunos captan en fresco uno o –por el contrario- múltiples patrones en una base de unos pocos o de cientos de millones de patrones previamente almacenados. Allí donde empleamos una llave, un tarjeta, un token… para acceder, para pagar, para abrir; en todos los lugares en los que hay una persona que controla una puerta de acceso, o comprueba si nos corresponde disfrutar de un derecho o de una prestación; en todas las

[15] WAYMAN, J. / JAIN, A. K. / MALTONI, D. / MAIO, D., 2005, pp4-5.

ocasiones cotidianas en las que se nos pide el DNI, un pase, un billete, una entrada… en todas ellas es posible establecer algún tipo de sistema de reconocimiento biométrico.

Resulta por ello muy difícil fijar una clasificación que, atendiendo a los objetivos operativos, nos agrupe los sistemas de forma eficiente. Hemos optado, por ello, por una clasificación que concentra su atención en los ámbitos de aplicación o escenarios operativos.

2.4 Clasificación empleada en este trabajo: atendiendo tanto a la tipología de escenarios operativos como a los objetivos que en ellos persigue el reconocimiento mediante Biometría.

1 LA BIOMETRÍA EN EL CONTROL DE LOS MOVIMIENTOS TRANSFRONTERIZOS Y EN LOS ESCENARIOS DE CONFLICTO BÉLICO.

1.1 Control de viajeros
1.2. Documentos de viaje con elementos biométricos
1.3. El control de la inmigración
1.4. Biometría y conflictos bélicos

2. LA BIOMETRÍA EN LAS RELACIONES ENTRE LOS ESTADOS Y SUS NACIONALES Y RESIDENTES.

2. 1 Lucha contra la criminalidad
2.2. Documentos de identidad de nacionales y residentes
2.3. La identificación en otros trámites con las administraciones públicas (registros tributarios, licencias de conducir, sufragio, etc)
2.4. El control de las ayudas sociales

3. LA BIOMETRÍA EN LAS RELACIONES ENTRE EMPLEADORES Y EMPLEADOS.

3.1. El control de recintos de seguridad (zonas militares y aeropuertos).
3.2. El control en las relaciones entre empleadores y empleados.

4. LA BIOMETRÍA EN LAS PRISIONES, HOSPITALES Y CENTROS DE ENSEÑANZA

4.1 Control de accesos y seguimiento; protección de zonas restringidas
4.2. Control de uso y sistemas de pago de servicios como las cafeterías o bibliotecas
4.3. Hospitales y programas de salud

5. LA BIOMETRÍA EN LA PRESTACIÓN DE SERVICIOS A LOS CONSUMIDORES

5.1. El control de abonados y de los socios
5.2 El ejercicio del derecho de admisión
5.3. Sistemas de pago y Banca eletrónica
5.4. Acceso a aparatos.
5.5. Algunas reflexiones de conjunto

6 BIOMETRÍA EN LA VIDEOVIGILANCIA "INTELIGENTE"

6.1. Cribado biométrico con biometrías fijas y biometrías dinámicas.
6.2. Almacenamiento disociado de datos biométricos.

3. La Biometría en el control de los movimientos transfronterizos y en los escenarios de conflicto bélico.

3.1 Control de las personas que cruzan las fronteras. Los *legales* y *los ilegales*. Algunas advertencias.

> Explica James Anderson[16] que las fronteras y los territorios fronterizos fascinan en su infinita diversidad, arbitraria permeabilidad y naturaleza contradictoria. Separan o unen economías, sociedades y culturas, países y personas de igual o de diferente nivel de desarrollo. Las fronteras son *barreras o filtros* que protegen contra un mundo exterior, pero también *puentes o puertas de acceso* a éste y *oportunidades de beneficio*, según la perspectiva desde la que las miremos; son además *símbolos ideológicos* –al menos para algunos-. Uno de los fenómenos más curiosos que se da en relación con las fronteras es, precisamente, que todas esas facetas de barrera, puente, oportunidad de beneficio o ideología), a veces se contradicen y otras, sin embargo, parece que se refuerzan entre sí[17].

El neoliberalismo ha impulsado una visión del mundo como una unidad global, sin fronteras para las oportunidades de negocio (capitalista). Pero ese oportunismo, como documentó David Bacon, nos ha traído también fugas de capitales, delincuencia transnacional, movimientos en masa de personas "*ilegales*", y una mayor polarización y división en las sociedades[18]. Las tecnologías biométricas, de las que se predica un potencial de singularizar con agilidad a cada ser humano, han encontrado un nicho de aplicación en el control de los movimientos transfronterizos. En como se usan estas tecnologías quedan reflejadas a la perfeccion esas contradicciones y paradojas de las actuales fronteras: las personas en tránsito se clasifican en distintos *estamentos.*

1) El iris de los pasajeros "de bajo riesgo", de los privilegiados que viajan por negocios o en ocio de alto *standing,* les permite cruzar fronteras con gran agilidad. Este privilegio suele ocultarse bajo el pseudónimo de *programas para viajeros frecuentes*, aunque la frecuencia de los viajes no consta entre los requisitos para ser admitido en ellos.

2) El resto de los viajeros es sometido a una criba biométrica en cada vez más fronteras a lo largo y ancho del planeta. Ello terminará por clasificarlos en tres grupos:

a. Los bienvenidos. Esto es, aquellos que se reconozcan como portadores de un título válido (un pasaporte, un visado un salvoconducto).

b. Los que se aceptan como *solicitantes de asilo* y, aceptados temporalmente, quedan a la espera de que se les confirme si finalmente son aceptados o no.

---

[16] Anderson, J. "Towards a theory of borders: States, political economy and democracy", *ANNALES. Series historia et sociologia*, 11, 2001, 2(26), p220.
[17] Anderson, J. "Towards a theory of borders", *ANNALES. Series historia et sociologia*, 11, 2001, 2(26), p220.
[18] Bacon, D. *Illegal People: How Globalization Creates Migration and Criminalizes Immigrants*, Beacon Press, 2009.

c. Los que recibirán la etiqueta de "*ilegal bodies*" (cuerpos ilegales)[19]. Aquellos que se viajan indocumentados, sin papeles o son interceptados en situación irregular y no son aceptados como solicitantes de asilo. En algunos países y regiones del mundo, como los EE.UU., Canadá, los Emiratos Arabes Unidos o la UE esta *etiqueta de ilegal,* vinculada a su Biometría, quedará almacenada y accesible para todos los puestos fronterizos asociados al sistema biométrico de que se trate (vid. infra el caso de *Qahtani*).

Sin necesidad de cruzar las fronteras, pero con una clara vocación de servir de referencia en el control de los movimientos transfronterizos, ha surgido otro escenario más de control biométrico de las personas. Nos referimos al que aplican los militares occidentales en zonas como Afganistán, Irak, Siria, Pakistán, etc. Aunque este control, como veremos, se justifica teóricamente por la necesidad de distinguir entre *combatientes enemigos* y *población civil (o no combatiente)*, lo cierto es que también se persigue captar datos de personas que en el futuro puedan desplazarse a países occidentales (sobre todo si lo hacen indocumentados o con pasaportes falsos) y rastrear, al mismo tiempo, si personas que fueron rechazadas en caliente en las fronteras de los países occidentales reaparecen en zonas *sensibles*, como Oriente Medio y Próximo.

3.2. Los programas de viajeros frecuentes.

Los controles de fronteras que persiguen poner freno a la inmigración ilegal o capturar a terroristas y delincuentes suponen un inconveniente para *el resto* de los viajeros. En ese conjunto, relativamente amplio, los gobiernos de cada vez más países han decidio privilegiar y mejorar el transito portuario y aeroportuario de un grupo de personas al que se refieren como *viajeros frecuentes*. Como ya se ha dicho, no se piensa en cualquier tipo de viajero frecuente, sino más bien en aquellos que suelen viajar en clase preferente, por negocios o representaciones institucionales, y tienen reservadas para sí las zonas más exclusivas de los aeropuertos. Piénsese, por ejemplo, en la cantidad de miembros y asesores de las instituciones europeas que viajan los lunes a Bruselas y vuelven a sus países de origen a pasar el fin de semana, o personas que trabajan en Londres pero tienen fijada su residencia en la Europa Continental, o que residiendo en Canadá tienen negocios en los EE.UU. o viceversa.

Desde la década de los 90 se vienen empleando en viajeros *frecuentes* sistemas automatizados con elementos biométricos en varios puntos de acceso a los EE.UU.. Entendiendo que el control biométrico excluía la suplantación, se enroló a los viajeros frecuentes y de bajo riesgo para agilizar su acceso a los medios de transporte; con ello, explicaba el INS, podían concrentrarse los

[19] VAN DER PLOEG, I. "The ilegal body", *Ethics and Information Technology,* 1999, pp295ss.

esfuerzos y recursos en el control del resto de personas[20]. Véase las IMÁGENES 3.f y 73. Los primeros dispositivos en emplearse fueron el INSPASS[21] de geometría manual (con versiones para aeropuerto y tierra), y los PORTPASS, con reconocimiento de voz. De forma similar, en Canadá se estableció en septiembre de 2002 el *CANPASS-Air*, un sistema de la Agencia de Aduanas Canadiense basado en tecnologías de reconocimiento del iris. La idea era la misma: permitir el acceso agilizado de personas que han sido autorizadas para su enrolamiento, por considerarse viajeros de bajo riesgo y que, además, fueran ciudadanos o residentes permanentes de los Estados Unidos de América o de Canadá (aeropuertos de Toronto, Vancouver, Calgary, Edmonton, Halifax, Montreal, Ottawa y Winnipeg).[22]

También existen sistemas de este tipo en Europa. En el aeropuerto de Schiphol, en los Países Bajos, las personas que han sido enroladas en la tarjeta *Privium Smart card* emplean su iris y su pasaporte para un acceso agil a las aeronaves. Esta tarjeta inteligente contiene un patrón del iris y los datos del pasaporte, y el sistema de reconocimiento lo que hace es comparar los datos almacenados en la tarjeta con, de una parte, el pasaporte que se le muestra y, de otra, el iris captado en fresco. Existen también sistemas similares en el aeropuerto de Heathrow (Proyecto IRIS) y en Frankfurt internacional, así como, desde agosto de 2015, en siete aeropuertos españoles y en el puerto de Algeciras. Vease en el anexo la lujosa sala de tránsito que se ha previso en Schiphol para los viajeros Privium (IMAGEN 1.5).

Conforme a la normativa europea los patrones biométricos captados con la finalidad de participar en estos programas de viajeros frecuentes no pueden ser cedidos para su uso con otros fines a menos que la persona lo consienta. Un elemento que contribuye a garantizar el buen uso de los datos es el hecho de que en muchos de estos sistemas no existe una base de datos central que almacene los patrones creados en el enrolamiento, sino que es el usuario quien lleva consigo esos datos, almacenados en un dispositivo integrado en una tarjeta inteligente.

3.3. El control "del resto "de movimientos transfronterizos, especialmente de la llamada inmigración *económica* y de los solicitantes de asilo

3.3. 1. La diferente motivación de las personas que viajan a otro país.

Dejando al margen a los viajeros ilustres, la mayor parte de las personas que se mueven de un territorio a otro ha tenido desde antiguo una situación *poco clara* en un esquema de poder

[20] WOODWARD, J. D. "Biometrics: Privacy's Foe or Privacy's Friend?", *Proceedings of the IEEE*, VOL. 85, n.. 9, 1997, 1480 y ss. 1482; HAYS, R. J. *INSPASS: INS Passenger Accelerated Service System*, 1996, http://www.vitro.bloomington.in.us:8080/ bc/REPORTS/INSPASS.html; DAVIS, A. "The body as password," 1997.
[21] BÄUMLER, 2001, p46.
[22] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008,, p103.

político organizado en soberanías territoriales. Esa situación sigue sin clarificarse en nuestra época, aunque ya no pude decirse que la inmigración sea sólo una cuestión territorial o nacional[23]. Conforme a los datos de la web *Flightradar* en 2014 se superaron los cien mil vuelos diarios, con un total de 2790 millones de pasajeros desplazados a lo largo de todo el año. De entre ellos 1133 millones viajaron a otro país, a los que se suman más de veinte millones que se trasladaron en barco según los datos de la Organización Mundial del Turismo (OMT). En esas estadísticas no están reflejados aquellos que viajaron por carretera ni, obviamente, los que arriesgan su vida cruzando por tierra o por mar sin apenas medios.

Una vez se intercepta a una persona en la frontera –o se localiza dentro del territorio a una persona que ha cruzado de forma irregular- se plantea la necesidad de distinguir entre:

1) Las personas nacionales (o, en Europa, los ciudadanos comunitarios), que tienen derecho a desplazarse libremente por el territorio y a establecerse donde consideren oportuno.

2) Las personas que acuden con visado de turista, estudiante u otro tipo de permiso temporal o definitivo.

3) Y aquellos que llegan sin ningún tipo de titulo que les permita acceder al país, y solicitarán asilo o permiso de acceso.

Pensemos ahora en el número de puertos, aeropuertos y estaciones de tren y autobús que hay en un país, más las fronteras terrestres. ¿Cómo gestionar el tránsito de todas las personas y proceder a clasificarlas con celeridad?¿Cómo saber si quienes llegan por tierra, mar o aire al territorio de un país vienen de visita o con intención de quedarse? ¿Cómo verificar que quienes llegaron temporalmente, retornan a sus países de origen cuando pasa dicho plazo?

- En algunos casos tendremos la referencia de la documentación (el pasaporte, el visado, un salvoconducto) y el reto será determinar que quien lo lleva es, realmente, su titular. III.3.2.2.
- En otros, sin embargo, no habrá soporte documental. Es comprensible que las personas que están en una situación irregular, sea cual sea, traten de esconder o incluso destruyan sus documentos para evitar se expulsadas o, según el caso, encarceladas. 3.3.2.3

3.3.2.2. Biometría en los documentos de viaje (visados y pasaportes)

Tradicionalmente en los Estados Unidos de América se ha visto como una amenaza que el Estado almacene información sobre los ciudadanos y, por ello, no se ha llegado siguera a expedir

[23] VAN DER PLOEG, I. / SPRENKELS, I. "Migration and the Machine-Readable Body: Identification and Biometrics", en DIJSTELBLOEM, H. / MEIJER, A. (eds.), *Migration and the New Technological Borders of Europe*, Palgrave MacMillan, 2011, pp68s, p68.

células de identidad –ni siquiera sin biometría-[24]. No han tenido, sin embargo, inconveniente en forzar que millones de ciudadanos de otros países, entre ellos los Europeos, se hayan visto obligados a incorporar biometrías a los pasaportes. Fue un cúmulo de factores lo que disparó este proceso, especialmente a partir de los atentados del 11 de septiembre de 2001 y la casi inmediata elaboración de la que se conoce como *US Patriot Act*[25]. Aprobada en el Congreso Estadounidense por 98 a 1 en el Senado y 357 a 66 en la Cámara de los Representantes, esta ley amplió considerablemente las potestades del gobierno en materia de vigilancia e intercepción de comunicaciones telefónicas, orales y electrónicas. Entre lo más significativo de esta norma, el hecho de que impusiera a los ciudadanos de muchos países del mundo, entre ellos a los españoles, la obligación de incorporar Biometría a sus pasaportes.

Para poder acceder a un país los viajeros que no sean nacionales necesitan *un visado* –o autorización temporal expedida por el país que acoge-. Mediante algunos acuerdos internacionales es posible que algunos países se comprometan a dar automáticamente visado a los nacionales de los países que forman parte del convenio, permitiendo que sus ciudadanos viajen únicamente con un pasaporte en vigor. Si no media este tipo de acuerdo, la persona que viaja debe tramitar con antelación un visado ante la embajada del país al que quiere viajar; ese visado, muchas veces, se expresa con un sello impreso en el pasaporte de la persona. Como consecuencia de la US Patriot Act, la UE ha incorporado Biometría tanto a sus pasaportes como a los visados.

Las discusiones sobre el pasaporte biométrico en la UE, en Australia[26] y en Suiza fueron muy interesantes. En este último país se realizó, incluso, una consulta en forma de referendo. Y es que se cuestionaba la necesidad de incorporar este tipo de elementos a los pasaportes. "*¿Cuántas personas han intentado acceder alguna vez a los EE.UU. u otro país con un pasaporte alemán falso?*", preguntaba una parlamentaria en el BUNDESTAG[27]. ¿Qué es lo que lleva a suponer que nuestros pasaportes pueden falsearse o que pueden cederse a personas distintas a sus titulares? ¿Qué justifica la introducción de elementos biométricos? Las preocupaciones, sin embargo, topaban de pleno con la amenaza de los EE.UU.: *no imponemos que todo el mundo lleve este pasaporte; solo decimos que: "todo el que no tenga un pasaporte biométrico deberá pedir un visado cada vez que viaje a nuestro territorio."*

[24] THIERER, A. / CREWS, W. (ed.), *Who Rules the Net. Internet Governance and Jurisdiction*, Cato Institute, 2003, xxiii-xviii.
[25] *Uniting and Strenghening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism Act* de2001, Pub L. Nº 107-56, 115 Stat. 272 (2001).
[26] Department of Foreign Affairs and Trade, "The Australian ePassport", 2009.
[27] La cámara baja del Parlamento de la República Federal de Alemania.

¿Cómo funcionan los pasaportes biométricos? Estos pasaportes se expiden con base en el registro civil, los padrones municipales y los DNI nacionales, pero tienen como peculiaridad el hecho de incorporar un chip incrustado en el que se almacena la Biometría dactilar y del rostro de la persona para la que se expiden. De este modo, cuando la persona va a cruzar la frontera se comprueba: 1) que lleva un pasaporte válido; 2) que ese pasaporte válido se emitió "para ese cuerpo". Si ya era difícil falsificar los pasaportes europeos, la incorporación del chip con Biometría del rostro y de las huellas dactilares reduce aún más la posibilidad de suplantación.

El Reglamento 2252/2004[28] detalló que elementos biométricos debían incorporarse (facial y dactilar) y la conservación de los datos, insertos en un CHIP, *bajo el control del usuario*. Un problema que se plantea, con todo, es el hecho de que terceros países procedan a almacenar la información recogida en los microchips cuando viajamos a sus territorios. Esto sucede, por ejemplo, en algunos puntos de acceso a Rusia. ¿Podemos culpar al ePass de esta *usurpación de datos*, y de la desprotección en la que queda nuestra privacidad? En puridad cualquier país no europeo puede obligarnos a dejar captar nuestra Biometría como condición para entrar en su territorio; no olvidemos que deseamos entrar en su espacio de soberanía. Así que no debemos culpar tanto al chip, cuanto a la ausencia de una norma internacional que impida el almacenamiento masivo de datos de viajeros.

3.3.3 *Los sistemas de control de las personas que viajan "sin titulo válido" y de las que solicitan asilo. En especial EURODAC.*

Como ya se ha dicho, a toda persona que pise un territorio nacional sin titulo legítimo (o sin documento que acredite que tiene autorización para entrar) se le aplica algún tipo de medida. Algunas son expulsadas en caliente y con otras se realiza un estudio de situación hasta que se determina si merecen o no ser aceptadas como refugiados.

En aplicación de la normativa de las Naciones Unidas[29] la condición de refugiado se reconoce: "*a toda persona que, debido a fundados temores de ser perseguida por motivos de raza, religión, nacionalidad, opiniones políticas, pertenencia a determinado grupo social, de género u orientación sexual, se encuentra fuera del país de su nacionalidad y no puede o, a causa de dichos temores, no quiere acogerse a la protección de tal país*", o al apátrida "*que, careciendo de nacionalidad y hallándose fuera del país donde antes tuviera su residencia habitual, por los mismos motivos no*

[28] Reglamento modificado por el Reglamento CE 444/ 2009, del Parlamento Europeo y del Consejo, de 28 de mayo de 2009.
[29] Convención sobre el Estatuto de los Refugiados, hecha en Ginebra el 28 de julio de 1951, y su Protocolo, suscrito en Nueva York el 31 de enero de 1967.

puede o, a causa de dichos temores, no quiere regresar a él". El Estado receptor se ve, por ello, ante la situación de tener que determinar si en la persona que llega concurren, o no, estas circunstancias. La referencia en esta toma de decisión son convenios de cooperación, como el Acuerdo Schengen y el Tratado de Prüm, que abordan no sólo la lucha contra la inmigración ilegal, sino también el terrorismo o el tráfico de personas.

Sistemáticamente, especialmente en Norteamérica y de forma creciente en Europa, se procede a enrolar la Biometría de todas las personas que llegan sin titulo válido, aunque el fondo y las formas de estos controles no son iguales. El control en Norteamérica es muy severo; distintas biometrías de las personas (sobre todo las diez huellas dactilares y el iris) son tomadas de todas las personas que llegan, aún incluso en el caso de que sean devueltas en caliente. A esa información tienen acceso numerosas agencias gubernamentales, con el objetivo de poder cruzar datos sobre la geolocalización de personas que –por ejemplo- habiendo sido captadas en algún conflicto en Oriente Medio, después tratan de acceder con pasaporte de otro país a los EE.UU.. En el caso de la UE, la forma de aplicar este control ha venido siendo algo más comedida, aunque hemos de advertir que este trabajo se cierra en plena crisis del Acuerdo Schengen y con el anuncio de un próximo endurecimiento del control en las fronteras con ocasión de las masas de personas que procedentes de Siria han comenzado a llegar a la UE en la segunda mitad del año 2015. La cantidad de datos y la finalidad con la que éstos pueden emplearse están, como se explicará a continuación, mucho más acotadas que en EE.UU., a pesar de que han existido propuestas de que interoperen todas las bases disponibles.

Según el código de fronteras de Schengen cuando los viajeros tienen una visa para poco tiempo o no tienen visa, las autoridades del país en el que estén deben chequear su entrada y valorar si representan una amenaza para el orden público, la seguridad internacional, la salud pública o las relaciones internacionales entre los Estados asociados al Convenio de Schengen. Entre las herramientas con las que cuentan está la consulta a las bases del sistema SIS, en el que puede estar recogido, por ejemplo, que una persona está buscada por por la policía[30] o que necesita protección. Además de consultar las bases, se indagan los motivos del viaje, si tiene fondos para asumir la estancia proyectada y si los documentos que porta son válidos. Obviamente quienes tratan de alegar, sin ser cierto, que son originarios de un país en guerra (como Siria, Sierra Leona o Eritrea) ocultarán o destruirán los papeles e inventarán historias con las que engañar a las autoridades; y demostrar que son perseguidas por su orientación sexual o por su ideología puede resultar una tarea imposible. Desde el punto de vista de los controladores también es difícil decidir si las personas merecen o no el asilo, y más aún cuando las personas no tienen papeles ni embajadas que las reconozcan o que refrenden sus historias. Parece como si las tecnologías de

[30] VAN DER PLOEG, I. / SPRENKELS, I. *Migration and the Machine-Readable Body*, cit. 2011, pp69-70.

reconocimiento biométrico hubieran llegado en un momento en el que las autoridades de inmigración estaban "desesperadas" por encontrar medios de producción de identidades que contraponer a las historias que narran personas[31].

EURODAC fue el primer sistema automatizado de reconocimiento biométrico de base institucional en la UE, y entró en funcionamiento en enero de 2003, con base en el Reglamento (UE) 2752/ 2000, para la aplicación de la Convención de Dublín[32]. Se trata de un sistema de chequeo que comprueba, en una base de datos centralizada, si unas huellas dactilares concreta están o no registradas[33] y consta que pertenecen a alguien que ha solicitado asilo en otro país, alguien a quien se le denegó o alguien a quien, por algún motivo, no le está permitido solicitar asilo. Con ello trata de evitar el *asylum Shopping*, esto es, la solicitud simultánea de asilo en varios países con el objetivo de escoger el más favorable o los intentos de acceder con diferentes identidades. No obstante, su uso se ha extendido hasta abarcar no sólo a los que efectivamente solicitan asilo, sino a todos los inmigrantes *potencialmente* irregulares de al menos 14 años de edad. Así, quienes han sido detenidos tratando de cruzar ilegalmente las fronteras o por permanecer irregularmente en un Estado Miembro de la Unión, quedan también incorporados a EURODAC.

El sistema VIS, por su parte, es un sistema creado como apoyo para emitir un tipo de visado que es válido para toda la UE y que sustituye a los que emitían los Estados. El Reglamento CE nº 767/ 2008 sobre el sistema de Información de Visados previó una aplicación progresiva del sistema VIS, de acuerdo con criterios tales como el riesgo de inmigración ilegal, las amenazas a la seguridad interna de los Estados miembros y la viabilidad para una recogida de datos biométricos de todas las localidades de una región. Este sistema de información de visados (o SIS) se puso en marcha en 2009 para una serie de regiones del mundo: el Norte de África, Oriente Próximo y la región del Golfo fueron seleccionadas. Uno de los inconvenientes que plantea este sistema SIS, en comparación con EURODAC, es que sí almacena información sobre cada uno de los individuos, lo cuál que, potencialmente, pueda servir a más fines que los que inicialmente han dado lugar a su creación y, paradójicamente, restringe el tipo de consultas que pueden hacerse al mismo[34].

Desde el punto de vista político-jurídico, más que la creación de estas bases lo que se ha cuestionado en la UE es qué tipo de datos incorporan y cuáles son los grupos de población que son enrolados en los sistemas. Preocupa también, y mucho, la propuesta de que dichas bases –junto con otras bases de la Europol, Eurojust o de las sistemas de información nacionales- puedan llegar

[31] VAN DER PLOEG, I. "The Illegal body: 'Eurodac? And the politics of biometric identification", *Ethics and Infomation Technology* 1/ 1999, pp295-302.
[32] La Convención de Dublín se sustituyó por el Reglamento del (CE) n° 343/2003 del Consejo.
[33] VAN DER PLOEG, I. / SPRENKELS, I. Migration and the Machine-Readable Body, cit., p83-84.
[34] BROUWER, E. R. en *Digital Borders and Real Rights*: *Effective,* Brill, 2008, p137.

en algún momento a interoperar[35]. En este sentido, se ha producido un debate polarizado entre, de una parte, las autoridades de seguridad interior y exterior y, de otra, las autoridades a las que está encomendada la protección de datos de carácter personal. A favor de promover la interoperatividad se ha mostrado el Consejo Europeo (en el que participan todos los gobiernos de los Estados Miembros) y la Comisión. El Consejo Europeo, en su declaración sobre la lucha contra el terrorismo de 25 de marzo de 2004, invitaba a la Comisión a realizar propuestas sobre la interoperatividad del sistema Eurodac (y VIS), junto con otras bases de datos, *a fin de poder poner dicha información al servicio de la prevención y lucha contra el terrorismo*[36]. En respuesta, la Comisión publicó en 2005 una comunicación sobre la mejora de la efectividad, interoperabilidad y sinergias entre las bases de datos de la UE. Entre las bases de datos con las cuáles se proponía la interoperatividad estaba la base SIS y su versión de segunda generación, el SIS II, aunque se registraron también propuestas sobre la creación de un AFIS Europeo (European Criminal Automated Fingerprints Identification System) o un registro unificado de los pasaportes y tarjetas de identificación de los ciudadanos de la UE. Frente a esta opinión, encontramos sin embargo la respuesta de las autoridades a las que está encomendada la protección de datos de carácter personal. El SEPD y el GT-WP 29 fueron contundentes al expresar su preocupación por los almacenamientos masivos tanto en casos como los de los visados[37], como en los de los pasaportes o los salvoconductos y afirmaron que no estaba justificada la creación de una base de datos centralizada que contuviera los datos personales y, en particular, los datos biométricos de todas las personas autorizadas a recibir un pasaporte[38], un visado o un salvoconducto. Que ello vulneraba el principio de proporcionalidad[39].

Los Estados Unidos y Canadá, sin embargo, hace años que registran datos biométricos de o viajeros, y se centralizan en sistemas como IDENT. En el aeropuerto de Ben Gurion, en Israel, también se instaló un sistema de geometría manual en 2001[40] y en Australia, el departamento de Inmigración y Ciudadanía comenzó a configurar una base da datos de escaneado facial, dactilar y de iris hace unos años, con la intención de conectarlo con un sistema de procesamiento global de

[35] Dictamen de 23 de marzo de 2005 sobre la propuesta del Sistema de Información de Visados (VIS)y el intercambio de datos sobre visados de corta duración entre los Estados Miembros (COM 2004 83 in fine, DO C 181).

[36] DE HERT, P. / GUTWIRTH, S. "Interoperability of Police Databases within the EU?", *International Review of Law Computers & Technology*, vol 20, 1-2/ 2006, pp. 21-25; J. A. LEWIS, J. A. "Biometrics and Security", *Center for Strategic & International Studies*.

[37] Opinión 3/ 2005 del GT-WP 29, relativa al sistema SIS II; Opinión 7/ 2004 sobre la inclusión de elementos biométricos en los permisos de residencia y visados teniendo en cuenta el establecimiento del Sistema Europeo de Información Sobre visados (WP 96), adoptado el 11 de agosto de 2004.

[38] Dictamen de 23 de marzo de 2005 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS); Dictamen de 19 de octubre de 2005 sobre tres propuestas relativas al Sistema de Información de Schengen de segunda generación (SIS II), COMO 2005 230 final, COM 2005 236 final, y COM 2005 237 final, DOUE C 91.

[39] C 313/ 38, inciso 3º del apartado 12.

[40] REDPATH, J., "Biometrics and International Migration Law", en Integration al Migration Law, nº 5/ 2005.

tramitación de los visados para todas Australia. Los datos de los extranjeros que entran en Australia pasarían así a almacenarse en un registro central para verificar la identidad y hacer chequeos cruzados entre el departamento federal y los cuerpos de control anti-fraude nacional e internacional, además de los sistemas de control de las fronteras[41].

También ha de destacarse el sistema que se emplea en los Emiratos Árabes, por la elevada tasa de personas enrolados. La policía de Abu Dhabi instaló en 2001 un sistema de reconocimiento del iris en el control de aduanas de tierra, mar y aire. Implica el enrolamiento del iris de los prisioneros y los expulsados de los centros de deportación de los Emiratos Árabes Unidos. El sistema chequea en tiempo real *1 a n* el iris de todos los pasajeros que llegan de visita o tratan de usar un visado en cualquier control aduanero de los EAU. Con novecientos mil enrolados en el año 2008, su base de datos de iris era una de las mayores en todo el mundo. Según los datos oficiales, en siete años de funcionamiento impidió la entrada de sesenta y cinco mil personas que trataban de entrar empleando nombres falsos, en algunos casos probando suerte en varios puntos aduaneros en el mismo día.

3. 4. Biometría y conflictos bélicos. Control encubierto y preventivo de la inmigración futura.

En el siglo XVII Hugo GROCIO, en sus libros sobre el *Derecho de la Guerra y de la Paz*, explicaba que *por causas justificadas* puede que: tengamos que defendernos; debamos obtener aquello que es nuestro o que en justicia nos corresponde; o nos corresponda responder a otro imponiéndole un castigo. La guerra, viene a decir Grocio, es a veces algo necesario. Esa construcción teórica de *la guerra justa* no es, sin embargo, fácil de trasladar a la práctica. Y es que aún aceptada la necesidad, siglos después seguimos discutiendo sobre cómo establecer: qué es la autodefensa y cuándo está justificada, qué es lo que *en justicia corresponde* (y *a quién*), y en que modo resulta legítimo recuperar lo que es nuestro o castigar al enemigo[42]. Entre tanto, y esto es curioso, sí que al menos hemos establecido un conjunto de normas internacionales sobre lo que es (y no es) aceptable en los escenarios de guerra y en los de posguerra (el *Ius in Bello*, y el *Ius post Bellum*).

El problema es que esta tradición de la guerra justa se desarrolló en torno a conflictos en los que los enemigos eran culturalmente similares, y aceptaban al enemigo como un ser humano con identidad moral similar a la propia. En muchos de los conflictos actuales, en los que los enemigos

[41] LIU, Y. "Privacy Regulations on Biometrics in Australia", 2010, pp355-367.
[42] CANEY, S. *Justice Beyond Borders*, Oxford Universiy Press, 2006, pp192-194.

difieren en creencias religiosas, lengua, etnia o cultura, y además tienden a considerarse unos a otros de menor dignidad moral, parece que ya no hay demasiado espacio para ese *Ius in Bello*[43].

En cualquier caso, la comunidad internacional sigue esperando que los combatientes traten, por ejemplo, de minimizar los daños colaterales. Y dentro de ese objetivo ha sido frecuente en el último siglo que soldados de uno y otro bando identifiquen sistemáticamente y clasifiquen a las personas en una de estas categorías: de una parte, los *combatientes enemigos; de otra, las personas no combatiente*s (población civil, refugiados en tránsito, sanitarios, ONGs, fuerzas amigas, etc.). Esa clasificación, nótese, no es irrelevante, puesto que legitima o resta legitimidad a los posibles objetivos de los ataques e intervenciones.

> Hemos encontrado explicación de esta forma de proceder en las Reales Ordenanzas del Ejercito español de Tierra: "*El centinela que observe que una persona o grupo sin identificar se acerca a su puesto le dará el alto diciendo: "¡Alto al centinela! ¿Quién va?". Si la respuesta no es convincente o su actitud es sospechosa dará la voz de:.¡Alto o disparo!", y avisará a la guardia accionando el sistema de alarma. Si el individuo o grupo no obedeciera* –dicen las ordenanzas- *usará el arma,"*[44].

Las posibilidades de "respuestas no convincentes" aumentan en un escenario en el que existen enemigos con alta movilidad, que se esfuerzan en eludir cualquier tipo de afiliación real. Emplean alias, tienen documentos oficiales con identidades falsas y ya no son personas uniformadas en escenarios tradicionales de combate; visten de civil y actúan de incógnito ante los ciudadanos de a pie. Ante esta situación, el reconocimiento mediante Biometría ha encontrado un importante espacio de expansión y, de algún modo, es donde con más claridad se expresa esa idea de querer distinguir *a los lobos entre los corderos.* De forma masiva la información biométrica se obtiene, procesa y almacena por fuerzas militares, que en el caso de los EE.UU. colaboran estrechamente con otras agencias gubernamentales (como el FBI o el Departamento de Interior, e incluso autoridades locales). Cooperan, además, con las fuerzas aliadas. Por ejemplo, es sabido que las fuerzas armadas canadienses y estadounidenses que operan, entre otros, en Afganistán emplean tecnologías biométricas. El sistema HIDE (Handhad Interagency Detection Equipment) de las fuerzas Canadienses registra datos biométricos del rostro, de las huellas dactilares y del iris y los envía a una base de datos central en la que se informa, en minutos, de si la persona es sospechosa de ser una amenaza para la ISAF (International Security Assistance Force) de la OTAN[45]. IMAGEN 75.

---

[43] MOSELEY, A. "Just War Theory", en *The Internet Encyclopedia of Philosophy*, ISSN 2161-0002, http://www.iep.utm.edu/.

[44] Art. 383 del Real Decreto 2.945/1983, de 9 de noviembre, por el que se aprueban las Reales Ordenanzas del Ejército de Tierra (España).

[45] MITCHELL, A. "Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics", *Canadian Yearbook of International Law*, 50 2012 (2013), pp289ss.

Otro sistema que se emplea en las zonas de conflicto es el que estableció el ACNUR en octubre de 2002, para reconocer mediante iris a las personas afganas refugiadas en Pakistán. Como parte de los procesos de repatriación, las personas son autorizadas para recibir un único paquete de asistencia que incluye apoyo básico y subvención para el viaje. El objetivo del sistema es detectar los fraudes y evitar que las personas reciban la ayuda más de una vez, por equidad respecto del conjunto de las personas que están en esta situación. El enrolamiento es anónimo (no se asocia a datos), siendo así que el sistema sólo comprueba que el patrón de iris que se le muestra en fresco no está enrolado como perteneciente a alguien que ya recibió ayuda. Desde su creación y hasta el año 2008 se calculó que aproximadamente cinco mil personas se enrolaban voluntariamente en el sistema[46]. En 2005 comenzó a emplearse el mismo sistema en Congo.

La introducción de estas tecnologías ha contribuido, según las fuerzas armadas de países como Canadá, a mejorar la seguridad de los soldados que operan en Afganistán y ha facilitado, dicen, la captura de los enemigos. Pero algunos países emplean también esta información con fines muy distintos a la distinción entre combatientes y *no combatientes*. Existe un objetivo adicional, cual es el de detectar a personas con *perfiles de alto riesgo* que en el futuro puedan desplazarse a los países occidentales. Este hallazgo es citado como muestra de la *dominación identitaria* de las fuerzas armadas como las estadounidenses; al igual que en otras artes de la guerra (como el desarrollo de armas y estrategias), existe una lucha por dominar las amenazas terroristas y para la seguridad nacional a través de la dominación de las identidades. Esa dominación pasa por vincular biométricamente a un combatiente enemigo o a una potencial amenaza para la seguridad nacional con sus identidades y actividades pasadas, especialmente las relacionadas con el terrorismo u otros crímenes[47]. ¿Ha sido arrestada esta persona en los EE.UU. o en otro país? ¿Usa alias o documentos oficiales falsos? ¿Ha sido detenida por los EE.UU. o las fuerzas de la coalición, o se le ha denegado la entrada en algún territorio? ¿Tiene vínculos con alguna actividad terrorista? ¿Se han hallado sus huellas en los restos de algún dispositivo de explosión, o ha sido visto en alguna multitud cometiendo algún acto de terrorismo?

Como suele suceder, a las críticas a este tipo de prácticas suele responderse con algún caso *espectacular*. Así por ejemplo, se cuenta el caso de la detención del llamado *Secuestrador número 20* de los atentados del 11-S. En diciembre de 2001 las fuerzas militares estadounidenses detuvieron a Mohamed Al Qahtani en el Sudeste de Asia; en los interrogatorios Qahtani, con una identidad falsa, negaba ser un combatiente y explicaba los motivos –inocentes- de su presencia en la región; pero mientras estaba bajo la custodia de los militares, el FBI tomó las huellas rodadas de

[46] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008, p105.
[47] WOODWARDS, J. J. "Using Biometricts to Achieve Identity Dominance in the Global War on Terrorism", *Military Review*, sept-oct 2005, pp29-30.

sus diez dedos (de uña a uña) y las remitió para su estudio a los Estados Unidos. El sistema advirtió que unas huellas similares habían sido*"rechazadas en frontera"* en el aeropuerto JFK de Nueva York agosto de aquel mismo año; he aquí una prueba del almacenamiento de los *ilegal bodies* al que nos referíamos al principio de este apartado. Pero no solo eso; además, se estimó que aquellas huellas coincidían con las de un individuo al que en la investigación de los atentados del 11-S se había dado el nombre del *secuestrador número 20.* Un secuestrador que, realmente, no fue tal, porque no accedió al territorio estadounidense, ni por tanto a los aviones. Pero las fuentes policiales entendían demostrado: 1) que había pruebas de que los terroristas (que sí cometieron los atentados) esperaban a una persona más ; 2) que, de hecho, habían preparado su llegada, pero éste nunca llegó; 3) y que dado que le esperaban el mismo día y en el mismo aeropuerto en que Qahtani fue devuelto en caliente, *era obvio que debía ser el.*

Este caso, además de para hacerse una idea del fin con que se recaban los datos, genera una cierta preocupación sobre la forma en la que la información biométrica se asocia a muchos otros datos, a veces contrastados y otras veces no tanto. Vemos con preocupación el impacto que estas formas de "inteligencia" pueden estar teniendo y tendrán a futuro en los derechos de las personas.

4. LA BIOMETRÍA EN LAS RELACIONES ENTRE LOS ESTADOS Y SUS NACIONALES Y RESIDENTES.

4. 1. Entre el miedo al control, y la necesidad de identificación.

La relación entre los ciudadanos y los gobiernos ha sido un espacio de histórica preocupación en lo que se refiere a la privacidad de las personas[48]; la obtención masiva de datos y, en especial, su gestión centralizada son vistos como algo peligroso, pero parece difícil–si no imposible- que los Estados puedan mantener relación con la ciudadanía, recabar impuestos, gestionar el derecho de sufragio o prestar servicios de todo tipo (sanidad, educación, etc.) sin una forma que garantice la identificación de las personas. ¿Cuál es una injerencia proporcionada en este sentido? ¿Es aceptable el uso del reconocimiento biométrico? Muestra de lo difícil de hacer este equilibrio la encontramos en las reflexiones que GHANDI realizó en relación con el registro de huellas dactilares de los inmigrantes chinos e indios que residían en la provincia Sudafricana de Transvaal durante el tiempo en que fue colonia británica. De una intensa resistencia a este registro –que aunque fue pacífica se cobró la vida de varias personas-, un importante matiz en el formato del mismo hizo que GHANDI pasase a defender, incluso que fuera el primero en enrolarse en una nueva versión del sistema. Las claves, la voluntariedad del segundo sistema, su finalidad no ya de control sino de protección de los inmigrantes. Un

[48]MCFARLAND "Biometric state, public surveillance, Orwellian State" en WATNER, C/ MCELROY, W (eds.), *National Identification Systems. Essays in Opposition*, 2004.

mismo esquema técnico de registro, basado en la misma información biológica, como se ve en esta historia, recibe un diferente enjuiciamiento en términos de legitimidad y de proporcionalidad.

> «En 1906 el gobierno de Transvaal (en Sudáfrica) promulgó una ley que obligaba a los inmigrantes indios y chinos a registrarse aportando sus huellas dactilares. Ello originó una propuesta en la que GHANDI impulsó la llamada resistencia pacífica. Los inmigrantes desafiaron abiertamente, pero sin violencia, dicha ley, aceptando el castigo que se les quisiera imponer. Algunos fueron encarcelados, azotados e incluso fusilados por protestar o rehusar a registrarse. La denuncia exterior de estos excesos obligó al general sudafricano Jan C. SMUTS a negociar una solución con Mahatma GHANDI, entonces en prisión. Después de negociar con SMUTS, GHANDI se reunió con un millar de indios en Johannesburgo. "*Nos registraremos voluntariamente para mostrar que no pretendemos que ni un solo indio entre en el Transvaal subrepticiamente o mediante fraude*" –les dijo. Terminado el discurso, uno de los oyentes, del grupo de los musulmanes (Pathan), le dijo[49]: "*tú mismo nos dijiste que nos negásemos a que se tomasen nuestras huellas, que sólo se tomaban a los criminales*". Ghandi contestó: "*en el contexto de la Black Act hubiera sido un pecado permitir que se registrase nuestra firma, por no hablar ya de las huellas dactilares. Pero las circunstancias han cambiado. Si me obligas a que te salude por la fuerza y yo lo hago, estaré condenado ante mis ojos, los tuyos y los de los demás. Pero si yo decido saludarte como hermano o amigo, eso demuestra mi humildad y mi cortesía*". El *pathan* respondió que nunca prestaría sus huellas y que no permitiría que otros lo hicieran; jurando por Aláh como testigo que mataría al primer hombre que se registrase.
>
> GHANDI respondió que no se tomarían las huellas de aquellos que hubieran jurado no darlas y se comprometió en ayudar a cualquier *pathan* u otro ciudadano que quisiera registrarse sin prestar las huellas. Añadió, sin embargo, que no le gustó que se amenazase de muerte a nadie, y menos en nombre de Dios. "*Como responsable de esta reunión y servidor de la comunidad, es mi deber ser el primero en dar mis huellas y ruego a Dios que así se me permita. Morir a manos de un hermano, en vez de por enfermedad o de otra forma no puede ser para mí fuente de sufrimiento. Incluso en ese caso estoy libre de pensamientos de rabia u odio frente a mi asaltante, porque sé que ello contribuirá a mi bienestar eterno y que incluso mi asaltante se terminará dando cuenta de mi inocencia*".
>
> Días después GHANDI y algunos de sus colegas fueron a registrarse; ocho *pathan*, guiados por Mir ALAM les siguieron. Al llegar a la oficina preguntaron a Ghandi por el motivo de esa visita, y GHANDI explicó lo que iba a hacer. Entonces ALAM sacó un palo y lo golpeó, y posteriormente recibió golpes y patadas del resto de los *pathan*. Tras la agresión, varias personas llevaron a GHANDI a la oficina de los europeos para recibir atención sanitaria, pero en cuanto recobró el conocimiento GHANDI solicitó que le fuera realizado el registro de sus huellas. Le dijeron que aquello podía esperar, pero GHANDI dijo: "*Me comprometí a ser el primero en registrarme si estaba con vida y ello era aceptable para Dios. Por ello insisto que los papeles me sean traídos aquí y ahora*". Y postrado en la cama, conmoviendo a los que le rodeaban, prestó sus huellas. »

En los EE.UU., por ejemplo, en las décadas posteriores a la Segunda Guerra Mundial se produjo una importante acumulación de información[50], coincidente con la confianza de la ciudadanía en el gobierno, en las empresas y en los sectores sin ánimo de lucro. Los estándares que se empleaban para la toma de decisiones sobre derechos, beneficios y oportunidades de los individuos eran

[49] Extracto adaptado del libro de Tendulkar, D. G. *Mahatma Lige of Mohandas Karamachand Ghandi*, páginas 199-291 publicado en www.internetarchive.org

[50] WESTIN, A. F. "Social and Political Dimensions of Privacy", *Journal of Social Issues*, vol. 59, nº 2, 2003, pp.431-453, pp. 435-436.

mayoritariamente aceptados, y desde el punto de vista jurídico (que aplicaba conceptos jurídico-constitucionales tradicionales y del *Common law*) aceptaba estas prácticas como prácticas que no violentaban ningún derecho individual. Será a partir de 1961 cuando comience a hablarse de un *lado oscuro* de las tecnologías de la información y salten las alarmas[51]. También dieron que hablar polémicos proyectos relacionados con los ficheros policiales, como el *SAFARI* en Francia (1974). Aunque prevenir malos usos de los datos de carácter personal sea beneficioso para la privacidad, no hay beneficio mayor –ni mejor prevención- que evitar toda acumulación universal y centralizada de datos cuyos fines sean *difusos.*

Vamos a presentar a continuación los espacios en los que se emplean estrategias de identificación y en los que, en la ultima década, se han extendido sistemas de reconocimiento biométrico. Aunque se agrupan por escenarios operativos (la persecución de la criminalidad, las relaciones entre la Administración y los Administrados, el ejercicio del derecho de sufragio y la prestación de ayudas sociales), en la valoración de la aceptabilidad de este tipo de controles hemos podido concluir que: 1) se tiende a aceptar como necesaria la identificación de las personas en estos espacios de relación con el Estado, es decir, no se cuestiona en sí misma la necesidad; 2) y lo que se hace es enjuiciar, en concreto, el tipo de uso que se hace de la identificación biométrica.

A este ultimo respecto, y con independencia del escenario operativo concreto, se considera que son menos lesivos:

- Los sistemas en los que el reconocimiento mediante Biometría se traduce en un almacenamiento anónimo, que únicamente permitirá comprobar (a futuro) si una persona que se desea enrolar presenta, en fresco, una Biometría no almacenada o, por el contrario, ya está enrolada.
- Los sistemas que prestan una utilidad de verificación de identidades alegadas (1:1), en comparación con los sistemas que, en sentido estricto identifican (1:n).
- Los sistemas en los que la información biométrica, el patrón, es almacenado en una tarjeta que porta el titular y únicamente se emplea a los efectos de verificar que la persona que porta el documento es la persona para la que éste se expidió.
- Los sistemas en los que, si bien el registro o enrolamiento biométrico es centralizado (algo que puede estar justificado para el uso de test de independencia que garanticen la singularidad de los patrones enrolados), la incorporación del resto de los datos de las personas y el acceso a esta información son únicamente locales (en bases de datos no comunicadas).

[51] BRENTON, M: *The privacy invaders*, Cornell University Press, Thaca, 1964; PACKARD, V.: *The nacked Society*, Editorial Davic MCCAY, New York, 1964; WESTIN, A. F.: *Privacy and Freedom*, 1967.

- Los sistemas en los que el acceso a la información biométrica almacenada en una base de datos –aunque esté en red- tienen un mecanismo que garantiza que sólo se accederá a la información por personas autorizadas y con los fines que, en sentido estricto, han justificado la creación e la base.

4.2. Lucha contra la criminalidad

La lucha contra la criminalidad es un escenario operativo clásico de los sistemas de reconocimiento mediante biometría. Como hemos visto en la parte introductoria, este es el espacio en el que históricamente se establecieron los primeros sistemas (el Bertillonage, y la identificación mediante huellas dactilares) [52]. El objetivo de persecución de las personas que han cometido crímenes se estima de tal relevancia que, sin que ello suponga que las personas investigadas o detenidas dejan de tener derechos y libertades fundamentales, lo cierto es que en todas las sociedades democráticas aceptan que necesariamente se limitará el ejercicio de dichos derechos (entre ellos el derecho a la privacidad).

Históricamente los retratos robot y las huellas dactilares eran almacenados de forma ordenada, como patrones de referencia, a comparar con los datos en fresco de los potenciales sospechosos, junto con otros elementos de referencia como la escritura[53], y la principal novedad de los sistemas biométricos contemporáneos residirá, fundamentalmente, en la celeridad y en la capacidad de almacenamiento que ofrecen los dispositivos automatizados. En 1992 se estableció el sistema AFIS, que enrolaba patrones. Y con posterioridad se desarrollaron sistemas que combinaban el reconocimiento facial y la videovigilancia, como el malogrado sistema que se estableció en Ybor City[54], Florida, USA, o en Newham, Reino Unido. En comparación con los sistemas que enrolan a sospechosos y a condenados, estos sistemas de rastreo plantean el inconveniente de que personas que no son sospechosas son, sin su conocimiento, objeto de una vigilancia colateral[55].

En lo que se refiere al uso de las bases de datos de personas sospechosas o condenadas por la comisión de delitos, las mayores diferencias de unos países a otros se producen, en nuestra opinión, a la hora de determinar: 1) quién y en qué circunstancias tiene acceso a la información contenida en las bases de datos con fines de investigación criminal; 2) y cuánta información adicional recibirá en el caso de que se produzca *match* o coincidencia. A este respecto no es lo

[52] BÄUMLER, H./ ET ALT., *Stand der nationalen und internationalen Diskussion*, Unabhängiges Landeszentrum, 2001, pp.41-42.
[53] BÄUMLER, H./ GUNDERMANN,L./ ET ALT. *Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen*, 2001, p41; RACHOR, F. *Handbuch des Polizeirechts*, 2007, paragr. 233.
[54] TRIGAUX, R.: *Cameras scanned fans for criminals*. St. Petersburg Times, 31.1.2001
[55] BÄUMLER, H./ ET ALT., *Stand der nationalen und internationalen Diskussion*, 2001, pp.41-42.

mismo que, por ejemplo, esa coincidencia nos de total acceso a la información que exista sobre esa persona o que nos indique que podemos dirigirnos al juez y solicitar autorización para que nos envíen la información que se estime que pueda tener relevancia con nuestra investigación.

Desde las perspectiva de la protección de la privacidad en la Unión Europea, por ejemplo, es impensable un conjunto de bases de datos que interoperen y a las que tengan acceso cualquiera de las personas que trabajan en las fuerzas y cuerpos de seguridad y en las policías judiciales de los 27 países miembros. No cabe perder de vista, entre otras cosas, que entre los perfiles de ADN, huellas dactilares y otros patrones biométricos se enrola a personas condenadas, sí, pero también a sospechosos que quedan absueltos e incluso a profesionales de la policía que incidentalmente pueden contaminar la escena de un crimen. Los procesos de búsqueda de coincidencias tienen, por ello, algunas cautelas que algunas voces critican –por excesivamente garantistas para los reos, y otros ven como imprescindibles.

El esquema es muy distinto en los Estados Unidos. Las agencias federales tienen autorización para obtener información de identificativa de las personas, y hemos llegado a un punto en que no parece distinguirse entre criminales que cometen delitos en los EE.UU., y personas que por diferentes circunstancias son controladas mediante Biometría –mucho más allá de las fronteras del país-. Esta práctica, que se estima altamente lesiva para la privacidad de las personas y un tanto arriesgada por las probabilidades de falsos positivos es, sin embargo, aplaudida cuando una huella latente en el volante de un coche bomba en Iraq se da por coincidente con las huellas rodadas que se tomaron a una persona en una ocasión que trató de viajar a los EE.UU..

Universitat d'Alacant
Universidad de Alicante

IAFIS e IDENT son los principales sistemas que operan en la actualidad. EL IAFIS es la base de datos de identificación automatizada del FBI y contiene las huellas y el historial criminal de las personas; el IDENT, por su parte (Automatic Biometric Identification System) es del Departamento de Homeland Security y recoge la biometría, algunos datos biográficos e información sobre los momentos en que estos datos han sido captados. Aunque se creó originariamente para el control de la inmigración, a esta base se incorporaron, entre otros, los datos que son captados por el programa US Visit, esto es, el programa de registro de entrada de todos los no-ciudadanos estadounidenses. Al margen de estos sistemas federales, veremos que los Estados que son parte de la federación o algunas ciudades emplean también reconocimientos mediante Biometría en algunos contextos.

Muestra de la diferente sensibilidad en Europa, ha de recordarse aquí una sentencia que, en algunas de sus afirmaciones, se ha comentado en el capítulo anterior. Nos referimos a la Sentencia *S. and Marper contra Reino Unido* del TEDH (2009). La misma aborda la cuestión de la retención y

el almacenamiento de los datos de carácter personal por parte de la autoridades públicas. En el arresto y procesamiento de los demandante se obtuvieron sus huellas y muestras de ADN y el TEDH consideró desproporcionado que el sistema británico permitiese un almacenamiento indefinido de dichas muestras, toda vez que –independientemente del uso que se haga de los datos- *la mera retención* tiene un impacto en la vida privada de la persona afectada. Cuando una persona sospechosa ha sido absuelta, el hecho de que *pueda cometer un crimen en el futuro* no parece razón suficiente como para conservar esta información. Nótese que esta perspectiva distingue la *persecución de los delitos ya cometidos*, de la *prevención de la comisión de delitos*. La prevención del delito, advertía hace ya décadas GARCÍA-PABLOS DE MOLINA[56], es un tópico a veces equívoco o vacío de contenido. Prevención puede ser disuadir a los potenciales infractores o a los que reincidirán, puede ser dificultar la comisión de los delitos o incluso tratar de neutralizar las causas que los generan, pero ninguno de esos objetivos legitimará intervenciones con un elevado coste social.

4.3. Documentos de identidad nacional y sistemas de identificación en las relaciones entre la Administración y los Administrados (pago de impuestos, administración electrónica, etc).

Keith BRECKENRIDGE[57] advierte de que en diferentes momentos de la historia y países el hecho de tomar las huellas de las personas de forma universal y centralizada ha derivado en políticas autoritarias, como sucedió en su opinión en Sudáfrica; ello, advierte, mucho antes de que existieran tecnologías que permitieran la captación y gestión automatizada de las mismas. Si no prestamos atención a aquellos excesos, advierte, volveremos a repetir los mismos errores.

Pero, en si mismo, un mínimo enrolamiento o registro civil de las personas se estima imprescindible para la protección de los derechos de éstas, especialmente de las personas más vulnerables. Por ello, en países con grandes bolsas de población sin registrar las biometrías están impulsando campañas masivas de registro de las personas y emisión de los correspondientes documentos. Así, especialmente en países desarrollo,antiguas colonias europeas. Vid. en el anexo un mapa del mundo en el que aparecen en gris los países que tienen implantado (a fecha de 2014) un sistema biométrico civil o de registro del sufragio (IMAGEN 76). En algunos lugares el registro es del conjunto de la población (Sudáfrica, Gambia, India); en otros, el registro concentra su atención en la identificación de las personas en situación de pobreza y a las que se reconoce algún tipo de ayuda (como, por ejemplo, en Brasil y en México). IMÁGENES 1.6, 1.9 7 1.10.

[56] GARCÍA-PABLOS DE MOLINA, A. La prevención del delito en un estado social y democrático de derecho, Estudios penales y criminológicos, nº 15, 1990-1991, pp79-98.
[57] BRECKENRIDGE, K. Biometric State. The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present, Cambridge University Press, 2014,

Las tecnologías automatizadas han permitido hacer realidad planes que, en otros momentos de la historia resultaron fallidos. Por ejemplo en los años 50, en Sudáfrica, Hendrik Verwoed impuso lo que se conoce como *Bewysburo*. Todo hombre y, por primera vez, toda mujer africana debían portar una tarjeta de identificación vinculada a un libro de referencia (Bewysboek) y ese registro, que incluía su historial de empleo, residencia y pago de impuestos, se combinaba con una colección centralizada de huellas dactilares. Aunque tardaron años en admitirlo, la obtención y –sobre todo- la clasificación de tantas huellas dactilares, sin el apoyo de métodos automatizados, terminó dándose por imposible[58]. Las nuevas tecnologías, en cambio, están permitiendo registros de hasta cien mil personas al día, algo que ha posibilitado en India un enrolamiento de 600 millones de personas en unos pocos años.

4.3.1. La emisión de tarjetas de identidad de ciudadanos y de residentes

En algunos países la versión automatizada, con CHIP, de los documentos nacionales de identidad de ciudadanos y de residentes ha sido vista como una mera evolución de los sistemas instalados previamente. Ya desde los años 50 los documentos de identidad de varios países se expedían con fotografía y obteniendo las huellas dactilares, y la Biometría no se ha visto con recelo. En España, por ejemplo, la transición del DNI al DNI electrónico, y la incorporación de Biometría a los pasaportes se han producido con poco más que algunas lineas en alguna página interior de los periódicos.

Universitat d'Alacant
Universidad de Alicante

Contrasta esta situación con los encendidos debates que se han producido en otros países. Por ejemplo, en el Reino Unido, hubo en el año 2006 un intento fallido de emisión de un DNI con biometría. Tras una compleja tramitación parlamentaria, terminó aprobándose la *Protection of Freedoms Act* (2012) que regula la destrucción, retención y el uso de las huellas dactilares, huellas de pisadas y muestras de ADN y refuerza la protección que (débilmente) ofrecía al respecto la Police and Criminal Evidence Act de 1984. El movimiento favorable a la introducción de una tarjeta de identidad tiene sus raíces en una propuesta del que fuera ministro Jack STRAW. Alcanzó un apoyo social considerable en torno a los atentados del 11-S en los EE.UU. y el 7-J en Londres, pero la Ley finalmente aprobada (Identity Card Act, 2010) concentró su atención en los fraudes de identidad, el control de la inmigración y la posibilidad de presentar, con más facilidad, una prueba de identidad cuando se viaja, se abren cuentas o se alquilan propiedades. Se dice que el intento fue fallido en tanto la tarjeta de identidad sólo es obligatoria para los no europeos[59] y los trabajadores de áreas de riesgo, siendo voluntaria para el resto. Esa supuesta voluntariedad, sin embargo,

[58] BRECKENRIDGE, K. *Biometric State*, 2014, pp90-95.
[59] WARREN, A. / MAROUDI, E. "Surveillance and identity management: Migrant Perspectives on UK Biometric Residence Permits," *Computer Law & Security*, 27/ 2011, pp245-249.

queda quebrada *de facto* en tanto de no registrarse en la base de datos (con foto, número de la seguridad social, Biometría de las huellas, datos de nacimiento, etc.), las personas ya no podrían proceder a futuras renovaciones del pasaporte.

También el Consejo Constitucional francés se pronunció en contra de recabar biometrías para verificar la titularidad del DNI o tan siquiera a los efectos de comprobar la identidad en la renovación del DNI. No excluyó, sin embargo, el uso de esta información con otros fines administrativos o de naturaleza policial. La CNIL (2001)[60], por su parte, destacó la notable diferencia entre aquellos sistemas de identificación en los que el titular de los datos los conserva consigo (por estar almacenados en exclusiva en un CHIP insertado en su documento de identidad) y los sistemas en los que el titular no mantiene ese control, por estar los datos almacenados en otro lugar. Estos casos de almacenamiento externo, especialmente si son en red, exponen los datos a usos que se excedan de aquellos que han justificado el almacenamiento.

El Consejo de Estado de los Países Bajos, que cumple funciones equivalentes a un Tribunal o Corte Suprema en materia administrativa, planteó ante el Tribunal de Justicia de la UE una consulta motivada por el caso de tres ciudadanos holandeses a los que se les había denegado el pasaporte y de un cuarto al que se le negó la emisión del DNI por su negativa a facilitar las huellas dactilares. En su pronunciamiento sigue una línea similar a la del CC Francés: "*la legislación debe garantizar que los datos biométricos no se recogerán, procesarán y emplearán para más fines que la propia emisión del documento*"[61].

En la República Federal de Alemania, por su parte, se planteó un caso en relación con el registro de los residentes extranjeros. Este país emplea un diferente esquema para registrar, de una parte, a los nacionales y, de otra, a los extranjeros residentes (sin distinguir dentro de éstos a ciudadanos de la UE, personas de otros países con permiso de residencia o solicitantes de asilo) llegó al Tribunal de Justicia de la UE: el caso de Heinz Huber. El registro de extranjeros residentes o *Ausländerzentralregister* es un registro central, automatizado, que alberga información de todos los extranjeros que viven o han vivido más de tres meses en Alemania[62]. En el año 2011 contenía datos de aproximadamente 20 millones de personas y en torno a 6500 tipos de autoridades alemanas tenían acceso al mismo con fines muy diversos (tanto administrativos en sentido estricto, como estadísticos o de investigación criminal). Heinz Huber, un ciudadano austriaco que se trasladó a trabajar a Alemania, se negó a ser incluido en el registro considerando que la

[60] REJMAN-GREENE, M. "Privacy Issues in the Application of Biometrics: an European Perspective", en WAYMAN ET ALTERE, 2005, p342.
[61] *Oxford Pro Bono*, p31.
[62] Sentencia del Tribunal de Justicia de la UE (Gran Sala) de 16 de diciembre de 2008, Heinz Huber contra la República Federal de Alemania, Asunto C524/06.

presencia de sus datos en el mismo era discriminatoria dado que no existía un sistema de registro similar, con tanta amplitud de acceso, para los ciudadanos Alemanes. El Tribunal de Justicia de la Unión Europea advirtió que si bien era legítimo obtener datos de los residentes extranjeros, los datos del registro no debían emplearse más allá de la estricta finalidad de aplicarles la legislación relativa a los permisos de residencia.

Fuera de la UE, en Israel, los tribunales mostraron su rechazo a un proyecto de creación de una base de datos de identificación biométrica de los ciudadanos israelíes. Antes incluso de la aprobación de la Ley, el rechazo se manifestó en contra de un *proyecto de Ley para la Inclusión de Métodos de Identificación Biométrica y Datos de este tipo en los Documentos de Identificación y en las Bases de Datos*[63]. Paralizó un proyecto piloto diseñado para dos años, como paso previo a una Ley que preveía incluir datos biométricos encriptados en los documentos de identidad y en los pasaportes. El motivo del recurso, que terminó paralizando la ley, fue el hecho de que se autorizaba la creación de una base de datos centralizada con los datos biométricos de todos los ciudadanos israelíes. La sentencia afirmó que la petición era prematura –aun no había datos concluyentes ni se había perfilado el proyecto en su totalidad-, aunque mostró su preocupación por el hecho de que pudiera llegar a existir una base de datos centralizada con la información biométrica de los 9 millones de israelíes[64].

4.3.2. El *Aadhaar*

El *Aadhaar,* como venimos diciendo, es un sistema automatizado de reconocimiento mediante Biometría que está en proceso de implantación en India (IMAGEN 1.6). Se trata del sistema de reconocimiento más ambicioso de cuantos están en marcha en el mundo, en tanto atribuye un número de identificación único, llamado *AADHAAR* a todas las personas residentes en la República de la India. La Unique Identification Autority of India (UIDAI) acometió la tarea de asignar a todas las personas un número de identificación único de 12 dígitos configurado a partir de la Biometría de las diez impresiones dactilares y el iris[65]. Se trata éste de un proyecto muy complejo; las publicaciones más recientes –aunque no es fácil contrastar el dato- hablan ya de unos 600 millones de personas enroladas, es decir, aproximadamente la mitad de los que se espera enrolar en total. En 2013 un grupo de juristas de la Universidad de Oxford preparó un informe comparativo sobre este sistema por encargo del *Center for Law and Policy Research India*[66] atendiendo a un conjunto de decisiones adoptadas o tomadas en consideración por instituciones

[63] Israeli Law for Including Biometric Identifying Means and Data in Documents of Identification and in Databases, 2009.
[64] Informe *Oxford Pro Bono*, 2013, pp12-13.
[65] JAIN, A. K. / ET ALTERE, *Introduction*, 2011, pvii.
[66] *Biometric Identitification and Privacy*, Comparative Research Prepared for the Centre for Law and Policy Research India, feb. 2013, University of Oxford, Oxford Pro Bono Publico.

de los Estados Unidos, Israel, Australia, el Consejo de Europa, la UE y, dentro de la UE, Reino Unido, Francia y Alemania.

Lo referimos aquí, de forma separada a los sistemas de identificación en sentido estricto, porque el sistema registra tanto a ciudadanos como residentes y tiene una finalidad múltiple[67]. Esto es, atiende a las diversas motivaciones que en otros lugares han llevado al establecimiento de sistemas de reconocimiento biométrico de la población civil y pretende dar servicio a todas ellas: seguridad nacional, registro civil, asistencia social,.. Se captan la Biometría dactilar y del iris de las personas, y a partir de esos patrones es generado un numero de identificación que se conoce como UID, que ya ha sido asignado para varios cientos de millones de personas. El UID no genera una tarjeta de ningún tipo, no reconoce ningún derecho ni se traduce en un documento que demuestre el registro; su funcionamiento es totalmente digital[68].

Ha de tenerse en cuenta que la ausencia de un esquema de identificación civil previo representaba un importante problema en un país tan poblado como la República de la India[69]. Generar, en pocos años, un sistema de reconocimiento eficiente y con garantías es algo que hubiera resultado impensable antes del desarrollo de estas tecnologías de reconocimiento automatizado.

Como elementos que contribuyen a reforzar las limitaciones que desde el punto de vista de la singularidad plantean estos sistemas de reconocimiento, el Aadhaar es un sistema multimodal que trabaja con patrones obtenidos de varias características biométricas. Ello permite, también, compensar de algún modo las limitaciones que se producen desde la perspectiva de la universalidad[70].

Universitat d'Alacant
Universidad de Alicante

4.3. 3 Licencias y sufragio biométrico

Hemos encontrado algunas referencias de sistemas de reconocimiento que refuerzan algunas parcelas concretas de la relación entre las personas y las administraciones públicas. En Argentina, por ejemplo, la Resolución General nº 2811/ 2010 de la Administración Federal de Ingresos Públicos (AFIP) implementa un Registro tributario y establece que para conformar el perfil de las personas físicas que actúen por sí mismas o en representación de terceros debe procederse a una identificación y registro de éstas, empleando dispositivos de digitalización de la fotografía, la firma, la huella dactilar y la imagen reproducida del documento nacional de identidad.

---

[67] JAIN/ KUMAR, 2012.
[68] BRECKENRIDGE, K. *Biometric State*, 2014, pp17-19.
[69] MATHRE, A./ PALLA, S./ CHIKKERUR/ ET ALT, "Efficient search and retrieval in biometric databases", *Proceedings of SPIE Defense and Security Symposium*, vol. 5779, pp265-273.
[70] SUN, Z. A. / PAULINO, A./ FENG, J./ CHAI, Z,/ TAN, T. / JAIN, A. K. "A study of multibiometruc traits of identical twins", Proceedings of the SPIE Biometrics, Florida, 2010.

En Australia (Quennsland y Nueva Gales del Sur) y en los Estados Unidos las licencias de conducción general de algunos Estados (como Texas o Georgia) [71] contienen referencias biométricas pero no se trata de un sistema centralizado a nivel federal. De hecho existe la preocupación de que un uso *sin escrúpulos* de la información asociada a las licencias de conducir, más allá de la gestión de las infracciones de tráfico, pueda suponer una intromisión excesiva en la privacidad de las personas, reeditando una preocupación que –en relación con las licencias en general- ya expresó en los años 70 el Congreso de los Estados Unidos[72].

Al margen de los documentos de identidad o los pasaportes, incluimos un pequeño excurso en relación con otro uso de los elementos biométricos en el ámbito de las relaciones entre ciudadanos y estados: el llamado sufragio *biométrico.* (Imagen 1.7, pesona votando; Imagen 77 padrón biométrico de Bolivia) La Biometría puede ser empleada como herramienta de reconocimiento tanto en procesos electorales presenciales en los que se plantean problemas en la verificación de las identidades de las personas con derecho al voto, como en procesos electorales a distancia (eVoting). Los sistemas de verificación pueden ser de diferentes tipos; de una parte, sistemas en los que el día de la convocatoria electoral se comprueba que las huellas mostradas *no pertenecen a nadie que haya votado ya* (lo cual requiere, necesariamente, un sistema de referencia centralizado al que se conectan los dispositivos de control instalados en los colegios electorales), o sistemas en los que se han expedido células de identificación *ad hoc* o se han creado padrones electorales con una base biométrica. Deben citarse aquí el sistema propuesto por el Instituto Federal Electoral de México destinado a enrolar a 72 millones de votantes en dos años[73] y una Ley de la República de Bolivia, de reforma del Régimen Electoral, que prevé la elaboración de un "padrón electoral biométrico"[74].

En relación con el eVoting, algunos países han desarrollado proyectos de investigación e incluso probado experiencias piloto de voto electrónico (el Reino Unido, la ACM[75], el NIST[76], Austria[77], Suiza o Alemania), con el doble objetivo de reducir los costes de los procesos electorales y promover el interés y la participación de los ciudadanos. La máxima preocupación de a este respecto es la de evitar accesos fraudulentos a los sistemas. Ello ha llevado a algunos expertos a

[71] PETERMAN, 2002, p61; ALBRECHT, 2001, p70.
[72] WOODWARD, J. 1997, p1482_1483; PARKER, R. B. "A definition of privacy," *Rutgers University Law Review*, vol. 27, p. 275, 1974.
[73] *Biometric Technology Today*, Mayo de 2006, p3
[74] Ley nº 4021 del Régimen Electoral Transitorio de la República de Bolivia, de 2009.
[75] Association for Computing Machinery, Estados Unidos de América.
[76] NIST Voting Standards Symposium.
[77] SMITH, E. / MACINTOSH, A. "E-Voting: Powerful Symbol of E-Democracy", *proc. EGOV*, 2003, pp240-245.

analizar la medida en que herramientas biométricas pueden complementar este tipo de iniciativas[78].

4.3.4 El control de las ayudas sociales

En la década de los 90 comienzan a emplearse en algunos países unas ayudas que implican pagos directos a las familias desfavorecidas. El sistema *Oportunidades* de México, apoyado por el Banco Mundial, es considerado como precursor de los que se aplicarían en otros países como Brasil, Indonesia o India[79]. Los sistemas de ayudas de Sudáfrica, de la misma época, fueron implementados a nivel nacional y su gestión descansaba de forma importante en un sistema de registro y pago biométricos desde el principio; México no introdujo el pago con identificación biométrica hasta el año 2010[80].

Desde los primeros sistemas de registro y pago biométrico desarrollados en Zululand [81], los sistemas se han expandido en muchos países con un elemento común: la tendencia a la centralización del registro de identidades, el control privado de las finanzas y el pago local de las ayudas en metálico; la mayoría de los sistemas dice Breckenridge, emplean como referencia la huella dactilar[82]. Diferentes tipos de ayudas en metálico fueron consolidadas en Brasil en 2003 con la tarjeta del *Cadastro Unico*, y su pago se centralizó mediante la *Caixa Economica Federal*. Esta Caixa anunció en 2012 que establecería un sistema de reconocimiento biométrico en los cajeros automáticos locales a los que las personas acuden a cobrar; muchos de los usuarios no disponen de cuentas bancarias y acuden una única vez al cajero automático a cobrar, y el olvido de los passwords o los PINS se traduce en muchas gestiones en las oficinas bancarias.[83] En Sudáfrica, por su parte, funciona la SASSA-Card de la Agencia Sudáfricana de la Seguridad Social; una tarjeta para los benefciarios de pensiones y otras ayudas sociales, creada en colaboración con Master Card, y en la que el enrolamiento se hace con Biometría dactilar. La tarjeta puede ser utilizada en los cajeros automáticos, y da acceso a otros servicios financieros a aquellas personas que por

[78] HOF, S. "E-Voting and Biometric Systems?", en las Actas de *Electronic Voting in Europe - Technology, Law, Politics and Society*, Workshop of the ESF TED Programme together with GI and OCG, July, 7th-9th, 2004, in Schloß Hofen/ Bregenz (Austria).
[79] HANLON, J. / HULME, D. / BARRIENTOS, A. *Just Give Monet to the Poor: The Development Revolution from the Global South*, Kumarian Press, Sterling, 2010, p130-131.
[80] LEVY, S. *Progress against Poverty: Sustaining Mexico's Progresa-Oportunidades Program*, Brookings Institution Press, Washington DC, 2006, p114; ARTEAGA, N. "Biological and Political Identity: The Idenntification System in Mexico", Current Sociology 59, nº 6, 2011, pp754-770.
[81] GELB, A. / CLARK, J., "Identification for development: the Biometrics Revolution", Centre for Global Development, 28 de enero de 2013; GELB, A./ DECKER, C., "Cash at your fingertips: Biometric Technology for Transfers in Developing Countries", Review of Policy Research 29, nº 1, 2012, pp91-117.
[82] Breckenridge, Biometric State, pp192-194.
[83] "Brazilian Bank CAIXA Deploys Lumidigm Fingerprint Sensors in ATMs", publicado en www.lumidigm.com, en julio de 2012.

diferentes circunstancias (como su ubicación en entornos rurales) no pueden acceder a las infraestructuras de la banca formal. IMAGEN del enrolamiento para la obtención de la Sassa Card: 1.9.

En España, en concreto en el País Vasco, se ha debatido recientemente la posibilidad de incluir un sistema de estas características en el control del fraude de la Renta de Garantía de Ingresos (RGI). El debate, muy encendido, se zanjó de pleno por la mayoría de las fuerzas políticas, entendiendo que la propuesta estigmatizaba a los perceptores de la RGI. Nótese, sin embargo, que existen diversos tipos de reconocimiento que pueden realizarse con la misma finalidad –la de evitar el fraude- y no todos ellos resultan igual de invasivos. Por ejemplo, en el condado de Santa Clara (en California) se emplea un sistema de *identificación negativa* que garantiza que la persona que trata de acceder al sistema con una nueva identidad no está ya enrolada en el mismo[84]; ya antes, a finales de los noventa, un programa piloto había demostrado en el Condado de los Ángeles que este tipo de reconocimientos podía contribuir a detectar y reducir el fraude en las ayudas[85] y se extendió a varios condados y ciudades. Así funciona también la SASSA-Card; el patrón biométrico sólo es una referencia para la obtención de la tarjeta (asociada a una cuenta bancaria) en la que se realizará el ingreso de la ayuda correspondiente. Las huellas en fresco son contrastadas *1 a n* con las almacenadas en la base, para determinar la no coincidencia. Determinada ésta, se considera que la persona tiene pleno acceso al sistema de ayudas sociales y no es necesario volver a emplear tecnologías de reconocimiento biométrico. En nuestra opinión este tipo de verificación negativa, en el momento de la emisión del documento que da acceso a la ayuda, no resulta desproporcionado en comparación con el esquema que en España se emplea para la identificación civil de los nacionales y los extranjeros residentes. A todos ellos se les toman la Biometría facial y la dactilar para la emisión del DNI, y esa referencia es empleada como indubitada en las relaciones con la administración. Cuando los receptores de esta RGI son personas *sin permiso de residencia* (y sin documentación equivalente al DNI) no parece desproporcionado emplear algún sistema de identificación indubitada (equivalente al de nacionales y residentes con permiso), con la garantía de que dicha información no será empleada con ningún otro uso. Cabe, además, la posibilidad de establecer un sistema de enrolamiento *voluntario* que permitiría a estas personas expresar su opinión sobre la legitimidad y proporcionalidad de un sistema de estas características.

5. LA BIOMETRÍA EN LAS RELACIONES ENTRE EMPLEADORES Y EMPLEADOS.

[84] WAYMAN, JAIN, MAIO, 2008, p5-6.
[85] Woodward, 1997, p1482_1483; General Accounting Office, "Electronic benefits transfer: Use of biometrics to deter fraud in the nationwide EBT program," Sept. 1995.; D. Milbank, "Measuring and cataloguing body parts may help weed out welfare cheats," The Wall Street Journal, Dec. 4, 1995.

5.1. El control de recintos de seguridad (zonas militares y aeropuertos)*[86]

El control del acceso a recintos de seguridad, como zonas militares, aeropuertos o instalaciones que por algún motivo se consideran altamente sensibles fue uno de los primeros espacios en los que se dio uso a las tecnologías de reconocimiento biométrico. Es muy difícil acceder a información sobre este tipo de sistemas, porque en muchos casos constituyen información clasificada, pero sí es sabido que la NSA ha sido una de las organizaciones que más ha invertido en la investigación de las tecnologías biométricas[87]. (IMÁGENES 1.13 y 1.19)

Desde la década de los años 90, explican WAYMAN (ET ALT) se viene empleando geometría manual en el acceso a zonas de seguridad de aeropuertos internacionales como el de San Francisco, en el que 18000 usuarios enrolados transitan por sus 180 lectores[88]. Las tarjetas de empleado llevan una banda magnética que al ser puesta a disposición del sistema alega una identidad; a continuación el sistema procede a verificar que la identidad alegada coincide con el patrón mostrado en fresco, algo que impide que una persona no enrolada pueda acceder al sistema con una tarjeta prestada o robada.

Se están desarrollando, asimismo, sistemas que (por ejemplo mediante Biometría de la forma de teclear) verifican que la persona que está en un puesto de trabajo altamente sensible, como puede ser el caso de una torre de control aéreo, no ha sido suplantada por un intruso, y sistemas que –aplicados por ejemplo a conductores- comprueban que el empleado mantiene intactos sus reflejos.

La Biometría ha encontrado, además, espacio en aquellos casos en los que los empleados –a veces por categorías –acceden de forma remota a la información que la empresa tiene en un sistema informático. Las empresas almacenan y gestionan información tanto para desarrollar algunas de sus actividades (como prestar servicio a clientes o gestionar la relación con proveedores) como para poder reflexionar sobre su funcionamiento y diseñar mejoras. Se trata de una información sensible para los intereses de la empresa y es clave que se garantice : la confidencialidad (o prevención del acceso de terceros no autorizados); la integridad (o garantía de que los datos no se alteran de forma inadecuada o por personas no autorizadas); y la disponibilidad (o garantía de que la información estará disponible cuando se necesite)[89]. Dado que no puede gestionarse esa

[86] (*) Con excepción de las prisiones, hospitales y centros de enseñanza, que se abordan en el siguiente apartado.
[87] WOODWARD, J. D. "Biometrics: Privacy's Foe or Privacy's Friend?", *Proceedings of the IEEE*, vol. 85, nº 9, 1997, p1480 y ss. 1482.
[88] WAYMAN, J. / JAIN, A. K. / MAIO, D. " An Introduction to Biometric Authentication", 2008, p5.
[89] CLARKE, N. *Transparent User Authentication. Biometrics, RFID and Behavioural Profiling*, Springer, 2011, pp3-4.

información sin que los empleados (o algunos de ellos) accedan a incorporar información y/o a trabajar con ella, lo que se hace es establecer lo que se conoce como *triple A*, es decir: *Authentication* (acreditación de identidad) , *Authorisation* y *Accountability* (responsabilidad).

Diferentes razones justifican la exigencia de una acreditación de identidad para entrar en estos sistemas; así, la protección de los intereses de la empresa o, en su caso, de los datos de las personas –empleados, clientes, etc.- que se manejen en el sistema informático de que se trate. En relación con la biometría, sin embargo, la pregunta es hasta qué punto a esa necesidad de acreditar la identidad de quien accede se le debe dar cauce a través de un sistema tan invasivo en la privadidad de las personas. Hay sistemas en los que la acreditación es, además, especialmente intensa; además de una acreditación en el punto de acceso (que es bastante frecuente), en ocasiones se requiere volver a acreditar la identidad en momentos sucesivos o para ejecutar determinadas acciones. Los medios con los que es posible acreditar la identidad, venimos diciéndolo desde el comienzo de este trabajo, son: algo que el usuario sabe (como las contraseñas para acceder a ordenadores, redes, cuentas bancarias o páginas web de diferentes tipos de servicios); algo que el usuario tiene (los *token*) o algo que el usuario *es* (el reconocimiento mediante biometría)[90]. Los token refuerzan algunas de las desventajas de las contraseñas y códigos de usuario, porque la información no corre el riesgo de ser olvidada/copiada, pero plantean el problema de que pueden ser sustraídos o extraviados y ocasionar que terceros no autorizados accedan con ellos. Y por ello se ha dicho que el reconociento mediante Biometría es *una forma de autenticación robusta*[91]; pero tiene sus desventajas. A nadie se le ocurriría llevar escrito en el rostro, en un lugar visible, el PIN que da acceso a su terminal de trabajo; por razónes obvias, tampoco parece muy razonable que el elemento que de acceso al sistema sea, por ejemplo, la geometría del rostro.

5.2. El control biométrico en las relaciones entre empleadores y empleados.

Creemos que hay importantes razones para distingur entre ese control de seguridad, al que acaba de hacerse referencia, y el control horario de los trabajadores. Las nuevas tecnologías de la información y de la comunicación se han traducido en importantes cambios en relación con la capacidad de control y supervisión que puede ejercer la empresa sobre aquél para verificar, por ejemplo, si el trabajador utiliza adecuadamente los instrumentos que el empresario pone a su disposición (entre ellos internet) y si cumple con su quehacer diario[92]. La forma en la que se

[90] WOOD, H.: "The use of passwords for controlling the access to remote computer systems and services", en DINARDO, C.T. (ED.) *Computers and Security*, vol. 3, p. 137. AFIPS Press, Montvale, 1977.
[91] ASHBOURN, 2000.
[92] MOLINERA MATEOS, J. F. "El control empresarial del correo electrónico. Conflicto de derechos", *Absentismo laboral. Causas. Control y análisis. Nuevas formas. Técnicas para su reducciónm* Fundación CONFEMETAL, 2001,

controla ese cumplimiento es muy diversa, aunque la normativa (en el caso de España la libertad de empresa que protege la Constitución) ampara al empresario a la hora de organizar su empresa en aras a alcanzar su objeto social. También existe por parte de las Administraciones Públicas una potestad de vigilancia y control de sus empleados, y ésta incluye entre otros el control horario. Así, recuerda la Sentencia de 2 de julio de 2007 del Tribunal Supremo español[93] advierte que *"cumplir con el control horario es una obligación inherente a la relación que une a los funcionarios con la Administración"*[94].

¿Quiere ello decir que los empresarios y, en su caso, la Administración pueden emplear cualquier tipo de sistema, incluyendo los biométricos, para controlar que los trabajadores cumplen con su tarea, incluyendo su puntual asistencia al trabajo? Esta potestad de control debe conjugarse con los derechos de los trabajadores. Así, el Estatuto de los Trabajadores recuerda en España que las potestades de control del empresario tienen como límite los derechos de los trabajadores, algo que expresamente recuerda el Estatuto de los Trabajadores (ETT) en su artículo 20.3: "*El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso*". Entonces, ¿en qué quedamos? Lo cierto es que en el conjunto de la Unión Europea encontramos sentencias para todos los gustos.

Desde el año 2005 son varios los casos en que empleados de países occidentales, fundamentalmente europeos, han acudido a los organismos a los que se encomienda la protección de datos de carácter personal o a las autoridades judiciales denunciando el establecimiento de sistemas de reconocimiento mediante Biometría en su control horario. El fundamento de las reclamaciones, como se verá, es diverso. En algún caso, empleados alegan que el empleador no había comunicado ni solicitado consentimiento de los empleados para el establecimiento de un sistema de este tipo. En otros, consideran que el empleador no tiene legitimidad para obtener y almacenar este tipo de datos, bien atendiendo a la normativa de protección de la autonomía

pág. 153 y ss; MOGUEL FERNÁNDEZ, J.: "El poder de control y vigilancia del empresario sobre las actividades de los trabajadores, y sus implicaciones penales", *Noticias Jurídicas*, Febrero de 2006.

[93] Sala de lo Contencioso-Administrativo del Tribunal Supremo, constituida en su Sección Séptima por los Magistrados indicados al margen, el recurso de casación nº 5017/2003, sobre derechos fundamentales, interpuesto por la Confederación General del Trabajo de Cantabria (CGT Cantabria), y por el Sindicato de Trabajadores de la Enseñanza de Cantabria (STEC), contra la Sentencia dictada el 21 de febrero de 2003 por la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Cantabria, recaída en el recurso nº 763/2002, sobre la implantación del nuevo sistema de control horario.

[94] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID, *Guía de protección de datos personales para Universidades,* 2008, págs. 456 a 459.

informativa bien en relación con el derecho a la integridad personal (artículo 15 CE) o el derecho a la intimidad (art. 18).

Por ejemplo fijándonos en resoluciones previas a la Opinión del WP 29 de 2012[95], encontramos una reflexión similar en la sentencia del tribunal provincial Administrativo de Varsovia (2008)[96], que considera que la utilización de un control de horas de trabajo mediante procedimientos biométricos no es proporcional en relación con la finalidad que se persigue, y considera que sólo podrían emplearse si el empleado está en condiciones de consentir libremente o rechazar sin por ello sufrir ningún perjuicio. También la Magistratura laboral austriaca[97] entiende que se trataría de un control de alta intensidad, que requiere chequeo diario de las huellas, para un objetivo que es considerado relativamente "trivial", opinión hacia la que también se inclina el Garante italiano. Por su parte, la autoridad portuguesa de protección de datos tomó una decisión desfavorable a la utilización de un sistema de huellas digitales en el control de la asistencia y puntualidad del personal no docente[98].

En España, la *Confederación General del Trabajo* y el *Sindicato de Trabajadores de la Enseñanza de Cantabria* interpusieron un recurso en 2003 contra[99] una Resolución del Gobierno de Cantabria que implantaba un sistema de control horario con lectura biométrica de la mano. El escáner captaba la imagen tridimensional de la mano, transformándola en un algoritmo de 9 bytes, y dicha información se asociaba en una base de datos con la identidad de los empleados públicos haciendo posible efectuar el control horario en cuestión. La sentencia del TSJ de Cantabria fue objeto de recurso al Tribunal Supremo que resolvió en Sentencia de 2 de julio de 2007 y a la reclamación de uno de los empleados implicados en este caso atendió también un Auto del TC[100]. Por su parte, el Tribunal Superior de Justicia de Andalucía, en Sentencia de 25 de enero de 2010 en el recurso presentado por los representantes de los trabajadores en el caso *Hermandad Farmacéutica del Mediterráneo* [101] también entendió que no vulneraba el derecho a la

[95] GT-WP 29, Opinion 3/ 2012 on developments in biometric Technologies, adoptado el 27 de abril de 2012, WP 193, p3.
[96] "Sentencia del Tribunal Provincial Administrativo de Varsovia, de 27 de noviembre de 2008, sobre la utilización de datos biométricos de los trabajadores", Publicada integramente en la *Revista Española de Protección de Datos*, nº 7, julio2009-junio 2010, pág. 477 y ss.
[97] OGH, Sentencia de 20 de diciembre 2006, 9 ObA 109/06d - ArbVG § 96, ABGB § 16, DSG 2000 § 4, *Fingerscanning in Betrieben*.
[98] Informe 368/ 2006 de la AEPD.
[99] Resolución de la Consejería de la Presidencia, publicada en el B.O.C. el 28 de Mayo de 2002 sobre la implantación del nuevo sistema de control horario, y en la Orden de la misma Consejería de Presidencia de fecha 5 de Junio de 2002.
[100] ATC 57/ 2007 de 26 de febrero.
[101] STSJ 47/2010, en el recurso de suplicación interpuesto por ASOCIACION DE TRABAJADORES DE HEFAME (ATRAHE contra la sentencia número 470/09 del Juzgado de lo Social número Tres de Murcia, REC 1071/ 2009.

intimidad y tiene pleno encaje en el artículo 20.3 del ETT la implantación de una máquina de control horario que emplea elementos biométricos en una empresa.

El Tribunal Supremo español, en la Sentencia de 2 de julio de 2007, considera que los empleadores pueden emplear tecnologías de reconocimiento biométrico en el control horario, al no haber "*norma que prohíba el recurso a la tecnología escogida para realizar el control del cumplimiento del horario de trabajo"*. Aunque los trabajadores, en el recurso presentado, alegaban que estos sistemas vulneraban la dignidad o derechos fundamentales (como la intimidad[102] o la integridad física[103]) la Sala de lo Contencioso del TS entiende que si su "*novedad o complejidad"* no convierten estos sistemas en lesivos[104]. Por su parte, el ATC 57/ 2007, en su fundamento jurídico 6º indica "*que los datos sobre la Biometría de la mano del recurrente sean datos personales no convierte su exigencia y posterior tratamiento automatizado en ilegítimos*."

Por su parte, la AGPD se ha pronunciado en varias ocasiones en relación con supuestos similares y en resoluciones relativas a otros escenarios (como el de la enseñanza) explícitamente se refiere a la diferencia entre el control de los trabajadores y las necesidades de identificación en otros ámbitos. Publicó un informe inicial sobre el uso de la huella dactilar en el control de los trabajadores que ha servido de referencia en la resolución de cuantas cuestiones y recursos se han presentado con posterioridad. Así en la resolución de la denuncia presentada contra el *Ayuntamiento de Villena*, por la instalación de un sistema de control de presencia del personal basado en datos biométricos[105], describía cómo el sistema en cuestión almacenaba el patrón biométrico de una huella dactilar en un modo en que resultaba posteriormente imposible reconstruir la huella a partir de dicho patrón. La AEPD destacaba con esta afirmación que no podía revertirse el proceso de conversión del dato en crudo en un patrón biométrico. En la entrada y salida de las instalaciones se requería a los empleados teclear un número personal de identificación (o PIN) y posteriormente colocar su dedo en uno de los 10 lectores instalados al efecto. Esto es, el sistema procedía a un reconocimiento 1:1 (o de verificación). A juicio de la AEPD, "*tratándose del tratamiento de la huella digital, la información contenida no contiene ningún*

[102] Diversas SSTSJ de Cantabria, Sala de lo Contencioso-Administrativo, de 10 y 23 de enero, y de 28 de marzo de 2003, han considerado que no existía ninguna vulneración de la intimidad. SSTSJ de Cantabria, Sala de lo Contencioso-Administrativo, de 10 de enero de 2003 (rec. 760/2002 y rec. 822/2002); STSJ de Cantabria, Sala de lo Contencioso-Administrativo, de 23 de enero de 2003 (rec. 166/2002), y STSJ de Cantabria, Sala de lo Contencioso-Administrativo, de 28 de marzo de 2003 (rec. 759/2002).
[103] El ATC 57/ 2007, de 26 de febrero rechaza la petición del recurrente por falta de acreditación de los posibles daños para la salud producidos por el control biométrico y la ausencia de restricción de ningún derecho fundamental. Tampoco considera que hay intromisión en la intimidad corporal. Destaca que, aunque el derecho a la intimidad personal forma parte del derecho a la intimidad corporal, ésta no se extiende a todo el cuerpo, de modo que "*no pueden entenderse como intromisiones forzadas en la intimidad aquellas actuaciones que, por las partes del cuerpo sobre las que operan o por los instrumentos mediante los que se realizan, no constituyen una violación del pudor o recato de la persona"*
[104] APDMADRID, *Guía de protección de datos personales para Universidades,* 2008, págs. 456 a 459.
[105] Expediente nº E/ 00057/2005.

aspecto concreto de la personalidad" y consideró que el tratamiento que se hace de este dato trae su origen en la necesidad de asegurar el cumplimiento de las obligaciones derivadas de la relación administrativa o laboral que vincula a los funcionarios o al personal laboral con la Corporación[106].

La AGPD se pronunció también a este respecto en un Procedimiento contra la *Autoridad Portuaria de Baleares*[107], insistiendo en que el tratamiento de los datos biométricos no tenía en su opinión mayor trascendencia que el de los "*datos relativos a un número de identificación personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos*" (Fundamento de Derecho nº II). En este caso, no obstante, resolvió en contra de la Autoridad portuaria, pero por una cuestión a la que prestaremos atención en el siguiente apartado. Aunque en este caso resuelve que la autoridad infringió la LOPD al no estar dado de alta el fichero correspondiente.

En estas primeras resoluciones no se tuvo en cuenta la peculiaridad de los datos biométricos ni el hecho de que directa o indirectamente puedan quedar expuestos (ya sea por el patrón en sí, ya por el funcionamiento del sistema) datos sensibles a los que nos hemos referido en el apartado 5 del capítulo anterior. Es también llamativo que diversas sentencias del STJ de Cantabria afirmaban que los sistemas *computaban información* (en aquel caso relacionada con la geometría de la mano)[108] pero no almacenaban ninguna imagen, como si en términos de privacidad el almacenamiento de la muestra biométrica completa (antes de extraer el patrón), o su formulación digital implicasen una intromisión menor. Y, por ultimo, la falta de distinción entre sistemas con almacenamiento incorporado a tarjetas que porta el usuario y sistemas en los que el almacenamiento es periférico (y en red o no). Hay razones que apuntan que la doctrina de la AGPD se está adaptando y tiende a restringir este tipo de usos, al hilo de la que se está asentando en la UE.

Universitat d'Alacant
Universidad de Alicante

6. LA BIOMETRÍA EN LAS PRISIONES, HOSPITALES Y CENTROS DE ENSEÑANZA.

[106] Véanse, asimismo *Resolución del Expediente E/ 01126/ 2010*, sobre instalación de un sistema de fichaje biométrico para el personal de rampa de la empresa *Spanair*; Resolución del expediente E/ 02635/ 2009, contra la empresa *Servicios Logísticos Integrados, S. A.*, por la instalación de un sistema de fichaje mediante huella digital; Resolución del procedimiento PS/ 00272/ 2005. Por la instalación de un sistema de control horario mediante huella digital en la empresa *Rótulos Ayllón*.; *Resolución del Procedimiento nº TF/ 01755/ 2009*, por ejercer un trabajador el derecho de oposición a sus datos biométricos en el control de jornada laboral del personal funcionario por parte del *Ayuntamiento de Andújar*.

[107] Procedimiento nº AAPP/00020/ 2007. Denuncia de un miembro del Comité de Empresa contra la *Autoridad Portuaria de Baleares* por la recogida de datos de carácter biométrico de los trabajadores. Asi también en el procedimiento AP/ 00075/2008 contra la *Consejería de Trabajo y Empleo de la Junta de Comunidades de Castilla La Mancha*, o el AAPP/00028/2005 y AAPP/ 0029/ 2005 por implantación de sistemas de control de presencia de los trabajadores en el *Ayuntamiento del Puerto de la Cruz* y en la Universidad Popular *Francisco Afonso Carrillo*, y el Expediente E 00057/2005 relativo a los S*ervicios periféricos de la Junta de Andalucía en Málaga*.

[108] SSTSJ de Cantabria, Sala de lo Contencioso-Administrativo, de 10 de enero de 2003 (rec. 760/2002 y rec. 822/2002); STSJ de Cantabria, Sala de lo Contencioso-Administrativo, de 23 de enero de 2003 (rec. 166/2002), y STSJ de Cantabria, Sala de lo Contencioso-Administrativo, de 28 de marzo de 2003 (rec. 759/2002); A. ROIG, "Comentario jurisprudencial. Derecho público y tecnologías de la información y la comunicación (TIC)", *Revista Catalana de Dret Públic*, núm. 35, 2007, p1 y ss.

En los recintos que aquí se agrupan conviven de forma cotidiana los empleados y los usuarios (presos, internos del hospital y alumnos), además de visitantes incidentales como pueden ser los familiares que acuden a estas instalaciones. A pesar de la, en apariencia, diferente naturaleza de estos escenarios operativos, se producen en ellos una serie de circunstancias comunes que explican, como veremos, que se hayan establecido en ellos una serie de tecnologías biométricas de similares características.

A la hora de evaluar las implicaciones de las mismas no podemos pasar por alto, sin embargo, las importantes diferencias entre las situaciones en las que internos carcelarios, enfermos hospitalizados o alumnos, y el trato que en coherencia corresponde a las personas que los visitan.

> Un elemento común, que da lugar a la aplicación de tecnologías con un perfil bastante similar, es la necesidad de controlar los accesos a las instalaciones de los centros de reclusión, los hospitales y los centros de enseñanza, gestionar asimismo el acceso a las zonas restringidas y, hasta cierto punto, contar con la posibilidad de que algunas personas puedan estar geolocalizadas dentro de estos recintos (6.1.)
>
> Veremos, además, la instalación de tecnologías de reconocimiento biométrico en el control de la asistencia y la geolocalización de los alumnos (6.2), la prestación de algunos servicios (bibliotecas, restauración, cafeterías) en este tipo de instalaciones (6.3.) y alguna particularidad, en concreto, sobre los sistemas que gestionan la atención hospitalaria (6.4).

Universitat d'Alacant
Universidad de Alicante

6.1 Control de accesos y seguimiento, y protección de zonas restringidas.

En el año 2001 se estableció un sistema para el control de la seguridad en el acceso en la prisión del condado de Lancaster (Pensilvania, EE.UU.). Además de los empleados, se dio opción de enrolamiento voluntario a los visitantes que deseasen agilizar sus procesos de admisión en la prisión. Este tipo de sistemas, que hoy día se emplean en más prisiones estadounidenses y, entre otros, en las prisiones de Nueva Gales del Sur (Australia) identifican a los reos en su ingreso y en el momento de su puesta en libertad, para evitar fraudes de identidad[109], y en algunos casos también enrolan a los familiares. En España, que nos conste, no se emplean sistemas similares aunque sí surgió el debate sobre la posibilidad de establecerlos a raíz de una fuga de la cárcel modelo de Barcelona; un reo paquistaní se fugó tras una visita, haciéndose pasar por su hermano.

[109] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008, p106.

El control, seguimiento y la finalización de las visitas que, en algunas prisiones, superan el millar, no suele hacerse con apoyo tecnológico y en algunos casos la comprobación de las huellas dactilares debía realizarse a mano. Un sistema de reconocimiento biométrico puede agilizar este tipo de trámites y aportar mayor fiabilidad, y no necesariamente debe ser invasivo. Por ejemplo, un sistema que enrola sólo a los reos comprobará (al salir) que ninguno de los que abandonan la prisión como visitantes coincide en su Biometría con los enrolados; se trata de un sistema de verificación negativa que no almacena ningun dato de los visitantes. También es posible, con poca invasividad, un sistema que realiza un almacenamiento temporal (solo el día de la visita) y, si se desea, limitado a aquellos visitantes que por sus características pueden confundirse con el personal interno de la prisión.

En el caso de los hospitales, los puntos más sensibles suelen señalarse en las farmacias y las zonas de maternidad, además, claro está, los puntos de acceso a las historias clínicas de los pacientes. En noviembre de 2002 se estableció en la ciudad de Bad Reichenhall (Alemania) un sistema de reconocimiento de iris en la zona de maternidad, en el que fueron enrolados los médicos y personal sanitario y las madres. Los datos del iris de estas últimas sólo se conservaban en la base de datos en el lapso de tiempo –en la mayoría de los casos muy breve- en el que tras dar a luz permanecían con sus bebés en el hospital[110]. En relación con las historias clínicas, en el año 2002 se estableció en tres Hospitales Universitarios del Sur de Alabama un sistema conocido como CARLOS (Computer Aided Record Location and Deficiency Sistems), que mediante reconocimiento de iris restringía el acceso de la información clínica a los médicos.

En los centros de enseñanza el objetivo más común es el de evitar que accedan intrusos (haciéndose pasar, por ejemplo, por familiares de los alumnos) o los intentos de suplantar a las personas que recogen a los bebés y niños de corta edad. Por citar un ejemplo, en el año 2003 se instalaron cámaras de reconocimiento del iris en tres escuelas del distrito de Plumstead (en Nueva Jersey), destinadas a mejorar la seguridad de las escuelas New Egypt Elementary School, Middle School and High School de Plumstead. Se enroló a los empleados y a los progenitores y otros ciudadores, estos últimos en relación con los procesos de recogida de los menores[111].

Para algunos de estos casos, dependiendo de la zona en la que estén los centros o de las franjas de edad de los escolares, en algunos países se está permitiendo el establecimiento de sistemas de control biométrico. Como mínimo requieren un enrolamiento, temporal o sostenido durante el tiempo en que el alumno/a al que estén vinculados vaya a permanecer en el centro, a los efectos de verificación de la identidad.

---

[110] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008,, p108.
[111] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008, p107.

6.2. El control de asistencia a los centros de enseñanza y los sistemas de geolocalización

Vamos a referirnos por último a una serie de casos relacionados con la prestación de servicios de enseñanza (en el nivel escolar, universitario o profesional) en relación con los cuáles se han pronunciado la CNIL, el Garante italiano, la Autoridad portuguesa de Protección de Datos y la AEPD. El *Garante* abordó un caso en el que se estableció un sistema de verificación de la presencia de los asistentes a un curso de formación forense; se trataba de abogados en prácticas[112]. La CNIL, por su parte, se pronunció en un caso de control de acceso al comedor escolar, y la AEPD en relación con el uso de huellas dactilares en el control de acceso a un colegio y de tecnología de reconocimiento facial en el control de asistencia de los alumnos a un centro universitario.

En relación de los alumnos del colegio, la AEPD consideró[113] que este tratamiento de datos biométricos era desproporcionado, aplicando al efecto los argumentos desplegados por el documento de Trabajo sobre Biometría de 1 de agosto de 2003 del GT-WP29. Los usos de la identificación biométrica pueden resultar excesivos, dice dicho informe, "*si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva*". Considera la AEPD que en este caso la misma finalidad de controlar el acceso y la salida del centro escolar puede conseguirse una forma menos intrusiva para los derechos de los alumnos. También la CNIL se mostró contraria al uso de huellas dactilares en el acceso de menores a un comedor escolar, si bien consideró que no resultaba tan intrusivo el empleo de la geometría de la mano con esos mismos fines.

En el caso del centro universitario, por su parte, el sistema de reconocimiento facial mediante Biometría tenía el doble objetivo de garantizar la asistencia y de contribuir a la identificación de los alumnos en la realización de las pruebas correspondientes. La AEPD resolvió que[114], pese a que ninguno de los alumnos del centro consultante, en su mayor parte mayores de edad, había presentado objeción alguna a este tipo de control, el uso de este sistema era desproporcionado. Que por su naturaleza guardaba más analogía con el control de los alumnos en los colegios, que con los casos de control horario de los empleados y funcionarios públicos. En similares términos se pronunció el *Garante* en el citado caso *Consiglio dell'ordine degli avocati degli Santa Maria Capua Vetere* (2008).

Tampoco creemos que se aceptaría en la UE un sistema de geolocalización que situe en todo momento a las personas dentrol del recinto escolar o incluso en el seguimiento de los trayectos de

[112] Caso del C*onsigio dell'ordine degli avvocati degli Santa Maria Capua Vetere*, Garante, Provvedimento del 23 de gennaio 2008, doc 1487903.
[113] Informe 368/ 2006 de la AGPD.
[114] Informe 0392/ 2011 de la AEPD.

autobús. N. Nguyen[115] analiza el caso de las escuelas publicas de Bellville, en Nueva Jersey (EE.UU.), en las que los escolares y los empleados llevan acreditaciones con RFID. Estas acreditaciones envían cada veintiocho segundos una señal de localización (permitiendo registrar, por ejemplo si hay personas que van demasiadas veces al baño o siempre juntas y conviene comprobar si hay un posible uso de drogas); tambien regulan el acceso a ciertas áreas y advierten de la localización de los alumnos en el trayecto de autobús, algo que no gusta a los sindicatos de transporte. No se trata sólo de controlar los accesos o la seguridad e ciertas áreas, como sucede en el distrito escolar de Pummstead –en que se controla mediante escáneres de iris si un visitante es seguro- sino que se produce un seguimiento de la movilidad que recuerda al Marauder's Map de *Harry Potter y el Prisionero de Azkaban*[116] (véase la IMAGEN 78). Creemos que esta vigilancia está muy lejos de los estándares que son actualmente admitidos en la UE.

6.3. Control de uso y sistemas de pago de servicios como las cafeterías o bibliotecas

Las escuelas de *Pinellas County* (Florida, EE.UU.) fueron las primeras en establecer el sistema de pago *Palm Secure* (véase imágenes 84 y 85) en los comedores escolares. En más de 59 escuelas y 160 hospitales de 15 Estados existían este tipo de sistemas, según Brian Shane de USA TODAY (2012)[117]. En total cincuenta mil estudiantes de enseñanzas medias, escuelas y centros de estudios superiores las utilizan en cafeterías y bibliotecas. En Europa, aunque no existen datos oficiales, se cree que en torno al 50% de las escuelas de secundria y un 10% de las escuelas de primaria del Reino Unido emplean sistemas biométricos. En 2002 empezaron a introducirse en la gestión de las bibliotecas, para sustituir a las tarjetas, y posteriormente se extendió al pago en las cantinas. Además de evitar los problemas de las tarjetas, no se percibe qué alumnos tienen becas de comedor, pero desde *2012 la Ley de Protección de Libertades* (2012) ha establecido que este tipo de sistemas de pago requieren, en todo caso, que se solicite previamente el permiso paterno[118].

Según se va tomando conciencia de la intromisión que implican estos sistemas, se va constatando que algunos gobiernos están restringiendo o prohibiendo algunas de estas prácticas, como en 2014 ha hecho una Ley que prohíbe el uso de Biometría en las escuelas de Florida. Después de una difusión, como venimos advirtiendo, acelerada y poco reflexionada de los sistemas, es esperanzador que el cambio de opinión se esté traduciendo en gestos tan valientes.

---

[115] NGUYEN, N. "Chokepoint: Regulating US Student mobility through biometrics", *Political Geography*, 46, 2015, pp1-10.
[116] Mapa de *Harry Potter y el Prisionero de Azkaban*, tomado de la edición de1999, pp192/193.
[117] Brian SHANE, USA today, 25 nov 2012. *Palm Scanners get thumbs up in schools and hospitals*.
[118] DARROCH, A. "Freedom and Biometric in UK Schools", *Biometric Technology Today*, jul-ago 2011, p5s.

6. 4. Identificación de pacientes

Hemos encontrado algunas referencias sobre el uso de sistemas de geometría manual en el reconocimiento de los usuarios de programas de metadona en los Países Bajos[119] y sistemas que vinculan la tarjeta y la historia sanitaria de un paciente con Parkinson a su huella dactilar, para facilitar su identificación en algunas situaciones. Se trata de prácticas que han sido autorizadas. El *Garante* italiano, por su parte, se ha mostrado favorable a la utilización de tecnologías de identificación de este tipo cuando el objetivo es, por ejemplo, garantizar la seguridad de las transfusiones en un hospital, ya sea para evitar errores en la identificación de los pacientes, ya de las unidades de sangre trasfundida[120].

Distinto es el caso de la asistencia sanitaria, en sí misma. Que nos conste, no se ha planteado aún en la UE un uso de la Biometría en relación con la identificación de qué personas tienen o no acceso a la asistencia sanitaria, probablemente por los términos en los que ésta se ha venido dispensando en el seno de la UE. En los EE.UU., sin embargo, sí se han implantado algunos sistemas de reconocimiento de los usuarios en la prestación de servicios sanitarios por parte de las aseguradoras[121].

7. LA BIOMETRÍA EN LA OFERTA DE BIENES Y EN LA PRESTACIÓN DE SERVICIOS A LOS CONSUMIDORES

Antes de analizar el uso que de las tecnologías de reconocimiento biométrico se hace en estos escenarios, hemos de advertir que el espacio de relación entre empresarios y consumidores es el espacio en el que, con independencia del tipo de datos que se manejen, más intromisiones injustificadas se realizan en la privacidad de las personas. En este sentido podemos decir que, e algún modo, el recurso a las tecnologías de reconocimiento biométrico no supone sino un síntoma más –y en algunos casos una agravación- *de una tendencia* social características de nuestra era. La referencia normativa para la evaluación del uso de datos biométricos en este escenario es la que venimos aplicando desde el comienzo del presente capítulo: en principio sólo han de obtenerse y tratarse aquellos datos cuya necesidad esté justificada bien para la transferencia de los bienes, bien para la prestación de los servicios.

[119] PETERMANN, 2002, p61.; ALBRECHT, 2001, p15s.
[120] GARANTE – *Trattamento dei dati biometrici nelle operazioni di trasfusiones*, 19 de junio de 2008, doc 1532480.
[121] Vid. *Biometrics and HIPAA conference* (Health Insurance Portability and Accountability Act), "Please put your hand on the scaner"; James B. RULE, *Privacy in Peril*, pp. 110-112.

Ese marco normativo, no obstante, contrasta con situaciones en las que sistemáticamente se recaba un gran número de datos de las personas, tanto clientes en sentido estricto como cualquier ciudadano que en un momento indeterminado pueda llegar a serlo. Vamos a analizar de forma separada la relación con los clientes en sentido estricto y las captaciones de datos de personas que no tienen ninguna vinculación contractual con el titular de los ficheros.

7.1. La Biometría en la identificación de los consumidores y usuarios, en sentido estricto

Aunque ya se ha explicado que las empresas tiene gran interés recabar y analizar datos sobre las distintas fases de su actividad, incluida la interacción con los consumidores y el publico en general, desde la perspectiva de la protección de la privacidad de las personas no siempre se considera justificado que quien ofrece bienes y servicios almacene datos de carácter personal. La normativa no establece aquí ninguna excepción respecto al régimen general: la obtención de datos ha de satisfacer los principios de necesidad, proporcionalidad y finalidad.

Estos principios se aplican tanto a los a los casos en los que el Estado el que obliga al empresario a guardar datos de las personas a las que vende bienes o presta servicios, como a los casos en los que la obtención y almancenamiento de datos tienen como finalidad una adecuada prestación de los servicios. Así, por ejemplo, cuando se venden armas o mercancías peligrosas o vehículos los empresarios registran una información que se facilita a las autoridades públicas, y los hosteleros deben registrar algunos datos de quienes pernoctan en sus establecimientos del mismo modo que las aerolíneas guardan datos de quienes viajan en avión. También las entidades bancarias guardan datos de los titulares de sus cuentas. En estos casos la obligación legal sustituye al requisito del consentimiento, pero no se requerirán más datos que los legalmente establecidos ni podrá darse a esos datos otro uso que el que ha justificado su recolección.

Más complejos son los casos en los que no existe una obligación legal de obtención de datos de carácter personal pero el empresario estima *que los necesita para prestar un adecuado servicio* porque en esos casos ha de analizarse hasta qué punto está justificada esa necesidad y cuáles son los datos cuya obtención resulta proporcional. Vamos a ver a continuación con que fines se usan en estos escenarios las tecnologías biométricas y qué respuesta están recibiendo por parte de las autoridades de protección de datos de carácter personal.

7. 1.1. *El control de los abonados y los socios y el ejercicio del derecho de admisión.*

Las características de algunos de los establecimientos que ofrecen bienes y servicios a los ciudadanos hacen necesario controlar que quien accede a ellos *lo hace con titulo válido* (un cine,

un teatro, un estadio de fútbol). En muchas ocasiones existe la posibilidad de adquirir una *entrada ocasional* peropara fidelizar a los clientes, facilitar su acceso o evitar que se cuelen intrusos es frecuente la creación de abonos personales y tarjetas de clientes. Esa comprobación de los títulos de acceso difiere de lo que se conoce como ejercicio del llamado *derecho de admisión.* A quienes tienen un establecimiento abierto al público (tanto si se accede mediante entrada como en el caso de que el acceso sea libre –por ejemplo a un bar) y a quienes organizan espectáculos o actividades recreativas, la ley les reconoce la facultad de determinar *las condiciones de acceso a su recinto* y esa facultad se conoce como *derecho de admisión*. Aunque el nombre puede dar a entender que se tiene derecho a *escoger quién entra, y quien no*, lo cierto es que esa facultad no es absoluta; la Constitución exige el respeto a la dignidad de las personas y a sus derechos fundamentales y no acepta la discriminación, con lo que no puede negarse entrar a nadie de forma arbitraria o improcedente. El objetivo, como dice la Ley, es impedir que accedan a los recintos personas que se comporten de forma violenta o que puedan producir molestias a los usuarios, así como personas que puedan interferir en el normal desarrollo del espectáculo o actividad. El derecho de admisión también permite limitar el acceso cuando se haya superados el aforo permitido[122].

Las tecnologías de reconocimiento biométrico se emplean en estos escenarios con dos finalidades diferentes. De una parte, para la verificación de la identidad de quienes acceden con titulo válido. Este es el uso más frecuente. De otra, aunque sólo en algunos países, el reconocimiento biométrico se emplea también como instrumento para ejercer el derecho de admisión, ayudando a evitar el acceso futuro de personas que en algún momento hayan producido molestias o interferido en el normal desarrollo de un espectáculo.

Universitat d'Alacant
Universidad de Alicante

Los sistemas que se emplean en este tipo de escenarios son, por lo general, sistemas de verificación (1 a 1). En lo que se refiere a la afectación de la privacidad de las personas, han de distinguirse entre, por un lado, aquellos sistemas que verifican la Biometría contra información almacenada en una tarjeta inteligente que conserva el propio titular de los datos y, por otro, aquellos sistemas en los que el almacenamiento queda bajo el control de un operador (ya sea si conexión en red, o en red). En el primero de los casos la verificación sólo podrá producirse si el titular de los datos lo permite; dependiendo del tipo de los sistemas, sin embargo, en el segundo grupo de casos cabe la posibilidad de una verficación de identidad sin la autorización del titular de los datos. En instalaciones de práctica deportiva en las que se considera incómodo llevar tarjetas o es fácil perder éstas (gimnasios, piscinas, etc.) encontramos sistemas de reconocimiento biométrico en los que la alegación de la identidad se realiza tecleando un PIN. Con la referencia de esa clave el sistema busca un patrón almacenado y acto seguido procede a compararlo con el que

[122] Artículo 24.2. de la Ley 17/1997, de 4 de julio, de Espectáculos Públicos y Actividades Recreativas, en su versión vigente desde el 24 de diciembre de 2013.

se muestra en fresco a su dispositivo de captación. Se trata de sistemas, nótese, en los que no siempre sería posible comprobar "*1 a n*" un patrón biométrico. Es decir que si obtuviéramos huella dactilar y la mostrásemos al dispositivo de captación puede que el sistema no sea capaz de realizar una búsqueda comparativa en su base indicándonos a qué persona pertenece. Mucho más invasivos para la privacidad resultan, sin embargo, aquellos en los que sí se realiza una comparación *1 a n* o aquellos que junto con los patrones almacenan información que va mucho más allá de una mera verificación de la identidad.

Existen también algunos sistemas que más que la identidad de una persona en sentido estricto lo que determinan es si una persona pertenece o no a una determinada categoría o grupo. Así, se han diseñado sistemas de reconocimiento biométrico destinados a comprobar que la persona que accede a un recinto o la que desea adquirir alcohol o tabaco tiene la edad mínima que la ley exige para ello. Véase en el anexo, en la IMAGEN 81, una máquina expendedora que aplicando tecnologías de reconocimiento facial ofrece un servicio de estas características. Fue creada tras un estudio comparado de cien mil personas de entre 14 y 60, y en un test de funcionamiento demostró una precisión del 90% en el test de identificación, concentrando sus errores en aquellos menores que parecían tener más edad y en los adultos de rostros aniñados.

Entre los ejemplos de control de acceso que se citan en la literatura uno de los primeros del mundo fue el establecido en el club deportivo de los oficiales del Pentágono (*Pentagon Officer's Athletic Club*) en Washington. Emplea un primer sistema de verificación de identidad (1 a 1) mediante Biometría del iris, en el que el patrón mostrado se compara con el almacenado en la tarjeta que porta el usuario; un segundo sistema, exterior y sin tarjeta, está destinado al reconocimiento de los corredores[123]. En España, uno de los sistemas que más notoriedad ha adquirido es el que ha implantado la Liga de Futbol Profesional en 2015 para acceder a las llamadas gradas de animación o zonas de grupos fan, a las que se asocia una tasa elevada de incidentes graves. La decisión de implementar estos sistemas se enmarca dentro de un conjunto de "Medidas para evitar actos violentos, racistas, xenófobos o intolerantes", pero realmente el control se produce en dos fases. Primero, se escoge a qué personas, identificadas, se les permitirá enrolarse para acceder a esas gradas. En un segundo momento se procede a enrolar la Biometría dactilar de estas personas con la intención de verificar que son ellas y no otras las que accederán a las gradas con las tarjetas de autorización que se les hayan expedido.

En los análisis de las autoridades de protección de datos y de las asociaciones implicadas en la defensa de las libertades civiles, las piscinas y los clubes de *fitness*, así como los abonos para los parques de ocio han sido de los establecimientos más criticados por usar Biometría. Los

[123] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008, p106.

empresarios alegan la necesidad de evitar la picaresca de que varias personas hagan uso de una única tarjeta de abonado, pero el protector de datos danés consideró que las soluciones biométricas son excesivamente invasivas[124],[125]. En ese mismo sentido se discutió el establecimiento de un sistema de reconocimiento mediante biometría en unas piscinas comunales de Suiza[126]. En dicho debate se introdujo un elemento interesante toda vez que algunos usuarios consideraban que el uso combinado de un número PIN y el lector de huella era más cómodo que tener que llevar consigo objetos identificativos. ¿Es la comodidad del usuario un criterio para admitir la invasión en la privacidad? La literatura y las autoridades de protección de datos consideran que comodidad y necesidad no van siempre de la mano. De hecho la Resolución de la 27ª Conferencia Internacional de Comisionados de Protección de datos expresó su preocupación por el aumento de sistemas privados, mayoritariamente voluntarios, que procesan datos biométricos[127].

Aplicando la normativa europea, el *Garante italiano* ha expresado que para que el consentimiento de los abonados y socios en el enrolamiento biométrico sea valido es imprescindible que se ofrezca a las personas la opción de escoger y que las alternativas que se ofrezcan sean equiparables. Dicho de otro modo, cuando la única forma de abonarse o de acceder es prestarse a la captación de la Biometría o resulta muy gravoso el modo de acceso alternativo, se considera que las personas no han tenido oportunidad de escoger con libertad. Sí que existe un consentimiento libre cuando se ofrece, por ejemplo, una pulsera electrónica de un solo uso como alternativa al uso de la huella dactilar. Como puede observarse en el acceso al *Mouseplanet*, IMAGEN 79, una misma columna de control de acceso es capaz de reconocer, alternativamente, las huellas o las pulseras electrónicas.

Universitat d'Alacant
Universidad de Alicante

Por nuestra parte, creemos discutible que la pérdida económica que les pueda suponer la picaresca en el uso de un abono justifique la intromisión que, respecto a todos los usuarios (en su mayoría honrados) implica el establecimiento de un sistema de verificación biométrica. En un Estado social y democrático de Derecho no todo vale para prevenir los delitos. Nótese, por ejemplo, lo restrictivos que son los jueces cuando se trata de establecer medidas destinadas a evitar que personas con un perfil de agresor tengan acceso a potenciales víctimas de la violencia

---

124 JUUL, N. C. *Recommendation on the Use of Biometric Technology*, en Campisi (ed), Security and Privacy, 2013, p415ss.

125 DATATILSYNET. *Adgangssystem til motionscenter baseret på fingeraftryk*. Decisión 2004-219-028 de la Agencia de Protección de Datos Danesa. http://www.datatilsynet. dk/afgoerelser/arkiv-over-afgoerelser/artikel/adgangssystem-til-motionscenter-baseret-paafingeraftryk/

126 HARB, B./ SCHMID, D. „Der Einsatz biometrischer Systeme". Verfassungsrechtliche Aspekte und Umsetzung der datenschutzrechtlichen Anforderungen beim Einsatz von Biometrie", DIGMA - Zeitschrift für Datenrecht und Informationssicherheit, 5 (4), Zürich, diciembre de 2005, pp. 158 a 161; HERMSTRÜWER, Y. / HAMMANS, H. / DIERS, R. M. K. *Schwimmen mit Fingerabdrück? Die Biometrischen Herausforderungen für das Recht der Gegenwart und Zukunft*, Schriftenreihe der Stiftung der Hessischen Rechtsanwaltschaft, Göttingen, 2012.

127 Vid. MORDINI, E. / TZOVARAS, D. (eds.), *Second Generation Biometrics*, Springer, 2012, pp. 97-98.

de género. ¿No resulta excesivo admitir la invasión de la privacidad para evitar hurtos de unos pocos euros mientras asistimos impasibles a muertes por violencia de genero ante las cuáles no se hizo nada? ¿Está justificado adoptar cualquier tipo de mecanismo para evitar delitos menores, pero no así los más graves? Es obvio que la situación habrá de reconducirse hacia un mejor equilibrio. Si bien la prevención general de los delitos tiene un importante interés social, también consideramos que el castigo penal debe ser adecuado al delito cometido, y equilibrarse adecuadamente con los derechos de los ciudadanos.

Tampoco es previsible que vaya a admitirse el reconocimiento mediante Biometría como sustituto único de las llaves o pases que se emplean en los establecimientos hosteleros (llaves de habitación, sistemas de acceso al restaurante o al restaurante, pago en los bares, etc) [128]. Será imprescindible ofrecer alternativas equivalentes.

Vamos a señalar ahora dos ejemplos de sistemas biométricos en los que el enrolamiento de las personas tiene una finalidad distinta de las que se han mencionado ya. Algunas cadenas de clubes nocturnos estadounidenses proceden a enrolar a los clientes que acceden por primera vez a sus establecimientos (bares, restaurantes, discotecas, etc) [129], vinculando sus huellas dactilares a una serie de datos. Entre las *excusas* para esta obtención suele recurrirse a la obligación legal de comprobar la mayoría de edad de los que acceden. Los usuarios enrolados, a cambio de prestar sus datos, tienen la ventaja de que en el futuro podrán acceder de forma más ágil que aquellos que acceden identificándose por otros medios. Este almacenamiento, sin embargo, permite a su vez un uso ulterior. Y es que cuando un usuario es rechazado por comportamiento inadecuado se envía una alerta –asociada a su Biometría- a todos los establecimientos asociadosa dicha cadena. De ese modo los clubes podrán impedir en el futuro que dicha persona acceda a sus instalaciones. Aunque es difícil afirmarlo con rotundidad, creemos que un sistema así no tendría fácil aceptación en el marco normativo europeo.

El segundo de los ejemplos lo hemos recogido en Canadá. Allí se analizó la posibilidad de establecer un sistema biométrico de reconocimiento facial en el que pudieran enrolarse voluntariamente aquellas personas que deseasen ser *excluidas* en el acceso a los establecimientos de la corporación de *Loterías y Juegos de Azar*[130]. El sistema se presentó como alternativo a un escenario en el que, siempre de forma manual, cada casino venía aplicando un diferente sistema

[128] SOLER FUENSANTA, J. R. / GUASH PORTAS, V. "Identificación de clientes en establecimientos de hostelería", Revista de Análisis turístico nº 16, 2/ 2013, pp13-20-

[129] JUUL, N. C. *Recommendation on the Use of Biometric Technology*, en Campisi (ed), *Security and Privacy*, 2013, p415ss.

[130] CAVOUKIAN, A. / MARINELLI, T. / STOIANOV, A. / ET ALT,. "Biometric Encryption: Creating a Privacy-Preserving 'Watch-List' Facial Recognition System", en CAMPISI (ed.), Springer, 2013, pp215 y ss.

de reconocimiento con fines de exclusión[131]. Tras su análisis, el Privacy Conmmissioner de Ontario (Canadá) mostró su preocupación por la vigilancia colateral que el establecimiento de un sistema de reconocimiento facial implicaría para las personas *no enroladas* aun incluso en el caso de que la base del sistema de reconocimiento la constituyesen las mismas fotografías que suelen obtenerse para el chequeo manual en los programas de auto-exclusión.

7.1.2 *Sistemas de pago y Banca electrónica, y acceso a teléfonos inteligentes y otros dispositivos electrónicos.*

El uso del reconocimiento biométrico en el pago ha venido asociándose a dos ideas: la comodidad para el cliente, expresada en imágenes en las que se paga con sólo poner un dedo o asomar la palma de la mano a un lector, y la garantía (tanto para el cliente como para el empresario) de que no se producirán usurpaciones o falseamiento en la identidad[132],[133]. El estado del arte en relación con estas tecnologías y algunas implicaciones de su uso han reducido, sin embargo, las expectativas en este sector.

En algunas operaciones realizadas por empleados sí que se han establecido este tipo de mecanismos. Por ejemplo el Banco Central de Asia (Indonesia) y el Banco del Cairo emplean Biometría del iris para garantizar que las personas de la plantilla que realizan las transacciones son personal autorizado. Sustituyen los PIN y las contraseñas por un sistema *Identix*[134]. También Armguard Australia, una de las compañías más importantes del mundo en el transporte de dinero en metálico, fue una de las primeras en emplear dispositivos portátiles de *Indetix.* Los guardias de seguridad llevan consigo un sensor que es empleado para verificar la identidad y abrir la puerta de seguridad en los casos en que debe reponerse el dinero en metálico de un cajero automático (ATM) [135]. Se emplean también en el acceso a los bancos o en la comparación de las firmas, como es el caso del Banco Conavi de Medellín o las sucursales del Banco Popular de China[136].

En comparación con los empleados, que son un número más limitado de usuarios, la extensión de los sistemas de pago biométrico a los consumidores resulta mucho más compleja. Por concepto, una tarjeta de crédito ofrece a las personas la oportunidad de extraer dinero de cajeros automáticos o de realizar pagos en todos aquellos establecimientos que pertenecen a una red

[131] *Self Exclusion* (2009), ONTARIO LOTTERY AND GAMING CORPORATION. http://www.knowyourlimit.ca/self-exclusion.html
[132] GELB, A. / DECKER, C. "Cash at Your Fingertips", *Review of Policy Research*, vol. 29, nº 1, 2012, pp91 y ss.
[133] A. BEILLEL, *E-Privacy. Le marché des donées personnelles: protection de la vie privée á l'âge d'internet*, Ed Dunod, 2001.
[134] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008, p109.
[135] SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008, p109.
[136]SHONIREGUN, C. A/ CROSIER, S. *Securing biometrics applications*, Springer, 2008,, p110.

interbancaria (como son en España, por ejemplo, *Servired*, Euro 6000 o *4B*). Introducida la tarjeta en un dispositivo *ad hoc* se realiza una conexión con un operador central que es el que autoriza la operación una vez comprueba la validez del PIN introducido o del DNI mostrado. Algunas autoridades de protección de datos consideran que sustituir las tarjetas y emplear reconocimiento biométrico en estas operaciones sería desproporcionado. Así lo advirtió la CNIL francesa quien admitió en 2010 el testado experimental de un sistema de pago biométrico instaurado por el banco *Accord* (grupo Auchan), que empleaba como base las huellas dactilares[137].

En el mismo sentido se pronunció el *Garante italiano* (2008)[138] subrayando la invasividad que supondría el uso de datos biométricos en un escenario de sistemas bancarios que interoperan. Ello conlleva, en su opinión, un riesgo real y desproporcionado, exponiendo a las personas al peligro de abusos en relación con datos particularmente sensibles[139]. En otros países la sensibilidad es, sin embargo, diferente. Más de sesenta mil cajeros de 280 bancos japoneses emplean reconocimiento vascular de las personas como medida para reducir la operaciones fraudulentas con tarjetas robadas; su esquema de autenticación combina tarjeta, PIN y huella[140]. Véase IMAGEN en el anexo (finger-vein recognition in ATM), número 1.15.

La Biometría en los teléfonos inteligentes y en algunos dispositivos informáticos está abriendo nuevas reflexiones porque cabe la posibilidad de que la verificación para acceder online no se realice de forma deslocalizada, sino a través de un sistema de reconocimiento instalado en el ordenador o el teléfono que es propiedad del usuario, (IMAGEN 82) sin transmisión en línea de estos datos y sin que puedan acceder a esa información terceras personas (*ApplePay*)[141]. No sólo con fines de pago sino, en general, las huellas dactilares, el patrón venoso de dedos y/o manos y la geometría del rostro son empleados en algunos dispositivos para sustituir los PIN de acceso. Tratan de evitar que terceros accedan a móviles y ordenadores personales de alguien, o que en el caso de tecnologías que se comparten algunos usuarios aquellos que sean menores de edad no puedan acceder a contenidos o juegos para adultos, o incluso acreditar la identidad en el tránsito en fronteras son algunas de las utilidades que ofrecen[142].

[137] Vid. Info Sfr, *La CNIL autorise le paiement biométrique*, de 8 de junio de 2010.
[138] *Instituti di Credito: Trattamento dei datti biometrici presso Banca do Sao Paulo*, 2008, doc 1490533; *Trattamento dei dati biometrici presso Cariprato S.p.A*, 2008, doc web 1490382.
[139] GARANTE, *Instituti di Credito, Rilevazione di impronte digitali ed immagini: limiti e garanzie*, 2005, doc web 1246 675; vid. también *Linee guida per le tecnologie biometriche*, 8 de octubre de 2004, p4.2.
[140] ITU-T, 2009, p10.
[141] GRUDZIEN, W. "Biometrie im Banking. Ein Pladoyer gegen Vorurteile", *DuD*, 1/ 2015, pp7ss.
[142] BUSCH, C. "Biometrische Zugangskontrolle mit Smartphones", DuD, 7/2014, pp475-477.

7.1.3. *Evaluación del uso del reconocimiento biométrico en la relación con los consumidores y usuarios.*

En relación con diferentes tipos de usos de tecnologías biométricas en estos escenarios las autoridades de protección de datos de carácter personal (como la AGPD o el Supervisor Europeo) han centrado su esfuerzo en destacar una serie de criterios clave.

La primera reflexión que debe hacerse, en cada caso, es sobre la obligatoriedad o, en su caso, necesidad de que el consumidor se identifique en el caso concreto. Si no es obligatorio (por ley) o necesario para la prestación del servicio (en sentido estricto), entonces no está justificado que el empresario solicite a los consumidores que se identifiquen o que se registren como clientes. Nótese que, por ejemplo, al mostrar el DNI para realizar el pago con una tarjeta el consumidor se está identificando (como pide la normativa), pero ello no implica que el empresario pueda captar esos datos, almacenarlos y emplearlos con otro fin que vaya más allá de acreditar que el nombre que consta en la tarjeta coincide con el nombre que figura en el DNI. El Supervisor Europeo para la Protección de Datos viene advirtiendo que si en un caso en que no está justificada la necesidad de identificación un empresario solicita que los consumidores se identifiquen – o se registren como clientes- y lo establece como requisito para el acceso a los bienes y servicios que ofrece se está produciendo una contravención de la normativa de protección de datos. A golpe de denuncia muchas páginas web que ofrecen bienes y servicios están corrigiendo esta situación y permitiendo adquirir bienes o contratar servicios tanto registrándose como cliente fidelizado como identificándose de forma puntual única y exclusivamente para la compra de que se trate. El control no ha llegado aún, sin embargo, a muchos ficheros *en situación de alegalidad*. Si bien en todo caso esos registros al margen de la ley pueden ser perseguidos y sancionados, creemos que ha de tenerse una especial cautela ante aquellos que, en concreto, usan tecnologías de reconocimiento biométrico.

Como propuesta, creemos que cabe la posibilidad de requerir que las empresas proveedoras de tecnologías de reconocimiento biométrico envíen a la AGPD notificación sobre los sistemas que instalen en establecimiento que atienden a consumidores. Se trataría de una especia de preaviso a la AGPD a la espera de que el titular del fichero active la solicitud de autorización para la puesta en funcionamiento del mismo. En esta línea, ha de recordarse que la AGPD ya ha advertido que los sistemas de reconocimiento mediante huellas dactilares[143] son, a los efectos de la ley, un "fichero de datos de carácter personal" y deben por tanto ser registrados conforme a la LOPD.

[143] El Informe 0082/ 2010 de la AGPD.

La segunda pregunta a plantearse es hasta qué punto, con que intensidad, es necesario identificarse en aquellos casos en los que sí se estima justificada la necesidad de identificación; es decir con qué datos o qué documentos debe identificarse el consumidor o cliente cuando se estima que hay una causa que justifica la necesidad de identificación. Más que en positivo, describiendo qué medios de identificación son los adecuados, las autoridades de protección de datos lo que hacen es advertir cuándo hay una desproporción. Por ejemplo, el SEPD ha advertido de que la obtención de huellas de los clientes resulta desproporcionada en muchos casos, dado que es posible obtener una obtención con las suficientes garantías empleando un sistema *menos intrusivo para los derechos y las libertades de los clientes*; se ponen como ejemplo las tarjetas de fidelización[144].

En la consideración de esa desproporción está el hecho de que el reconcimiento mediante Biometría –más allá de su utlidad- tiene un importante coste social[145]. A las limitaciones en términos de eficacia y seguridad, que se han analizado en el lugar oportuno[146], se suma la invasión de la privacidad de las personas y, especialmente, el riesgo de exposición innecesaria de datos que pueden resultar especialmente sensibles. .

7.2 La captación de datos de las personas *fuera* de los contratos de compraventa de bienes y prestación de servicios.

7.2.1. Que los datos sean interesantes, no quiere decir que sea *legítimo recabarlos*

Desde la perspectiva del empresario, la información que le resulta de utilidad no es únicamente aquella que puede obtener de las personas que, habiendo adquirido bienes o servicios en alguna ocasión, puede considerar como "sus clientes". El uso de la informática en las sociedades contemporáneas es ubicuo y afecta a muchas más personas de las que pudiera parecer. Además de por su interacción directa en la red a través de sus ordenadores o de sus teléfonos inteligentes y tabletas, hay ciudanos que sin saberlo están expuestos a que diferentes dispositivos capten información sobre ellos. Las personas se encuentran sistemas informáticos cuando acuden al banco o a los comercios o en el suministro de servicios básicos como el agua o la electricidad. Son sistemas que, en principio, se han creado para dar cauce al funcionamiento ordinario de la empresa, como por ejemplo un contador de luz que envia los datos para que se haga la factura o una terminal de pago en tienda que va sumando datos a la contabilidad y enviando alertas de los productos que será necesario reponer. Pero, además, son una valiosa

[144] Véase, también la opinión del Garante en *Trattamento di dati personali biometrici per l'acceso a un complesso polifunzionale*, 1 feb 2007, doc 1381983, párr. 3.3.
[145] CCNE, Avis nº 98 "Biométrie, donnés identifiants et droits de l'homme", 2007, pp16-17.
[146] EUROPEAN COMMISSION (ed.), *Biometrics in Europe. Trend Report*, UNISYS – European Biometrics Portal, 2007, pp14-16.

fuente de información para que la misma empresa (u otras empresas) decidan enviarnos ofertas personalizadas o generen perfiles de referencia para poder estudiar nuevas lineas de actuación empresarial. La información no sólo es poder, sino también dinero. En esa captación de datos sobre los "procesos" de una empresa se captan también, claro está, datos de personas; y no sólo de personas que son clientes sino también de personas que se acercan al reclamo de una publicidad y muestran interés o rechazan el producto por las razones que sea. Algunas redes de telefonía, por ejemplo, nos advierten que captarán de nuestros dispositivos datos relativos a las personas con las que mantenemos contacto, aunque esta información suele ofrecerse normalmente en esas interminables páginas de condiciones generales que pocos usuarios llegan a leer.

¿Es legítimo que una empresa capte datos de las personas más allá de la prestación de bienes y servicios? Hasta hace unos años la obtención de este tipo de información, al margen de las relaciones comerciales en sentido estricto, se hacía a través de encuestas (presenciales o telefónicas), visitas puerta a puerta o promociones postales y reclamos adheridos a productos ya asentados o el agotador puerta a puerta. Pero Internet ha revolucionado este escenario. En tiempo real las empresas reciben datos sobre cuántas personas han entrado a visitar su web y en qué productos se han fijado y pueden por ejemplo conocer cuántas personas han incorporado a la cesta de la compra cosas que, en el ultimo momento, han descartado comprar. Aunque no hayan dejado constancia de su nombre sí que se registran la hora de acceso y la localización del dispositivo desde el que han entrado, pudiendo a veces almacenar su dirección IP y permitiendo, quien sabe, que si vuelven a entrar desde la misma dirección les ofrezcamos alguna oferta o les mostremos que su cesta de la compra sigue esperándoles. El pobre usuario, sin percatarse de esa vigilancia, quizá no se pregunte cómo es que aquel par de zapatos que le llamó la atención hace unos días aparece hoy en en un recuadro de "anuncio" intercalado entre las noticias de la versión digital de un periódico. *Qué casualidad* –pensará - *¡encima con descuento!.*

La prueba más tangible del valor que tienen estas informaciones son empresas como *Datacoupy Luth Research* que no compran los datos a las empresas proveedoras de telefonía, sino que pagan directamente a las personas que les permiten usar los datos obtenidos de sus teléfonos inteligentes, tabletas y/o PCs. Pero la mayoría de los usuarios desconoce lo que sucede cuando aceptan que se instalen *cookies* en su ordenador. Desde la Directiva 2009/136/CE la ley que regula los servicios de la Sociedad de la Información y el correo electrónico en España exige que se notifique al usuario el uso de estos cookies (archivos que almacena nuestro ordenador y ofrecen información sobre su uso), al menos en los casos en que este tipo de archivos se empleen con fines analíticos o estadísticos, publicitarios o sociales. No es imprescindible advertirlo, dice la ley, cuando se trata de *cookies* instaladas para el correcto funcionamiento del navegador o, por

ejemplo, requeridas para impedir ataques a la página o a los usuarios. El mensaje estándar de las cookies voluntarias es: "*Utilizamos cookies propias y de terceros para ofrecerte una mejor experiencia y servicio, de acuerdo a tus hábitos de navegación. Si continuas navegando, consideramos que aceptas su uso. Puedes obtener más información en nuestra política de cookies.*" Si deseamos consultar una página todo parece indicar que sólo podremos hacerlo si "aceptamos" esas cookies y las cláusulas en las que se explican las condiciones en que se nos aplicarán estas. Son varias ya las voces que advierten sobre los abusos que se están cometiendo en este sector, pero dos son los principales obstáculos para tomar medidas al respecto. La primera, el hecho de que la mayoría de los usuarios hacen *click* voluntariamente y aceptan las condiciones generales con las que se les aplican las *cookies*. La segunda, más preocupante, que muchas autoridades no consideran datos de carácter personal los datos que se obtienen de los PCs y dispositivos móviles.

7.2.2 Como excusa, intentan decir que no son datos de carácter personal

La normativa de protección de datos de carácter personal permite, en algunos casos, proceder a una anonimización de los datos que son recogidos con alguna finalidad. Así, por ejemplo, cuando se están recogiendo datos con fines de investigación científica o para realizar algún tipo de estadística es posible separar los datos recabados con cualquier tipo de información que pueda contribuir a la identificación de la persona. Pero como antes de ser anónimos han sido datos personales, datos asociados a una persona *identificada* o *identificable*, antes de anonimizarlos ha de pedirse el consentimiento de la persona.

Universitat d'Alacant
Universidad de Alicante

Las empresas que ofrecen bienes y servicios por internet, sin embargo, no es que realicen una anonimización, sino que sostienen que *no se trata de datos de carácter personal.* Consideran que se trata de datos que, de forma automatizada, se obtienen a partir de un ordenador y no de una persona. Aunque el usuario pueda llegar a identificarse a través de su dirección IP sostienen que la información obtenida se ha obtenido del ordenador y no de la persona.

Obviamente, aprovechan aquí un vacío legal. La normativa actual no cuenta con recursos para afrontar los abusos que se producen como consecuencia de esta situación, especialmente en los casos en los que el ordenador o el teléfono inteligente de que se trate lo utiliza, únicamente, una persona o un número reducido de éstas. A ello debemos añadir que, de facto, las empresas hacen todo lo posible por desentrañar el perfil de quien está detrás de cada IP, geolocalizan los aparatos, registran los horarios, y tienen mecanismos (legales o no) para vincular esa IP con operaciones en las que las personas sí han cedido voluntariamente sus datos, a veces con la excusa de ofertas de descuentos, premios y sorteos que, casi siempre, terminan con un "entre en la web y regístrese".

Cuanta más interacción hay, más información se filtra[147]. Pero, por desgracia, las autoridades de protección de datos de carácter personal no tienen forma de conocer cuánta información y de que tipo se almacena y dónde. Al no ser considerados ficheros de datos de carácter personal a día de hoy no se exige que estén dados de alta.

7.2.3. El reconocimiento biométrico en este contexto

Emplear la Biometría en este contexto, por ejemplo para *acceder a la IP* o *para entrar en Google,* generaría para la privacidad de las personas muchos riesgos. Se verían aún más expuestas sin saber ante quién. Implicaría, de algún modo, adosar a la dirección IP una información que puede, ya más claramente, identificar a la persona y a quienes forman parte de su unidad de convivencia.

En nuestra opinión no hay ninguna razón que justifique la necesidad de este uso, con lo que no ha lugar a considerar si es proporcionado o no. La estrecha vinculación entre los datos biométricos e información sensible de las personas (relativa a su corporeidad, a su origen o a su salud) requeriría consentimiento expreso e impediría ocultar la solicitud de consentimiento en esos largos listados de cláusulas generales, pero creemos que no es suficiente garantía. El hecho de que, además, la normativa vigente no haya acertado aún con el modo de dar respuesta a estos peligros y a los problemas que genera que el almacenamiento se produzca en países no europeos (tratando de eludir la normativa) es otra razón para abstenerse de darles cauce.

Universitat d'Alacant
Universidad de Alicante

8. EL RECONOCIMIENTO BIOMÉTRICO EN LA LLAMADA "VIGILANCIA INTELIGENTE", EN LAS REDES SOCIALES Y EN RELACIÓN CON LOS BIG DATA.

8.1. Cribado biométrico con biometrías estáticas y biometrías dinámicas. Los escenarios de la vigilancia inteligente.

Los sistemas biométricos encubiertos se utilizan para identificar a las personas sin su conocimiento (o, al menos, sin su colaboración). Son muchas las posibilidades de aplicación de estas tecnologías en escenarios de vigilancia. Así, por ejemplo, está en primer lugar la vigilancia que se justifica por motivos de protección de la seguridad colectiva o, en su caso, con el objetivo de facilitar la detección, persecución y detención de personas sospechosas. Se trata este de un escenario hasta cierto punto conocido, toda vez que se reflexionó sobre él con la expansión de los primeros sistemas de videovigilancia. En comparación con la videovigilancia clásica, las tecnologías de la información y de la comunicación y el desarrollo de las herramientas de análisis

[147] CLARKE, N. *Transparent User Authentication. Biometrics, RFID and Behavioral Profiling*, Springer, 2011, p99.

biométrico lo que han hecho es depurar e intensificar las posibilidades de control. DUNSTONE/ YAGER describían en 2009 el prototipo de escenario biométrico de estas características[148]:

> *"una bomba es detonada en hora punta en una estación de tren, causando un alto número de heridos y fallecidos. En minutos, las autoridades revisan las cámaras de videovigilancia que graban a los viandantes de la estación y obtienen una imagen del rostro de un individuo que justo antes de la detonación dejó en ese lugar un paquete sospechoso. {..} Saben que si no lo detienen, se esconderá. Así que activan un sistema de vigilancia en todas las cámaras de zonas públicas, carreteras de la ciudad, todas ellas conectadas con una base de datos central de reconocimiento facial. Se enrola el rostro del sospechoso en el sistema. En pocos minutos, el sistema da la alarma; una serie de cámaras fuera de la ciudad lo han detectado y la policía puede seguirle en tiempo real. Apenas unos minutos después de la explosión, el individuo ha sido detenido".*

La identificación y posterior localización y detención de los criminales del atentado que en abril de 2013 se produjo en la línea de meta del Maratón de Boston se asemeja mucho a lo descrito por en ese pasaje, aunque también podemos ver en ese acontecimiento la distancia que aún separa la utopía de la realidad. La identificación y detención de los criminales de Boston no se produjo "en unos pocos minutos", ni estaban asociadas todas las cámaras de videovigilancia del lugar, pero sí que se tuvo noticia del exhaustivo análisis de miles de horas de grabación. De ese análisis se obtuvieron primero una serie de imágenes de los sospechosos y a partir de ellas no sólo se consiguió su detención sino que se estableció su vinculación con la comisión de otros crímenes anteriores. Las tecnologías biométricas, frente al ojo humano experto, ofrecen como mayor ventaja potencial su mayor velocidad de análisis y la posibilidad de incluir, al mismo tiempo, un elevadísimo número de criterios de búsqueda. Emplean en buena medida tecnologías de reconocimiento facial, aunque complementado, por ejemplo, con el reconocimiento por biometría de la marcha (capaz de detectar los casos en los que un sospechoso ha cambiado de ropas o de aspecto) y analizan otros patrones como la ropa o los gestos, el comportamiento, cuando tratan de identificar las intenciones de un indivuo.

Pero no es ésta, sin embargo, la única vigilancia inteligente a la que estamos expuestos. MAYER-SCHÖNBER/ CUKIER, en su ensayo *Big Data: La revolución de los datos masivos*[149], se refieren al fenómeno de la acumulación masiva de datos. Se trata de datos que directa o indirectamente se fabrican constantemente, a partir de un sinnúmero de procesos e interecciones, y sobre ellos se aplican una serie de procedimientos que persiguen identificar patrones recurrentes dentro de los datos (datos de negocio, publicitarios, datos sobre enfermedades infeccionas, espionaje tanto institucional como de la población civil, etc). Son los *Big Data.*

---

[148] DUNSTONE, T./ YAGER, N. *Biometric Systems and Data Analysis*, 2009, 223-224.
[149] MAYER-SCHÖNBERGER, V./ CUKIER, K. *Big Data: A Revolution that will transform how we live, work and think*, Houghton Miffling Hartcourt, Boston-New York 2013.

No puede definirse el concepto de Big Data de forma unidimensional; más que de un concepto, se trata de un tema complejo[150]. De las muchas definiciones que se han publicado una mayoría vincula a estos datos masivos con tres o cuatro características especiales: volumen[151], velocidad, variedad[152] y veracidad (*las tres V's*, o cuatro según algún autor)[153] y *las 3 F's* (Fast, fexibel, focused), aunque esas definiciones nada advierten sobre la finalidad que mueve a los Big Data. El reto de su gestión es el de tomar decisiones o realizar pronósticos sobre la base de una comparación de grandes cantidades de datos estructurados de formas diferentes y procedentes de fuentes diferentes.

Los datos tienen muy diversas procedencia. Algunos datos los generan las personas particulares; a modo de ejemplo, suele decirse que un solo teléfono inteligente genera a día de hoy más información (directa o indirectamente) que[154] los ordenadores de la NASA en el tiempo en que el hombre llegó a la luna. Millones de emails, tuits, whatsapp, búsquedas en google, videos de *Youtube*, diariamente se incorporan a la red miles de millones de nuevas fracciones de información. A eso han de sumarse transacciones de datos (como los metadatos de transacciones bancarias), el seguimiento de trazas del marketin digital o los datos que las *máquinas* –sin nuestra intervención- se envían entre sí (los GPS, las redes Wi-Fi que nos captan, Bluetooth,…).

A ese escenario se han incorporado, seamos conscientes de ello o no, las lecturas de los escáneres (o captaciones de la muestra biométrica) , los metadatos de las transformaciones en patrones y los patrones mismos, especialmente cuando son almacenados en bases de datos que actúan en red. Tras el escándalo de la NSA en los años 2013 y2014 el concepto de *Big Data* se asocia cada vez más con un *Big Brother orweliano* de base tecnológica, un entramado de sistemas informáticos que emplean algoritmos inteligentes y son capaces de perfeccionarlos y de tomar decisiones con base en los nuevos datos que van incorporando en su interacción con seres humanos que desconocen totalmente esta realidad.

[150] DORSCHEL, J. (ed), *Praxishandbuch Big Data*, Springer, 2015, pp1-2
[151] El aumento de la capacidad de almacenamiento se traduce en un aumento sustancial del volumen de datos que se manejan en todo el mundo. RUDOLPH, T. / LINZMAJER, M. "Big Data im Handel", *Marketing Review St. Gallen*, 10/2014,
p. 12–24, p13.
[152] En el sentido de heterogeneidad de fuentes y de formatos de los datos. Muchos datos relevantes para los Big Data no están estructurados.
[153] KUDYBA, S. / KWATINETZ, *Introduction to the Big Data Era*, en Kudyba, S. (ed.), *Big Data, Mining, and Analytics*, Boca Raton (FL): CRC Press, 2014, pp2ss; PAGE, C./ CAMPBELL, R./ COGGESHALL, S./ GILLESPIE, E./ JOHNSON, R./ OLSON, M. /PERKINS, P., *Demystifying Big Data: A Practical Guide To Transforming The Business of Government Microsoft*. p11; SCHROECK, M., SHOCKLEY, R., SMART, J., ROMERO-MORALES, D. & TUFANO, S.: *Analytics: The real-world use of big data*. New York, USA: Somers. 2012, pp4ss.
[154] PANIAGUA, S. "A world of sensors, from Data to Big Data", Tevista Telos, junio-septiembre de 2013.

8.2. *Los datos biométricos en el minado de los Big Data*.

En esa gran masa de datos las técnicas de análisis asocian, analizan (o *minan*) en busca de patrones predictivos; determinan similitudes entre individuos y tratan de obtener resultados. El *minado de los datos* es un análisis automatizado de los datos mediante algoritmos matemáticos. Se persigue captar nuevos patrones y relaciones en los datos, y viene a ser el primer paso del KDD – *Knowledge Discovery in Databases* (o Hallazgos de Conocimiento en las Bases de Datos). En conjunto se trata de identificar, validar patrones de datos novedosos antes no descubiertos y que pueden ser útiles en algún sentido[155]. Con ello se persigue generar un valor adicional a la masa de datos de que se dispone. Dos son los principales riesgos de estas prácticas: el riesgo de discriminación y la invasión de la privacidad. A ellos se unen otros como la des-individualización y las posibles pérdidas de autonomía, la estigmatización o el riesgo de ser confrontado con información no deseada.

El perfilado (o aplicación de perfiles para individualizar y representar a un sujeto, o para identificarlo como perteneciente a un grupo o categoría[156]). Puede resultar muy valioso para las empresas, los gobiernos y los ciudadanos, pero existen riesgos importantes para las personas a las que se vincula un determinado pefilado. Los departamentos de recursos humanos se informan sobre los candidatos y, por ejemplo, las grandes superficies obtienen de los teléfonos móviles información sobre las rutas que hemos seguido en cada una de nuestras visitas. Y existen empresas que son conocidas como "corredores de datos", en el sentido de que poseen datos de millones de usuarios de internet, y pueden resumir indicadores de estilo de vida, intereses o actividades. Cruzando los datos de sus sistema de salud con las búsquedas que los ciudadanos habían hecho en *Google* sobre los síntomas de la *Gripe A* en 2009, Nueva Zelanda observó cómo esas búsquedas podrían ayudar a predecir la actividad de la gripe con más antelación que los sistemas tradicionales, pero esa misma técnica puede emplearse para detectar otros tipos de patrones (sin que las personas se percaten de ello).

Los riesgos que la gestión de los *Big Data* generan para los derechos de las personas se agrupan, fundamentalmente en estos conjuntos[157]:

---

[155] CUSTERS, B. /CALDERS, T./ SCHERMER, B. / ZARSKY, T. (eds), *Discrimination and Privacy in the Information Society*, Springer, 2013, pp22-23.

[156] HILDEBRANDT, M.: "Defining Profiling: A New Type of Knowledge?", en HILDEBRANDT, M./ GUTWIRTH, S. (eds.) *Profiling the European Citizen, Cross-Disciplinary Perspectives*, Springer, 2008.

[157] Hemos empleado la referencia de SCHEMER, aunque el los desglosa en más apartados; véase SCHEMER, B. "Risk of Profiling and the Limits of Data Protection Law", en CUSTERS, B./ CALDERS, T./ SCHERMER, B./ ZARSKY, T. (eds.), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Springer, 2013, pp139-140.

a) Riesgo de discriminación de las personas. El perfilado implica clasificar y dividir, y, por consiguiente, "discriminar" en cierto sentido. El conflicto se plantea cuando la discriminación se considera contraria a la ética o a la legislación, como es el caso de perfilados que explícita o implícitamente tienen su base en la etnicidad, el sexo, la religión o las preferencias sexuales.

b) Riesgo de des-individualización y estereotipado. Por definición los perfiles de clasificación son limitados y esas categorías finitas no llegan nunca a reflejar la riqueza de la diversidad de las personas. Una vez las personas son agrupadas puede suceder que el perfil del grupo no sea igual de válido para todos los miembros que han sido asignados a éste. Además, y según cual sea el criterio de clasificación, es posible que el haber sido incluido en un grupo y no en otro implique para las personas una estigmatización de la que sea difícil escapar.

c) Riesgo de una asimetría en el manejo de la información. La posición del controlador de los datos mejora con el perfilado, mientras que la del titular de los datos se mantiene igual.

d) Imprecisiones y la *probatio diabólica*. El perfilado implica necesariamente asumir un umbral de tolerancia (falsos positivos y falsos negativos), y en ocasiones hará que un sujeto tenga que demostrar "que encaja o no encaja en un perfil", oponiéndose a la clasificación que inicialmente se le haya asignado.

e) Abusos. Los mayores riesgos de abuso se producen cuando se establece un vínculo entre el perfilado y algo que de forma indubitada permita situar a la persona dentro de esa masa de perfiles anónimos.

Las características de la información biométrica, especialmente su inherencia y su estrecha vinculación con información sensible (y permanente) en las personas, intensifican los riesgos a los que se acaba de hacer referencia. Su manejo aumenta los riesgos de discriminación, perfilado grupal y estereotipado, y esa aura mítica de *verdad absoluta* que se le atribuye a veces aparece como un factor que acentuará las consecuencias de las imprecisiones y los errores. A ello se añade, en relación con el riesgo de abusos, su elevado potencial singularizante; todo identificador sólido, lo advertía CLARKE en los años 90, representa una amenaza, porque sitúa y geolocaliza a la persona mucho más que cualquier sistema de identificación numérico[158].

Con o sin reconocimiento mediante Biometría, este escenario de vigilancia masiva –en su mayor parte imperceptible- nos genera una gran preocupación. IMAGÉNES 87, 88, 89, 90. Como advertíamos ya en el escenario de las relaciones entre empresas y consumidores, la normativa de protección de datos no ha conseguido aún encontrar una vía adecuada para dar respuesta a este flujo masivo de datos[159]. El número de actores actualmente implicados en cadenas de información[160], computación en nube[161] y (potencialmente) en la inteligencia digital[162] es tan

[158] CLARKE, R. "Human Identification in Information Systems", *Information Technology & People*, Vol. 7 No. 4, 1994, 34-35; Davies, S. D. "Touching Big Brother: how biometric technology will fuse flesh and machine", *Info Technol People*, 1994, p24.
[159] GURTWIRTH, S. / POULLET, Y./ ET ALT, *Computers, Privacy and Data Protection*, 2011, pp41-42.
[160] *Cadenas de información* es el nombre que se da a un escenario en el que diferentes actores comparten información con fines organizacionales. En la práctica implican que pequeñas bases de datos finalmente se

elevado y son tan complejas las relaciones que se producen entre ellos que se antoja imposible determinar qué situaciones son aceptables y cuáles abusivas, por no hablar ya de tomar algún tipo de medida. Creemos que exponer los datos biométricos a este escenario es algo temerario, aunque hay autores que le resten importancia[163].

Queremos destacar por último, que además de los datos que puedan quedar expuestos en el funcionamiento de los sistemas, existen invitaciones a que las personas faciliten datos biométricos pertenecientes *a otros individuos* vinculándolos de forma inocente a etiquetas en las que pueden leerse el nombre y apellidos y la ciudad de origen de la persona. Por ejemplo, Facebook introdujo el reconocimiento facial en su plataforma en 2011, permitiendo a los usuarios etiquetar las fotos de sus amigos. Poco después Google se aventuró también en la misma empresa y Apple incorporó el reconocimiento facial en *iPhoto*. Es deseable que la normativa se actualice para no tener que andar a expensas de las decisiones que sobre estos abusos van tomando poco a poco las autoridades de protección de datos de carácter personal.

8. 3. Qué podemos rescatar de la normativa vigente

Si nos fijamos en las decisiones que los tribunales –entre ellos el Tribunal Constitucional Español- han emitido sobre la videovigilancia clásica, llama mucho la atención que nada se haya hecho ante el espectacular despliegue que acabamos de describir. El TC ha advertido con insistencia de que la videovigilancia vinculada a la seguridad es particularmente invasiva. La Ley de Seguridad Privada y las que regulan la Seguridad Ciudadana establecen una serie de previsiones. En concreto, en el caso de la seguridad privada la AGPD en su guía ha fijado que las grabaciones podrán conservarse como máximo un mes. Esa cautela, advierten, debe ser aún mayor en relación con las cámaras privadas que graban espacios públicos (aunque sean espacios públicos de uso privado, como por ejemplo, los centros comerciales). ¿Cómo explicar, entonces, que no se nos advierta de que nuestro teléfono cede datos al centro comercial en el que acabamos de entrar, o que nuestras búsquedas en Google, nuestros mensajes en el Facebook (IMAGEN 86) son

---

vuelcan en una mayor. Así, por ejemplo, cuando un ciudadano se dirige a una agencia estatal no siempre necesita enviar todos los documentos relevantes para que esa administración tome una decisión sobre su solicitud, porque la propia agencia los obtiene por la vía de otras entidades. Existen, asimismo, *bases de datos deslocalizadas*; por ejemplo, un supermercado contrata a una empresa que recoge y analiza los datos de su negocio,, algo que se ve favorecido por las posibilidades de un almacenamiento en la nube (GIANNOTTI, F./ LAKSHMANAN, V. S.,/MONREALE, A. PEDRESCHI, D/ WANG, W. H, "Privacy-preserving Data Mining form Ourtsourced Databases", en GRUTWIRTH ET ALTERE, *Computers, Privacy, and Data Protection*, 2011, p411.

[161] CAVOUKIAN, A."Privacy in the Clouds -a White Paper on Privacy and Digital Identity: Implications for the Internet " (Information and Privacy Commissioner of Ontario, 2008).; Robert Gellman, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, (The World Privacy Forum, 2009).

[162] Se refiere a arquitecturas en las que los ordenadores reciben información que les envían objetos cotidianos a los que se les ha instalado algún tipo de tecnología, y actúan conforme a esa información.

[163] MANSFIELD-DEVINE, S. "Social Identity: is biometric technology on social networks a benefit or threat?", Biometrics Technology Today, Noviembre/ Diciembre de 2012, p5.

también analizados y vigilados y que su contenido resulta, de algún modo, tan valioso que hay empresas dispuestas a pagar por él?

Recuerda la AGPD que "*los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre*". A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados;

b) y tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

Consideramos que el uso que se haga de la videovigilancia fuera de los estrictos términos de seguridad de los recintos también debería ser objeto de un control exhaustivo[164]. Las personas deberían saber, por ejemplo que está siendo captada información sobre su comportamiento en un espacio público[165] a cualquier efecto. Recientemente la AGPD se ha pronunciado advirtiendo a una empresa que grababa datos sobre las personas que atendían a una pantalla publicitaria en un centro comercial, indicándole que ese registro de audiencias implica captar datos de las personas (aunque se anonimicen) y debe advertirse expresamente de su actividad a las personas.

En coherencia con lo que hemos descrito en relación con la sensibilidad de los datos biométricos, creemos que el consentimiento tácito que se atribuye a quien, advertido por el cartel, se acerca a la pantalla, debería ser considerado insuficiente[166]. En el caso de los datos sensibles la normativa exige un consentimiento expreso, y hemos argumentado por qué los datos biométricos estáticos y los dinámicos pueden considerarse información sensible. Es decir, que como mínimo es imprescindible una interacción en la que el usuario o la usuaria, advertidos de que se le graba y conociendo el uso que se dará a sus datos, acepta de algún modo la captación de su Biometría.

9. COMPARATIVA DE LOS RESULTADOS DE LA EVALUACIÓN DEL USO DE SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO EN DIFERENTES ESCENARIOS OPERATIVOS.

Las tecnologías de reconocimiento biométrico han encontrado su oportunidad en un escenario global muy sensible a las consecuencias que el falseamiento y las suplantaciones de

[164] AGPD, Guía de Videovigilancia.
[165] SUTROP, M. / K. LASS-MIKKO, K., "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics", *Review of Policy Research*, vol. 29, nº 1/2012, pp21ss, pp30-32.
[166] Informe 0328/ 2012 de la AGOD, consulta sobre la implantación de un sistema de medición de audiencias con reconocimiento facial que clasifica los rostros según género y edad, y almacena las horas de aparición y desapariciónd e la persona y los tiempos en que ha estado prestando atención a la pantalla digital que emite contenidos.

identidad tienen en términos económicos y de seguridad individual y colectiva. Como hemos visto, su expansión se ha producido sin que hayamos enjuiciado adecuadamente hasta qué punto nos pueden ofrecer seguridad (y de qué tipo) y sin que se hayan analizado debidamente los riesgos asociados a estas tecnologías o las herramientas necesarias para amortiguarlos.

Benjamin FRANKLIN afirmó que aquel que sacrifica su libertad con la excusa de la seguridad no merece ninguna de ellas; muchos años después, abrumado por un escándalo de espionaje informático masivo OBAMA se defendió diciendo que su gobierno ya no es capaz de ofrecer a los estadounidenses seguridad y libertad, ambas al cien por cien. Es cuestionable, claro está, a quién corresponde determinar el porcentaje en que debe cederse en libertad para obtener seguridad. Y vemos aún menos claro porqué el resto de habitantes del Planeta debemos ceder libertad (y probablemente seguridad) para que los estadounidenses, supuestamente, disfruten mejor de ambas. ¿No deberían explicarnos que amenazas[167] justifican que, en el fondo, los estadounidenses se defiendan de nosotros? Nos estamos acostumbrando a no oponer resistencia, a no exigir nuestros derechos[168], y actualizando una apreciación de TOCQUEVILLE sobre la relación entre el individuo y el estado, es curioso cómo *la mentalidad individualista promueve paradójicamente el conformismo ante el refuerzo y el aumento de control por parte de quienes tienen el poder*[169].

Vivimos, advertía el que fuera Supervisor Europeo Stephano RODOTÁ, una época en la que la protección de los datos personales está caracterizada por fuertes contradicciones. Contradicciones, apunta, en las que podemos ver una "*verdadera y propia esquizofrenia social, política e institucional*". No obstante, el marco jurídico de protección de la privacidad sigue teniendo una vigencia que debe reivindicarse. Todavía es imprescindible para juzgar el efectivo nivel de democracia de un sistema político[170], en tanto que la democracia no se refiere sólo a las normas de funcionamiento de las instituciones, sino que se expresa también en las libertades y derechos fundamentales de los ciudaadanos. La protección de la privacidad y de las libertades civiles siguen siendo a día de hoy un elemento imprescindible para juzgar el efectivo nivel de democracia de un sistema político[171]. Desde esa referencia, las tecnologías de reconocimiento biométrico deben testarse no sólo *por las necesidades que pueden llegar a cubrir*, sino

[167] GRAY, "Urban Surveillance and panopticism: Will we recognize the facila recognition society?", *Surveillance & Society*, 2003, 1(3), pp314-330

[168] WOODWARD. J. D. "Biometrics: Privacy's Foe or Privacy's Friend", *Proceedings of the IEEE,* vol. 85, nº9, Septiembre de 1997, pp1480ss.

[169] DE TOCQUEVILLE, A. *Pratique de la Philosophie*, edición de E. Hatier, 1994.

[170] RODOTÁ, S. "Democracia y protección de datos", *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciciembre 2003), pp. 15 y ss.

[171] En el mismo sentido N. P. MUSAR, en AA. VV., "Workshop report. Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, security and defense", en *HIDE Newsletter*, vol. 2 (7), 2009, Diciembre, p2 y ss; HARB, B./ SCHMID, D.: "Der Einsatz biometrischer Systeme. Verfassungsrechtlische Aspekte", cit., 2005, pp. 158-161.

fundamentalmente atendiendo a la admisibilidad o no del uso de estas tecnologías con cada uno de los fines propuestos, como paso previo a testar posteriormente la adecuación de su organización técnica en relación con la finalidad pretendida.

Con el objetivo de contribuir a la definición de los criterios de uso de estas tecnologías a la luz de los principios de necesidad, proprocionalidad y finalidad se ofrece aquí un resumen de las principales propuestas que se han realizado a lo largo del análisis de los escenarios:

1. A pesar de sus limitaciones científicas y tecnológicas, el reconocimiento mediante biometría ofrece una poderosa herramienta para identificar, interconectar y perfilar a las personas, afectando de forma importante tanto a su privacidad como a otros derechos fundamentales; sus limitaciones científico-tecnológicas acentúan, además, ese riesgo para la privacidad. Creemos que su uso debe restringirse a lo imprescindible, no admitiéndose cuando existan alternativas equiparables (o suficientes en relación con el fin de identificación que se haya justificado). En nuestra opinión es engañoso ofrecer sistemas de reconocimiento biométrico y otras alternativas como equiparables sin advertir sobre Dado el desconocimiento por parte de la ciudadanía y la tendencia a aceptar clausulas generales sin haber procedido a su lectura, debería exigirse que quien ofrece el reconocimiento mediante biometría asesore a las personas y les informe sobre el riesgo que suponen para su privacidad.

2. Como paralelo al proceso de solicitud de autorizaciones para la creación de ficheros con información biométrica, convendría generar un sistema de alertas por el que las empresas proveedoras de tecnologías biométricas advirtieran a las agencias de protección de datos de que una institución o un particular ha adquirido uno de sus dispositivos. Ello dificultaría el uso alegal y mejoraría la transparencia.

3. En la medida de lo posible, y cuando se haya determinado esta necesidad, el uso de las tecnologías de reconocimiento biométrico debería limitarse a funciones de verificación que comparen el patrón en fresco con un patrón que ha quedado almacenado bajo el control exclusivo de la persona titular de los datos. Es decir, como sucede con el pasaporte biométrico europeo o las tarjetas *Privium.* Si los parlamentos de los países europeos han rechazado de plano que exista una base de datos biométricos para la confección de los pasaportes, consideramos que no ha lugar a justificar almacenamientos de datos que tengan finalidades mucho más triviales como el control horario de los empleados y alumnos, el pago en una cafetería o el acceso a una piscina.

4. El tránsito internacional supera los 2500 millones de personas al año y difícilmente puede pretenderse una gestión manual del mismo. En el caso de los movimientos transfronterizos y la

identificación en los conflictos bélicos no nos parece en sí mismo discriminatorio el hecho de que para las personas sin documentación indubitada se cree un sistema de identificación equiparable al que, desde el nacimiento, está establecido para los ciudadanos de la Unión Europea. Hay retos, claro está, en relación con el uso (el mal uso) que pueda darse a esa información; pero en sí mismo, creemos que es legítimo que se generen sistemas de documentación equiparables a los que existen para los nacionales. Si los ciudadanos nacionales se identifican en su relación con las administraciones públicas, en especial en relación con las autoridades tributarias, la seguridad social o la administración electoral, no es coherente considerar que discriminaríamos a los extranjeros por solicitar que a esos mismos efectos procedan a identificarse de forma equiparable.

5. Cuantas más personas son enroladas en un sistema mayor será el numero de afectados por el umbral de tolerancia del mismo y mientras no avance el conocimiento científico no seremos capaces de determinar la forma en la que las tasas de error se distribuyen entre los diferentes grupos de población. La interacción entre los sistemas de reconocimiento biométrico y el intercambio de datos aumentará nla presión sobre los grupos más propensos a la falsa aceptación o al falso rechazo. Del mismo modo que en la identificación forense no cabe sacar cualquier tipo de conclusión a partir de una *coincidencia*, habrá de velarse por evitar que a las meras conicidencias biométricas se asocien automáticamente informaciones que no tengan ningún otro soporte probatorio.

6. Es probable que el control biométrico genere en cambios en el comportamiento de las personas "normales"[172], sin que por ello cambie, necesariamente, el comportamiento criminal[173]. Los expertos señalan que con el reconocimiento biometríco y la vigilancia masiva lo que se está haciendo es alterar las estructuras sociales para tratar de dificultar los modos en que los criminales se mueven. No obstante, los destinatarios últimos de esas medidas, los afectados realmente por ellas, son el resto de las personas. HECK, el periodista del *Spiegel,* advertía que todos nos comportaremos del mismo modo, para evitar ser sospechosos [174].

7. En el caso de los usos entre empleados y empleadores, con la única excepción de los sistemas de reconocimiento que tienen su base en la seguridad de las instalaciones de la empresa o un fin equiparable, creemos que debería rechazarse el empleo de sistemas biométricos. En los casos en que el uso estuviera justificado, coincidimos con *Garante italiano*, en que un patrón parcial tiene menor entidad singularizante que uno más completo y resulta por ello menos invasivo; si la identificación necesaria puede obtenerse con un patrón parcial, habrá de preferirse esta opción a

[172] VAN DER PLOEG, I. *Identity, biometrics and behavior predictavility*, 2010.
[173] MCCAHILL, "Beyond Foucault. Towards a contemporary theory of surveillance", 1998, pp41-65.
[174] HECK, W. "EU to monitor deviant behavior in flight against terrorism", *Spiegel on line*, 21 oct 2009,www.spiegel.de

la de un patrón completo[175]. Así, en el empleo de un sistema de reconocimiento por geometría manual para acceder a un sitio arqueológico, advierte el *Garante* que el sistema no garantiza una identificación unívoca y cierta de la persona, pero que resulta suficiente como para verificar que se trata de una persona con derecho de acceso a esas instalaciones en concreto[176]. Para un mero control horario, sin embargo, entendemos que caben alternativas menos invasivas en la privacidad, a pesar de que el Tribunal Supremo español entendió en 2007 que este tipo de control está justificado en el caso de los funcionarios del Estado.

8. En relación con su uso en prisiones y hospitales, en los casos estrictamente necesarios, creemos que las pulseras electrónicas pueden ser una alternativa equiparable y menos invasiva. En los casos en los que no sea posible debería establecerse con claridad el periodo de conservación de los datos y el uso que se va a dar a los mismos, garantizándose que la información no se empleará fuera de los fines que justifican el sistema de reconocimiento concreto (como puede ser la gestión de las visitas en las prisiones).

9. En el control de los abonados y de los socios, siempre y cuando se considere que existe una necesidad que justifica el recurso a tecnologías biométricas, el almacenamiento debe restringirse a un objeto o tarjeta en la que quede almacenada la información, bajo el exclusivo control del usuario.

10. El uso en sistemas de pago o en cajeros automáticos, así como en escenarios de relación entre empresa y consumidor que impliquen que los patrones biométricos deban estar disponibles en una red informática implica un riesgo añadido al coste social que ya, de por sí, tienen los sistemas de reconocimiento biométrico. La falta de control que las personas tienen sobre su información biométrica, que está constantemente expuesta a la interacción con terceros, hace además que sea poco recomendable su uso en estos contextos.

11. Finalmente, y en relación con las consecuencias que puede tener la incorporación de datos biométricos a los *Big Data*, al margen de una imprescindible clarificación de la normativa que afecta al control de los datos másivos en general, consideramos que debe limitarse al máximo todo cauce mediante el cuál los datos biométricos de las personas puedan estar a disposición de las herramientas analíticas.

[175] GARANTE, *Sicurezza di diti archeologici e uso dei dati biometrici*, de 8 de noviembre de 2007.
[176] GARANTE, *Trattamento di dati personali biometrici per l'acceso a un complesso polifunzionale*, 2007.

PARTE III

Universitat d'Alacant
Universidad de Alicante

Universitat d'Alacant
Universidad de Alicante

Recopilación de conclusiones

1. El reconocimiento biométrico tradicional y el contemporáneo coinciden en su afán por captar métricamente la singularidad de cada persona respecto de un rasgo biológico (estático o dinámico) que es considerado universal y permanente en los seres humanos.

Lo que las distingue es que en la contemporánea, los sistemas de reconocimiento son automatizados. Ese componente de automatización se considera tan esencial que es el argumento por el cual buena parte de la literatura excluye al ADN del elenco de características que pueden servir de base a un sistema de reconocimiento biométrico en el sentido moderno de la expresión, toda vez que no existe aún una tecnología capaz de realizar de forma totalmente automatizada el proceso de captación, análisis y comparación de patrones ADN.

2. Aunque tiende a afirmarse que las tecnologías de reconocimiento biométrico han surgido en el momento más oportuno y para dar respuesta a una necesidad, consideramos demostrado que: estos sistemas son claramente una consecuencia de la evolución de la ciencia forense, enriquecidas por el desarrollo de las tecnologías de computación.

En su expansión del terreno estrictamente forense hacia muchos otros usos sociales han sido claves dos procesos, en nuestra opinión, diferentes: de una parte, la complejidad del entorno social contemporáneo, muy necesitado de sistemas de identificación agiles y eficaces; de otra, el desarrollo de un conjunto de tecnologías automatizadas de reconocimiento e identificación.

3. Aun no existe una terminología asentada en relación con las tecnologías de reconocimiento biométrico, aunque hemos expuesto las divergencias y nos hemos posicionado sobre los principales conceptos:

a) entre las diferentes acepciones con las que se emplea, hemos optado por usar la voz dato biométrico para referirnos al resultado que se obtiene a partir de un proceso de medición realizado sobre una *característica biométrica* estática o dinámica (concepto éste al que algunos trabajos se refieren como *fuente de datos* biométricos);

b) siguiendo la recomendación de la ISO, en vez de dato en crudo hemos empleado las expresiones *muestra biométrica* y *rasgos biométricos*: muestra para referirnos al resultado analógico o digital que el sistema captura a partir de una característica biométrica (o

fuente de datos); y rasgos para referirnos a aquellos elementos de dicha muestra que procede a almacenar, dado que rara vez se almacena la muestra en su totalidad;

c) y hemos empleado la expresión patrón biométrico para referirnos al modo en que se expresa un conjunto de atributos biométricos o elementos característicos presentes en una muestra biométrica.

4. En lo que se refiere al tipo de información biológica que puede servir de base a un sistema de reconocimiento biométrico, aunque no de forma unívoca, se emplean en la literatura las distinciones entre datos biométricos anatómico-físicos y comportamentales, o datos biológicos, fisiológicos y comportamentales. Cómo se ha justificado, se ha propuesto aquí emplear la distinción entre datos biométricos estáticos (para referirse a los que se obtienen en un *momento puntual* a partir de las *características anatómico-físicas de un ser humano*) y datos biométricos dinámicos (para referirse a los captados métricamente de las habilidades motoras y de las señales y parámetros corporales y comportamentales). Estos últimos captan por lo general información secuencial o cíclica que expresa la actividad interna o externa, voluntaria o involuntaria, del cuerpo de una persona.

5. Tras analizar diferentes propuestas, que ofrecen listados de entre 3 y 12 cualidades (los 7 Pillars of *Biometric Wisdom*, la propuesta de WAYMAN ET ALTERE, la del GT WP 29 y la de Clarke), hemos agrupado en tres conjuntos las cualidades que precisan los sistemas: 1) Cualidades que tienen que ver con la entidad de los rasgos y con el conocimiento científico que se tiene sobre ellos. *Universalidad, singularidad y permanencia*; 2) Cualidades que tienen que ver con la capacidad de los dispositivos y las aplicaciones informáticas. *Colectividad, capacidad de rendimiento y fiabilidad*; y 3) Cualidades que tienen que ver con la interacción entre los sistemas y las personas o el conjunto de la sociedad.

Universitat d'Alacant
Universidad de Alicante

6. En el último apartado del Capítulo 1 de los resultados, una vez presentadas las características biométricas que sirven de base a los sistemas contemporáneos, se han valorado éstas desde la perspectiva de las citadas cualidades. Se resumen aquí algunas de las conclusiones allí recogidas.

Para las Biometrías estáticas, y excluido el ADN de la mayoría de las referencias por la razón que ya se ha descrito, el rostro y el iris se consideran las características de referencia con mayor grado de universalidad, y en el caso de las dinámicas, las señales y parámetros corporales.

En relación con el potencial singularizante, conforme al actual estado de la ciencia y la tecnología se considera que el mejor servicio lo pueden ofrecer el iris y las huellas dactilares, siendo muy inferior el potencial singularizante de las Biometrías dinámicas.

En relación con la estabilidad son también las huellas dactilares y el iris las que se considera que mejor responden ante el envejecimiento, si bien se ven afectados temporal o

permanentemente por algunas enfermedades. Las Biometrías dinámicas son muy sensibles al envejecimiento, a la enfermedad y a los cambios en el estado de ánimo.

En relación con la colectividad, accesibilidad y resistencia al fraude, el iris plantea más dificultades de captación que –por ejemplo- las huellas dactilares, pero al tiempo resulta más complejo de suplantar.

En relación con el riesgo para la privacidad de las personas, se considera que las Biometrías dinámicas son más invasivas que la mayoría de las estáticas, sin que ello deba interpretarse en el sentido de que las estáticas no implican intromisión en la privacidad.

7. Entre los objetivos específicos nos propusimos determinar en qué sentido ofrecen estos sistemas un servicio de reconocimiento o de identificación de las personas. Se ha determinado que pese la gran diversidad de sistemas de reconocimiento mediante Biometría existe una estructura básica común a todos ellos.

En un primer paso de enrolamiento, se procede a captar de una muestra biométrica aquellos atributos que se consideran singularizantes para un sujeto; dichos atributos se almacenan digitalmente como patrón biométrico en un formato que permite, en el futuro, compararlos con los nuevos patrones que se presentarán al sistema.

En algunos sistemas la comparación futura se realiza uno contra uno respecto de una identidad alegada (sistemas de verificación); en otros, en los sistemas de identificación en sentido estricto, la comparación se realiza entre el nuevo patrón y todos los que están almacenados en el sistema (1 a n); y finalmente existen algunos sistemas de reconocimiento biométrico que tratan de hallar la presencia de un patrón biométrico en la corporeidad de todas las personas que son expuestas a su dispositivo de captación. Estos últimos son los sistemas de cribado biométrico.

8. Existe una distancia más o menos relevante entre la información en crudo y el llamado patrón biométrico. El patrón biométrico es consecuencia de la captación de determinados atributos, que se consideran singularizantes. Pero se produce una captación automatizada; es decir, que se le introducen unas reglas al sistema para que realice la captación, esperando que los atributos que obtiene sean suficientemente singularizantes; pero ello no tiene por qué ser así, Es posible que aparezcan gemelos biométricos.

9. La forma en que los forenses y los sistemas biométricos se enfrentan al reto de la unicidad tiene, en nuestra opinión, una diferencia a destacar. Prácticamente todos los procedimientos de identificación de cosas o personas, se realicen de forma manual o automatizada, implican algún tipo

de componente probabilístico respecto del cuál ha de determinarse qué es lo que, en rigor, se estima matemáticamente aceptable. Pero:

> los forenses además de aportar información probatoria, a la hora de tomar la decisión final sobre la coincidencia o la no coincidencia expresan desde su experiencia aquello que consideran que refuerza o debilita la probabilidad en el caso concreto;
>
> y los sistemas automatizados, en cambio, lo que hacen es aplicar aquellas reglas que, de forma anticipada y, por lo tanto, sin posibilidad de referencia alguna al caso en concreto, programó la persona encargada de su diseño.

10. Los sistemas de reconocimiento mediante Biometría tienen importantes limitaciones y riesgos desde el punto de vista de su base científica, desde el punto de vista de su arquitectura tecnológica y, asimismo, desde la perspectiva de su coste social.

11. En relación con su base científica, hemos concluido que universalidad, singularidad y permanencia se interpretan en un sentido flexible a la hora de diseñar los sistemas de reconocimiento mediante Biometría. Esa flexibilización supone, como contrapartida, admitir que todos los sistemas de estas características tendrán, desde su diseño, un margen más o menos amplio de error que, necesariamente, afectará a aquellas personas que por estar fuera de los rangos de universalidad, singularidad y/o permanencia establecidos para el sistema, resultarán atípicas para éste, ya sea de forma temporal o de forma permanente.

> Los datos actuales no permiten concluir detalladamente en qué términos esa flexibilización afectará, de una parte, a la eficiencia y la fiabilidad de los sistemas respecto del conjunto de personas que encajan entre *los típicos;* tampoco permiten establecer, de otra parte, cuántas serán y qué sucederá con las personas *atípicas* para el sistema (los *outlier*) que circunstancialmente o permanentemente no puedan ser adecuadamente identificadas por quedar en el limbo que no cubren esa casi-universalidad, casi-singularidad y casi-permanencia. Si hemos recogido, no obstante, datos que muestran la relevancia de estas limitaciones en relación con la universalidad de las características, la singularidad o la permanencia y la estabilidad.

12. También la eficiencia y la seguridad de los sistemas de reconocimiento biométrico son interpretados de una forma flexible y nos ha llamado la atención que se acepten como parte de un funcionamiento *razonablemente bueno*: una serie de importantes fallos intrínsecos (como por ejemplo problemas de enrolamiento, o almacenamiento de patrones sin previo testado de independencia), así como problemas de seguridad generados por ataques a distintos niveles de los sistemas (en los dispositivos de captación, de almacenamiento, de procesamiento o de toma de decisiones, entre otros).

13. El uso de tecnologías de reconocimiento mediante Biometría implica, en sí mismo y al margen de las limitaciones que acaban de exponerse, un coste social. Entre todas las implicaciones ético-sociales de estos sistemas, que se han referido al final del capítulo segundo de exposición de los resultados, hemos destacado dos.

Primera implicación: que su funcionamiento conlleva, en todo caso, una captación de información biométrica de las personas (bien en el proceso de enrolamiento de los sistemas de verificación y los de identificación, bien en los de re-identificación que realizan tanto dichos sistemas como los de cribado). Esa obtención de información de las personas, en aplicación del concepto de privacidad que ha establecido en su jurisprudencia el Tribunal Europeo de Derechos Humanos de Estrasburgo, supone un atentado contra el derecho a la protección de la vida privada.

Segunda implicación: favorecen el riesgo de hipervigilancia, sobre todo cuando la información se almacena y se gestiona en red.

14. En tanto información que concierne a una persona identificada o identificable –y al margen de que posteriormente puedan aplicarse procesos de anonimización- la información biométrica obtenida de una persona, es información de carácter personal. Consideramos, además, que en coherencia con la interpretación que se da a la información contenida en las muestras biológicas y en los perfiles de ADN, esta información debe considerarse información sujeta a especial protección o información sensible. El argumento para sostener que se trata de información sensible es, en nuestra opinión, el mismo que justifica tal reconocimiento en los citados casos: la posibilidad de que puedan expresar información relativa al origen de las personas, a su salud o a su vida sexual.

Universitat d'Alacant
Universidad de Alicante

15. En relación con la privacidad ha de destacarse, asimismo, que algunos tipos de información personal pueden quedar directa o indirectamente expuestos en los procesos de reconocimiento biométrico.

Especialmente preocupantes en relación con los derechos de las personas son : a) aquellas informaciones que expresan porqué una persona es atípica para el sistema o tiene un perfil que, injustamente, le adscribe al grupo de las personas sospechosas; b) las informaciones relativas a la identidad sexual (en los casos de los sistemas que emplean filtros de género); y c) los datos de salud que estén asociados a características biométricas o dinámicas.

Si nos fijamos en el modo en que se aplica la normativa de protección de datos a otros ámbitos sociales en los que pueden darse exposiciones similares (como por ejemplo, en la investigación biomédica y biocientífica) encontramos que estas circunstancias pueden determinar que se deniegue una autorización a una investigación a pesar del interés que pueda tener para la sociedad. No sería, por tanto, coherente, permitir que se asuman

riesgos de esta entidad para fines tan triviales como control el acceso de los abonados a una discoteca.

16. En lo que se refiere al análisis del uso de sistemas de tecnologías de reconocimiento biométrico en diferentes escenarios, se ha procedido a su exposición agrupada en los siguientes conjuntos.:

1) Biometría en el control de los movimientos transfronterizos y en los escenarios de conflicto bélico; 2) Biometría en las relaciones entre el Estado y sus nacionales y/o las personas que sin ser nacionales residen en su territorio (tarjetas de identidad, asistencia social, sufragio); 3) Biometría en las relaciones entre empleadores y empleados (recintos de seguridad y control de asistencia); 4) Biometría en hospitales, prisiones y centros de enseñanza; 5) Biometría en la oferta de bienes y servicios al os consumidores, incluyendo la banca electrónica; 6)Biometría en la llamada "vigilancia inteligente".

Analizada la necesidad que justifica cada uno de los usos, se ha valorado su aceptabilidad en coherencia con el nivel de intromisión que con los mismos fines se les permite en la actualidad a sistemas de identificación de otro tipo. En líneas generales hemos mostrado nuestra opinión favorable a restringir al máximo el uso de este tipo de sistemas, entendiendo que son muy pocos los fines con los que cabe entenderlos justificados. Y aún en los casos en los que se acepta el uso, se han explicado las razones por las cuáles consideramos que debe velarse porque sea el usuario titular de los datos el que conserve consigo esta información, evitando los almacenamientos que queden al control de terceros. Se trata de una información sensible cuyo manejo automatizado se enmarca, no podemos obviarlo, en un tiempo en el que la vigilancia masiva de las personas se está extendiendo de forma muy alarmante.

17. Retomamos en esta ultima conclusión la pregunta de partida de este trabajo. Decíamos que: "No hay duda de que en el actual contexto social necesitamos sistemas ágiles y fiables para gestionar la identidad de las personas. Pero, ¿Son los sistemas automatizados de reconocimiento biométrico, esos sistemas ágiles y fiables que necesitamos?". Creemos que no, que no lo son. Los algoritmos matemáticos pueden proporcionarnos para cada persona un código de identificación único, diferente, asignado de un modo tal que la variabilidad inter-persona se distribuya homogéneamente; la permanencia de ese número, también es sabido, puede mantenerse del mismo modo que en la mayoría de los casos mantenemos un número de DNI o de pasaporte para los ciudadanos de nuestro país.

Los datos científicos, sin embargo, parecen advertirnos de que la naturaleza no distribuye homogéneamente la variabilidad interpersonal, al tiempo que aún en lo permanente, necesariamente termina por mostrar las consecuencias del paso del tiempo. Es oportuno, en coherencia, no poner en el reconocimiento biométrico más fe de la que merece.

Universitat d'Alacant
Universidad de Alicante

En la mayoría de los escenarios operativos, es nuestra opinión, las tecnologías de reconocimiento biométrico no dan un servicio significativamente mejor que otros sistemas y generan, además, un coste social mayor que aquellos en términos de intromisión en la privacidad y afectación de otros derechos fundamentales. Afectan, especialmente, a las personas que el sistema estigmatiza como atípicas y a los injustamente adscritos a perfiles sospechosos. Pasado el tiempo de la fascinación, del aura mítica de esta tecnología, creemos que ha llegado ya el tiempo de abordar, con conocimiento de los hechos, una regulación *ad hoc* para las tecnologías de reconocimiento biométrico.

Universitat d'Alacant
Universidad de Alicante

Universitat d'Alacant
Universidad de Alicante

Anexo de Ilustraciones

Imagen 1. Panorámica de escenarios operativos en los que se aplica el reconocimiento mediante biometría. (Elaboración propia, se indican a continuación los enunciados de cada imagen y las fuentes de las que se ha obtenido cada una de las imágenes).

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

1. Puerta de acceso con pasaporte biométrico europeo (ePass lane)[1]
2. Control biométrico en las zonas de conflicto bélico (Afganistán)[2].
3. Control de refugiados, ACNUR, Tailandia (campo de Tham Him)[3].
4. Sistema de acceso Privium para pasajeros frecuentes[4].
5. Sala de tránsito de viajeros Privium, aeropuerto de Schiphol[5].
6. Tarjeta de Identidad Aardhaar, India.
7. Sistema de sufragio biométrico[6].
8. Control de inmigración en aeropuerto norteamericano[7].
9. Sistema de control de beneficiarios de ayudas sociales (SASSA Card)[8].
10. Sistema de visado electrónico en ELPASO[9].
11. Pago con Palm Secure en una escuela de EE.UU[10].
12. Acceso biométrico al parque Disney, en Orlando, EE.UU[11].
13. Sistema de geometría manual de acceso de los trabajadores[12].
14. Acceso biométrico (apertura de puerta)[13].
15. Cajero automático biométrico[14].
16. Máquina expendedora de soda[15].
17. Sistema de acceso a banca electrónica (Barclays)[16].
18. Captación de huellas en el Iphone de Apple[17].
19. Sistema de control horario de trabajadores[18].

Imagen 2. Ejemplos de características biométricas (*a) ADN; (b) oreja; (c) rostro; (d) termograma (Imagen termográfica) facial; (e) termograma de la mano; (f) patrones venosos de la mano; (g) huella dactilar; (h) marcha; (i) geometría de la mano; (j) iris; (k) huella palmar; (l) retina; (m) firma; (n) y voz.* [19].

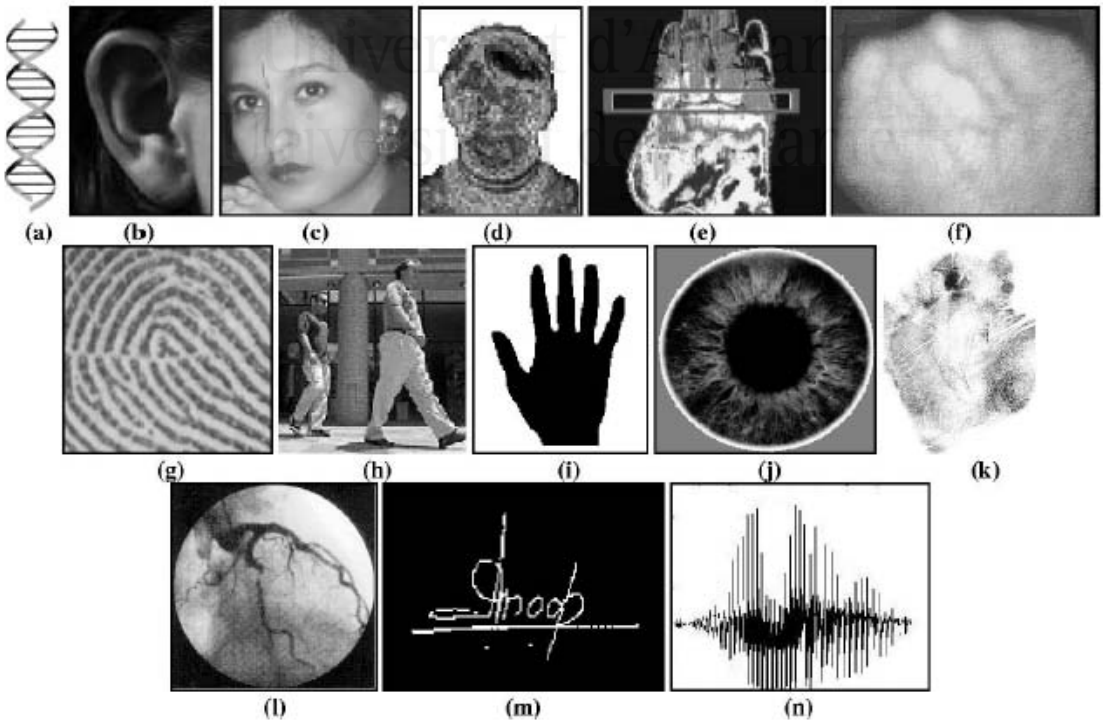


Imagen 3. Ejemplos de aplicaciones biométricas [20]: (a) Sistema de verificación de huellas dactilares, fabricado por *Digital Persona Inc.*, para el acceso a ordenadores y redes; (b) Punto de veta con base en reconocimiento dactilar, producido por *Indivos Inc.* Para la verificación de la identidad de los clientes antes de realizar cargos por las compras en sus tarjetas de crédito; (c) cerradura con acceso mediante biometría dactilar, de *BioThentica Corporation*; (d) Sistema INSPASS, del servicio de inmigración, desarrollado por *Recognition Systems, Inc*. e instalado en los principales aeropuertos estadonudenses y basado en la geometría manual: (e) Sistema de transito de fronteras con reconocimiento del iris, Aeropuerto de Heathrow en Londres; (f) Aeropuerto Ben Gurion de Tel Aviv, quioscos de entrada *Express Card* con geometría manual en el control de seguridad e inmigración; (g) sistema *FacePass* de *Viisage*, usado en la verificación en puntos de venta como cajeros automáticos para la sustitución de los PINs; (h) *TouchClock* de *Identix*, de control dactilar, en aplicaciones para el control del tiempo y la asistencia.

Universitat d'Alacant
Universidad de Alicante

Imagen 4. Cueva de Chauvet. [21]

Imagen 5. Huellas dactilares de Babilonia (de hace más de 4000 años)[22].

Imagen 6. El muro de las huellas, en la ciudad de Tongling (provincial de Anhui, China; 600 años de antigüedad)[23].

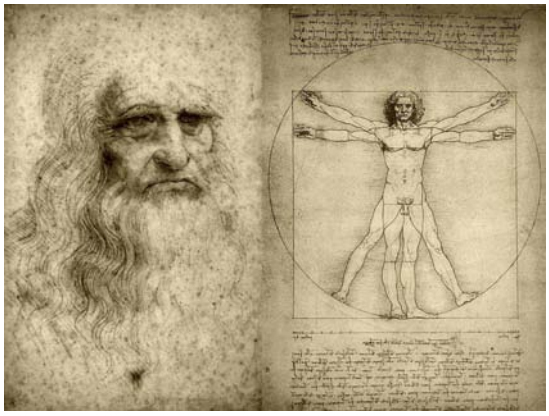


Imagen 7. Leonardo Da Vinci, El hombre de Vitruvio. [24].

Imagen 8. El hombre de Vitruvio, en el Euro que acuña la República de Italia[25].

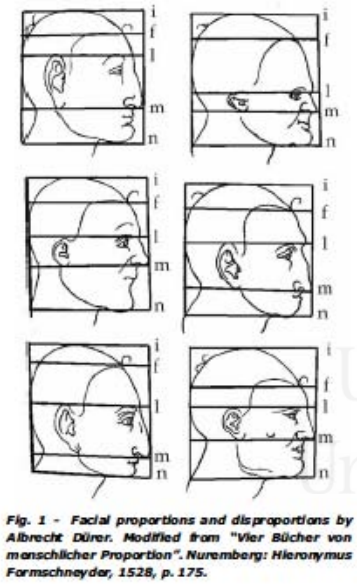


Imagen 9 . Proporciones de Durero. Tomado de "Vier Bücher von Menschlicher Proportion" (1528)[26].

Imagen 10. Lombroso. L'Homme Criminel, Atlas. Derechopenalonline. 1887

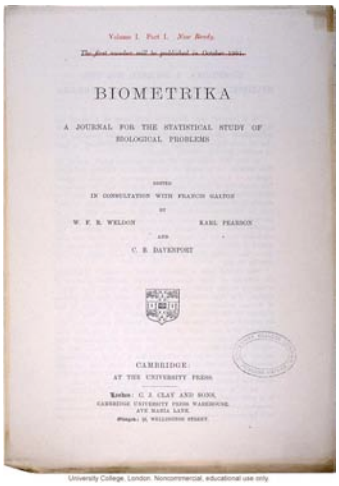


Imagen 11. Primer número de la revista Biometrika (1901)[27].

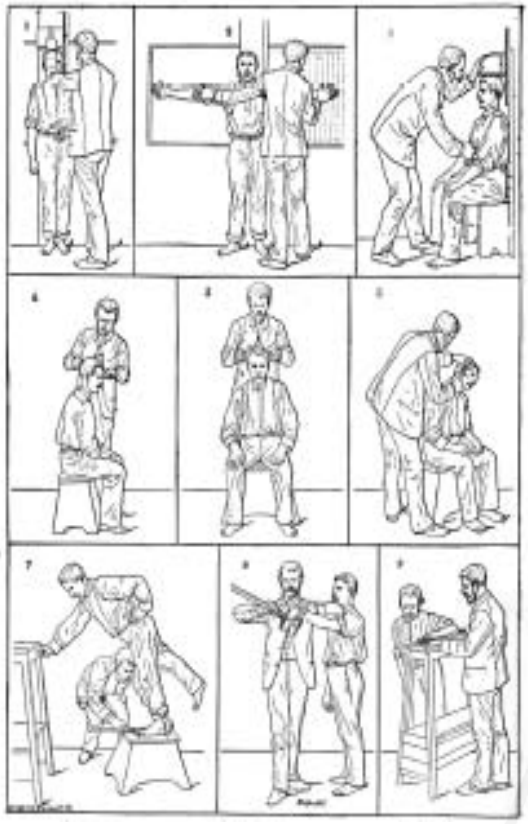


Imagen 12. Diagrama de medidas de Bertillon. Página del libro *Identification anthrométrique* (1893) de Alphonse Bertillon, editado en 1914.

Imagen 13, aplicación del Diagrama de Bertillón; empleado en la prisión de Illinois. [28]

Universitat d'Alacant
Universidad de Alicante

Imagen 14. Toma de medidas de Bertillon, Policía de Nueva York, 1908.[29]

Imagen 15. Ficha de Bertillon (Bertillon Card) de Francis Galton. Contiene la Imagen frontal y la Imagen de perfil, pero las medidas nunca fueron completadas [30] .

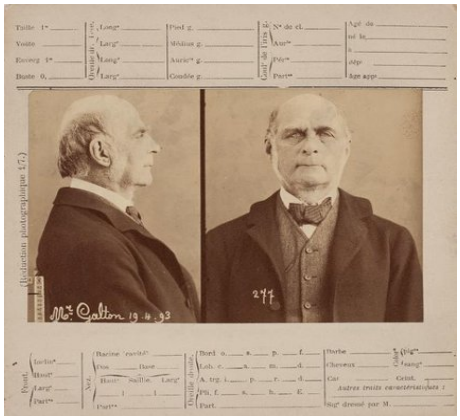
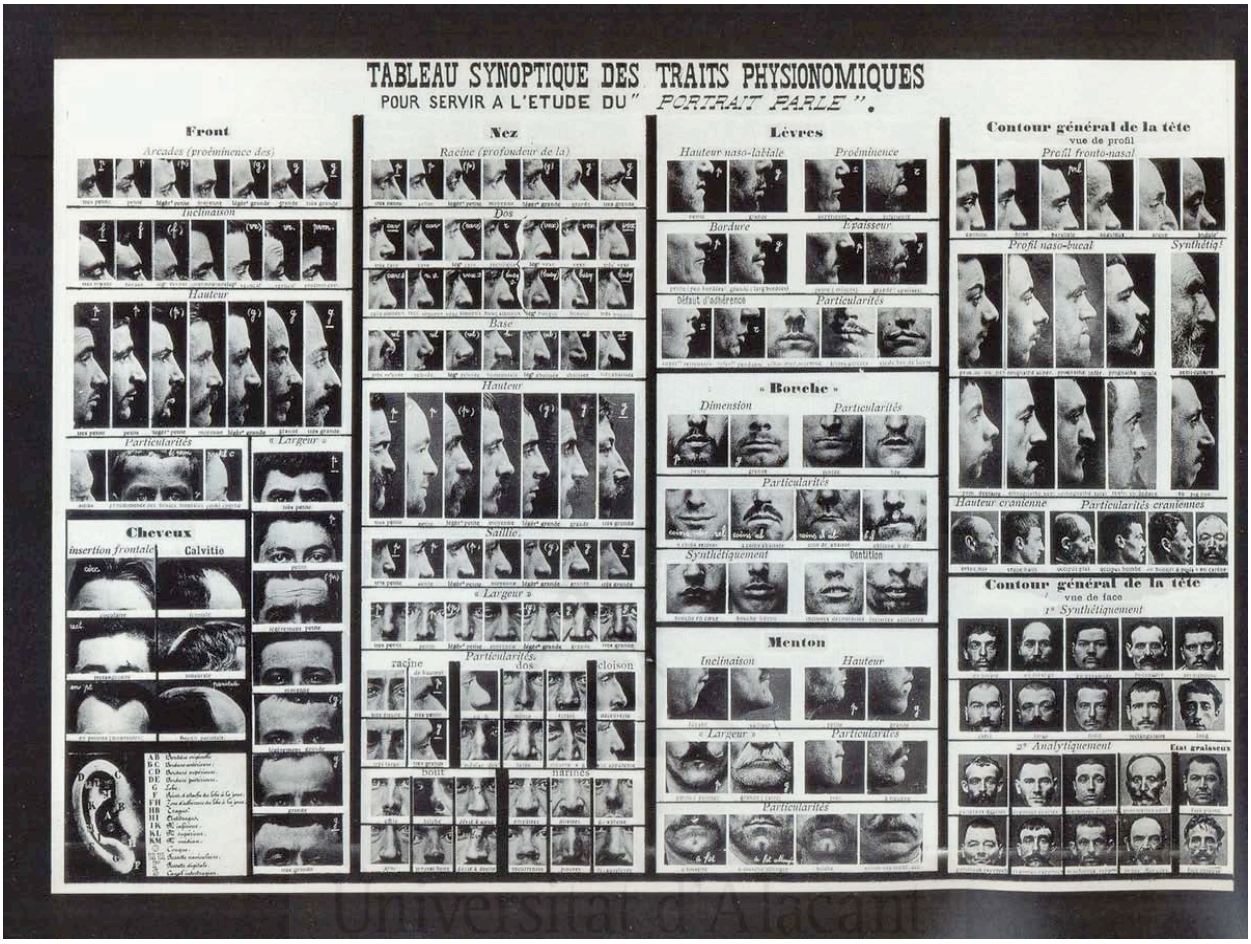


Imagen 16. Tabla sinóptica de rasgos fisionómicos (uso policial)[31].



Universitat d'Alacant
Universidad de Alicante

Imagen 17. Caso Will West, fotografías del frente y el perfil de los dos detenidos.[32]

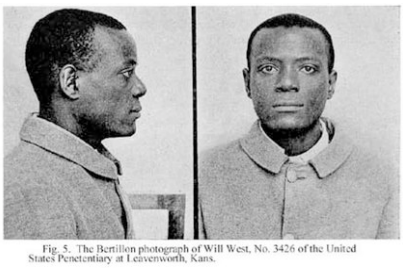


Fig. 5. The Bertillon photograph of Will West, No. 3426 of the United States Penetentiary at Leavenworth, Kans.

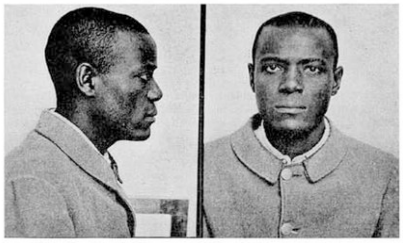


Fig. 6. The Bertillon photograph of William West, No. 2626 of the United States Penetentiary at Leavenworth Kans. This is a different man from the foregoing (Fig. 5.), bu has practically the same Bertillon measurements, and almost the same name. Both were at Leavenworth at the same time.

Imagen 18. huellas dactilares (índice izquierdo) de Will y William West.[33]

Imagen 19. Cálculo de los ingresos obtenidos por las tecnologías biométricas entre los años 1999 y 2003, distinguiendo tipo de biometría en la que se basan. [34]

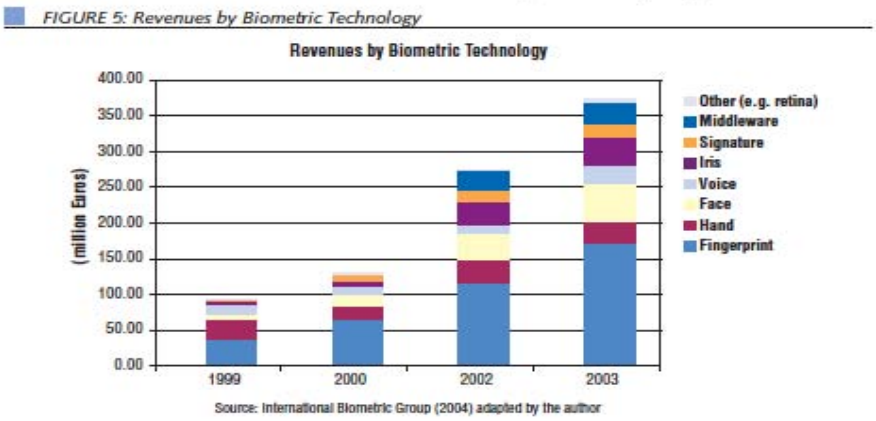


Imagen 20. Beneficios del sector de las tecnologías biométricas, 2009-2014. Predicción publicada en el año 2009[35].

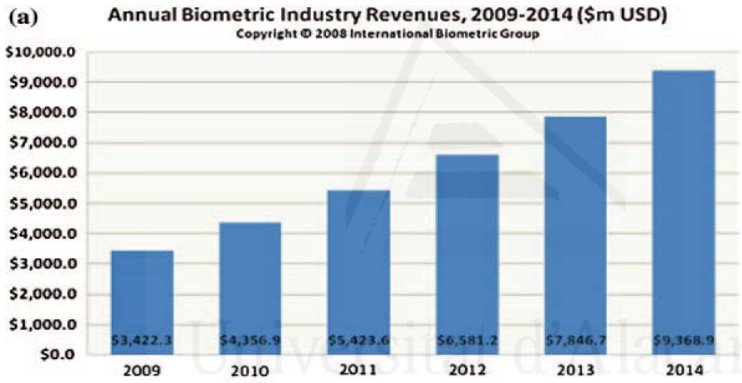


Imagen 21. Sistema biométrico de determinación del sexo. SexNet[36]. Red en dos niveles para la determinación del sexo en los rostros. La red de compresion codifica los rostros en 40 unidades ocultas que se emplean como inputs en la segunda red, que discriminal el sexo. El output es 1 para hombres, 0 para mujeres.

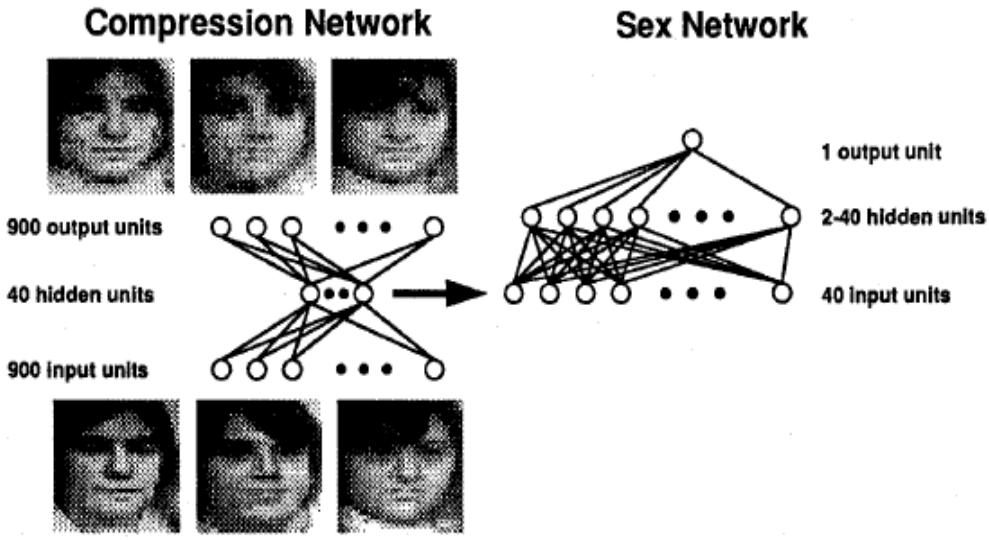


Imagen 22. Clases más comunes de huellas dactilares; clasificación según el esquema de Galton-Henry[37].

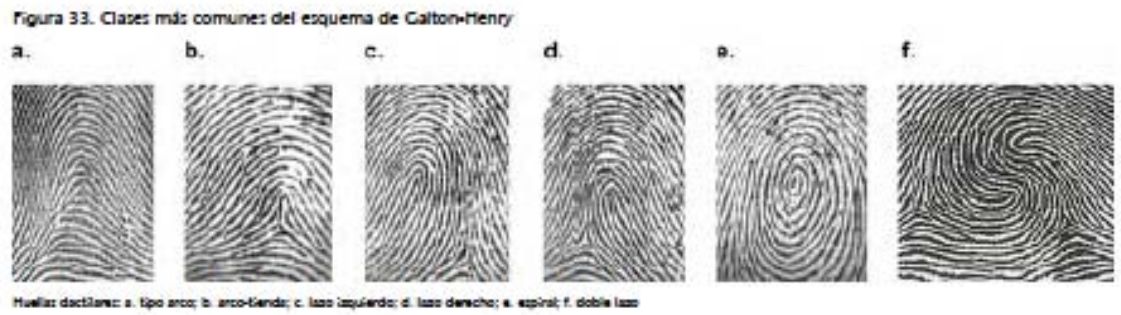
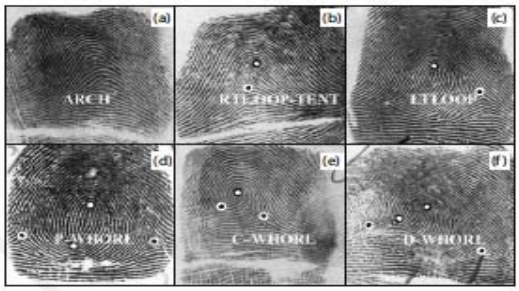


Imagen 23. Reconocimiento biométrico de la tipología de huellas dactilares. El sistema detecta los nucleos o puntos centrales (en circulos blancos) y los puntos delta en circulos negros.[38]



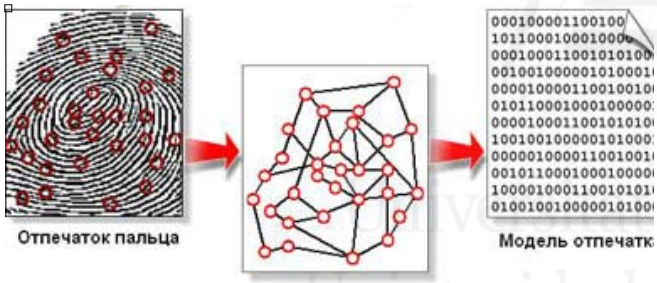


Imagen 24. Transformación de muestra biométrica en patrón digital (esquema de la conversión del patrón obtenido de una huella dactilar en un patrón binario)[39].

Universitat d'Alacant
Universidad de Alicante

Imagen 25. Ejemplo de búsqueda de coincidencia en las minucias[40]

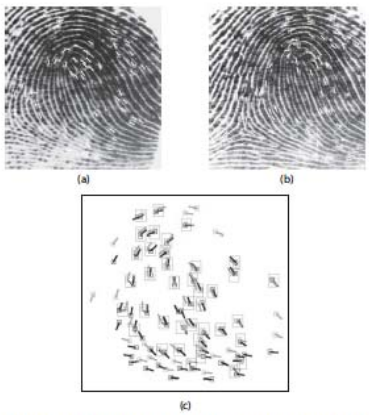
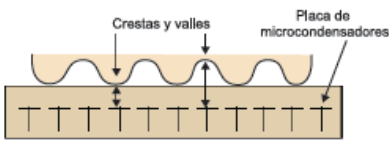
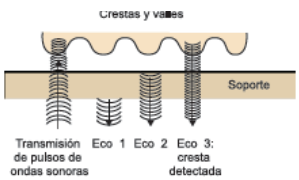


Imagen 26. Diferentes tipos de sensores de captación de huellas dactilares (de izquierda a dereecha: sensor que detecta la carga eléctrica dependiendo de si contactan o no con el sensor; sensor de ultrasonidos; y sensor térmico)[41]





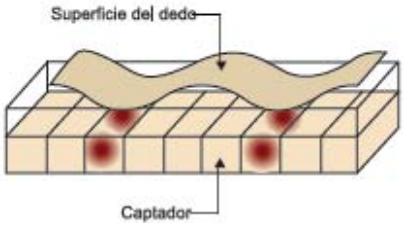
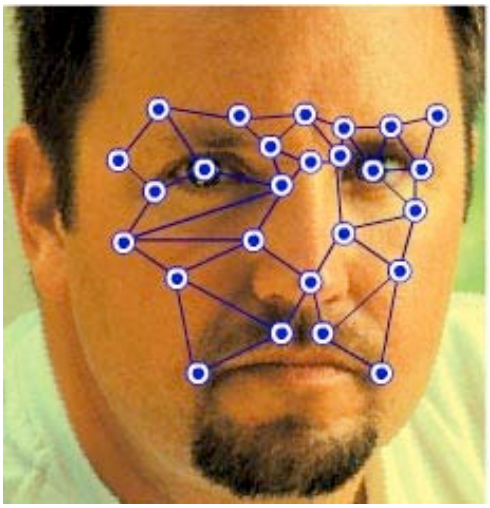


Imagen 27. Captación de la geometría del rostro. [42]



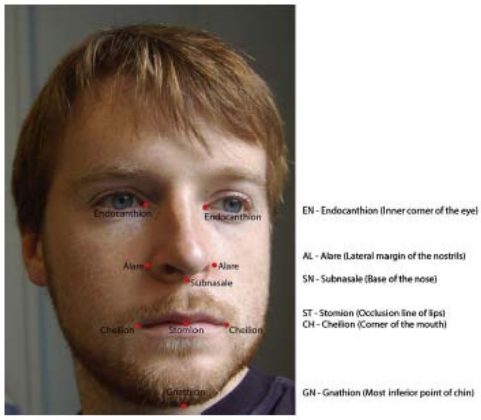


Imagen 28. Fotoantropometría. [43]

Imagen 29. Variabilidad de la biometría facial (intra- e interclase). [44]

Imagen 30. Sistema de cribado facial remoto [45]

Imagen 31. Localización de los puntos de medida en la geometría manual. [46]

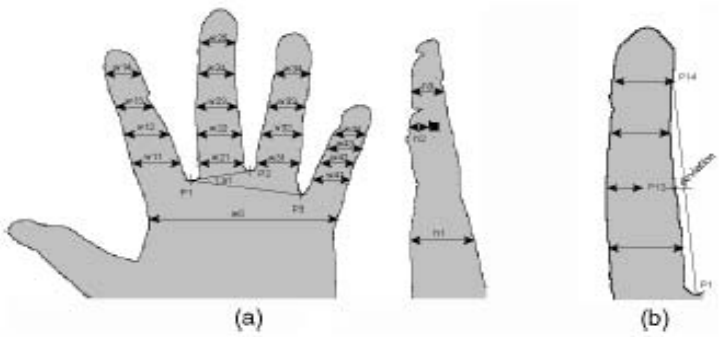


Fig. 2. (a) Location of measurement points for feature extraction. (b) Detail of the deviation measurement.

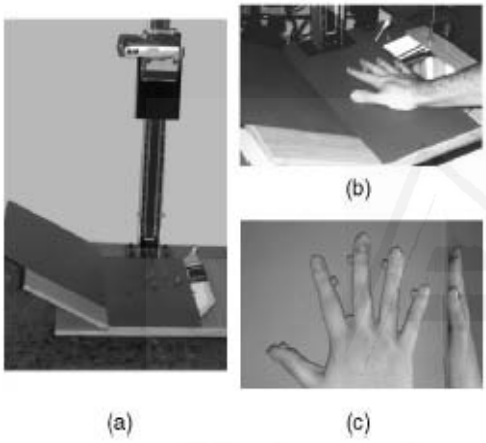


Imagen 32. Diferentes perspectivas del prototipo de extracción de la geometría manual. [47]

Imagen 33. Dispositivo de captación de la huella palmar y muestra digital que se obtiene[48].

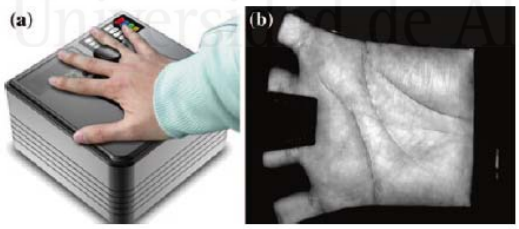
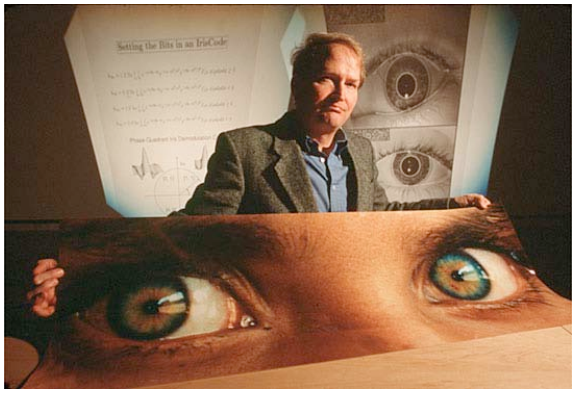
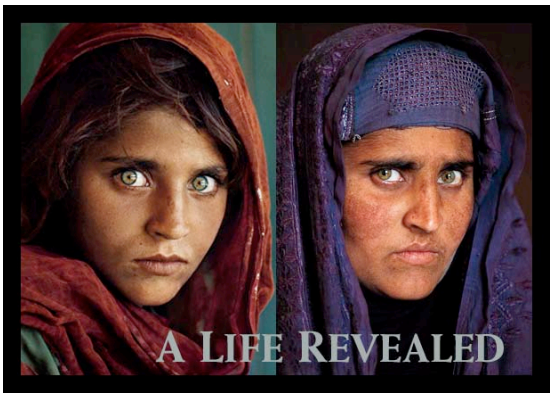


Imagen 34 . John Daughman y los ojos de Sharbat Gula. [49]





Universitat d'Alacant
Universidad de Alicante

Imagen 35. **Esquema de Iannarelli**. [50]

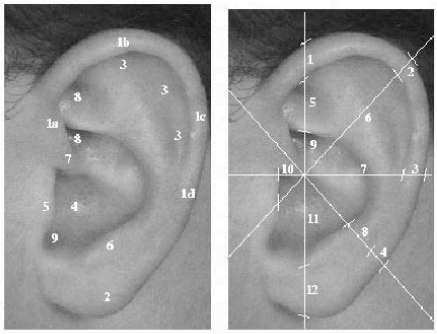
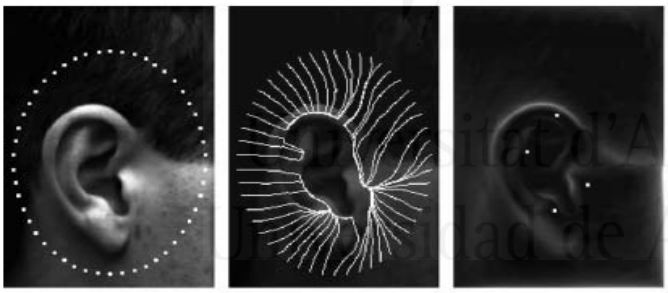


Fig. 2. (a) Anatomy, (b) Measurements. (a) 1 Helix Rim, 2 Lobule, 3 Antihelix, 4 Concha, 5 Tragus, 6 Antitragus, 7 Crus of Helix, 8 Triangular Fossa, 9 Incisure Intertragica. (b) The locations of the anthropometric measurements used in the "Iannarelli System". (Burge et al., 1998)

Imagen 36. **Huella de la Oreja.**[51]

Imagen 37. **Huella de la Oreja (2)** [52].

Imagen 38. **Obtención de la biometría auricular mediante ondas**[53].



(a) Initialisation (b) Channel formation (c) Well positions

Fig. 4. Extraction of potential wells and channels.

Imagen 39. **Obtención de la biometría auricular en 3 dimensiones (3D**)[54].

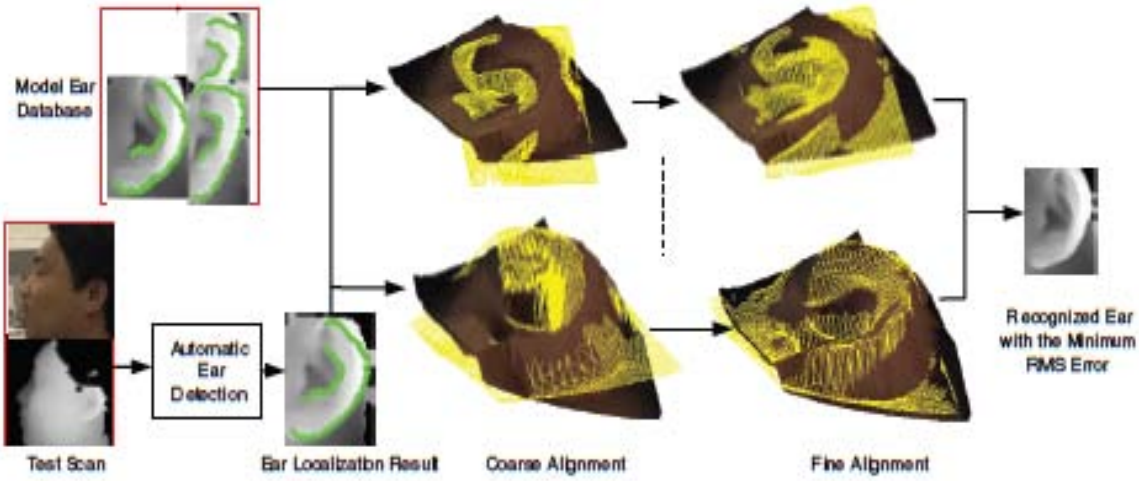
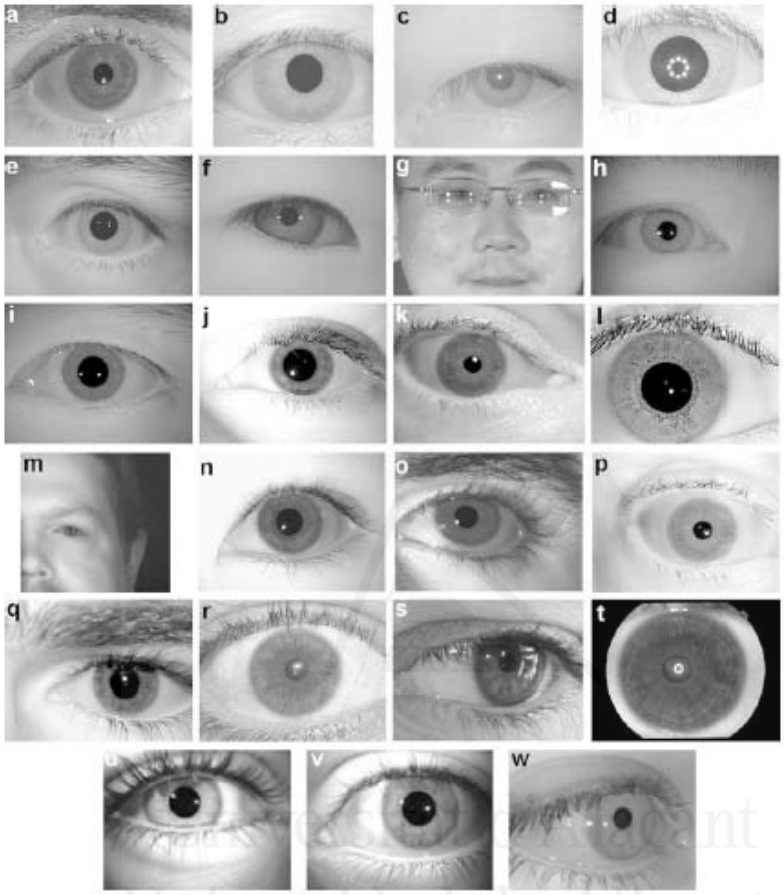
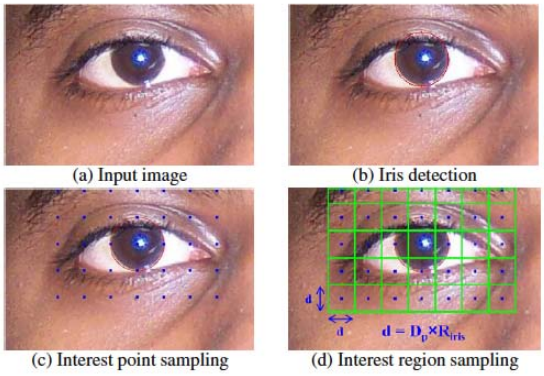


Imagen 40. Muestras biométricas del IRIS almacenadas en distintas bases de datos.[55] (a) Bath; (b) CASIA.v1; (c) CASIA.v2; (d) CASIA.v3-Interval; (e) CASIA.v3-Lamp; (f) VASIA.v3-Twins; (g) CASIA.v4-Distance; (h) CASIA.v3.Thousand; (i) CASIA.v4-Syn; (j) ICE 2005; (k) ICE 2006; (l) IIT-D; (m) MBGC.NIRVideo; (n) MMU.l; (o) MMU.2; (p) ND-CrossSensor; (q) ND-Iris-0405; (r) UBIRIS.v1; (s) UBIRIS v.2; (t) UPOL; (u) WVU-Biomdata.v1; (v) WVY-Biomdata.v2; (w) WVU-OffAxis.



Universitat d'Alacant
Universidad de Alicante

Imagen 41. Biometría periocular[56] (izquierda: alineamiento y extracción de características perioculares; Imagen de la derecha: extracción en cuadros envolventes).



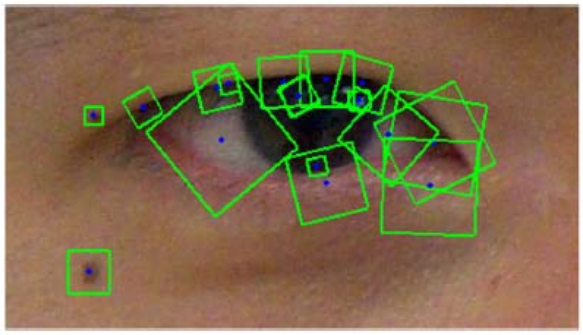
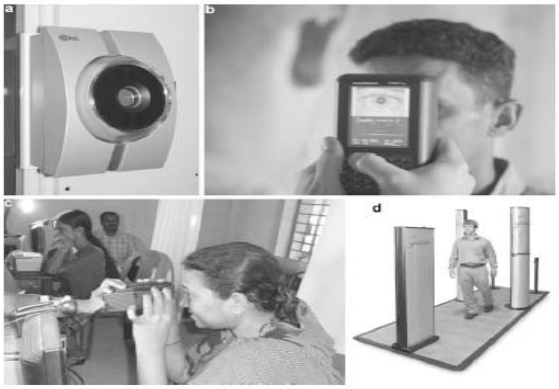


Imagen 42. Diferentes tipos de cámaras que captan la biometría del IRIS. (a) control de acceso, LG Iris Acces; (b) cámara de mano, IdentityPier; (c) tipo visor, Cogent 3M; (d) portal (SRI Sarnoff IOM Passport)[57]



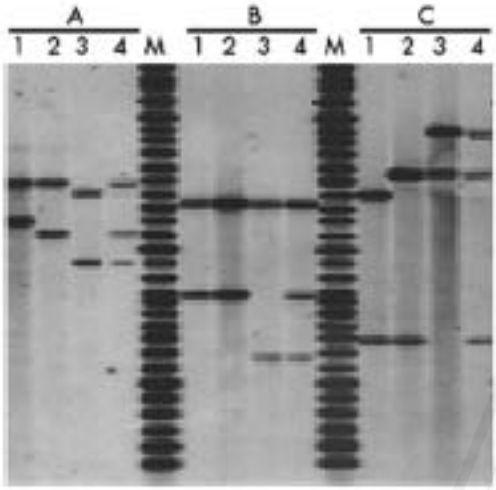
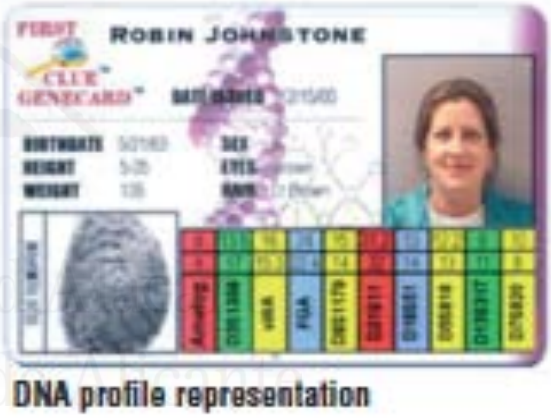


Imagen 43. Patrón de ADN representado como Imagen en la que se reconocen las secciones de los fragmentos, para permitir la comparación entre 3 personas diferentes, respect de 4 *loci*. [58].

Imagen 44. Representación del perfil de ADN en carnet de identidad. Imagen simulada en el informe IPTS[59].



Universitat d'Alacant
Universidad de Alicante

Imagen 45. Diagrama de la nariz electrónica ENose y prototipos[60].

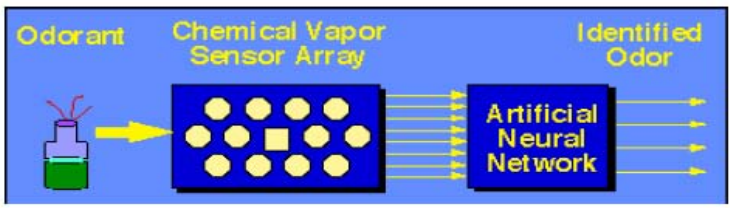


Figure 2: Schematic Diagram of ENose [12]

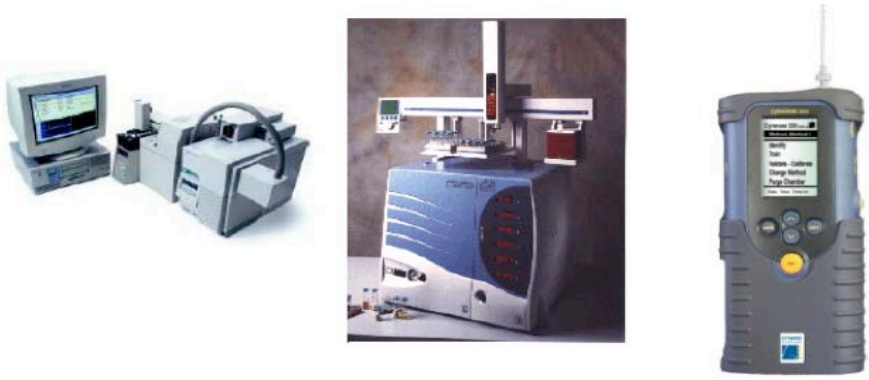


Imagen 46. Biometría dental (bandas Hunter Scheger)[61].

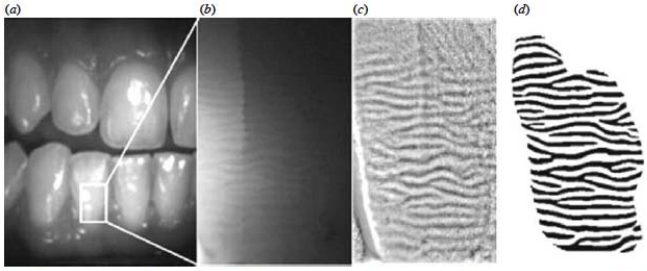


Imagen 47. Huella de la lengua (tongue print). Diferentes formas (se pre-procesan a partir de la forma exterior), imagen superior; y diferentes texturas de lenguas (se preprocesa mediante equalización del histograma), imagen inferior[62].

Imagen 48. Lecho ungueal. Escaner del lecho ungueal AIMS de AuthenticScan.[63]

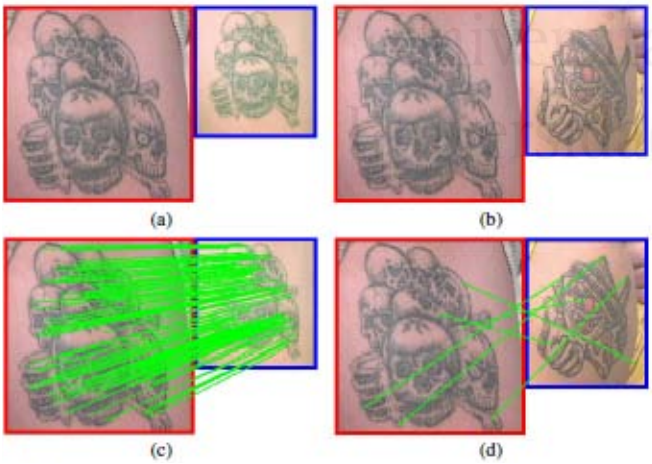
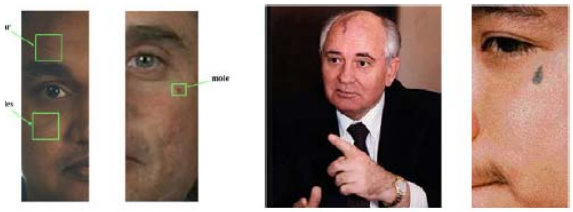


Imagen 49. Tattoo Matching. Ejemplos de reconocimiento de tatuajes (empleando dos tatuakes diferentes). En la comparación de las dos imágenes de (a) el sistema reconoce (en c) 129 puntos de coincidencia; en la comparación entre las imágenes que aparecen en (b) se detectan, véase d, sólo 12 puntos de coincidencia.[64]



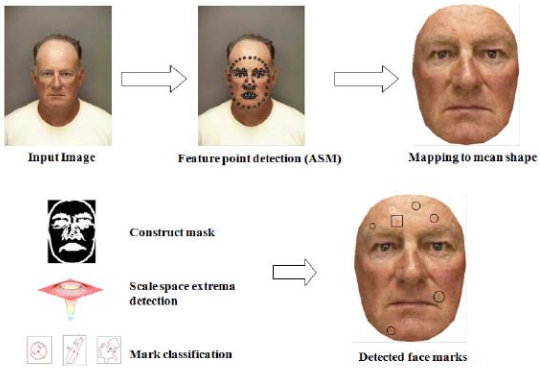
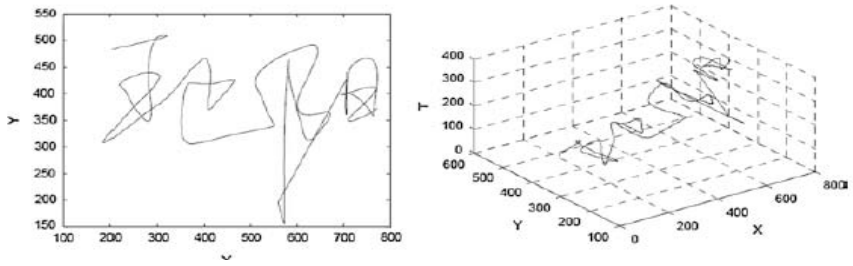


Imagen 50. Reconocimiento de Marcas faciales.[65] Cicatrices, manchas, lunares. Imagen superior: ejemplos de marcas faciales; imagen inferior: proceso de detección de las marcas faciales.

Imagen 51. Biometría de la firma dinámica, Expresión de una misma firma en 2 y 3 dimensiones [66]



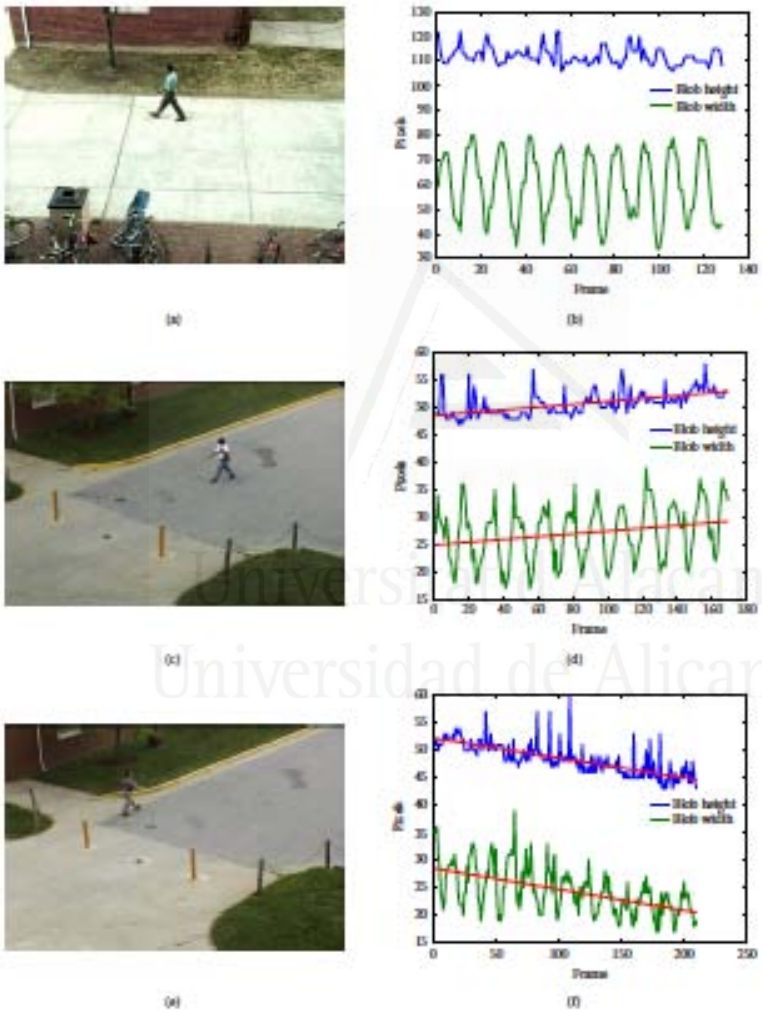


FIGURE 3: Template dimensions in pixels for (a), (b) a fronto-parallel sequence; (c), (d), (e), and (f) two non-fronto-parallel sequences (bottom two rows). The width and height increase when the person walks closer to the camera (middle row), and decrease as the person moves away from the camera (bottom row). The red lines correspond to the linear trend in both these cases.

Imagen 51b. Biometría de la marcha (Gait biometrics). [67]

Universitat d'Alacant
Universidad de Alicante

Imagen 52. Sensor *Enobio*, desarrollado por el laboratorio Starlab de Barcelona[68]. Sensor portatil, inalámbrico y capaz de funcionar sin necesidad de un gel conductivo. Consiste en cuatro electrods y una unidad que puede llevarse con una banda craneal. Transmite los datos recogidos a un receptor con conexión USB.

Imagen 53, BIOMETRIAS DINAMICAS- Proyecto FAST[69]. Imagen del proyecto FAST. El proyecto FAST (del *US Department of Homeland Security*), que significa Future Attribute Screening Technology, persigue detectar la mala intención antes de su ejecución, mediante una combinaciónd e señales corporales y motoras.

Imagen 54. Poder de discriminación de las tecnologías de reconocimiento biométrico y riesgo que implican para la privacidad. En la imagen puede apreciarse como el potencial singularizante de las biometrías dinámicas es significativamente menor pero, algunas de ellas, implican un riesgo mucho mayor para la privacidad de las personas[70].

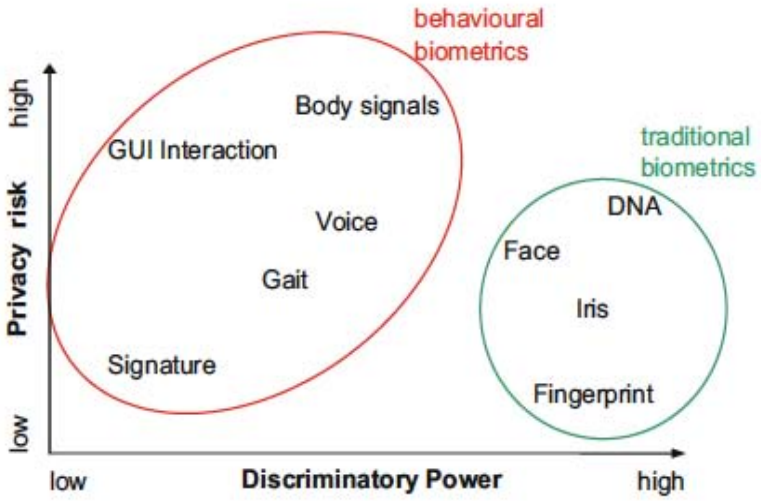
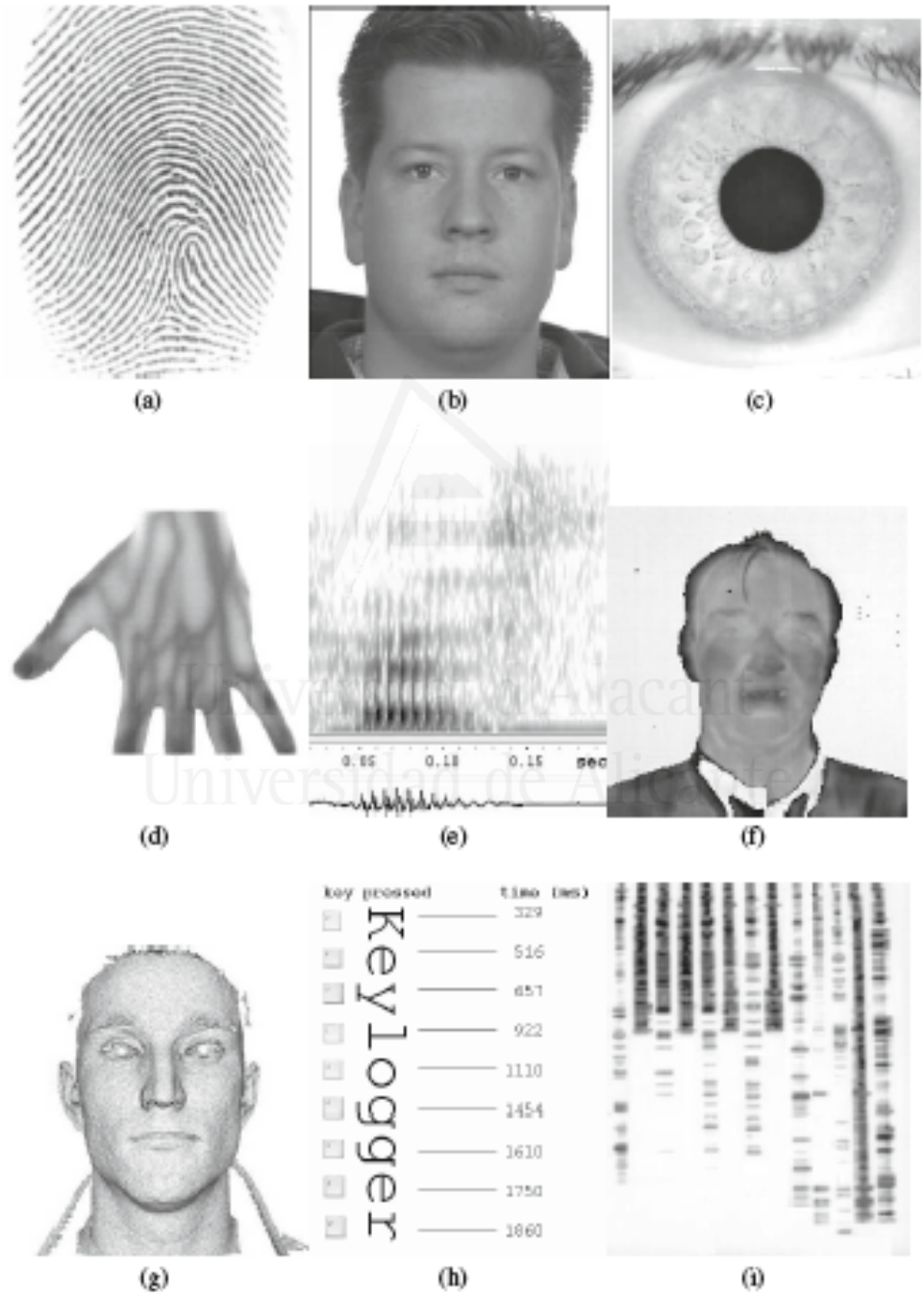
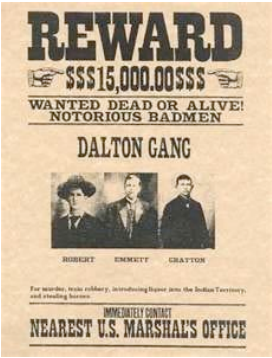


Imagen 55. "Muestra biométrica" (o dato en crudo). Diversidad. Ejemplos de muestras biométricas (analógicas o digitales). (a) Huella dactilar; (b) Rostro; (c) Iris; (d) patrón venoso; (e) huella de voz; (f) geometría facial en 3D; (h) dinámica del tecleado; (i) Imagen del ADN. [71]



Universitat d'Alacant
Universidad de Alicante

Imagen 56. Los carteles de "se busca", ejemplos históricos. Cartel de se busca a Percy Lefroy Mapleton[72]., y otros famosos carteles de "se busca"[73] (Billy el niño, Hermanos Dalton, Jesse James).



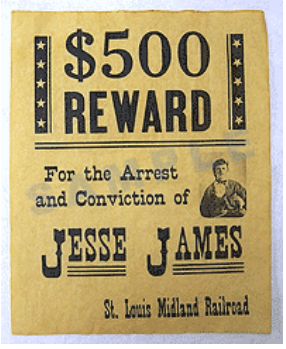
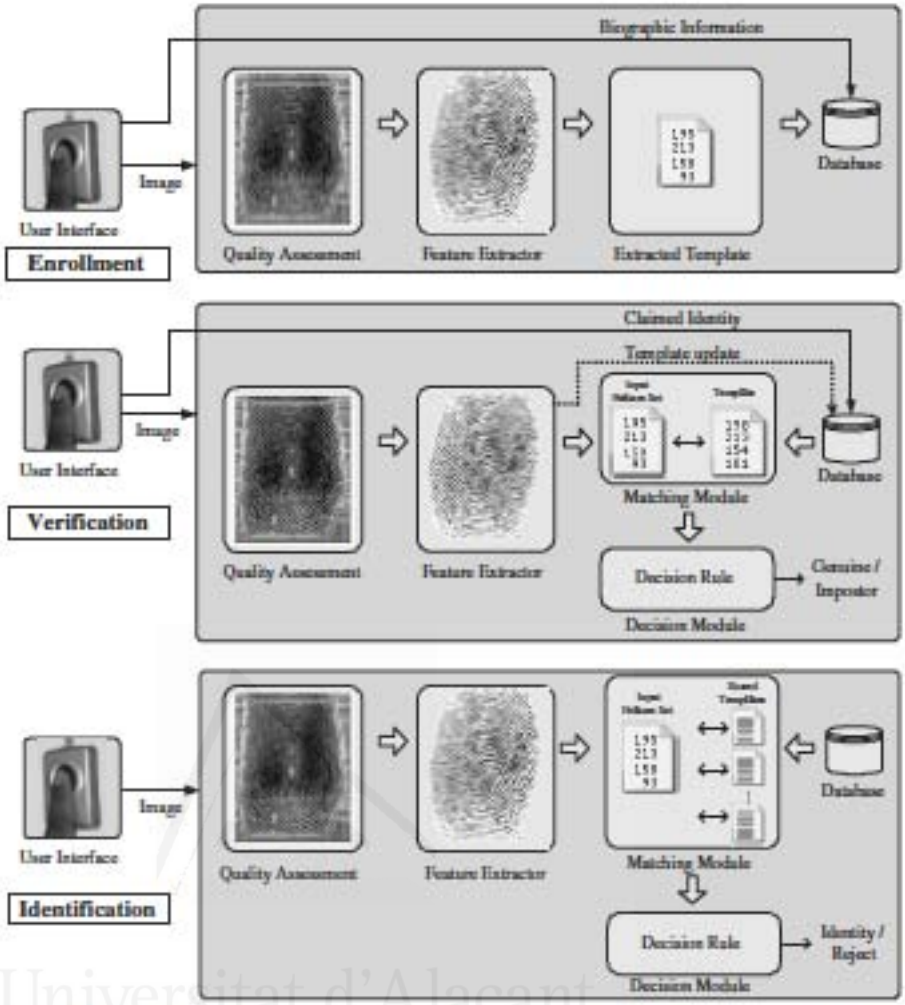


Imagen 57. Oferta de recompensa por El Chapo Guzmán, México 2015. La Policía Federal difundió a través de su cuenta de Twitter, el cartel en que ofrece una recompensa de 60 millones de pesos por datos que lleven a la recaptura de Joaquín Guzmán Loera, alias *El Chapo*. En su cuenta de la red social, @PoliciaFedMX presenta tres de las últimas imágenes de Joaquín Guzmán Loera y la activación de ficha roja (en la Interpol) significa que su búsqueda se ha extendido a 190 países.

Imagen 58. Retrato Robot de Bin Laden elaborado parcialmente a partir de la imagen de Gaspar Llamazares[74]. Bin Laden y Abd al-Rahman envejecidos. A la derecha, la foto de Llamazares de la que el FBI ha copiado el pelo de ambos.

Imagen 59. Esquema del funcionamiento básico de los sistemas. Enrolamiento, verificación, identificación[75].



Universitat d'Alacant
Universidad de Alicante

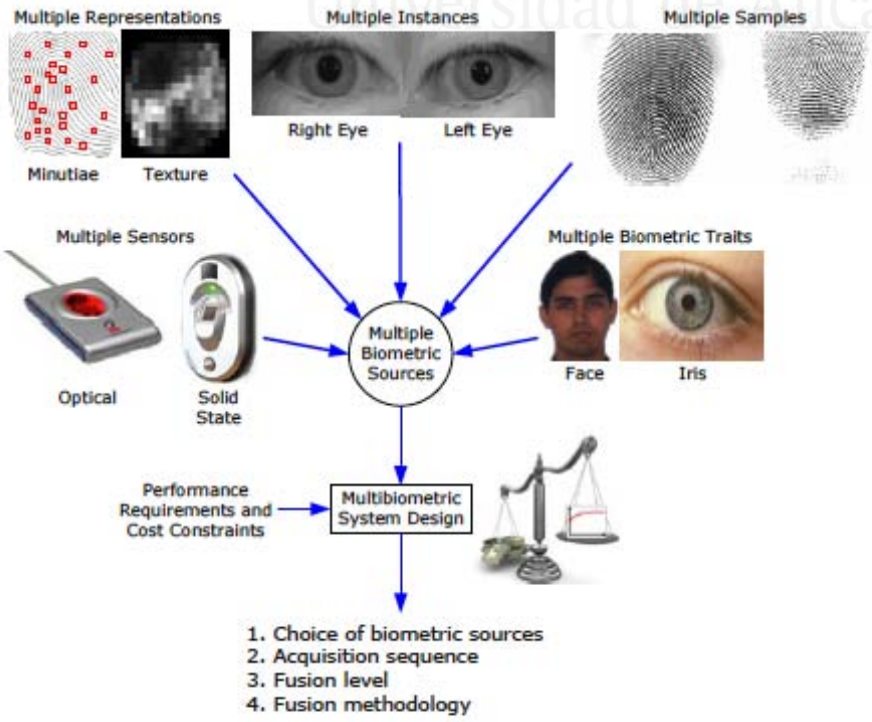


Imagen 60.
Ejemplo de SISTEMAS MULTIBIOMÉTRICOS (que emplean varias fuentes de información biométrica) [76].

Imagen 61. Distintas posibilidades de sistemas multibiométricos. 1) sensores multiples sobre una misma muestra biométrica; 2) varias biometrías; 3) diferentes unidades de análisis, por ejemplo, biometría de dos dedos diferentes; 4) captación multiple sobre una misma muestra biométrica; 5) aplicación de diferentes sistemas para la búsqueda de coincidencias entre los patrones –por ejemplo, localización de minucias y estructura de una huella dactilar. [77]

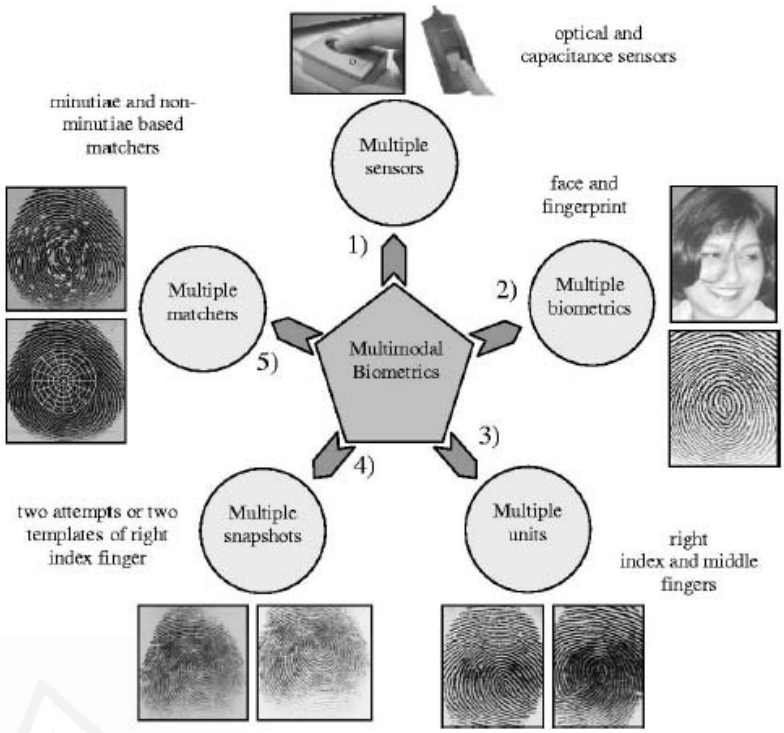
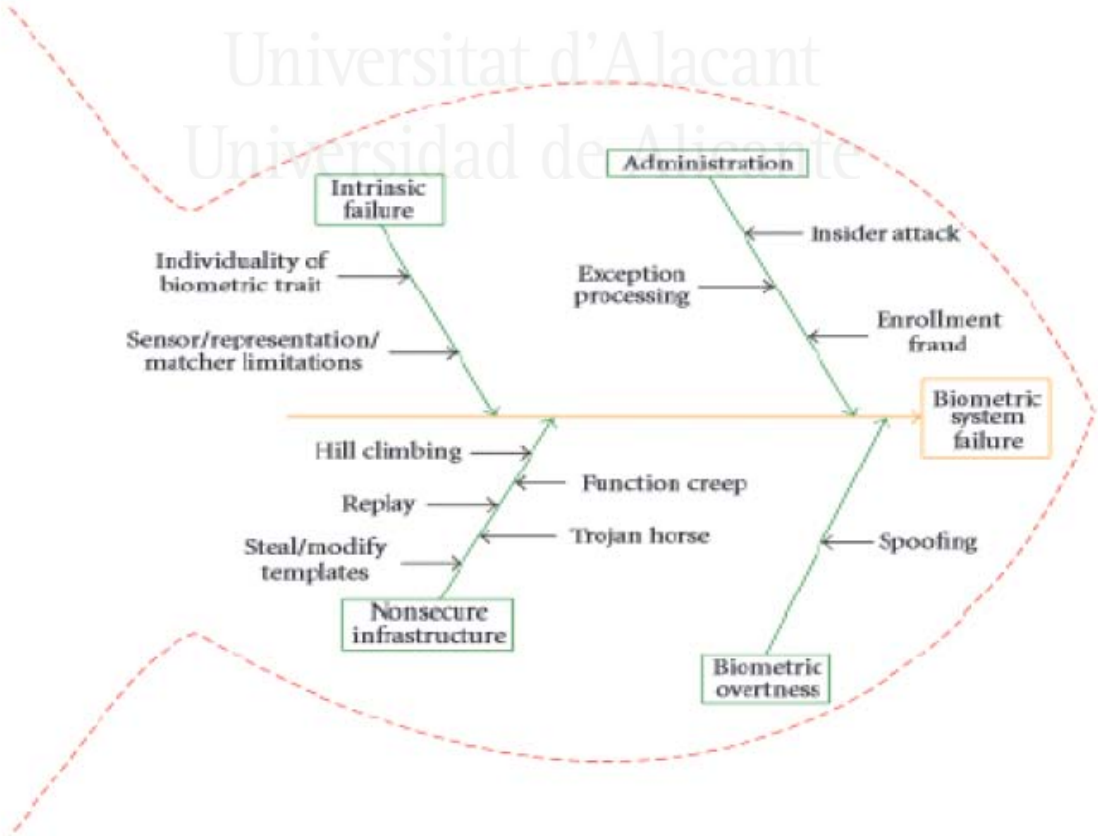


Imagen 62. Categorías de vulnerabilidades de los sistemas biométricos, expresadas en un modelo *fishbone* (espina de pez) [78].



Universitat d'Alacant
Universidad de Alicante

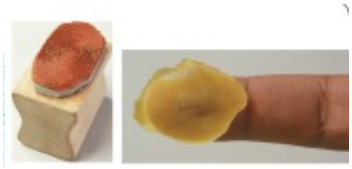


Imagen 63. Simulación de características biométricas [79].

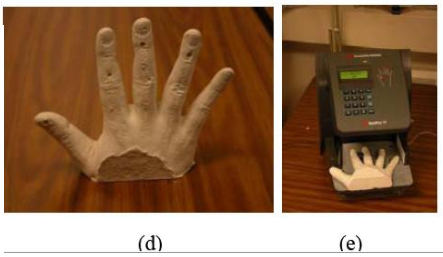


Imagen 64. Problemas de enrolamiento [80]. Cuatro impresiones diferentes de una misma huella dactilar, mostrando una baja calidad de las crestas debido a la falta de hidratación. En este caso resulta difícil enrolar a la persona, por la dificultad realizar una extracción fiable de la información de los dermatoglifos y la localización de las minucias.

Universitat d'Alacant
Universidad de Alicante

Imagen 65. Problemas de captación de las huellas. (a) Imagen de Buena calidad; (b) Presión insuficiente; (c) Presión excesiva; (d) Humedad o sudor; (e) Angulo desviado; (6) colocación inadecuada.[81]

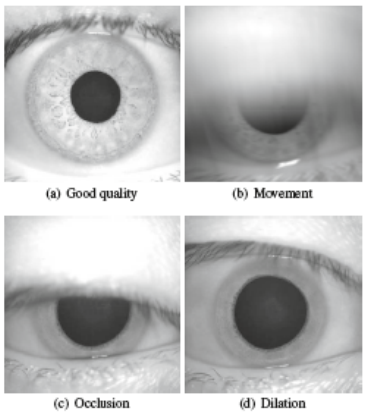


Imagen 66. Problemas de captación del iris. [82] Imagen a, buena calidad; imagen b, exceso de iluminación; imagen c) oclusión; imagen d, compresión del iris por excesiva dilatación de la pupila.

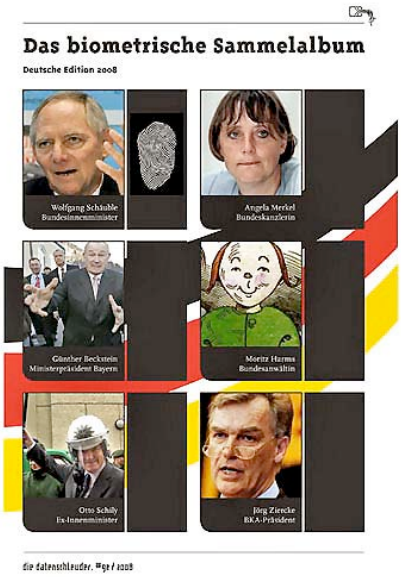


Imagen 67. Exposición involuntaria de la biometría. Das biometrische Sammelabum, Album para colección biomética, del Chaos Computer Club (CCC), 2004. Portada del número 92 de la revista Die Datenschleuder[83].

Imagen 68. Influencia de los factores ambientales y de iluminación en el reconocimiento biométrico (reconocimiento facial) [84].

Universitat d'Alacant
Universidad de Alicante

Imagen 69. Impacto del envejecimiento. Evolución del rostro en 9 fotografías de las misma persona a lo largo de su vida[85].

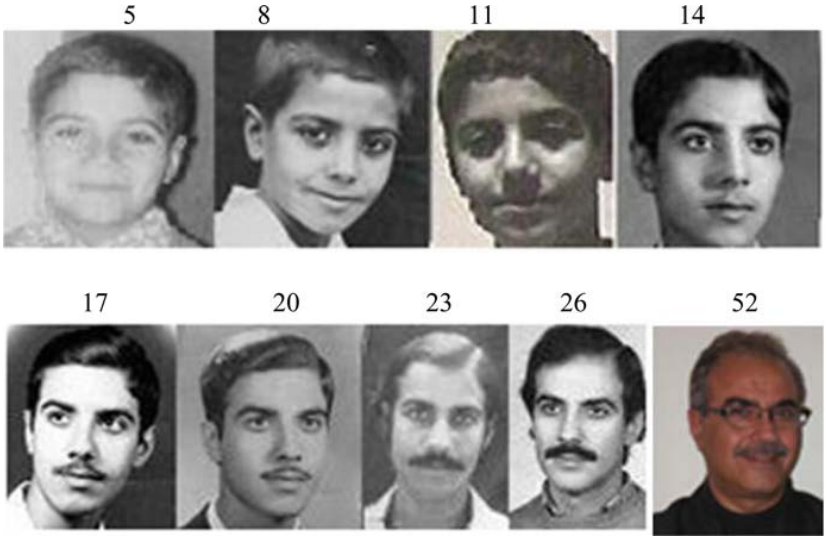


Imagen 70. Sistemas que requieren habilidades específicas de los usuarios. Imagen del HBOX que requiere que las personas accedan por su propio pie, manteniendo una postura erguida.[86]

Imagen 71. Ejemplos de patologías del iris [87] . Albinismo, tumor, aniridia, atrofia esencial del iris y keratopatía.

Imagen 72. Ejemplos de algunas enfermedades de la piel que afectan a las impresiones dactilares. (Verrugas y psoriasis)[88]

Universitat d'Alacant
Universidad de Alicante

Imagen 73. Pasaporte biométrico europeo destacando el logotipo que indica que lleva incrustado un microchip[89].

Imagen 74. Programa de viajeros frecuentes. SmartGate[90].

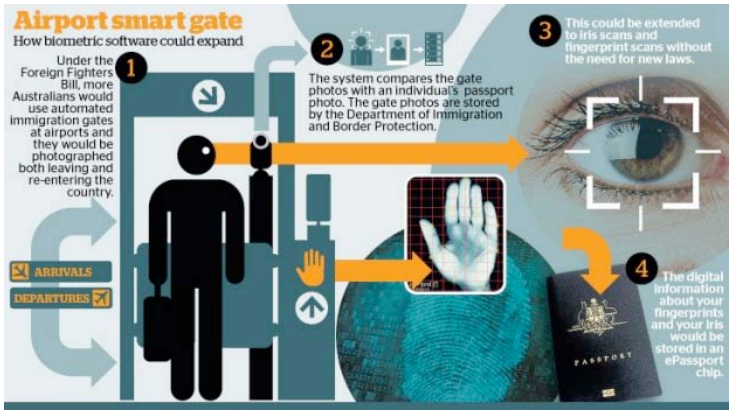


Imagen 75 Sistemas de control biométrico de personas desplazadas por conflictos bélicos (refugiados). Elaboración propia. 1) ACNUR [91]; 2) ACNUR[92], 3) Tarjeta de identificación que obtienen los refugiados en los campos del ACNUR [93] ;4) Bagdad, IRAK. [94] ; 5) ; IOM-OIM [95] .6) Ejército norteamericano. Afganistán[96].

1

2

3

4

5

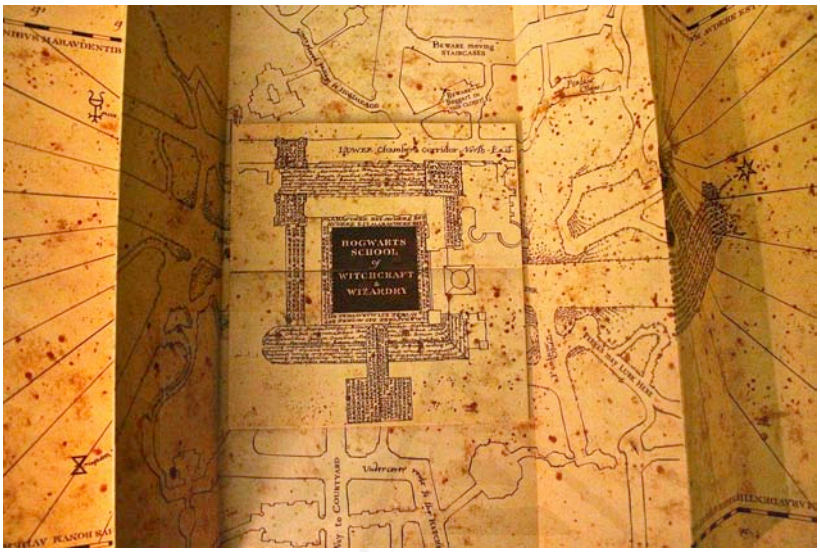
5

Countries with biometric civil and voting registration schemes

Imagen 76- Mapa del mundo en el que aparecen en gris los países que tienen implantado (a fecha de 2014) un sistema biométrico civil o de registro del sufragio [97]

Imagen 77. Padrón electoral de Bolivia.[98]

Imagen 78. Geolocalización. Mapa de Marauder, Harry Potter. Los puntos de tinta moviéndose en él portan una pequeña anotación escrita, en la que se puede leer el nombre de la persona cuya geolocalización trazan en tiempo real.[99]



Universitat d'Alacant
Universidad de Alicante

Imagen 79. Control de abonados en Mouseplanet, activables en la misma columna de control de acceso (biométrico[100] y mediante pulsera electrónica[101]).

Imagen 80. SodaTron (máquina expendedora de bebidas)[102].

Imagen 81. Máquina expendedora con sistema de reconocimiento biométrico de la edad que analiza las arrugas en torno a los ojos, la estructura ósea del rostro y la flacidez)[103].

Imagen 82. Telefono inteligente con captación de huella biométricas[104].

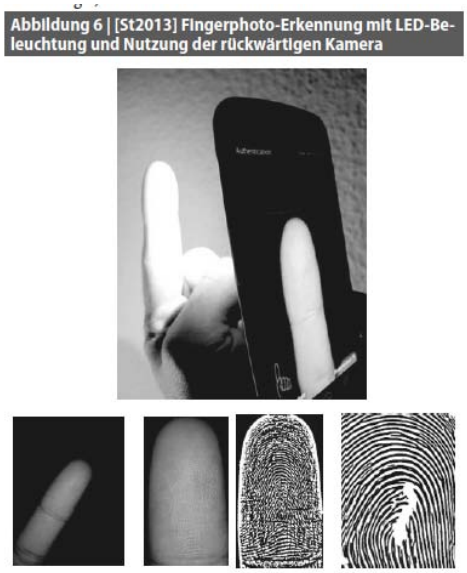


Imagen 83. Sensor de huellas dactilares EIKON[105].

Imagen 84. Sistema de pago PALM SECURE.[106]

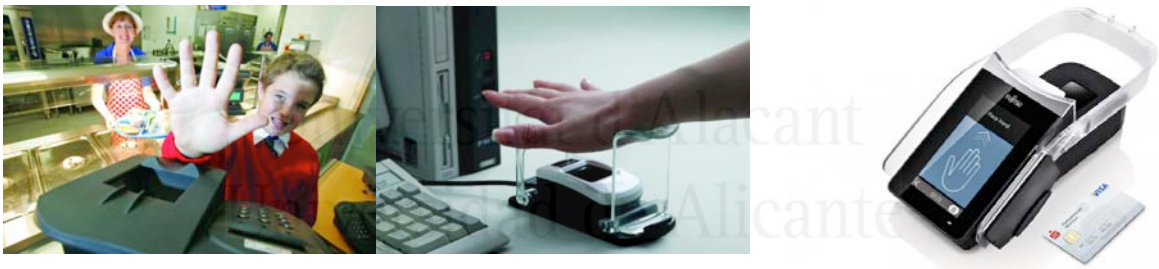


Imagen 85. Estudiantes de la Escuela Elemental de Cranberry, en Westminster, abonan la comida en el comedor escolar mediante escaner palmar. [107]

Imagen 86.
Etiquetado voluntario de fotos en Facebook[108].

Imagen 87. Vigilancia (re-identificación) [109].

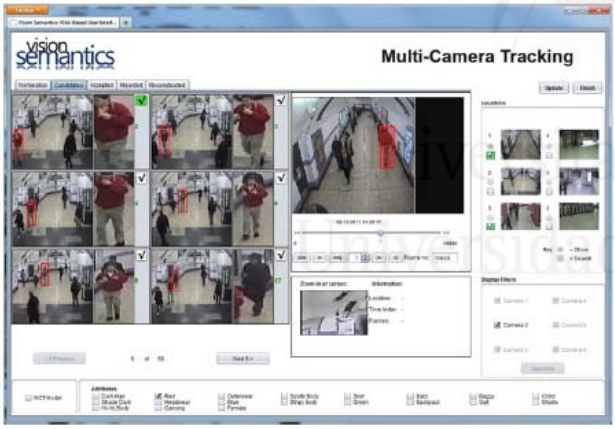


Imagen 88. Procesamiento de imágenes (vigilancia biométrica en espacios abiertos)[110].

Imagen 89.
Multicámera Tracking. Se realiza un seguimieto de los candidatos (itinerario, localización y etiquetado de comportamientos relevantes).[111]

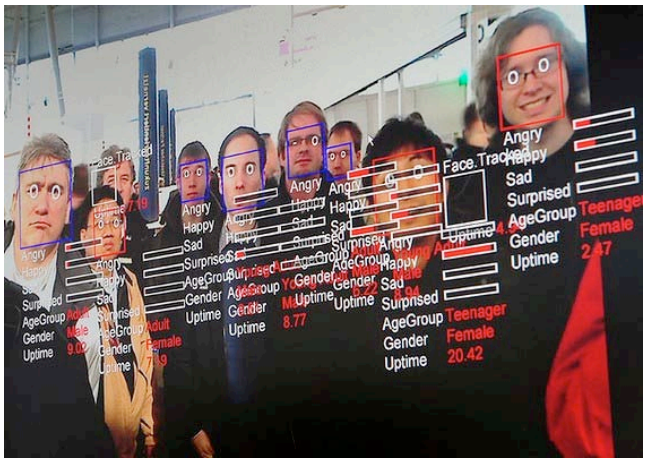


Imagen 90. Reconocimiento facial tipo Terminator[112].

Imagen.91 Captación de atributos de la vestimenta. [113]

Imagen 92. La vigilancia que pasa inadvertida[114]. Viñeta de humor publicada por la AGPD. "*Qué obsesión con eso de que nos están vigilando! Pues yo no veo camaras por ningun lado*".

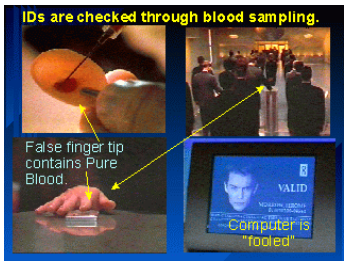
Imagen 93. La biometría en el cine. (a) Minority Report, Steven Spielberg, 2002[115]. Robots centinela escanean el iris del protagonista, que ha recurrido a un transplante de ocular para ocultar su identidad. (b) Fingerprints don't lie, Sam Newfield, 1951[116]. (c) *Blade Runner*, Ridlet Scott, 1982[117]. Máquina voight-Kampff para la distinción entre humanos y replicantes. (d) *GATTACA*, Andrew Scott, 1997. El protagonista inyecta en la falsa yema de su dedo una muestra de sangre cuyo ADN escaneará un sistema de control de acceso, aceptándolo como válido[118]. (e) *Demolition man*, de Marco Brambilla, 1993[119]. Simon Phoenix (interpretado por Wesley Snipes) consigue superar un acceso controlado por escáner de iris, extrayendo un ojo a una persona autorizada. (f) *Person of Interest* (serie de televisión) CBS 2011. Así se describe a *La Máquina:* "*Después de los ataques, el gobierno se otorgó el poder de leer cada correo electrónico, escuchar cada teléfono celular, pero necesitaban algo que pudiera filtrar todo eso... algo que identificara a los terroristas entre la población general antes de que pudieran atacar. (...) La gente quería ser protegida, sólo que no querían saber como, entonces cuando finalmente encontraron un sistema que funcionaba... Lo mantuvieron en secreto*"."

a

b

c

d



e

f

FUENTES DE LAS QUE SE HAN OBTENIDO LAS IMÁGENES

1 Epass Lane. Fuente: http://www.vosizneias.com/wp-content/uploads/2015/06/RTXVA3A-layout-comp.jpg

2 Fuente: The Economist. "Biometrics in Afghanistan. The eyes have it", 7 de julio de 2012

3 http://www.unhcr.org/55926d646.html

4 https://www.google.es/search?q=privium+schiphol&newwindow=1&biw=1385&bih=706&source=lnms&tbm=isch&sa=X&sqi=2&ved=0CAYQ_AUoAWoVChMIv7nk9PyoyAIVy1saCh375gBr#imgrc=vY5MLgdVKFTfoM%3A

5 Fuente: http://www.archello.com/sites/default/files/story/media/_L9H4813.jpg

6 Fuente: http://i1.tribune.com.pk/wp-content/uploads/2014/11/796126-ElectronicvotingPhotoSHAHIDBASHIRexpress-1416806373-286-640x480.JPG

7 Fuente: http://i.dailymail.co.uk/i/pix/2013/05/10/article-2322766-199C7D77000005DC-970_634x405.jpg

8 https://www.google.es/search?q=sassa+biometrics+card&newwindow=1&source=lnms&tbm=isch&sa=X&ved=0CAcQ_AUoAWoVChMI7_bnxYWpyAIVi51yCh0Z_w3o&biw=1385&bih=733#imgrc=aJwXmzKerKrgMM%3A

9 Fuente: http://www.state.gov/cms_images/fy2005pah_perf_sg3_2a.jpg

10 http://www.gannett-cdn.com/-mm-/ac1394dbdcca6a36cbf486633b129cd813095ac3/r=x404&c=534x401/local/-/media/USATODAY/GenericImages/2012/11/25/1-palm-scanners-4_3.jpg

11 Fuente: https://upload.wikimedia.org/wikipedia/commons/b/b0/Biometrics.jpg

12 Fuente: http://njaccesscontrol.com/uploads/5/3/6/1/5361547/855505554

13 Fuente: http://thumbs.dreamstime.com/x/biometric-access-18363044.jpg

14 Fuente: https://www.google.es/search?q=biometrics+and+social+welfare+fraud&newwindow=1&source=lnms&tbm=isch&sa=X&ved=0CAgQ_AUoAmoVChMIqub1pv6oyAIVgj8UCh07CAI8&biw=1385&bih=733#imgrc=I2XCn97y5bXbvM%3A

15 Fuente: https://tctechcrunch2011.files.wordpress.com/2009/07/hitachi_vending_machine_2.jpg?w=298&h=450

16 Fuente: http://static.trustedreviews.com/94/00002df6b/07c2_orh350w620/Barclays.jp

17 . Fuente: http://blog.m2sys.com/wp-content/uploads/2014/11/apple-biometric.jpg

18 Fuente: http://www.handpunch.com/images/Vignette01a.jpg

19 Jain, A. K. / Ross, A./ Prabhakar, S. "An Introduction to Biometric Recognition" IEEE Transactions On Circuits And Systems For Video Technology, VOL. 14, NO. 1, JANUARY 2004, p8..

20 Jain, A. K. / Ross, A./ Prabhakar, S. "An Introduction to Biometric Recognition" IEEE Transactions On Circuits And Systems For Video Technology, VOL. 14, NO. 1, JANUARY 2004, p12..

21 Fuente: http://www.bradshawfoundation.com/chauvet/hand_mammoth.php

22 Saeed, K./ Nagashami, T. Biometrics and Kansei Engineering, Springer, 2012, p4.

23 Fuente: http://www.chinatour.com/blog/wp-content/uploads/2015/01/wall.jpg

24 Fuente: http://www.andreabalt.com/wp-content/uploads/2014/02/leonardo-da-vinci-06.jpg

25 Fuente: http://static-numista.com/catalogue/photos/italie/g2068.jpg

26 Fuente: Sforza, C./ Ferrario, V. F. , "Soft-tissue facial anthropometry in three diomensions: form anatomical landmarks to digital morphology in research, clinics and forensic anthropology", Journal of Anthropological Sciences, vol, 84, 2008, p97.

27 https://xianblog.wordpress.com/2013/03/05/biometrika-volume-100/

28 "Bertillon Method of Measurement, Illinois State Prison, Joliet," Chronicling Illinois, accessed July 22, 2015, http://alplm-cdi.com/chroniclingillinois/items/show/13237.

29 George Bain Collection, Biblioteca del Congreso de los EE. UU.http://www.weirduniverse.net/blog/comments/bertillon_measurements/

30 Bertillon-Card. UCL/ Galton Collection

31 Fuente: https://www.privacyinternational.org/?q=node/166

32 Imágenes tomadas de: Wilder and Bert Wentworth, "Personal Identification: Methods for the Identification of Individuals, Living or Dead." Boston: Gorham, 1918, 31.

33 Imagen tomada de: Wilder, H. H. / Wentworth, B. "Personal Identification: Methods for the Identification of Individuals, Living or Dead." Boston: Gorham, 1918, 31.

34 Cave, J. "Economic Aspects of Biometric Technologies", en pp69 y ss del informe IPTS, 2005.

35 Comparative market sharing bybiometrics technologies in 2009 (International Biometric Group 2009).

36 T. J. Sejnowski. "SexNet: A neural network identifies sex from human faces", en D. S. Touretzky (eds) Advances in Neural Information Processing Systems, Morgan Kaufmann, US 1991. B. A. Golomb, D. Tl. Lawrence.

37 Francesc Seratosa, Reconocimiento de las personas por la huella dactilar, UOC.

38 Imagen tomada de: Allen/Sankar et altere, 2005, p26.

Universitat d'Alacant
Universidad de Alicante

39 Jain, A. K. / Ross, A./ Prabhakar, S. "An Introduction to Biometric Recognition" IEEE Transactions On Circuits And Systems For Video Technology, VOL. 14, NO. 1, JANUARY 2004, pp8-10.

40 R. Allen/ P Sankar/ Sl Prabkar, Fingerprint Identification Technology, Wayman et alt (eds) Biometric systems, Springer, 2005, p21.

41 F. Seratosa, Reconocimiento de las personas por la huella dactilar, UOC.

42 Imagen tomada de: What are Biometric Finger and Facial Scans?, 2008. The real ID. http://therealid.blogspot.de/2008/02/what-are-biometric-finger-and-facial.html

43 R. Moreton/ J Morley, Investigation into the use of photoanthropometry in facial image comparison, Forencis Science International 212 (2011) 232.

44 Publicada por L. Introna/ E . Nissbaum, 2010, p14, y tomada de National Science and Technology Committee, Subcommittee on Biometrics Face Recognition, 2006.

45 Handbook of remote biometrics, 2009, p16.

46 Sánchez-Reillo, R. / Sánchez-Avila, C. / González-Marcoz, A. :"Biometric identification through Hand Geometry Measurements", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, nº 10, october 2000, 1168ss, 1169.

47 Sánchez-Reillo, R. / Sánchez-Avila, C. / González-Marcoz, A. :"Biometric identification through Hand Geometry Measurements", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, nº 10, october 2000, 1168ss, 1169.

48 Zhang et altere, 3D Biometrics, 2013, p12.

49 http://ngm.nationalgeographic.com/static-legacy/ngm/0204/feature0/images/zm_zoomin.0.8.jpg

50 http://fingerchip.pagesperso-orange.fr/biometrics/types/ear/ear_iannarelli.jpg

51 Imagen obtenida de http://img.irtve.es/v/1837888/

52 http://www.diariodeleon.es/noticias/sociedad/huella-oreja-tambien-permite-capturar-delincuentes_252287.html

53 Hurley, 2002

54 Bir Bhanu/ Hui Chen, Human Ear Recognition by Computer, Springer, 2008, p62.

55 C. Rathgeb/ A. Uhl/ P. Wild, Iris Biometrics. From Segmentation to Template Security, Springer, 2013.

56 Anil K. Jain, Introduction to Biometrics, Springer, 2011, pp191, 192, 194.

57 C. Rathgeb/ A. Uhl/ P. Wild, Iris Biometrics. From Segmentation to Template Security, Springer, 2013, p9.

58 E. Kindt. Privacy and Data, pág. 168.

59 IPTS, Informe de 2005, p125.

60 Korotkata, 2003, p4

61 Imagen tomada de L. L. Ramenzonim S. R. P. Line, Automated biometrics-based personal identification of the Hunter-Schreger bands of dental enamel, Proceedings of the Royal Society B., 2006, 273, pp1155-1158.

62 Diwakar, M. / Maharshi, M. "Extraction and Recognition of Tongue-Print Images for Biometrics Authentication System", Journal of Computer Applications, vol. 61, nº 3, 2013, pp 36-42

63 http://fingerchip.pagesperso-orange.fr/biometrics/types/nail.htm

64 A. K. Jain, Introduction, 2011, p205

65 Anil K. Jain, Introduction to Biometrics, Springer, 2011, 196.

66 Li, S. Z. / Jain, A. K/ et altere, Enciclopedia of Biometrics, 2009

67 Chiraz BenAbdelkader/ Ross G. Cutler/ Larry S. Davis, EURASIP Journal on Applied Signal Processing 2004:4, 572–585.

68 Tomado de Second Generation Biometrics, Springer, 2012, p156.

69 Schumacher, en Mordini/ Tsovaras, Second Generation, p220.

70 Tomada de: Mordini/ Tzovaras, Second Generation biometrics.

71 . Dunstone/ N. Yager, Biometric System and Data Analysis. Design, Evaluation and Data Mining, Springer, 2009, p15.

72 http://kttfacialimages.com/2014/08/29/percy-lefroy-mapleton/

73 Imágenes tomadas de Historical Documents c.i. Westernd Wanted and Reward posters. http://www.histdocs.com/home/categorypages/Western%20Wanted%20and%20Reward%20Posters.php

74 Llamazares prepara la demanda contra el FBI por la foto que recrea a Bin Laden ElPAIS, 10 de octubre de 2011. http://politica.elpais.com/politica/2011/10/10/actualidad/1318275187_955572.html

75 Biometrtic functionalities, p11.

76 A. K. Jain, Introduction, p213

77 An Introduction to Biometric Recognition Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004
, p17.

78 Fishbone model for categorizing biometric system vulnerabilities (de A. K. Jain et al, Journal of Advances in Signal Processing 2008.

79 Jain, A. K, Introduction, 2008.

80 An Introduction to Biometric Recognition Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004, p-15.

81 T. Dunstone/ N. Yager, Biometric System and Data Analysis. Design, Evaluation and Data Mining, Springer, 2009, p15.

Universitat d'Alacant
Universidad de Alicante

82 T. Dunstone/ N. Yager, Biometric System and Data Analysis. Design, Evaluation and Data Mining, Springer, 2009, p15

83 Imagen tomada de: Fuente: http://www.interessantes.at/wissenswertes/ueberwachung/schauble-finger.htm (acceso julio de 2015).

84 Tomada de N. Clarke, Transparent User authentication, Springer, 2011, p113.

85 Shaeed, LK. / Nagashima, T. Biometrics and Kansey Engineering, Springer 2012, p15.

86 Tistarelli, M. / Li, S. Z. / Ramalingam (eds), Handbook of remote biometrics, Springer, p 54.

87 Tistarelli, M. / Li, S. Z. / Ramalingam (eds), Handbook of remote biometrics, Springer, p27

88 Selección de imágenes tomadas de: M. Drahansky/ M. Dolezel/ J. Urbanek/ et altere, Influence of Skin Diseases on Fingerpring Recognition, Journal of Biomedicine and Biotechnology, vol. 2012. ID 626148

89 Obtenida de Fuente: http://www.rajaliikenne.fi/eng/tietoa_rajaliikenteesta/automaattinen_rajatarkastus.htm

90 Fuente: http://www.smh.com.au/content/dam/images/3/i/2/y/y/image.related.articleLeadwide.620x349.116lur.png/1413434842623.jpg

91 Fuente: http://innovation.unhcr.org/wp-content/uploads/rsz_bims.jpg

92 Fuente: http://www.unhcr.org/thumb1/50dc58da6.jpg

93 http://www.unhcr.org/55926d646.html

94 Fuente: https://upload.wikimedia.org/wikipedia/commons/f/f6/USMC_Sergeant_identifies_Baghdaddi_city_council_member_with_iris_scanner.jpg

95 Fuente: https://www.iom.int/sites/default/files/press_release/pictures/cd20150505-1_0.jpg

96 Fuente: http://s.hswstatic.com/gif/fingerprint-6.jpg

97 Imagen tomada de K. Beckenridge, Biometric State,2014.

98 CNE, Padrón electoral Biométrico, 2009. Documento de información pública nº 1. Corte Nacional Electoral de Bolivia

99 J.K. Rowling, The Marauder's Map, en Harry Potter and the Prisoner of Azkaban, 1999, pp. 192e3

100 Fuente: http://www.mouseplanet.info/gallery/d/135241-1/EP_RFID_test_column-goldhaber.jpg

101 : Fuente: https://s-media-cache-ak0.pinimg.com/236x/dd/e9/61/dde961e54f1e95da790f4a22a4c2af09.jpg

102 SodaTron Fuente: http://www.jacobsschool.ucsd.edu/pulse/fall2006/images/SodaTron.jpg

103 ItuT 2009, p10.

104 Busch, C. "Biometrische Zugangskontrolle", DuD 7/2014, p478.

105 Fuente: Clarke, N. Transparent User authentication, Springer 2011, p40.

106 Fujitsu: The future of biometrics – Dr Joseph Reger, en Future Banking. http://www.banking-gateway.com/projects/fujitsu-the-future-of-biometrics-dr-joseph-reger/fujitsu-the-future-of-biometrics-dr-joseph-reger3.html. Acceso, agosto de 2015.

107 Students at Cranberry Station Elementary School in Westminster, Md., use a palm-scanning device to pay for their school lunches.(Photo: Jack Gruber, USA TODAY)

108 http://www.businessreviewusa.com/public/uploads/large/large_article_im4241_facebook-tagging.jpg

109 Re-identification. Fuente: http://www.eecs.qmul.ac.uk/assets/img/uploads/page-image/behaviour.png

110 Surveillance. Fuente: https://realizethelies.files.wordpress.com/2013/08/bossurveillance.jpg

111 Gong, Person Re-Identificatin, p425.

112 Fuente: http://www.mobileinc.co.uk/2010/03/cebit-2010-terminator-style-facial-recognition-detects-gender-age-group-mood/

113 GONG, Person Re-Identification, 2015, p205.

114 Guia de videovigilancia de la AGPD, 2009.

115 http://lostintheframe.blogspot.com.es/2007_11_01_archive.html

116 http://lostintheframe.blogspot.com.es/2007_11_01_archive.html

117 http://projectcede.org/category/digital-empathy/

118 http://www.hollywoodjesus.com/gattaca.htm

119 http://i.dailymail.co.uk/i/pix/2011/05/11/article-1385959-0C01309F00000578-870_468x203.jpg

Universitat d'Alacant
Universidad de Alicante

Bibliografía y Referencias documentales

ABAD AMORÓS, R.: "El carácter sensible de los datos biométricos", en *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 4, 16 de septiembre de 2003.

ABS, M. "Biometrik", en *Historisches Wörterbuch der Philosophie*, vol. I, RITTER, J./ GRÜNDER, K. (eds.) Basilea, 1971, p945-946.

ACADEMIA BRITÁNICA DE LAS CIENCIAS FORENSES: *Opinion of the British Academy of Forensic Sciences regarding the Disadvantages of creating a DNA database of the entire population* (2007), enviada a la Consulta promovida por el Nuffield Council on Bioethics.

ACTIBIO (sin indicación de fecha), Unobtrusive authentication using activity related and soft biometrics. www.actibio.eu.

ADLER, A. 'Sample images can be independently restored from face recognition templates', en *Electrical and Computer Engineering 2003*, IEEE CCECE 2003. Canadian Conference, pp. 1163–1166, disponible en http://www.sce.carleton.ca/faculty/adler/publications/2003/adler-2003- ccece-restore-face-recognition-templates.pdf

ADLER, A. "Can images be regenerated from biometric templates?", en *Proceedings Biometrics Consortium Conference*, September 2003.

ADLER, A./ SCHUCKERS, S. "Biometric Vulnerabilities", en S. Z. LI/ A. K. JAIN (eds.), *Encyclopaedia of Biometrics*, Springer, consultada la edición de 2009, p63.

AGPD, Expediente E 00057/2005 relativo a los S*ervicios periféricos de la Junta de Andalucía en Málaga*.

AGPD, Guía de Videovigilancia, https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

AGPD, Resolución del expediente E/ 02635/ 2009, contra la empresa *Servicios Logísticos Integrados, S. A*., por la instalación de un sistema de fichaje mediante huella digital.

AGPD, *Resolución del Procedimiento nº TF/ 01755/ 2009*, por ejercer un trabajador el derecho de oposición a sus datos biométricos en el control de jornada laboral del personal funcionario por parte del *Ayuntamiento de Andújar*

AGPD, Resolución del procedimiento PS/ 00272/ 2005, por la instalación de un sistema de control horario mediante huella digital en la empresa *Rótulos Ayllón*.

AGPD. AAPP/00028/2005 y AAPP/ 0029/ 2005 por implantación de sistemas de control de presencia de los trabajadores en el *Ayuntamiento del Puerto de la Cruz* y en la Universidad Popular *Francisco Afonso Carrillo.*

AGPD. AP/ 00075/2008 contra la *Consejería de Trabajo y Empleo de la Junta de Comunidades de Castilla La Mancha.*

AGPD. Informe 0392/ 2011.

AGPD. Informe 368/ 2006.

AGPD. Procedimiento nº AAPP/00020/ 2007. Denuncia de un miembro del Comité de Empresa contra la *Autoridad Portuaria de Baleares* por la recogida de datos de carácter biométrico de los trabajadores.

AGPD. *Resolución del Expediente E/ 01126/ 2010*, sobre instalación de un sistema de fichaje biométrico para el personal de rampa de la empresa *Spanair.*

AGRE, Ph./ ROTENBERG, M. (eds.), *Technology and privacy: the new landscape*, Cambridge, Massachusetts, MIT press, 1998.

Universitat d'Alacant
Universidad de Alicante

AILISTO, H./VILDJIOUNAITE, E./LINDHOLM, M./ MÄKELÄ, S./ PELTOLA, J. 'Soft biometrics-combining body weight and fat measurements with fingerprint biometrics', *Pattern Recognition Letters* 2006, pp. 325–334.

AINSWORTH, R. 'Biometrics: Solving the Regressivity of VATs and RSTs with 'Smart Card' Technology', Boston Univ. School of Law Working Paper No.06–20, 2006, 82 p. Disponible en http://www.bu.edu/law/faculty/scholarship/workingpapers/documents/AinsworthR080706.pdf

AKRIVOPOULOU, C./ PSYGKAS, A. (eds.), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, Information Science Reference, New York, 2011, pp. xv-xvi.

ALARCÓN CARACUEL, M. R.: "Duración del contrato, jornada y salario", en la obra colectiva *La Reforma Laboral de 1994*, Marcial Pons, Madrid 1995.

ALBRECHT, A. 'Biometric Authentication from a Legal Point of View – A European and German Perspective', en COATS, W. BAGDASARIAN, A./ HELOU, T/ LAM, T. (eds.), *The Practitioner ' s Guide to Biometrics*, Chicago, ABA, 2007, pp. 87–138.

ALBRECHT, A. *BioVision. Privacy Best Practices in Deployment of Biometric Systems*, BioVision, 2003.

ALBRECHT, A.: "Biometrie am Arbeitsplatz - Konkrete Ausgestaltung der Mitbestimmung. Orientierungshilfe des TeleTrusT e.V. für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme", en *Datenschutz und Datensicherheit* (DuD), 31 (2007) 3, S. 171-175.

ALBRECHT, A.: *Biometrische Verfahren im Spannungsfeld zwischen Authentizität im elektronischen Rechtsverkehr und Persönlichkeitensschutz*, Serie Frankfurter Studien zum Datenschutz, Baden Baden, 2003.

ALBRECHT, A./ BROMBA, M./ HORNUNG, G./ LABMANN, G./QUIRING-KOCK, G. *Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme*. Arbeitsgruppe 6 "Biometrische Identifikationsverfahren", AK "Rechtliche Aspekte der Biometrie", Teletrust, 21 De septiembre 2005, 17 p. Disponible en http://www.teletrust.de/uploads/media/TTT-AG_Biometrie- Orientierungshilfe-Betriebsvereinbarung.pdf

ALBRECHT, A/ WALSH, M. (eds.), *BioVision. Report on legal and privacy issues*, BioVision, 2003.

ALBRIZIO, "Biometry and Anthropometry", *Journal of Anthropological Sciences*, vol. 85, 2007, pp101-123.

ALONSO-ZALDIVAR, R.: "Airports Test Express Security Lane", *Los Angeles Times*, 8 de julio de 2004.

ALTERMAN, A. 'A piece of yourself': Ethical issues in biometric identification', Ethics and Information Technology, 2003, pp. 139–150, disponible en http://www.hideproject.org/downloads/references/Alterman-A_Piece_of_yourself.pdf

ALTMANN, F. "Malformations of the auricle and external auditory meatus", *Arch Otolaryngology* 1951, 54, pp115-139.

ALTO COMISIONADO DE LA ONU PARA LOS DERECHOS HUMANOS, Informe *Birth registration and the right of everyone to recognition everywhere as a person before the law*, presentado en a la Asamblea General de las Naciones Unidas, A/HRC/27/22, 17 de junio de 2014.

AMBERG, FISCHER, RÖßLER: *Biometrische Verfahren*, 2003, p3ss.

AMGABEN, G.: "Bio-political tattooing", Le Monde, 11 de enero de 2004.

ANDRADE, N. N. G. d.: 'Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization', en GUTWIRTH, S./ POULLET, Y./ DE HERT, P./ LEENES, R. GUTWIRTH, S./ POULLET, Y./ DE HERT, P./ LEENES, R. Computers, *Privacy and Data Protection: an Element of Choice*, Springer, 2011.

ANDRADE, N. N. G. d.: "El olvido: El derecho a ser diferente... de uno mismo. Una reconsideración del derecho a ser olvidado", en V*II Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet, IDP. Revista de Internet, Derecho y Política,* 2012, N.º 13, pág. 67-83, UOC.

ANDRONIKOU, V./ YANNOPOULOS, A./ VARVARIGOU, TH. 'Biometric Profiling: Opportunities and Risks', en HILDEBRANDT, M/ GUTWIRTH, S. (eds.), *Profiling the European Citizen. Cross- Disciplinary Perspectives*, Springer, 2008, pp. 131–139.

ANSI/NIST-ITL, "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tatoo (SMY) Information", *FBI: Wavelet Scalar Quantization* (WSQ), 1-2000.

ANTÓN BARBERÁ, F./ DE LUIS Y TARAGANO, J. V. *Policía científica*, 5ª edición, Tirant lo Blanch, Valencia, 2004.

APARICIO SALOM, J. *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Pamplona, 2000.

APDMADRID, *Guía de protección de datos personales para Universidades,* 2008.

ARBEITSKREIS „TECHNISCHE UND ORGANISATORISCHE DATENSCHUTZFRAGEN"DER KONFERENZ DER DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND LÄNDER, *Orientierungshilfe „Biometrische Authentisierung – Möglichkeiten und Grenzen"*, noviembre de 2009.

ARMSTRONG, B. C./ M. V. RUIZ-BLONDET/ N. KHALIFIAN/ K. K. KURTZ/ Z. JIN, S. LASZLO, "Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics", Neurocomputing, 166 (2015), pp59-67.

ARONOV, R. F.: "Privacy in a Public Setting: The Constitutionality of Street Surveillance", QLR, vol 22, 2004, pp769 y ss.

ARROYO JIMÉNEZ, L.: "Ponderación, proporcionalidad y Derecho administrativo", *Revista para al análisis del Derecho - Indret*, nº 2, 2009.

ASHBOURN, J. *Biometrics in the New World. The Cloud, Mobile Technology and Pervasive Identity*, Springer, 2014.

ASHBOURN, J. *The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies. Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission, 2005, disponible en http://www.statewatch. org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf

ATAL, B. "Automatic recognition of speakers from their voices", *Proc. IEEE*, 1976, 64(4), 460–474.

AUGER, D. *Biométrie : l'équilibre entre «liberté individuelle » et promesse sécuritaire serait-il impossible ?*, Univ. Paris – La Sorbona, 2005.

AUS, J. P. "Eurodac: A Solution Looking for a Problem?", European Integration online Papers, EMOP, vol 10, 2006.

BACKHOUSE, J. 'Interoperability of Identity and Identity Management Systems', en *DuD* 2006, pp 568–570.

BACKHOUSE, J./HALPERIN, R. *A Survey on Citizen ' s trust in ID systems and authorities*, Frankfurt, FIDIS, 2007, 27.

BARBERO GONZÁLEZ, I.: *Globalización, Estado y Ciudadanía. Un análisis socio-jurídico del movimiento sin papeles*, Tirant lo Blanch, 2012.

BARBU, T. "Comparing various voice recognition techniques", en *IEEE proceedings of the5th conference on speech technology and human-computer dialogue,* 2009 pp 1–6. doi: 10.1109 SPED.2009.5156172.

BARKLAY, C./ J. CUTTING/ L. KUZLOZSKI, "Temporal and Spatial Factors in Gait Perception that influence Gender Recogniton", *Perception and Psychophysics*, vol. 23, n2, pp145-152 (1978).

BARTMANN, D. "On the design of an authentication system based on keystroke dynamics using a predefined input text", *International Journal of Information Security and Privacy*, 2006.

BARTMANN, D. "PSYLOCK - Identifikation eines Tastaturbenutzers durch Analyse des Tippverhaltens", http://wwwbrauer.in.tum.de/

BAUDOIN, J. Y./ TIBERGHIEN, G. "Gender is a dimension of face recognition,"Journal of Experimental Psychology, vol. 28 (2), 2002, pp362-365.

BAUER, M./ MEINTS, M. (eds.), *Structured Overview on Prototypes and Concepts of Identity Management Systems*, Frankfurt, FIDIS, 2004.

BÄUMLER, H./ GUNDERMANN, L./ PROBST, T. *Stand der Nationalen und Internationalden Diskussion zum Thema Datenschutz bei biometrischen Systemen*, Unaebhaengiges Landeszenntrum fuer Datenschutz Schleswig – Holstein, 2001.

BAYGIN, M. "Real time voice recognition based smart home application", *IEEE 20th signal processing and communications applications conference (*SIU), 2012, pp 1–4. doi: 10.1109/SIU.2012.6204694

BAZÁN, V. "El Habeas Data y el Derecho de autodeterminación informativa en perspectiva de Derecho Comparado", *Revista Chilena de Estudios Constitucionales*, vol.3, n´º 2 de 2005, pp85 y ss, 116-117.

BEHRENS, M./ ROTH, R. (eds.), *Biometrische Identifikation*, 2001.

BEILLEL, A. *E-Privacy. Le marché des donées personnelles: protection de la vie privée á l'âge d'internet*, Ed. Dunod, 2001.

BELGACEM, N./ R. FOURINIER/ A. NATT-ALI/ F. BEREKSI-REGUIG, "A novel biometric authentication approach using ECG and EMG signals", *Journal of Medical Engineering & Technology*, mayo de 2015, vol. 39, Issue 4, 226-238.

BELTRÁN DE FELIPE, "Qué es el derecho a la identidad", en VV. AA. *Robo de identidad*, 2010.

BENABDELKADER, C./ CUTLER, R./ NANDA, H./ DAVIS, L. "EigenGait: Motion-Based Recognition of People Using Image Self-Similarity", en *Audio- and Video-Based Biometric Person Authentication. Lecture Notes in Computer Science* Volume 2091, 2001, pp 284-294.

BENABDELKADER, C./ CUTLER, R./ NANDA, H./ DAVIS, L. "Gait Recognition Using Image Self-Similarity". *EURASIP Journal on Applied Signal Processing* 2004:4, 572–585.

BENDER, S./ POSTLEY, H. *Key sequence rhythm recognition system and method*. US Patent No. 7206938, 2007.

BERGGEN,L. "Iridology: a critical review", *Acta Ophtalm* 63 (1), 1985, 1-8.

BERNAL PULIDO, C.: El principio de proporcionalidad y los derechos fundamentales, CEPC 2007, pp199-200.

BERNECKER, O. 'Biometrics security: An end user perspective', Information Security Technical Report 2006, pp. 111–118, disponible en http://www.sciencedirect.com/science/ article/pii/S1363412706000379

BHAGWAT, A.: *The Myth of Rights. The Purposes and Limits of Constitutional Rights,* Oxford University Press, 2010.

BHANU, B. *Human ear Recognition by Computer*, Springer, 2008, 20-22.

BHANU, B./ CHEN, H. *Human ear recognition by computer*, Springer, 2008.

BIASOTTI, A.: *Le tecnologie biometriche. Sicurezza, contrattualistica e privacy*, EPC Libri, Roma, 2002.

BIEDERMAN, A./ BOZZA, S./ TARONI, F. "Decision theoretic properties of forensic identification: Underlying logic andargumentative implications", *Forensic Science International* 177 (2008) 120–132.

BIEL, L/ ET AL. 2001. "ECG analysis: A new approach in human identification", *IEEE Transactions on Instrumentation and Measurement* 50: 808–812.

BIERMANN, H/ BROMBA, M/ BUSCH, C/ HORNUNG, G/ MEINTS, M/ QUIRING-KOCK, G. (eds.) *White Paper zum Datenschutz in der Biometrie,* 2008. disponible en http://www.teletrust.de/ uploads/media/White_Paper_Datenschutz-in-der-Biometrie-080321.pdf

BIOMETRIC TASK FORCE, *Biometric History Timeline*, Department of Defense, Estados Unidos, en: http://www.biometrics.dod.mil/References/Biometrics_Timeline.aspx

BIZER, J. "Sieben Goldene Regeln des Datenschutzes", DuD, 2007.

BIZER, J.: "Ziele und Elemente der Modernisierung des Datenschutzrechts", *DUD* 2001, pp. 274-277.

BLANKENBURG, E. "Identität als Recht", en *Soziale Probleme, Zeitschrift für soziale Probleme und soziale Kontrolle*, 7/ 1996, núm. 1, pp18-26.

BLAS, D. 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom', *ERA Forum* 2010, pp. 233–250, consultado en http://www.springerlink.com/content/u6566750w5954262/

BLEUMER, G. 'Biometric Authentication and Multilateral Security', en MÜLLER, G./ RANNENBERG, K. (eds.), Multilateral Security in Communications. Technology, Infrastructure, Economy, München, Addison-Wesley, 1999, pp157–171.

BLOUSTEIN, E. 'Privacy as an Aspect of Human Dignity: An answer to Dean Prosser', 39 *New York University Law Review* 1964, p. 962 et seq.

BOBROWSKI,, M.: "Biometrie und Verbraucherschutz", *DuD* 1999, p159 et seq.

BOCK, K. 'EuroPriSe Trust Certification', en *DuD* 2008, pp. 1–5.

BOEHRINGER, S./ ET ALTERE, "Genetic determination of human facial morphology", European Journal of Human Genetics, 2011, 19, 1192-1197.

BOLLE, R. M./ CONNEL, J. H/ ET ALTERE, *Guide To Biometrics*, Springer, New York, 2004.

BOLLE, R. M./ CONNEL, JONATHAN H./ RATHA, N. "Biometric perils and patches", *Pattern Recognition* 35 (2002), 2727 – 2738.

BORGEN, H. "Simulationg the influence of Aging and Ocular Disease on Biometric Recognition Performance", *IEEE Advances in Biometrics, Lecture Notes in Computer Science*, vol 5558, 2009, pp857-867.

BOURLAI, T./ ROSS, A./ JAIN, A. 'On Matching Digital Face Images Against Scanned Passport Photos', en *Proc. of First IEEE Intern. Conf. on Biometrics, Identity and Security*, 2009, disponible en http://www.cse.msu.edu/rgroups/biometrics/Publications/Face/ BourlaiRossJain_BIDS2009.pdf

BOUSTA, R. "Controle Constitutionnel de proportionalité: La "specificité "française à l ' épreuve des évolutions

récentes", *VIII Congreso Mundial de la A.I.D.C., La Constitución y los Principios*, Mexico,6–10.12.2010. Disponible en http://www.juridicas.unam.mx/wccl/ponencias/9/159.pdf

BOWYER, K. 'Face Recognition Technology: Security versus Privacy', en *IEEE Technology and Society Magazine*, 2004, pp. 9–20.

BRADSHAW, S./ MILLARD, CH./ WALDEN, I. 'Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services', *Int Journal of Law and Information Technology* 2011, pp. 187–223.

BREEBAART, J./ BUSH, C./ GRAVE, J./ KINDT, E. 'A reference architecture for biometric template protection based on pseudo identities',en A. BRÖMME (ed.), *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, Bonn, Gesellschaft für Informatik, 2008, pp. 25–37.

BREEBAART, J./ YANG, B/ BUHAN-DULMAN, I./ BUSCH, CH. 'Biometric Template Protection. The need for open standards'en *DuD* 2009, pp. 299–304.

BREITENSTEIN, M. *Überblick über Biometrische Verfahren*, en NOLDE, V./LEGER, L. (ed.), *Biometrische Verfahren*, 2002, pp35ss.

BRENNA, R. G. "Los ciudadanos de Cristal. Vigilancia, Privacidad y Derechos Humanos", *Revista de Derecho Informático*, nº 127, 2009.

BRIDGES, B. C. *Practical fingerprinting*, Funk & Wagnalls, original de 1942, edición revisada publicada en 1963.

BRILLINGER, D. R. The National variability of vital rates and associated statistics, Biometrics, vol. 42/4, 1986, pp693-734.

BRINGER, J./ CHABANNE, H./ KEVENAAR, T./ KINDARJI, B. 'Extending match-on-card to local biometric identification', en FIERREZ, J/ ORTEGA-GARCIA, J/ ESPOSITO, A/ DRYGAJLO, A/ FAUNDEZ-ZANUY M. (eds.), B*ioID MultiComm ' 09 Proceedings of the 2009 joint COST 2101 and 2102 international conference on Biometric ID management and multimodal communication*, 2009, pp. 178–186.

BROMBA, M. "Die 14 Märchen der Biometrie", CeBIT-Special, WIK - Zeitschrift für Sicherheit der Wirtschaft,07/1, 2007,pp36ss.

BROMBA, M. *Bioidentifikation. Fragen und Antworten*, 2011. Disponible en: www.bromba.com/faq/biofaqd.htm

BROMBA, M. *On the reconstruction of biometric raw data from template data*, 2003 (first release), 2006, disponible en http://www.bromba.com/knowhow/temppriv.htm

BROUWER, E. R: *Digital Borders and Real Rights*: *Effective Remedies for Third-Country Nationals in the Schengen Information System,* Brill, 2008.

BROUWER, E. R.: "Eurodac: Its Limitations and Templations", en *European Journal of Migration and Law*, vol, 4. pp. 231-247.

BROWNSTEIN, R. "E-Commerce Becomes Mainstream amidst Security Concerns", *Electronic Design*, 52 (13), 2004, pp75ss.

BRUNELLI, R./ POGGIO, T. "Hyper BF networks for gender classification", *Proceedings of DARPA Image Understanding Workshop*, San Diego, 1992, 311–314.

BUCHACA FAXAS, E./ VÁZQUEZ VIGOA, A./ TORUNCHA CHUCKRAM, A./ RODRÍGUEZ VALDÉS, R./ SEIJAS FARIÑAS,H.: "Surco en lóbulo de la oreja y cardiopatía isquémica", *Revista Cubana de Medicina, 1995* (5), 31 (1).

BUITELAAR, H. (ed.), *Study on ID number policies*, Frankfurt, FIDIS, 2007.

BUITELAAR, J./ MEINTS, M./ KINDT, E. (eds.), *Requirements for privacy - friendly identity management in e - government*, Frankfurt, Fidis, 2009.

BÜLLINGEN, F./ HILLEBRAND, A.: "Biometrie als Teil der Sicherheitsinfrastruktur", en *Datenschutz und Datensicherheit* (DuD), 24 (2000) 6, p. 339-343.

BULMER, M. *Francis Galton: Pioneer of Heredity and Biometry*, John Hopkins Univ. Press, 2003.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK- BSI, *BioFace. Vergleichende Untersuchung von Gescigtserkennungssystemen*, 2003.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK- BSI, *Grundsätzliche Funktionsweise biometrischer Verfahren*. 2010.

BUNDESKRIMINALAMT, *Forschungsprojekt. Gesichtserkennung als Fahndungshilfsmittel Foto-Fahndung. Abschlussbericht*, Wiesbaden, Febrero 2007.

BUNDESKRIMINALAMT, *Öffentliche Anhörung im Innenauscchuss des Deutschen Budestages. Aufnahme biometrischer Merkmale in den Reisepass. Änderung des PassG,* PR/KT43-2007/1631/1, Berlin, 2007.

BURGE, M./ BURGER, W. "Ear Biometrics", en A. Jail/ R. Bolle/ S. Pankanti, *Biometrics – Personal Identification in a Networked Society*, Kluwer, 1999, cap. XIII, pp276 y ss.

BURTON, A.M./ BRUCE, V./ DENCH, N. "What is the difference between men and women? Evidence from facial measurement", *Perception* 22, 1993, 153–176.

BUS, J./ CROMPTON, M./ HILDEBRANDT, M./ METAKIDES, G. *Digital Enlightenment*. Yearbook 2012, Amsterdam, IOS Press, 2012.

BUSH, C. "Biometrische Zugangskontrolle mit Smartphones", DuD – Datenschutz und Datensicherheit, 7/2014, pp475-477.

BUSH, C. *Forschung für die Grenzkontrollen der Zukunft,* 2009, Darmstadt, Hochschule Darmstadt, 2009, 12 p. Disponible en https://www.fbi.h-da.de/fileadmin/gruppen/FG-IT-Sicherheit/Publikationen/2009/h_da_querschnitt 090403.pdf

BUTLER, J. 'Genetics and Genomics of Core Short Tandem Repeat Loci Used in Human Identity Testing', 51 Journal Forensic Science, pp. 253–265, disponible en http://www.cstl.nist.gov/div831/strbase/pub_pres/Butler2006JFS_coreSTRreview.pdf

BWG, *Biometric Security Concerns*, 2003. disponible en http://www.cesg.gov.uk/ publications/Pages/categorylist.aspx

BYGRAVE, L. 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', *International Journal of Law and Information Technology* 1998, pp. 247–284.

BYGRAVE, L. 'Minding the Machine: Article 15 of the EC Data Protection Directive 95/46/EC and Automated Profiling', *Computer Law & Security Report* 2001, pp. 17–24.

BYGRAVE, L. 'The Body as data? Biobank regulation via the 'Back Door' of Data Protection Law', *Law, Innovation and Technology* 2010, pp. 1–25.

BYGRAVE, L. 'The Place of Privacy in Data Protection Law', University of NSW Law Journal 2001, disponible en http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html

BYGRAVE, L. "The body as data? Reflections on the relationship of data privacy law with the human body."conferencia impartida en *Federation Square*, Melbourne, 8 de septiembre de 2003, disponible en https://www.privacy.vic.gov.au/privacy/web2.nsf/files/body-as-data-conference-2003-lee-bygrave-presentation/$file/conference_03_no2.pdf

BYGRAVE, L. *Data Protection Law. Approaching its rationale, logic and limits*, The Hague, Kluwer Law International, 2002.

CABRERA, D. H. *Lo tecnológico y lo imaginario: Las nuevas tecnologías como creencias*, Biblos, 2006.

CAMPISI, P. "Security and Privacy in Biometrics: Towards a Holistic Approach,"en P. Campisi (ed.), *Security and Privacy in Biometrics*, 2013.

CANOSA USERA, R.: *El derecho a la integridad personal*, Lex Nova – IVAP 2006.

CATTELL, R. B. "An Introduction to Essentials", *Biometrics. International Biometric Society*, vol. 21/1, 1956, pp1190-1215.

CAVOUKIAN, A. *Biometrics and Policing: Comments from a Privacy Perspective,* Information and Privacy Commissioner, Ontario, Canada, 1999.

CAVOUKIAN, A. *Consumer Biometric Applications: A Discussion Paper,* Information and Privacy Commissioner, Ontario, Canada, 1999.

CAVOUKIAN, A. *Laws of Identity. The case for privacy-embedded laws of identity in the digital age*, Ontario, IPC, 2006.

CAVOUKIAN, A. *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Information and Privacy Commissioner Ontario, 2009.

CAVOUKIAN, A. *Privacy and Biometrics*, Information and Privacy Commissioner, Ontario, Canada, 1999. disponible en http://www.ipc.on.ca/images/Resources/pri-biom.pdf

CAVOUKIAN, A./ CHIBBA, M./ STOIANOV, A. 'Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment', en *Review of Policy Research*, 2012, pp. 37–61.

CAVOUKIAN, A./ SNIJDER, M. *Discussion of Biometrics for Authentication Purposes: The Relevance of Untraceable Biometrics and Biometric Encryption*, 2009.

CAVOUKIAN, A./ STOIANOV, A.: *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication*, Security AND Privacy, 2007, online disponible en: http://www.ipc.on.ca/images/Resources/bio-encryp.pdf

CAVOUKIAN, A/ MARINELLI, T. *Privacy-Protective Facial Recognition: Biometric Encryption. Proof of Concept*, Information and Privacy Commissioner Ontario, Ontario Lottery and Gaming Corporation, 2010.

CAVOUKIAN, A/ PROSCH, M. *Privacy by ReDesign: Building a Better Legacy*, Information and Privacy Commissioner Ontario, 2011.

CAVOUKIAN, A/ PROSCH, M. *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, Information and Privacy Commissioner Ontario, Ontario, 2010.

CEHAJIC, S/ SPROKKEREEF, A. 'Germany' en KINDT, E/ MÜLLER, L. (eds.), *The privacy legal framework for biometrics*, Frankfurt, FIDIS, 2009, pp. 70–82.

CESAGEN, *2nd Focus Group on Privacy Enhancing Technologies*, HIDE PROJECT, febrero de 2008.

CEYHAN, A.: "Enjeux d'identification et de surveillance à l'heure de la biométrie", *Cultures & Conflicts*, 64/ 2006, 02 avril 2007 http://conflits.revues.org/2176.

CHAMPOD, C./ J. W. EVERTT/ B. KUCHLER, "Earmark as evidence: A critical Review", *Journal of Forensic Science*, 2001, 46 (6), 1275-84.

CHAMPOD, C. "Identification/individualisation", en: J.H. Siegel, P.J. Saukko, G.C. Knupfer (Eds.), *Encyclopaedia of Forensic Science*, Academic Press, 2002.

CHANG, C. *Human identification using one lead ECG*. Master thesis. Department of Computer Sciences and Information Engineering, Chaoyang University, Taiwan, 2005.

CHAOS COMPUTER CLUB E. V (2004). CCC: *Biometrische Merkmale in Ausweisen erhöhen Sicherheit nicht*, Rueda de prensa de 21 de octubre de 2004.

CHARETTE, R.: "Here´s looking at you, and you, and you", *IEE Spectrum*, 2011.

CHELLAPPA, R./ WILSON, C. L./ SIROHEY, S. "Human and machine recognition of faces: a survey", *Proc. IEEE*, 83(5), 705–740, 1995.

CHERRY, S./ CORLEY, A. M. "Loser: Bad vibes", *IEEE Spectrum*, enero de 2010.

CHERTOFF, M. "Managing Identity: A Global Challenge", en *Orbis - A Journal of World Affairs*, vol. 53, nº 1/ 2009, pp. 137 y ss.

CLARKE, N. *Transparent User Authentication, Biometrics RFID and Behavioural Profiling*, Springer, 2011.

CLARKE, R. 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' en S. FISCHER-HÜBNER, G. QUIRCHMAYR, L/ L. YNGSTRÖM (eds.), *User Identification & Privacy Protection: Applications in Public Administration & Electronic Commerce, Kista, Sweden, 1999, IFIP WG 8.5 and WS 9.6,* disponible en http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html

CLARKE, R. "Chip-Based ID: Promise and Peril", Invited Address to a Workshop on 'Identity cards, with or without microprocessors: Efficiency versus confidentiality', en la International Conference on Privacy, Montreal, 23-26 de septiembre de 1997. http://www.rogerclarke.com/DV/IDCards97.html

CLARKE, R. "Human Identification in Information Systems: Management Challenges and Public Policy Issues", *Information Technology & People*, Vol. 7 No. 4, 1994, pp. 6ss.

CLARKE, R. (2001), "Person location and person tracking - Technologies, risks and policy implications", *Information Technology & People*, Vol. 14 Iss 2 pp. 206-231.

CLARKE, R. *Biometrics and Privac*y, 15 De abril de 2001, disponible en http://www.rogerclarke.com/DV/Biometrics.html

CLAUSS, S./ PFITZMANN, A./ HANSEN, M./ VAN HERREWEGHEN, E. *Privacy - Enhancing Identity Management*, IPTS report, 2002, disponible en http://ipts.jrc.ec.europa. eu/home/report/english/articles/vo l67/IPT2E676.htm

CNE – Corte Nacional Electoral de Bolivia, *¿Qué es el Padrón Electoral Biométrico?* Documento de Información Pública, nº 1, La Paz, junio de 2009.

CNIL, 'Homo informaticus en 2005 entre servitude et liberté. L'homo informaticus biomaîtrisé', 26 ième Rapport d'Activité 2005.

CNIL, *Biométrie comportementale: la reconnaissance de la frappe au clavier autorisée dans le cadre de démonstrations*, 28.7.2011.

CNIL, *Biométrie: la Cnil encadre l'utilisation de certain dispositifs et simplifie leur déclaration*, 18.05. 2006.

CNIL, *Biométrie: plusieurs condamnations judiciaires contre la société EASYDENTIC*, 14.03.2011.

CNIL, *Communication de la CNIL relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, 28 De diciembre de 2007, 12 p.

CNIL, *Délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'Etat modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques*, 11.12.2007.

CNIL, *Délibération n°02-001 du 8 janvier 2002 concernant les traitements automatisés d'informations nominatives mis en oeuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration*, 8.01.2002, Norme simplifiée N° 42.

CNIL, *Délibération n°04-017 du 8 avril 2004 relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en oeuvre d'une contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy*, 8.04.2004.

CNIL, *Délibération n°2006-0102 du 27 avril 2006 portant autorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail*, 27.04. 2006.

CNIL, *Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail*, 7.05. 2009.

CNIL, *Délibération n°2011-074 du 10 mars 2011 portant autorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalités le contrôle de l'accès aux postes informatiques*, 10.03.2011.

CNIL, *Délibération n°2012-322 du 20 septembre 2012 portant autorisation unique de mise en oeuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle de l'accès ainsi que la restauration sur les lieux de travail*, 20.09.2012.

CNIL, *La CNIL ordonne l'interruption d'un dispositif biométrique illégal,* 20.05.2010.

COATS, W./ BAGDASARIAN, A./ HELOU,T./ LAM, T. (eds.), *The Practitioner ' s Guide to Biometrics*, Chicago, American Bar Association, 2007.

COHEN, J. 'The right to read anonymously: a closer look at 'copyright management' in cyberspace', 28 Conn. L. Rev. 1996, pp. 981–1039.

COLE RA, MARIANI J, USZKORET H, ZAENEN A, ZUE A (1997) *Survey of the state of the art in human language technology*. Cambridge University Press.

COLE, S. A. *Suspected identities. A history of fingerprint and criminal identification*, Cambridge/Massachusetts, Harvard University Press, 2001.

COLE, S.' Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate', en LAZER, D. (ed.), *The Technology of Justice: DNA and the Criminal Justice System*, disponible en http://www.ksg.harvard.edu/dnabook/

COMISIÓN EUROPEA - EUROPEAN COMMISSION (ED.), *Biometrics in Europe. Trend Report*, UNISYS – European Biometrics Portal, 2007, pp22-23.

COMISIÓN EUROPEA - EUROPEAN COMMISSION, 'Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21 st Century', COM(2012) 9 final, 25.1.2012.

COMISIÓN EUROPEA - EUROPEAN COMMISSION, Communication from the Commission to the European Parliament and the Council, Smart borders – options and the way ahead, COM(2011) 680 final, 25.10.2011.

COMISIÓN EUROPEA - EUROPEAN COMMISSION, DG JRC and the Institute of Prospective Technological Studies, *Biometrics at the Frontiers: Assessing the Impact on Society*, Sevilla, European Commission, 2005.

COMISIÓN EUROPEA - EUROPEAN COMMISSION, Information Society and Media Directorate-General, eGovernment Unit, A Roadmap for a pan - European eIDM Framework by 2010, v1.0, Block VIII. Disponible en http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

COMISIÓN EUROPEA. Commission Regulation No (EC) 1560/2003 of 2 September 2003 laying down detailed rules

for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, O. J. L 222, 5.09.2003, pp. 3–23.

COMITÉ CONSULTATIF NATIONAL D'ETIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, Avis n ° 98. «Biométrie, données identifiantes et droits de l ' homme », disponible en http://www.libertysecurity.org/IMG/pdf_avis098fr.pdf

COMITÉ DEL CONVENIO 108 DEL CONSEJO DE EUROPA, *The introduction and use of personal identification numbers: the data protection issues*, Consejo de Europa, 1991.

COMITÉ EUROPEO DE EXPERTOS EN INMIGRACIÓN. Comments Standing Committee of experts in international immigration, refugee and criminal law on the draft proposal for a Regulation concerning the Visa Information System (VIS), COM(2004) 835, Utrecht, 2005.

COMMANDUCCI, P.: "Interpretazione della Costituzione", en *Assaggi di metaetica due*, Torino: Giapichelli, 1998.

COMPTROLLER GENERAL-CG, (1980), "Re-issuing Tamper Resistant Cards Will Not Eliminate Misuse of Social Security Numbers", US Comptroller-General (Contralor General), Washington DC.

CONSEJO DE EUROPA - Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23.11.2010.

CONSEJO DE EUROPA - Council of Europe, Recommendation No. Rec(97)5 of the Committee of Ministers to Member States on the Protection of Medical Data, 17.02.1997.

CONSEJO DE EUROPA - Council of Europe, *The need for a global consideration of the human rights implications of biometrics*, Doc. 12522, Parliamentary Assembly, 16.02.2011.

CONSEJO EUROPEO (UE). Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the Second Generation Schengen Information System (SIS II), O. J. L 205, 7.08.2007, pp. 63–84.

CONSEJO EUROPEO (UE). Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime, O. J. L. 210, 6.08.2008, pp. 1–11.

CONSEJO EUROPEO (UE). Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime, O. J. L. 210, 6.08.2008, pp. 12–72.

CONSEJO EUROPEO. Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, O. J. L. 218, 13.08.2008, p. 129–136.

CONSEJO EUROPEO. Council Decision of 8 June 2004 establishing the Visa Information System (VIS), 2004/512/EC, O.J. L. 213, 15.06.2004, pp. 5–7.

CONSEJO EUROPEO. Council Regulation No (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, O. J. L 316, 15.12.2000, pp. 1–10.

CONSEJO EUROPEO. Council Regulation No (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac"for the comparison of fingerprints for the effective application of the Dublin Convention, O. J. L 62, 5.03.2002, pp. 1–5.

CONSEJO EUROPEO. Council Regulation No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, O. J. L 385, 29 2004, pp.1–6.

COUDERT, F. 'When video cameras watch and screen: Privacy implications of pattern recognition technologies', Computer Law & Security Review 2010, pp. 377–384.

CRANE, H. D./ OSTREM, J. S. "Automatic signature verification using a three axis force-sensitive pen", *IEEE Trans. on Systems, Man and Cybernetics*, *SMC*- 13(3), 329–337, 1983. V. S. Nalwa, Automatic on-line signature verification. Proc. IEEE, 85(2), 215–239, 1997.

CREWS jr., C. W. "Human Bar Code. Monitoring Biometric Technologies in a Free Society", *Policy Analysis*, nº 452, 2002, pp1 y ss.

CROWLEY, M. 'Cyber Crime and Biometric Authentication – The Problem of Privacy Versus Protection of Business Assets', en BHAVANI, M. (ed.) *Biometrics. Techno - Legal Issues*, Hyderabad, India, ICFAI University Press, 2008, pp. 41–55.

CURIEL LOPEZ DE ARCAUTE/ GRANELL NAVARRO, "La huella de la oreja como método de identificación", *Acta Otorronolaringológica Española* 2006, 57: 329-332.

CURTO, D. R. (1995): "Crimes e Antropologia Criminal", *Revista Lusitana,* n°13-14. pp.179-199.

CUSTERS, B./CALDERS, T./ SCHERMER, B./ ZARSKY, T. (eds.), Discrimination and Privacy in the Information Society, Springer, 2013, pp22-23

CUTTING, J./ KOZLOWKI, L. "Recognizing Friends by their Walk: Gait Perception without Familiarity Cues", *Bulletin Psychodinamic So*c, vol 9. Nº 5, pp3535-356, 1977.

DAMASIO, Alain: "Construisons ensemble la civilité de l'internet", *Le Forum des dorits sur l'internet*. En su intervención en los debates del *FDI*, de 12 de marzo de 2002. Acceso (agosto de 2015), en http://www.bugbrother.com/spip.php?article205

DARROCH, A. "Freedom and Biometric in UK Schools", Biometric Technology Today, jul-ago 2011, p5s.

DÄUBLER, W.: "Das neue Bundesdatenschutzgesetz und Seine Auswirkungen im Arbeitsrecht", *NZA*, 2001, págs. 874-881.

DAUGMAN, J. ' How Iris Recognition Works ', *IEEE Transactions on circuits and systems for video technology*, 2004, pp. 21–30, disponible en http://www.cl.cam.ac.uk/~jgd1000/csvt.pdf

DAUGMAN, J. 'Interview. Pattern recognition: Biometrics, Identity and the State – An Interview with John Daugman', en *BioSocieties* 2008, pp. 81–86.

DAUGMAN, J. *Biometric decision landscapes. Technical Report 482*, Cambridge, University of Cambridge Computer Laboratory, Enero de 2000. Disponible en http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR482.pdf

DAUGMAN, J. D. "High confidence visual recognition of persons by a test of statistical Independence", *IEEE Trans. Pattern Analysis and Machine Intelligence*, 15(11), 1148–1161, 1993.

DAVID HUME INSTITUTE, *Privacy and Property*, Edinburgh, Edinburgh University Press, 1994.

DAVIES, S. "Touching Big Brother: how biometric technology will fuse flesh and machine", *Information Technology and People*, 7 (4), 1994.

DAVIS, R. *Biometrics Myths: Six of the Best*, *CEO of ISL Biometrics*, 2001.

DE ANTON Y BARBERÁ, F.: "Las Huellas Dactilares a Examen", *Revista del Instituto Universitario de Investigación Criminológica y Ciencias Penales de la Universidad de Valencia*, 2009, 20-26.

DE BUSSER, E. *Data Protection in EU and US Criminal Cooperation*. A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities, Antwerpen, Maklu, 2009.

DE DIEGO DÍAZ, L. A.: *Identificación fotográfica y reconocimiento en rueda del inculpado*, BOSCH, Barcelona, 2003.

DE DIEGO DÍAZ, L. A.: *La Prueba Dactiloscópica*, Bosch, Barcelona, 2001.

DE HERT, P. 'Balancing security and liberty within the European human rights framework. A critical reading of the Court' case law in the light of surveillance and criminal law enforcement strategies after 9/11', Utrecht Law Review, 2005, pp. 68–96, disponible en http://www.utrechtlawreview.org/index.php/ulr/article/view/4

DE HERT, P. 'Identity management of e-ID, privacy and security in Europe. A human rights view', *Information Security Technical Report*, 2008, pp. 71–75.

DE HERT, P. *Biometrics: legal issues and implications. Background paper for the Institute of Prospective Technological Studies*, DG JRC, 2005, Sevilla, European Commission, disponible en http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf

DE HERT, P./ GURTWIRTH, S.: "Data Protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action", en GURTWIRTH, S./ POULLET, Y./ DE HERT, P/ TERWAGNE, C/ NOUWT, S. (eds.), *Reinventing Data Protection*, Springer, Dordrecht, 2009, pp25ss.

DE HERT, P./ GUTWIRTH, S./ MOSCIBRODA, A./ WRIGHT, D/ GONZÁLEZ FUSTER, G. "Legal Safeguards for Privacy and Data Protection in ambient intelligence", *Pers Ubiquit Comput* 13/ 2009, 435–444.

DE HERT, P./ LONCKE, M. 'Camera surveillance and workplace privacy in Belgium', en S. NOUWT,/ B. DE VRIES/C. PRINS (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, Den Haag, Asser Press, 2005, pp. 167–209.

DE HERT, P./ NOUWT, J./VOETS, I./ VAN DER WEES, J. 'SMS, opsporing en privacy', *Computerrecht* 2008, pp. 154–160.

DE HERT, P./ RIEHLE, C. 'Data protection in the area of freedom, security and justice. A short introduction and many questions left unanswered', *ERA Forum* 2010, pp. 159–167, disponible en http://www.springerlink.com/content/u6566750w5954262/

DE HERT, P./ SCHEUERS, W./ BROUWER, E.: "Machine-readable identity documents with biometric data in the EU – part III- Overview of the legal Framework", *Keesing Journal of Documents and Identity*, 2007/ 22.

DE HERT, P./ SPROKKEREEF, A. 'Regulation for biometrics as a primary key for interoperability?' en KINDT, E/ MÜLLER, L. (eds.), *Biometrics in identity management*, Frankfurt, FIDIS, 2007, pp. 47–55.

DE HERT, P./ SPROKKEREEF, A. *An Assessment of the Proposed Uniform Format for Residence Permits: Use of Biometrics*, CEPS Briefing Note for the European Parliament's committee on Civil Liberties, Justice and Home Affairs, IP/C/LIBE/FWC/2005-xx, disponible en www.ceps.be

DE TERWANGNE, C.: "Privacidad en Internet y derecho a ser olvidado/ derecho al olvido", IDP, Número 13, (Febrero 2012), *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, monográfico "VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet", páginas 52 y ss.

DE VRIES, K./ BELLANOVA, R./ DE HERT, P./ GUTWIRTH, S. "The German Constitutional Court Judgement on Data Retention: Proportionality overrides Unlimited Surveillance (Doesn't it?)", en GUTWIRTH, S./ POULLET, Y./ DE HERT, P./ LEENES, R. (eds.), *Computers, privacy and data protection : an element of choice*, Dordrecht, Springer, 2011, pp. 3–24.

DEANE, F/BARRELLE, K./ HENDERSON, R./ MAHAR, D.: "Perceived acceptability of biometric security systems", Computes & Security, 14(3), 1995, pp225-231.

DELLEN, M. (eds.), *Digital Anonymity and the Law – Tensions and Dimensions*, The Hague, Asser Press, ITeR, 2, 2003, pp.121–135.

DENBY, B./ T. SCHULTZ, K. HONDA, T. HUEBER, J. M. GILBERT, J. S. BRUMBERG, Silent speech interfaces, Speech Communication 52 (4) (2010) 270–287.

DEPARTMENT OF HEALTH, EDUCATION AND WELFARE - HEW (1973), "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems", US Department of Health, Education and Welfare, MIT Press, Boston, MA, pp114-22. Disponible en: http://www.justice.gov/opcl/docs/rec-com-rights.pdf

DEPARTMENT OF THE TREASURY (EE.UU.), *The Use of Technology to combat identity theft, Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003*, 2005.

DÉTRAIGNE, Y./ ESCOFFIER, A.-M. Rapport N° 441. *Respect de la vie privée à l'heure des mémoires numériques*, Senate, 2008–09.

DHALL, A./ R.GOECKE,/ J JOSHI/ M. WAGNER/ T. GEDEON, "Emotion Recognition in the will challenge", *Proceedings of the 15th ACM on International conference on multimodal interaction*, 2013, pp509-516.

DHARAO, A. S./ M. THAN: "Five anthroposcopic traits of the ear in a Malaysian population", *Antropol Anz* 1995, 53 (4), pp359-363.

DI NATALE, C./ MACAGNANO, A./ MARTINELLI, E./ PAOLESSE, R./ PROIETTI, E./ D'AMICO, A. "The evaluation of quality of post-harvest oranges and apples by means of an electronic nose", Journal *Sens. Actuators B* 78, 2001, pp. 26–31.

DÍAS, C. *La police technique et scientifique*, PUF, Paris, 2000.

DIAZ, C./ SEYS, S./ CLAESSENS, J./ PRENEEL, B. 'Towards measuring anonymity', en FEDERATH, H. (ed.), *Designing Privacy Enhancing Technologies*, vol. 2482, LNCS, 2002, disponible en http:// citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.986

DIETRICH PLAZA, C. "El tratado de Prüm en el marco de la regulación de la protección de datos personales en la Unión Europea", *Revista Europea de Derecho Constitucional*, REDCE año 4, nº 7, enero-junio de 2007.

DINANT, J.-M. 'The Concepts of Identity and Identifiability: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society', en GUTWIRTH, S./ POULLET, Y./ DE HERT, P./ DE TERWANGNE, C./ NOUWT, S. (eds.), *Reinventing Data Protection?*, Springer, 2009, pp. 111–122.

DOBRIŠEK, S.: "Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, Security and Defense", *The Newsletter of HIDE: Homeland, Security, Biometric Identification and Personal Detection Ethics*, vol 2, nº 7, 2009, Dialogue, p.2

DOBRIŠEK, S.:"Workshop report. Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, security and defence", en *HIDE Newsletter*, vol. 2 (7), 2009, pp2 y 3.

DOBZHANSKY, T. *Genetic diversity and human equality. Facts and fallacies in the explosive genetics and education controversies*, The John Dewey Society Lecture. New York: Basic Books. 1973.

DODDINGTON, G./ LIGGETT, W./ MARTIN, A./ PRZYBOCKI, M./ REYNOLDS, D. "Sheep, Goats, Lambs and Wolves", en *A Statistical Analysis of Speaker Performance in the NIST* 1998.

DORSCHEL, J. (ed.), *Praxishandbuch Big Data*, Springer, 2015.

DOTSON, K. A.: "Your Good Name: Identity Theft and the Consumer – A Case Note of Andrews v. TRW, inc", Quinnipiac Law Review (QLR) Vol 22, nº 3, 2004, pp611-612.

DOTZLER, F.: *Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen: eine exemplarische Betrachtung von Systemen auf der Grundlage des biometrischen Merkmals Tippverhalten,* Kölner Wissenschaftsverlag, 2010.

DOTZLER, F.: *Eignung biometrischer Authentifizierungsverfahren zur Lösung der Sicherheitsproblematik bei unternehmensübergreifenden hochflexiblen Geschäftsprozessen* – eine datenschutzrechtliche Analyse-, forFLEX, 2011. http://www.forflex.de/uploads/AB/forflex-2011-001.pdf

DRAHANSKY, M./ M. DOLEZEL/ J. URBANEK/ ET ALTERE, Influence of Skin Diseases on Fingerprint Recognition, *Journal of Biomedicine and Biotechnology*, vol. 2012. ID 626148

DRIRA H./ AMOR, B.B./ DAOUDI, M./ SRIVASTAVA, A. "Nasal region contribution in 3D face biometrics using shape analysis framework", *Proceedings of the 3rd IAPR/IEEE International Conference on Biometrics*, 2009, Alghero, Italy, 357–366.

DUANGPHASUK, A./KURUTACH, W. "Tattoo skin detection and segmentation using image negative method,"Proceedings of the 13th International Symposium on Communications and Information Technologies, pp. 354-359, 2013 (http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6645881).

DUMORTIER, J./ GOEMAN, C. *Roadmap for Advanced Research in Privacy and Identity Management (RAPID)*, 2003, disponible en https://www.law.kuleuven.be/icri/deliverables/421rapid.pdf?where=

DUNSTONE, T./ YAGER, N. Biometric Systems and Data Analysis. Design, Evaluation, and Data Mining, Springer, 2009.

EISENBERG, A.: "Is That You, Son? Voice Authentication Trips Up the Experts", *New York Times*, 13 de noviembre de 2003.

ELECTRONIC PRIVACY INFORMATION CENTER AND PRIVACY INTERNATIONAL, *Privacy and Human Rights* 2006.*An International Survey of Privacy Laws and Developments*, Washington – London, Electronic Privacy Information Center and Privacy International, 2007.

ELECTRONIC PRIVACY INFORMATION CENTER, Comments of the Electronic Privacy Information Center to the Federal Trade Commission. Face Facts: A Forum on Facial Recognition, project number P115406, 31 de enero de 2012. Disponible en http://epic.org/privacy/facerecognition/EPICFace- Facts-Comments.pdf

ELLERBROK, A. "Playful biometrics: Controversial Technology through the Lens of Play", The Sociological Quarterly 52 (2011), pp528-547, p529.

ENISA. *ENISA briefing: Behavioural biometrics*. European Network and Information Security Agency, 2010, en http://www.enisa.europa.eu/act/rm/files/deliverables/behavioural-biometrics/at_download/fullReport..

ERICKSON, E. H.: *Identity and the Life Cycle*, Norton & Company, 1994.

ERTZSCHEID, O.: *Qu'est-ce que l'identité numérique?*, Open Edition Press, 2013.

ESCAJEDO SAN EPIFANIO, L. "Fragmentation of the fundamental right to life: between territorial decentralization and the knowledge-based economy", A. LÓPEZ BASAGUREN/L. ESCAJEDO SAN EPIFANIO, *The Ways of Federalism in Western Countries - II*, Springer, 2013, pp437ss.

ESCAJEDO SAN EPIFANIO, L. "La libertad fundamental de investigación y los nuevos controles éticos a la investigación biomédica", en VV. AA. *El Derecho ante los avances de la Medicina*, Thomson-Civitas, 2008, pp. 1189 y ss.

ESCAJEDO SAN EPIFANIO, L. «El inconsistente estatuto del embrión humano extracorpóreo en la Unión Europea. Proyecciones Constitucionales de la Sentencia TJUE *Brüstle v. Greenpeace* (As c-34/10)», en *Revista de Derecho Constitucional Europeo*, núm. 17, 2012.

ESCAJEDO SAN EPIFANIO, L. "Reproducción humana, Medicina genética y derechos fundamentales"*Ética de la Vida y de la Salud: su problemática biojurídica*, Universidad de Sevilla, 2008, pp. 107 y ss.

ESCAJEDO SAN EPIFANIO, L. "Constitucionalismo transnacional y nuevos derechos. Sobre la validez del Corpus Iuris de los Derechos Humanos y la Biomedicina, como paradigma", en I. Filibi/J. M. Belise (coords.), *Constitucionalismo transnacional. Derecho, democracia y economía política en la Globalización*, Universidad de Córdoba (Argentina), 2010, pp. 161 y ss.

ESCAJEDO SAN EPIFANIO, L. "Identidad Genética y Libertad de Ciencia", C. AGUADO RENEDO/ A. LÓPEZ CASTILLO (DIRS.), *Identidad, Derecho y Política,* AFDUAM 17 (2013), pp19-74.

ESCHENBURG, F./ G. BENTE/ H. TRITZSCH, R. POWIERSKI/ O FISCHER, "The Biosec Mobile Usability lab for biometric security systems", Third Cost 275 Workshop. Biometrics on the Internet, 27-28, 20.2005, University of Hertfordshire, UK, pp63-7.K. UNYSIS, Research Shows Growing Global Acceptance of Biometrics among Consumers for Protectiong Identities and Personal Information, 10.11.2009.

EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES, Report on the Charter on Fundamental Rights related to technological innovation as requested by President Prodi onFebruary 3, 2000, 23 de mayo de 2000.

EUROPEAN NETWORK AGAINST RACISM, *Ethnic Profiling*, Brussels, ENAR, 2009.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, ENISA Briefing: Behavioral Biometrics, 2010, en en www.enisa,europa.eu.

EUROPEAN PRIVACY AND DATA PROTECTION COMMISSIONERS, *Declaration adopted on the Spring Conference of European Data Protection Authorities*, Rome, 17–18 De abril 2008, disponible en https://www.ip-rs.si/index.php?id=272&tx_ttnews%5Btt_news%5D=367&cHash=47956ed169f8c49b72d2a7cbe042d9d4

EUROPEAN PRIVACY AND DATA PROTECTION COMMISSIONERS, *Declaration on leadership and the future of data protection in Europe*, Edinburgh, 23–24 de abril de 2009.

FAIRHURST, M (ed.) *Age Factors in Biometric Processing*, 2014.

FAIRHURST, M./ M. ERBILEK, "Analysis of physical ageing effects in iris biometrics", *Computer Vision*, vol. 5, 2011, pp358-366.

FAIZ SYUAIB, M. "Anthropometric study of farm workers on Java Island, Indonesia, and its implications for the design of farm tools and equipment", *Applied Ergonomics* 51, 2015, 222-235.

FALGUERA, J.R./ FALGUERA, F.P.S./ MARANA, A. N. "Frontal sinus recognition for human identification", 2008, *Proceedings of SPIE*, vol. 6944, Orlando, FL, 69440S.

FARELO, A. *A History of Fingerprints*, Interpol, abril de 2009, p2.

FARKAS, L. G. "Ear Morphology in Treacher Collins', Apert's, and Crouzon's syndromes", *Arch Otorhinolaryngology* 1978: 220 (1-2), pp153-157.

FAYYAD, U. M/ PIATETSKY-SHAPIRO, G. (eds.), *Advances in Knowledge Discovery and Data Mining*, AAAI Press- MIT Press, 1996..

FBI, State - of - the - Art Biometric Excellence Roadmap (SABER) Report, 24.11.2008, disponible en http://www.biometriccoe.gov/SABER/index.htm

FDI – Forum des Droits sur l'Internet, Rapport "Le Project de carte nationale d'identité numérique (CNIE)", de 16 de junio de 2003. Disponible en www.foruminternet.org, doc RECO-CNIE 2005016.

FDI, *Rapport Le Project de Carte Nationale di identité numerique,* 16 de junio de 2006.

FEDERAL ADVISORY COMMITTEE ON FALSE IDENTIFICATION - FACFI (1976), "The Criminal Use of False Identification: The Report of the Federal Advisory Committee on False Identification", Departamento de Justicia de los Estados Uniods, Washington DC.

FEDERAL TRADE COMMISSION (FTC), *Privacy Online: A Report to Congress*, Washington, 1998.

FEDERAL TRADE COMMISSION, *Facing Facts. Best Practices for Common Uses of Facial Recognition Technologies*, 2012. Disponible en http://ftc.gov/os/2012/10/121022facialtechrpt.pdf

FEJFAR, A./ MYERS, J. "The testing of 3 automatic ID verification techniques for entry control", *2nd Int.Conf. on Crime Countermeasures*, Oxford, 25–29 de julio de 1977.

FENKER, S. P./ BOWYER, K. W. "Experimental evidence of a template aging effect in iris biometrics", C. RATHGEB (ed.) Iris Biometrics, 2011, p149.

FERRI, E. *Principios de Derecho Criminal* (trad. J. A. RODRÍGUEZ), Reus, Madrid, 1933, pp45 y ss.

FICHES, Michael: BioMetrics: The Future is Today, *Access Control & Security Systems*, 46 (7), 2003, pp20-26.

FIDIS Project. 2009. Behavioural biometric profiling and transparency enhancing tools. Deliverable FIDIS Project (Future of Identity in the Information Society), document URL: http://

FIDIS, Budapest Declaration on Machine Readable Travel Documents (MRTDs), Frankfurt, FIDIS, 2006, 4 p. Disponible en http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_ on_MRTD.en.20061106.pdf

FILLIT, H. M./ K. ROCKWOOD/ K. WOODHOUSE, "Aging and the skin", Brocklehurst Textbook of geriatric Medicine and Gerontology, 7ª ed, Elsevier, 2010, pp133-136.

FINOCCHIARO, G.: Diritto all'anonimato: anonimato, nome e identità personale, Cedam, Padua, 2008.

FISCHER-HÜBNER, S. IT-*security and Privacy. Design and use of privacy - enhancing security mechanisms*, Springer, 2001.

FISCHER-HÜBNER, S/ ZWINGELBERG, H. (eds.), D.4.3.2, UI prototypes: Policy administration and presentation. Version 2, Primelife, 2010.

FLAHERTY, D. 'On the Utility of Constitutional Rights to Privacy and Data Protection', 41 Case W. Res. L. Rev. 831, 1990–1991, pp. 831–855.

FLOR, R. "Phising y delitos relacionados con el fraude de identidad: un World Wide Problem en el World Wide", e I. SALVADORI, "La Lucha contra el hurto de identidad", ambos en AAVV, *Robo de identidad y protección de datos*, 2010, pp. 77-80 y 221-222 respectivamente.

FLOR, R.: "Phishing y delitos relacionados con el fraude de identidad: un World Wide Problem en el World Wide", AAVV, *Robo de identidad y protección de datos*, 2010, pp. 77 y ss.

FOESSEL, M./GARAPON, A. "Biométrie: les nouvelles formes de l'identité",*Esprit*, août-septembre 2006, pp. 165 y ss.

FRADEN, J. *Handbook of Modern Sensors: Physics, Designs, and Applications*, 3rd Edition, New York, NY, USA: Springer Science+Business Media, Inc., 2004.

FRANKE, H./ KOEKKOEN, A. K.: "The protection of Fundamental Rights in a Digital Age", en *International Academy of Comparative Law*, Brussels, Bruylandt, 2006, pp1147-1164.

FRIEDEWALD, M./ WRIGHT, D./ GUTWIRTH, S/ MORDINI, E. 'Privacy, data protection and emerging sciences and technologies toward a common framework', *The European Journal of Social Science Research* 2010, pp. 61–67.

FROST & SULLIVAN, *Biometrics in Europe – Future Technologies and Applications*, 2009, disponible en http://www.frost.com/prod/servlet/segment-toc.pag?segid=9834-00-04-00-00

FUJITSU LABORATORIES LIMITED. Fujitsu PalmSecure selected as a "world changing idea"for

FUJITSU LABORATORIES LIMITED. The future of biometrics – Dr Joseph Reger, en Future Banking. http://www.banking-gateway.com/projects/fujitsu-the-future-of-biometrics-dr-joseph-reger/fujitsu-the-future-of-biometrics-dr-joseph-reger3.html. Acceso, agosto de 2015.

GAINOTI, S. A. G. SPAGNOLO, "Test-genetici: a che punto siamo in Europa? A margine di Rapporto e della Raccomandazioni della Commissione Europea sugli aspetti etici, giuridici e sociali du test genetici", en *Medizina e Morale*, 2004, nº 4, pp750-751.

GALTON, F. 'Finger print evidence', Nature 1902, p. 606, disponible en http://galton.org/bib/JournalItem.aspx_action=view_id=291

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI – Linee guida in materia de trattamento di dati personali di lavoratori per finalitá di gestione del rapporto di lavoro alle dependenze di datori de lavoro privati. Deliberazione nº 53 del 23 de noviembre de 2006, 1368365.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI – Uso delle impornte digitali per i sistemi di rilevamento delle presente nel luoghi de lavoro (2005).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI – Uso delle impronte digitali per i sistemi di rilevamento delle presente nei luoghi di laboro, 21 de julio de 2005. Linee guida in materia di trattamento di dati personali di lavoratori (deliberazione nº 53, del 23 nov. 2006, doc 1368365).

GARANTE, *Il decalogo su corpor é libertá*, Comunicado de 9 de mayo de 2006.

GARANTE, *Sicurezza di diti archeologici e uso dei dati biometrici*, de 8 de noviembre de 2007, doc 1461908.

GARANTE, Sicurezza merci e controllo delle pressenze presso aeroporti, 26 de julio de 2006, doc 1318582.

GARANTE, *Trattamento di dati personali biometrici per l'acceso a un complesso polifunzionale*, 1 feb 2007, doc 1381983.

GARCÍA MESTANZA, J.: "Impulso al desarrollo de la sociedad de la información. El DNI electrónico como catalizador", *Ei* 370, pp111 y ss.

GARFINKEL, S. *Database Nation: The Death of Privacy in the 21st Century*, Sebastopol, CA: O'Reilly & Associates, 2000.

GARÓFALO, R. *La Criminología. Estudio sobre el delito y sobre la teoría de la represión* (trad. P. Dorado), Editorial La España Moderna, Madrid, 1900. –versión digital DOI:968-7804-11-4-

GASSON, M./ MEINTS, M/ WARWICK, K. (eds.), *A study on PKI and biometrics*, Frankfurt, FIDIS, 2005.

GATES, C. *Ancient Cities: The Archaeology of Urban Life in the Ancient near East and Egypt, Greece and Rome*, Rutledge, Londres, 2003.

GATTI, U./ VERDE, A. "Cesare Lombroso: Methodological ambiguities and brilliant intuitions, International Journal of Law and Psychiatry", *International Journal of Law and Psychiatry* 35 (2012), 19-26.

GELB, A./ DECKER, C.: "Cash at your fingertips: Biometric Technology for transfers in developing countries", Review of Policy Research, 29 (1), 2012, pp91-117.

GERADTS, Z./ GLOE, TH. (eds.), *Identification of images*, Frankfurt, FIDIS, 2009.

GERADTS, Z./ SOMMER, P. (eds.), *Forensic Implications of Identity Management Systems*, Frankfurt, FIDIS, 2006.

Gharaibeg, W. Correcting for the Effect of Orientation in Geometric Morphometric Studies of Side-View Images of Human Heads, en Modern morphometrics, 2005, pp117-142.

GHILARDI, G./ KELLER, F.:"Epistemological Foundations of Biometrics", en E. MORDINI/ D. TZOVARAS (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012, pp23 y ss.

GHOUTI, L./ BAHJAT, A. A. "Iris fusión for multibiometric systems", Proc IEEE on Signal Processing and Information Technology, 2009, pp248-2009. Kisku, p260. E. Mordini, European Journal of Social Science, 2012, 23.

GIANNOTTI, F./ LAKSHMANAN, V. S./MONREALE, A. PEDRESCHI, D/ WANG, W. H, "Privacy-preserving Data Mining form Ourtsourced Databases", en Grutwirth et altere, *Computers, Privacy, and Data Protection*, Springer, 2011.

GILLET, G. *Subjectivity and Being somebody. Human identity and neuroethics*, Imprint Academic, Exeter, 2008.

GIROTTO, S.: "Il tratamento dei Dati Biometrici", en Stefano Rodotá/ Paolo Zatti (dirs.), *Tratatto di Biodiritto. Tomo II – Il Governo del Corpo*, Giuffré, Milán, 2011.

GISH, H. "Elements of Speaker Verification", en J. WAYMAN/ A. JAIN/ D. MALTONI/ D. MARIO, ET ALT, *Biometric Systems. Technology, Design and Performance Evaluation*, Springer, 2005, pp125ss.

GIULIANO, A.: *Dieci e tutti diverse o Studio sui dermatoglifiumani*, Tirrena Stampatori, Turín, 2004.

GOBIERNO DE MÉXICO. (2003) Face recognition technology to eliminate duplicate voter registrations in upcoming presidential elections. http://www.shareholder.com/identix/ReleaseDetail.c fm?ReleaseID=53264.

GODARD, B./ SCHMIDTKE, J./ CASSIMAN, J.-J/ AYMÉ, S. 'Data storage and DNA banking for biomedical research: informed consent, confidentiality, quality issues, ownership, return of benefits. A professional perspective', *European Journal of Human Genetics* 2003, disponible en http://www.nature.com/ejhg/journal/v11/n2s/pdf/5201114a.pdf

GOLDSTEIN, D.B./ CAVALLERI, G.L. "Understanding human diversity", *Nature*, vol 437, 27 de octubre de 2005, pp1241ss.

GOLEMBIEWSKI, C./ PROBST, Th. *Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen,* Unabämgiges Landeszentrum für Datenschutzrecht, 2003.

GOLOMB, B.A./ LAWRENCE, D.T./ SEJNOWSKI, T.J. "SEXNET: A neural network identifies sex from human faces", *en Advances in neural information processing systems*, vol. 3, 1991, ed. D.S. TOURETZKY AND R. LIPPMANN, 572–577. San Mateo: Morgan Kaufmann Publishers.

GONG, S./ CRISTANI, M./ YAN, S./ CHANGE LOY, C. (eds.), *Person Re-identification*, Springer, 2014.

GONZÁLEZ BEILFUSS, M. *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional,* Aranzadi, Pamplona, 2003.

GOULD, S. J. *Der falsch vermessene Mensch*, Franfurt a. M. 1988.

GOULD, S. J.: *Der falsch vermessene Mensch, Franfurt a. M. 1988. Peter Strasser, Verbrechermenschen. Zur kriminalwissenschaftlichen Erzeugung des Bösen,* Frankfurt a. M. 2005 (original de 1984), Kap. II („Der Mythos als Wissenschaft"), pp41 y ss,

GOUVALI, M. K./ BOUDOLOS, K. "Match between scjool furnoture dimensions and children's anthropometry", *Applied Ergonomics* 37 (2006), 765-773.

GP-WP 29, Opinión 4/ 2007 de 20 de junio de 2007.

GRAALMANN-SCHEERER, K. "DNA – Analyse – 'Genetischer Fingerabdruck", en *Kriminalistik* 5/ 2000, pp328-335.

GRAHAM-GROWE, D. "Secure Signature Means No ONe Can Steal Your ID. A New Approach to ID Card Biometrics Will Enhance Security and Privacy", *New Scientist*, 182/ 2004, pp22-23.

GRIJPINK, J. 'Identity fraud and biometrics, an assessment model for the use of biometrics', Computer Law and Security Report 2006, pp. 261–319.

GRIJPINK, J. 'Two barriers to realizing the benefits of biometrics: a chain perspective on biometrics, and identity fraud as biometrics' real challenge', *Computer Law and Security Report* 2005, pp. 138–256.

GRIJPINK, J. Understanding Biometrics, 15 p. Disponible en http://www.uu.nl/staff/JHAMGrijpink

GRIMALDI, K./ LOOK, M./ SCIOLI, A./ COLL CLAVERO, J./ MARINOS, S./ TAGARIS T. 'Personal genetics: regulatory framework in Europe from a service provider's perspective', *European Journal of Human Genetics* 2011, pp. 382–388.

GROTHER, P./ QUINN, G/ PHILLIPS, P. *Multiple - Biometric Evaluation (MBE) – Report on the Evaluation of 2D Still - Image Face Recognition Algorithms*, NIST Interagency Report 7709, 2010, 59 p. Disponible en http://biometrics.nist.gov/cs_links/face/mbe/MBE_2D_face_report_NISTIR_7709.pdf

GRUDZIEN, W. "Biometrie im Banking. Ein Pladoyer gegen Vorurteile", *DuD*, 1/ 2015, pp7ss.

GT-WP 29, Opinion 3/ 2012 on developments in biometric Technologies, adoptado el 27 de abril de 2012, WP 193, p3.

GUCHET, X.: *Contribuciones de expertos al debate CNIE*, de 30 de marzo de 2005, organizado por el FDI, pp46ss de las actas.

GUILD, E. 'Unreadable Papers? The EU's first experiences with biometrics: Examining EURODAC and the EU's Borders',en J. LODGE (ed.), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen, Wolf Legal Publishers, 2007, pp. 31–43.

GUINCHARD, S./ DEBARD, T.: *Lexique des Termes Juridiques*, Dalloz, 2012, p.275. Gérard CORNU, *Vocabulaire juridique*, 9ª edición, 2011.

GUINIER, D.: "Biometrie: classification au vu des nouveaux motifs", *Expertises*, febrero de 2005, pp62-68.

GUNN, S. R./ NIXON, M. S. "A robust snake implementation: a dual active contour". *IEE Transactions PAMI* 19 (19. (1998), 63-67.

GURTWIRTH, S./ POULLET, Y/ ET ALT, *Computers, Privacy and Data Protection: an Element of Choice*, Springer, 2011.

GUTIÉRREZ, F.J./ HORRILLO, M. C./ SAYAGO, I/ ET ALT, *Electronic olfactory nano-microsystems for recognition in biometrics*, presentación en el congreso WISTP- Sevilla, mayo de 2008.

GUTMANN, P. "Why biometrics and RFID are not a panacea (A Comedy of Errors, in Three parts)", Universidad de Auckland, 2007. http://www.cs.auckland.ac.nz/~pgut001/pubs/biometrics.pdf

GUTWIRTH, S: "Beyond identity?", IDIS – Identity in the Information Society, Vol. 1, n.º 1, 2009, pág. 122-133.

GUTWIRTH, S. 'Biometrics between opacity and transparency', Ann Ist Super Sanità 2007, pp. 61–65.

GUTWIRTH, S. *Privacy and the information age*, Oxford, Rowman & Littlefield, 2002.

GUTWIRTH, S./ GELLERT, R./ BELLANOVA, R./ FRIEDEWALD, M./ SCHÜTZ, P./ WRIGHT, D./ MORDINI E/VENIER, S. *Legal, social, economic and ethical conceptualisations of privacy and data protection*, Prescient, D.1, 23.03.2011, disponible en http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

GUTWIRTH, S./ POULLET, Y./ DE HERT, P./ DE TERWANGNE, C./ NOUWT, S. (eds.), *Reinventing DataProtection?* Springer, 2009, 352 p.

GUTWIRTH, S./ POULLET, Y./ DE HERT, P./ LEENES, R. Computers, *Privacy and Data Protection: an Element of Choice*,

Springer, 2011.

HÄBERLE, H.: *La garantía del contenido esencial de los derechos fundamentales*, Dykinson, Madrid, 2003.

HACKING, I. *The taming of chance*, Cambridge, Cambridge University Press, 1990, pp 186-188.

HACKING, I.: *The taming of chance*, Cambridge, Cambridge University Press, 1990.

HAIDT, R: "Review of: Juliet McMaster, Reading the Body in the Eighteenth-Century Novel", Eighteenth-Century Fiction, vol 20(1), 2007, pp257ss.

HALLER, J. S.: *Outcasts from evolution: scientific attitudes of racial inferiority*, 1859-1900, SIU Press, 1995.

HALPERIN, R/ BACKHOUSE, J. (eds.), *A qualitative comparative analysis of citizens' perception of eIDs and interoperability*, Frankfurt, FIDIS, 2009.

HAMMARBERB, T. *Informe Temático sobre Derechos Humanos e Identidad de Género*, Ed TvT,, Berlin, 2010. Acceso en www.transinterqueer.org

HAN, H./ JAIN, A. K. "Tattoo based identification: Sketch to image matching", Proceedings of the International Conference on Biometrics Compendium, pp. 1-8, 2013 (http://www.cse.msu.edu/biometrics/Publications/SoftBiometrics/HanJain_TattooBasedIdentification_Sketch2ImageMatching_ICB13.pdf)

HANK, K./ JÜRGES,H./ SCHAAN, B. „Die Erhebung biometrischer Daten im Survey of Health, Ageing and Retirement in Europe. Befunde und Perspectiven", *Methoden – Daten-Analysen*, 2009, 3(1), pp97ss.

HANSEN, M.: "Biometrie in der Zeiten von eIDs, Social Networks und Cloud Computing – die Datenschutzsicht", Workshop *Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen*, Berlin, 2012.

HAO, Y./ R. FOSTER, "Wireless body sensor networks for health-monitoring applications", Physiological Measurement 29 (11), 2008, pp27-56.

HARB, B./ SCHMID, D.: "Der Einsatz biometrischer Systeme". Verfassungsrechtliche Aspekte und Umsetzung der datenschutzrechtlichen Anforderungen beim Einsatz von Biometrie", *DIGMA - Zeitschrift für Datenrecht und Informationssicherheit*, 5 (4), Zürich, diciembre de 2005, pp. 158 a 161.

HARMON, L. D./ KHAN, M. K./ LASCH, R./ RAMIG, P. F. "Machine recognition of human faces", *Pattern Recognition,* 31(2), 97–110, 1981.

HARVATI, K./ T. D. WEAVER, *Human cranial anatomy and the Differential Preservations of Population History and Climate Signature*, 2006.

HAUSKELLER, C.: "Genes, genomes and identity. Projections on the matter", New Genetic Society 2004, 23 (3), pp. 285 a 299.

HAYES, B. 'There is no "balance"between security and civil liberties – just less of each', en *Essays for civil liberties and democracy in Europe,* 2006, disponible en http://www.ecln.org/essays/ essay-12.pdf

HAYS, B/ VERMEULEN, M. *Borderline. The EU's New Border Surveillance Initiatives. Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders"Proposals*, Heinrich Böll Foundation, 2012. Disponible en http://www.statewatch.org/ news/2012/jun/borderline.pdf

HENNESSY, R.J./ MCLEARIE S./ KINSELLA A/ WADDINGTON, J.L. 2006. "Facial shape and asymmetry by three dimensional laser surface scanning covary with cognition in a sexually dimorphic manner", *J Neuropsychiatry Cli Neurosci*, 18: 73-80.

HERNÁNDEZ VILLALÓN, Y.: "Situación actual del derecho de asilo en la Unión Europea", Revista Jurídica de la Comunidad de Madrid, nº15, 2003.

HERO, K. Der genetische und der daktylische Fingerabdruck- eine vergleichende Analyse im Lichte des Rechts auf informationelle Selbstbestimmung, Verlag Alma Matter, 2012, p38.

HERRANZ, J. "La biometría y su repercusión en los datos de carácter personal", *Computing*, 2010.

HEUMANN, B.: *Whitepaper Biometrie*, www.biometrie-online.de, 2006.

HIJMANS, H. 'Recent developments in data protection at European Union level', ERA Forum 2010, pp. 219–231,disponible en http://www.springerlink.com/content/55v28703k0401j06/?p=8deefc2e6fe44277952aa80998026 d61&pi=1

HILDEBRANDT, M. "*Profiling* and the Identity of European Citizens", en: RANNENBERG, K./ ROYER, A./ DEUKER, A. (eds.), *The future of identity in the information society: challenges and opportunities,* Springer, 2009, p274.

HILDEBRANDT, M./ BACKHOUSE, J. (eds.), D. 7. 2. Descriptive analysis and inventory of profiling practices, Frankfurt, FIDIS, 2005.

HILDEBRANDT, M.: "Defining Profiling: A New Type of Knowledge?", en Hildebrandt, M./ Gutwirth, S. (eds.) Profiling the European Citizen, Cross-Disciplinary Perspectives, Springer, 2008.

HILDEBRANDT, M.: "Privacy and identity", en E. CLAES. A. DUFF. S. GUTWIRTH (eds.). *Privacy and the criminal law* (pág. 43-57). Amberes: Interscientia. Oxford: Hart Pub, 2006.

HILDEBRANDT, M.: "Profiling and Am I", en K. RANNENBERG. D. ROYER. A. DEUKER (eds.). *The future of identity in the information society: challenges and opportunities*, Springer, 2009, pp273ss.

HILDEBRANDT, M./ S. GUTWIRTH (eds*.), Profiling the European Citizen. Cross – Disciplinary Perspectives*, Springer, 2008.

HILL, C. *Risk of Masquerade Arising from the Storage of Biometrics*, 2001, Australian National University.

HINDE, S. '2001: A privacy Odyssey Revisited', Computers & Security 2002, pp. 16–34, disponible en http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/h/Hinde:Stephen.html

HIROBAYASHI, S./ TAMURA, Y/ YAMABUCHI, T./ YOSHIZAWA, T. "Verification of individual identification method using bioelectric potential of plant during human walking", *Japanese Journal of Applied Physics* 2007, 46(4A): 1768–1773.

HOCKING, R. R. "A Biometrics Invited Paper: the Analysis and Selection of Variables in linear regression", *Biometrics. International Biometric Society*, vol. 1/32, 1976, pp1-49.

HOERNLEIN, M. 'Unites States Visitor and Immigrant Status Indicator Technology Program', en Coats, W./ Bagdasarian, A./ Helou, T/ Lam, T. (eds.), The Practitioner ' s Guide to Biometrics, Chicago, ABA, 2007, pp. 37–47.

HOF, S.: "E-Voting and Biometric Systems?", en las Actas de *Electronic Voting in Europe - Technology, Law, Politics and Society*, Workshop of the ESF TED Programme together with GI and OCG, 2004.

HOOGSTRATE, A. J./ VAN DEN HEUVELM H./ HUYBEN, E.: "Ear identification based on surveillance camera images", *Sci Justice* 2001, 41 (3), pp167-172.

HORNUNG, G. 'The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards', SCRIPTed 2007, pp. 246–262, disponible en http://www2.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp

HORNUNG, G. 'The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards', SCRIPTed 2007, pp246ss, http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp

HORNUNG, G.: "Biometrische Systeme - Rechtfragen eines Identifikationsmittels der Zukunft", Kritische Justiz 2004.

HORNUNG, G.: *The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, SCRIPTed 2007, p246 y ss.

HORNUNG, G./ STEIDLE, R.: "Biometrie am Arbeitsplazt – sichere Kontrolverfahren versus ausuferndes Kontrollpotential", Arbeit und Recht (AuR) 6/2005, p201, 203 y ss.

HOSHEIN, G.: "Privacy as Freedom", en R. F. Jorgensen (ed.), *Human Rights in the Global Information Society*, MIT Press, Cambridge, 2006, pp121 y ss.

HSIAO, H./ WHITESTONE, J./ WILBUR, M./ ROGER, J. LACKORE/ ROUTLEY, J. G. "Seat and seatbelt accommodation in fire apparatus: Anthropometric aspects", *Applied Ergonomics* 51 (2015), 137-151.

HUGENHOLTZ, P. "The New Database Right: Early Case Law from Europe", ponencia presentada en la *Ninth Annual Conference on International IP Law & Policy*, Fordham University School of Law, New York, 19–20 de abril 2001, disponible en http://www.ivir.nl/medewerkers/hugenholtz.html

HUIJGENS, R.: en EUROPEAN COMMISSION (ed.), *Biometrics in Europe. Trend Report*, UNISYS – European Biometrics Portal, 2007,pp20-21.

HURLEY, D. J./ NIXON, M. S./ CARTER, J. N. "Force Field energy functionals for image feature extraction", Image and Vision Computing 20, 2002, pp311-317.

IAMICELLI, P.: "Liceitá, corretteza, finalitá nel trattamento dei dati personali", en R. Pardolesi (ed.), *Diritto alla riservatezza e corcilazione dei dati personali*, Giuffré, Milano, 2003, pp480 y ss.

IANNARELLI, A. *Ear Identification*, Forensic Identification Sciences, Paramount Publishing Company, 1989.

ILLIES, M.: "La política de la Comunidad Europea sobre inmigración irregular: medidas para combatir la inmigración irregular en todas sus fases", *Documento de Trabajo 38/2009* del Real Instituto Elcano, Madrid. Disponible en www.realinstitutoelcano.org

INSPASS US Department of Homeland Security 2010. US Department of Homeland Security. *New biometric technology improves security and facilitates U.S. entry process for international travellers*. https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-fingerprint_consumer_friendly_content_1400_words.pdf.

INTERNATIONAL BIOMETRIC GROUP, Biometrics Market and Industry Report 2009 – 2014, 2008.

INTERNATIONAL BIOMETRICS GROUP (IBG), *How is "Biometrics"defined?*, en *Biometrics explained*, 2001.

INTRONA, L. D./ NISSENBAUM, H, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, The Centre for Catastrophe Preparedness and Response, New York University, Oct, 2009.

INTRONA, L. D./ NISSENBAUM, H. *Facial Recognition Technology. A Survey of Policy and Implementation Issues*, Center for Catastrophe Preparedness and Response, New York University, 2009, pp9-10.

IPTS - Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, European Commission, 2003.

IRISH COUNCIL FOR BIOETHICS, *Biometrics: Enhancing security or invading privacy?* Opinion, 2009. Disponible en http://www.scribd.com/doc/81418299/Irish-Council-for-Bio-Metrics

IRISH COUNCIL FOR BIOETHICS, *Human biological material: Recommendations for Collection, Use and Storage in research*, 2005. Disponible en http://irishpatients.ie/news/the-vault/bioethics/ human-biological-material-recommendations-for-collection-use-and-storage-in-research-2005/

IRVINE, J.M./ ISRAEL, S. A./ SCRUGGS, W. T./ WOREK, W. J. "Eigenpulse: Robust human identification from cardiovascular function", *Pattern Recognition* 2008, 41(11): 3427–3435.

IRWIN, J. O. "Biometric method: past, present, future", Biometrics, 1959, nº 15, pp363ss.

ISARIS, N. (Deputy Head of Unit, DG Home Affairs, Unit C3 Large-scale IT Systems and Biometrics, European Commission (ed.), "Biometrics in EU border controls: The move towards smarter borders", Biometrics Conference, 2012.

ISLAM, R./ SAYEED, S./ SAMRAJ, A. "Biometric Template Protection Using Watermarking with Hidden Password Encryption", *IT Sim* 2008, p296.

ISO 2006a. Citado por BUSCH, C.: "Biometrische Verfahren – Chancen, Stolpersteine und Perspectiven", en P. SCHAAR, cit. 2007, p29. TELETRUST DEUTSCHAND, G. LASSMAN, *Bewertungskirterien zur Vergleichbarkeit Biometrischer Verfahren*, 2002.

ISO/IEC JTC 1/SC 37, Standing Document 2 – Harmonized Biometric Vocabulary, version 12, N 3385, New York, ANSI, 2009.

ISO/IEC JTC 1/SC 37, Text of Working Draft 24779-1, *Cross-jurisdictional and societal aspects of implementation of biometric technologies – Pictograms, icons and symbols for use with biometric systems* – Part 1: Overview, N 3363, New York, ANSI, 18 de agosto de 2009.

ISO/IEC JTC 1/SC 37, Text of Working Draft 24779-2, *Cross-jurisdictional and societal aspects of implementation of biometric technologies – Pictograms, icons and symbols for use with biometric systems – Part 2: Fingerprint applications*, N 3363, New York, ANSI, 2009.

ISO/IEC: Information technology – Biometrics tutorial. *ISO/IEC TR 24741:2007(E)*. 2007.

ISRAEL, S./ ET AL. "ECG to identify individuals", *Pattern Recognition*, 2005. doi: 10.1016/j.patcog.2004.05.014.

ITU-T TECHNOLOGY WATCH REPORT, *Biometrics and Standards*, Dresde, 2009.

ITU-T, *Biometrics and Standards,* 2009, p5.

JAFFREDO, F./ F. FREUND/ S. GODICHAUD/ M. GABOYARD/ J. O. MOISAN, Complete automated DNA procedure to facilitate DNA database collection, Forensic Science International: Genetic Supplement Series, 3 (2011), e228-e229.

JAIN, A. K. *Introduction to Biometrics*, Springer, 2011.

JAIN, A. K./ FLYNN, P./ ROSS, A. A. *Handbook on Biometrics*, Springer, 2008.

JAIN, A. K./ BOLLE, R/ PANKANTI, S.: *Personal Identification in Networked Society*, Kluwer, 1999.

JAIN, A. K./ DASS, S. C./NANDAKUMAR, K. "Soft biometric traits for personal recognition systems", *Proceedings of International Conference on Biometric Authentication*, Hong Kong, 2004, 731–738.

JAIN, A. K./ FLYNN, P./ ROSS, A. (eds.), *Handbook of Biometrics*, Springer, Boston, MA, Springer, 2008.

JAIN, A. K./ K. Nandakumar, "Biometric System Design - Overview", S. Z. Li/ A. K. Jain, *Encyclopedia of Biometrics*, Springer, consultada la edición de 2009, p135.

JAIN, A. K./ KUMAR, A. "Biometrics of Next Generation: an Overview", en E. MORDINI/ D. TZOVARAS (eds.), *Second Generation Biometrics*, Springer, Heidelberg, 2010.

JAIN, A. K./ NANDAKUMAR, K. "Biometric System Desing. Overview", S. Z. LI/ A. K. JAIN, E*ncyclopaedia of Biometrics*, Springer, consultada la edición de 2009, pp135-136.

JAIN, A. K./ NANKUMAR, K./ NAGAR, A.: "Biometric Template Security", *EURASIP Journal onf Advances in Signal Processing* 2008, pp1-17

JAIN, A. K./ PANKANTI, S./ PRABHAKAR, S./ ET ALTERE: "Biometrics: A Grand Challenge", *Proceedings of International Conference on Pattern Recognition*, Cambridge, UK, 2004.

JAIN, A. K./ PANKATI, S./ ET ALTERE, "Biometrics: a Grand Challenge", *Proceedings of the International Conference on Pattern Recognition*, Cambridge, UK, 2004.

JAIN, A. K./ PARK, U. "Facial marks: Soft biometric for face recognition", *Proceedings of the International Conference on Image Process*, Cairo, Egipto, 2009.

JAIN, A. K./ PRABHAKAR, S./ PANKANTI, S. 'On the similarity of identical twin fingerprints', *Pattern Recognition*, 35, no. 11, noviembre de 2002, pp. 2653–2663

JAIN, A. K./ ROSS, A. voz "Biometrics"en la *Enciclopedia of Cryptography and Security*, Springer, 2005, p. 34-36.

JAIN, A. K././ ROSS, A./ PRABHAKAR, "Fingerprint Matching Using Minutiae and Texture Features", en P*roceedings of the International Conference on Image Processing*, IEEE Computer Society Press, Los Alamos, 2001, pp282-285.

JAIN, A. K./BOLLE, R./ PANKATI, S. *Introduction to biometrics*, en JAIN, A./ ET AL. (eds.) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.

JAIN, A. K./FENG, J. 'Latent Palmprint Matching', 31 IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 6, 2009, pp. 1032–1047,disponible en http://www.computer.org/portal/web/csdl/doi?doc=doi/10.1109/TPAMI.2008.242

JAIN, A. K./HONG L,/ BOLLE R "On-line fingerprint verification", *IEEE Trans Pattern Anal Mach Intell* 1997, 19:302–314. doi:10.1109/34.587996.

JAIN, A. K./NANDAKUMAR, K./ NAGAR, A. 'Biometric template security', *EuRASIP journal on Advances in Signal Processing* 2008.

JAIN, A.K./ ROSS, A./ PRABHAKAR, S. "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology* (IEEE Magazine), vol. 14. nº, 2004, pp4-5.

JAIN, A.K./PANKANTI, S. 'Beyond Fingerprinting. Security systems based on anatomical and behavioural characteristics may offer the best defense against identity theft', in Scientific American 2008, pp. 78–81.

JASINSKA, E. "Biometrie und Datenschutz"Proseminar Informationelle Selbstbestimung bei Peter Bitttner, Humboldt Universität zu Berlin, 2005.

JAY, R. *Data protection: law and practice*, London, Sweet and Maxwell, 2007.

JAYAPRAKASH, P. T. "Practical relevance of pattern uniqueness in forensic science", *Forensic Science International* 231 (2013), pp403e1 – 403e16.

Johansson, G. Visual motion perception, Scientific American, 1975, pp75-88.

JOHNSON, I. 'Theft of Biometric Data: Implausible Deniability',enCoats, W./ Bagdasarian, A./ Helou T/ Lam T. (eds.), The Practitioner ' s Guide to Biometrics, Chicago, ABA, 2007, pp. 79–86.

JONES, K. L./ JONES, M. C./ DEL CAMPO, M. *Smith's Recognizable Patterns of Human Malformation*, 7ª ed, ELSEVIER, 2013.

JONIETZ, E.: "Boosting Biometrics", *Technology Review*, 107 (5), 2004, pp20-21

JORGENSEN, C./ DUSAN, S. "Speech interfaces based upon surface electromyography", *Speech Communication* 52, nº 4 de 2010, pp354–366.

JOSHI, A.J./ CHANDRAN, S./ JAYARAMAN, V. K./ KULKARNI, B. D. "Arterial pulse rate variability analysis for diagnoses", *Proceedings of ICPR*, 2008, Tampa, FL, 1–4.

JUELS, A. MOLNAR, D/ WAGNER, D. *Security and Privacy Issues in E - passports*, 2005. Disponible en http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1607561&url=http %3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1607561

JUUL, N. C. *Recommendation on the Use of Biometric Technology*, en CAMPISI (ed.), *Security and Privacy*, 2013, p415ss.

KALLIES, *Biometrische Erkennungssysteme*, 2007.

KAPIL ET ALTERE, *Morphological Variation of Ear for Individual Identification in Forensic Cases*, 2013.

KARELITZ, S./ FISICHELLI, V. R: "The cry thresholds of normal infants and those with brain damage", *J. Pediat,* 61, 1962, 679-685.

KAUFER, B. *History of the finger-printing system*, 1912, Smithsonian Institution Annual Report – consultado en su reimpresión en *The Print*, vol 16 (2), 2000, pp1-13.

KAYE, D. 'Two fallacies About DNA Data Banks for Law Enforcement' 67 *Brooklyn Law Review*, 2001, pp. 179206, disponible en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=301650

KELLOKUMPU, V./ ZHAO, G./ LI, S.Z. et al. "Dynamic texture based gait recognition", *Proceedings of the ICB 2009,* Alghero, Italia, 2009, p1000–1009.

KENT, S./ MILLETT, L. (eds.), *Who goes there? Authentication Through the Lens of Privacy*, National Research Council, 2003.

KERSHAW, *Lawyer Linked to Bombing is Released*, New York Times, 20 de mayo de 2004 (por presunta coincidencia de las huellas de Brandon Mayfield con unas halladas en Madrid, en los atentados de 2004).

KIECKHOEFER H, INGLEBY M, LUCAS G. "The physical formation of ear-prints: optical and pressure mapping evidence", *Fearid report* 2. Work-package 2. University of Huddersfield, UK, 2003.

KINDT, E. 'Best Practices for privacy and data protection for the processing of biometric data' en CAMPISI, F. (ed.), *Security and Privacy in Biometrics*, Springer, 2013, pp. 339–366.

KINDT, E. 'Biometric applications and the data protection legislation' en B Havani, M. (ed.), *Biometrics. Techno - Legal Issues,* Hyderabad, India, ICFAI University Press, 2008, pp. 170–182.

KINDT, E. 'Biometric applications and the data protection legislation. The legal review and the proportionality test, *DuD* 2007, pp. 166–170.

KINDT, E. 'Need for Legal Analysis of Biometric Profiling', Reply to V/ronikou, A. Yannopoulos, Th. Varvarigou, 'Biometric Profiling: Opportunities and Risks',enM. Hildebrandt and S. Gutwirth (eds.), *Profiling the European Citizen. Cross – Disciplinary Perspectives*, Springer, 2008, pp. 139–144.

KINDT, E. 'The use of privacy enhancing technologies for biometric systems analysed from a legal perspective'enBezzi, M./ Duquenoy, P./ Fischer-Hübner, S./ Hansen, M/ Zhang, G. (eds.), Privacy and Identity Management for Life, Berlin – New York, Springer, 2010, pp. 134–145.

KINDT, E. "Biometric applications and the data protection legislation (the legal review and the proportionality test)", *Datenschutz and Datensicherheit (DuD)*, 31/ 2007, pp166ss.

KINDT, E. *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013.

KINDT, E./ DUMORTIER, J. Summary of legal data protection requirements for the processing of biometric data, European Biometrics Portal, 2005.

KINDT, E./ HILDEBRANDT, M. 'Vulnerabilities of the present legal framework regarding BBP', en HILDEBRANDT, M. (ed.) *Behavioural biometrics profiling and transparency enhancing tools*, 2009, pp. 38–46.

KINDT, E./ LIEVENS, E./ KOSTA, E./ LEYS, TH/ DE HERT, P. 'Constitutional rights and new technologies in Belgium', en LEENES, R./ KOOPS, B.-J./ DE HERT, P. (eds.), *Constitutional Rights and New Technologies. A Comparative Stud*y, The Hague, Asser, 2008, pp. 11–55.

KINDT, E./ MÜLLER, L. (eds.), *Biometrics in identity management*, Frankfurt, FIDIS, 2007.

KINDT, E./ MÜLLER, L/ MEINTS, M. 'Biometrics', en RANNENBERG, K./ ROYER, D./ DEUKER, A. (eds.), *The Future of Identity in the Information Society – Challenges and Opportunities*, Dordrecht, Springer, 2009, pp. 138–148.

KISKU, D. R./ GUPTA, P./ SING, J. K. *Advances in Biometrics for Secure Human Authentication and Recognition*, CRC press, 2014, pp9-10.

KIZZA, J. M. "Ethical, and Social Issues in the Information Age", *Texts in Computer Science*, 2010, p287.

KLEIST, V./ FRANKE, R. A./ PEARSON, T. A. "Evaluating Biometric as Internal Control Solutions to Organizational Risk", *Journal of American Academy of Business*, 6 (2), 2004, pp339-344.

KLINK, A.: "Die Anforderungen der ICAO an Reisedokumente mit Biometrie", Seminario *Biometrische Systema am Facharbeit Informatik der Technischen Universitat Darmstadt*, 2005.

KNIGHT, A./ SAXBY, S. "Identity crisis: Global Challenges of identity protection in a networked society", *Computer Law and Security Review* 30 (2014), pp617-632.

KOMMERS, D.P./ FINN, J. E./ JAKOBSON, G. J. *American Constitutional Law: Essays, Cases and Notes*, 3ª ed, Rowans & Littlefield, 2009.

KONG, A./ ZHANG, D/ KAMEL, M. 'Three measures for secure palmprint identification', en Pattern Recognition 2008, pp. 1329–1337.

KOOPS, B.-J./ LEENES, R.: "'Code' and the Slow Erosion of Privacy", *Michigan Telecommunications & Technology Law Review* 12 (2005), 1, pp115-188.

KOOPS, B.-J/ DE HERT, P. (eds.), *Constitutional Rights and New Technologies. A Comparative Study*, The Hague, Asser, 2008, pp. 159–197.

KORFF, D. *Automated processes of identification, behavioural analysis and risk detection, Paper and presentation at Security, privacy and data protection seminar*, organizado por la Agencia Española de Protección de datos, 9-11 de junio de 2010.

KORFF, D. *Comparative Study on Different Approaches to new privacy challenges, in particular in the light of technological developments*, Working Paper N° 2: Data protection laws in the EU: the difficulties in meeting the challenges posed by global social and technical developments, 20 de enero de 2010, Brussels, European Commission. Disponible en http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf

KOROTKAYA, Z.: "Biometrics Person Authentication: Odor", 2003. http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf

KORTE, U./ MERKLE, J./ NIESING, M. 'Datenschutzfreundliche Authentisierung mit Fingerabdrücken. Konzeption und Implementierung eines Template Protection Verfahrens – ein Erfahrungsbericht', *DuD* 2009, pp. 289–294.

KROENFELD, P. "Gross anatomy and embryology of the eye", EN H. DAVIDSON (ed.) *The Eye*, Academic, London, 1962.

KUDYBA/ KWATINETZ, Introduction to the Big Data Era. In S. Kudyba (Ed.), *Big Data, Mining, and Analytics*, Boca Raton (FL): CRC Press, 2014, p.1-15.

KUHN, M.: "Security-Biometric identification", University of Cambridge, 2003.

KUMAR, A./ S. SHEKHAR, "Personal identification using multibiometrics Rank-level fusion", *IEEE Transactions on Systems, Man and Cybernetics,* Part C: Applications and Reviews, 41 (5), 743-754, 2011.

KUMAR, A./ RAVIKANTH, CH. "Personal authentication using finger knuckle surface", *IEEE Transactions on Information Forensics and Security*, 2009, 4(1): 98–110.

KUMAR, A./ ZHOU, Y. "Human identification using knuckle codes", *Proceeding of BTAS* 2009.

KUMAR, A/ WONG, DAVID. C. M/ SCHEN, H. C./ JAIN, A. K. : "Personal verification using Palmprint and Hand Geometry in Biometrics", en J. KITTLER/ M. S. NIXON (eds.), *Proceedings fo the 4th International Conference on Audio- and Video-Based Biometric Personal Authentication*, Springer, Berlin, 2003, pp1-8.

KYOSO, M. "Development of an ECG identification system", en *Proceedings of 23rd Annual International IEEE Conference of Engineering in Medicine and Biology Society*, 2001, 4: 3721–3723.

LAFFAIRE M.-L/ ELM, T. 'Biometrie, la première décision d'une longue série', *Expertises* 2005, pp299ss.

LANGENDERFER, J./ S. LINNHOFF, "The Emergence of Biometrics", *Journal of Consumer affairs*, vol 39, nº 2, 2005, pp322.

LANITIS, A. "A survey of the effects of ageing on biometrical identity verification", *International journal of Biometrics*, 2 (1), 2010, pp34-52.

LANITIS, A./ N. TSAPATSOULIS, "Quantitative evaluation of the effects of aging on biometric templates", *IET Computer Vision Journal, Special Issue on Future Trends in Biometric Processing,* vol 5, issue 6, pp228-347.

LAWSON, W. J.: *Enhancing Assistive Technologies: Through the Theoretical Adaptation of Biometric Technologies to People of Variable Abilities*, Kennedy-Western University (School of Business – Dissertation), 2003.

LAZARAKOS, C.: "Biometrics: Protection of personal data through the processing of sensitive (personal) information", *PoinDik* 2001, pp1165ss

LEE, J.-E./ JAIN, A. K./ JIN, R. "Scars, marks and tattoos (SMT): Soft biometric for suspect and victim identification", *Proceedings of the Biometric Symposium, Biometric Consort Conference*, Tampa, Florida 2008.

LEPAGE, A. 'La Biometrie refoulée de l'entreprise', Comm. Comm. Electronique 2005, no 164, pp. 46–48.

LeVay, S. Queer Science: the use and Abuse of Research in to Homosexuality, MIT Press, Cambridge, 1996.

LEVY, L. W: "Unenumerated Rights", en L. W. LEVY/ K. W. KARST, *Encyclopedia of the American Constitution*, MacMillan, 2000, pp2752-2754.

LEWONTIN, R.C./ ROSE, S./ KAMIN, L. *Not in our genes*. New York: Pantheon Books, 1984.

LEXIS, W.: "Anthropologie und Anthropometrie", en J. CONRAD/ ET ALTERE (eds.), *Handwörterbuch der Staatswissenschaften*, vol I,, 1906, pp523-544.

LI, K. P./ DAMMANN, J. E./ CHAPMAN, W.D. "Experimental studies in speaker verification using an adaptive system", *J. Acoust. Soc. Am*., 1966, 40, 966–978.

LI, S. (ed.), *Encyclopedia of Biometrics*, Springer, 2009.

LI, X. "Modeling Intra-class variation for Nonideal iris recognition", en D. Zhang/ A. K Kain, eds, ICB 2006, LNCS 3832, pp419-427, 2005.

LIBERATORE, A. *Balancing Security and Democracy: the Politics of Biometric Identification in the European Union*, European University Institute, Working Paper RSCAS No. 2005/30, 2005.

LIBERTY (National Council for Civil Liberties): "*Memorando de LIBERTY*"en HOUSE OF LORDS – SELECT COMMITTEE ON THE CONSTITUTION. *Part. 1. Borders, Citizens and Immigration Bill Report*, 2009, pp103ss.

LIBERTY ALLIANCE PROJECT, White paper: Personal Identity, 23 De marzo de 2006, previously disponible en http://www.projectliberty.org/liberty/content/view/full/340/(offset)/30

LINVILLE, S. E. "The aging voice", The ASHA Leader, 9 819), 2004, pp12-21.

LIU-JIMENEZ, J./ SANCHEZ-REILLO, R. "Ageing in iris biometrics", *Age Factor*, 2014, p149.

LIU, F./ F. VAN DER LIJN/ C. SCHURMAN/ ET ALT, "A Genome-wide Association study Identifies Five Loci influencing Facial Morphology in Europeans", *P Los Genetics*, 2012, 8(9).

Liu, J. The principle of proportionality in biometrics, *Computer Law & Security R*., 25, 2009,, p239.

LIU, Y. 'Identifying Legal Concerns in the Biometric Context', *Journal of International Commerical Law and Technology*, 2008, pp. 45–54.

LIU, Y. 'The principle of proportionality in biometrics: Case studies from Norway', *Computer Law & Security Review* 2009, pp. 237–250.

LIU, Y. "Privacy Regulations on Biometrics in Australia", *Computer Law & Security Review* 26, 2010, 355-367, p357.

LLANOS, M.: "Modelos: riesgo, profesión y vacío legal", *Trastornos de la Conducta Alimentaria* 5/ 2007, páginas 507 a 543.

LODGE, J. (ed.), Are you who you say you are? The EU ad Biometric Borders, Nijmegen, Wolf Legal Publishers, 2007.

LOESCH, D. Z./ M. LAFRANCHI/ D. SCOTTE, "Anthropometry in Martin-Bell Syndrome", *American Journal of Medical Genetics* 1988, 30 (1-2), 149-64.

LONDON ECONOMICS, STUDY ON THE ECONOMIC BENEFITS OF PRIVACY-ENHANCING TECHNOLOGIES (PETS). *Final Report to the European Commission DG Justice, Freedom and Security*, Julio 2010. Disponible en http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

LÓPEZ CARVAJAL, J./ GONZÁLEZ PATIÑO, J.: "Estado del arte: reconocimiento automático del iris humano", en *Sciencia et Technica*, año XI, nº 29, diciembre de 2005, pp77ss.

LÓPEZ CARVAJAL, J./ LÓPEZ PATIÑO, J. "Estado del arte: reconocimiento automático del iris humano", *Scientia et Technica* Año XI, No 29, Diciembre de 2005, p77-80.

LÓPEZ GONZÁLEZ, J. I. E*l principio de proporcionalidad en Derecho Administrativo*, 1988, Sevilla, pp. 76 y ss.

LÓPEZ SALA, A.: *Inmigrantes y Estados. La respuesta política ante la cuestión inmigratoria*, Anthropos, Barcelona, 2005.

LOPUCKI, L.M. "Human Identification Theory and the Identity Theft Problem", *Texas Law Review* 89, 2001-2002, pp89-122.

LORENTE ACOSTA, J. A/ LORENTE ACOSTA, M.: *El ADN y la identificación en la investigación criminal y en la paternidad biológica*, Ed. Comares, Granada, 1995.

LOWRY, H. 'Transborder Data Flow: Public and Private International Law Aspects', *Houston Journal of International Law*, 1984, pp.159–174.

LRDP Kantor and Centre for Public Reform, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final report, Brussels, European Commission, 20.01.2010.

LU, J./ ZHANG, E, "Gait recognition for human identification based on ICA and fuzzy SVM through multiple views fusion", *Pattern Recognition Letters* 28, 2007, 2401-2411.

LU, S/ JAIN, A. 'Ethnicity identification from face images' en Proceedings SPIE Defense and Security Symposium, Orlando, 2004. Disponible en http://www.cse.msu.edu/biometrics/Publications/Face/LuJain_EthnicityFace_SPIE04.pdf

LUCAS, A./ DEVEZE, J./ FRAYSSINET, J.: *Droit de l'informatique et de l'Internet*, Editions Presses Universitaires de France, Collection Themis, Paris, 2001.

LUCAS, P. "Biometrics Come into Focus", *Collections & Credit Risk*, 10 (3), 2005, pp18-21

LUCK, J. "Automatic speaker verification using spectral measurements", *J. Acoust. Soc. Am*., 1969, 46, 1026–1031.

LUSOLI, W./ COMPAÑÓ, R./ MAGHIROS, I. *Young People and Emerging Digital Services. An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks*, Sevilla, European Commission, JRC, 2009, 86 p,disponible en http://ftp.jrc.es/EURdoc/JRC50089.pdf

LUTTGENS, K./ K.WELLS, *Kinesiology: Scientific Basis of Human Motion*, Saunders College Publishing, 7th ed, 1982.

LYON, D. "Surveillance as social sorting: computer codes and mobile bodies", en D. Lyon (ed.), *Surveillance as social sorting: privacy, risk and automated discrimination*, Routledge, London, 2003, pp13-31.

LYON, D.: *La societá sorvegliata. Tecnologie di controllo della vita cuotidiana*, Feltrinelli, Milan, 2002.

BUTLER, M. G./ A. BRUNSCHWIG/ L. K. MILLER/ R. J. HAGERMAN, "Standards for selected anthropometric measurements in males with the fragile X syndrome", *Paediatrics* 1992, 89 (6ª parte), 1059-1062.

SÁNCHEZ VIGIL, J. M./, B. FERNÁNDEZ FUENTES, "La fotografía como documento de identidad", *Documentación de las Ciencias de la Información*, 2005, vol 28, pp189-195.

MADUREIRA, N. "Policía sin ciencia: la investigación criminal en Portugal: 1880-1936", *Política y Sociedad,* 2005, Vol. 42, núm. 3, pp45-62.

MAGNET, S. A. *When Biometrics Fail: Gender, Race and the Technology of Identity,* 2011.

MALEY, J. R./ O. NARODITSKY/ K. HANNA/ R. KOLCYNSKI/ D. J. LOIACONO/ S MANGRU/ M. TINKER/ T ZAOOIA/ W. Y. ZHAO, "Iris on the move: Acquisition of Images for Iris Recognition in Less Constrained Environments", *Proceedings of the IEEE*, 2006, pp1936-1947.

MALTONI, D./ MAIO, D./ JAIN, A./ PRABHAKAR, S. *Handbook of Fingerprint Recognition*, London, Springer, 2009.

MANDERS-HUITS/ VAN DER HAREN, "Moral identification in identity management systems", en IFIP – INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING, *The Future of Identity in the Information Society*, 262, 2009, pp77-91.

MANSFIELD-DEVINE, S. "Social Identity: is biometric technology on social networks a benefit of a threat?", *Biometrics Technology Today*, Noviembre/ Diciembre de 2012.

MANSFIELD, A/ J. WAYMAN, *Best Practices in Testing and Reporting Performance of Biometric Devices*, 2002.

MARCEL, S./ MILLÁN, J. "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2007. doi: 10.1109/TPAMI.2007.1012

MARCIALIS, G./ A. RATTANI/ F. ROLI, "Biometric template update: An experimental investigaction on the relationship between update errors and performance degradation in face verification", en N. DA VITORIA/ T. KASPARIS (EDS.), *Structural, Syntactic and Statistical Pattern Recognition*, Springer, 2008, pp684-693.

MARET, S.: "Biométrie et Mobilité. Commen concilier facilité d'utilisation et securité? », *B&F*, Mai-Jun 2009, pp62-63.

MARINO, T. M. *Tecnologías biométricas aplicadas a la seguridad*, Alfaomega, 2005. SUÁREZ RUIZ/ FAJARDO PITO/ TIBADUIZA, "Autentificación de Personas a partir de la Biometría de las Venas de la parte posterior de la manos", *Revista Colombiana de Tecnologías Avanzadas*, nº 12, 2008, pp62ss.

MARSHALL BARBERÁN, P. "Los derechos fundamentales como valores", *Revista Telemática de Filosofía del Derecho*, nº 10, 2006/ 2007, pp207-228, 215.

MARTÍNEZ JARRETA, M. B. voz "*Biometría*", C. M. ROMEO CASABONA (dir.), *Enciclopedia de Bioderecho y Bioética*, vol I,Comares, 2011, pp257-261.

MART*ÍNEZ* MOYA, J. "El tiempo de trabajo: una visión jurisprudencial", *Revista del Ministerio de Trabajo y Asuntos Sociales*, nº 38, pp. 83ss.

MASEK L.: *Recognition of Human Iris Pattenrs for Biometric Identification*, School of Computer Science and Software Engineering, The University of Western Australia, *2003*, pp13-16.

MASTALI, N. "Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: a survey paper", *IEEE 5th international conference on broadband and biomedical communications*, 2010, pp 1–6. doi: 10.1109/IB2COM.2010.5723618

MASTRONARDI, P.: *Artículo 7*, en B. EHRENZELLER/ P. MASTRONARDI/ ET ALTERE, *Die Schweizerische Bundesverfassung. Kommentar*, 2ª ed, Dike-Schulthess, 2008.

MATSUMOTO, T./ MATSUMOTO H./ YAMADA, K./et al, "Impact of Artificial "Gummy"Fingers on Fingerprint Systems", 2002. Disponible en www.cryptome.org/gummy.htm

MAYER-SCHÖNBERGER, V.: *Delete: the virtue of forgetting in the digital age*. Princeton: Princeton University Press, 2009.

MCCARTHY, P. voz *Biometric Technologies*, en R. CHADWICK (ed.), *Encyclopedia of applied ethics*, 2ªed, 2102, Elsevier.

MCCONNEL, J. M. "Identity, Security, and the World Wide Web", ponencia destacada en la Conferencia del *Biometric Consortium*, 2009. Texto publicado en febrero de 2010 en la página web de Booz Allen Hamilton.

MCIVER, R. "Biometric Vocabulary – Standardization", en S. Z. LI/ A. K. JAIN (eds.), *Encyclopedia of Biometrics, Springer*, consultada la edición de 2009, pp157ss.

MCMAHON, Z. *Biometrics: History*, Indiana University, citado por el NSTC, *Biometric History*, 2006.

MEIJER, M. C.: *Race and Aesthetics in the Anthropology of Petrus Camper* (1722-1789), Rodopi, Amsterdam, 1999.

MEIJERMAN L,/ SHOLL S, DE CONTI F, GIACON M, VAN DER LUGT C, DRUSINI A, ET AL. "xploratory study on classification and individualisation of earprints", Forensic Science International 2004.140:91-99.

MEIJERMANA, L./ S. SHOLLB/ D. DE CANTIC, "Exploratory study on classification and individualisation of earprints", Forensic Science Int, vol 140, pp91-99, 2004.

MEINTS, M. 'Implementierung grosser biometrischer Systeme. Kriterien und deren Anwendung am Beispiel des ePasses', DuD 2007, pp. 189–193.

MESSMER, E. "Can behavioral biometrics help detect terrorists entering the US?", Networked World, 22 de sept de 2010, en www.networkedworld.com.

MEUTH, L. Z*ulässingkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen*, Duncker& Humblot, Berlin, 2005, pp35-36.

MEYER, Julia: *Identität und virtuelle Identität natürlicher Personen im Internet,* Nomos, 2011.

MEYSMANS, E. 'De verwerking van persoonsgegevens inzake consumentenkrediet', *Computerrecht* 1993, pp. 2–6.

MEZZADRA, A.: "Confines, migraciones, ciudadania", en *Fadaiat. Libertad de Movimiento – Libertad de Conocimiento*, Observatorio tecnológico del Estrecho, 2006, pp89 yss.

MICHAEL, K. *Innovative Automatic Identification and Location-Based services: From Bar codes to Chip Implants,* IG Global, 2009, pp220-221.

MILLER, B. "Vital signs of identity", *IEEE Spectr* 1994, 31:22–30. doi:10.1109/6.259484

MILLER, B. J. "If the body becomes password, does it cease to be the body?", en *Security, risk, and the biometric state: Governing borders and bodies*, Routledge, NY, 2010, p109.

MILLER, B. J."(Dis)qualified bodies: securitization, citizenship, and 'identity management'", en P- Nyers (ed.), Securitizations of Citizenship, 2010, Routledge, NY, 2010, pp77-93.

MILLER, P. 'Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age', Columbia Journal of Law and Social Problems 1986, pp. 89–143.

MITSILEGAS, V.: "Immigration Control in an Era of Globalization: Defelecting Foreingners, Weakening Citizens, Strengthening the State", *Indiana Journal of Global Legal Studies*, vol, 19 (1), 2012.

MOGHADDAM, B./ M. YANG, "Gender classification with support vector machines", *IEEE International Conference on Automatic Face and Gesture Recognition*, Grenoble, 2000, FR, 306–311.

MOGHADDAM, Y. "Leaning gender with support faces", *Pattern Analysis and Machine*, 2002.

MOGUEL FERNÁNDEZ, J.: "El poder de control y vigilancia del empresario sobre las actividades de los trabajadores, y sus implicaciones penales", *Noticias Jurídicas*, Febrero de 2006.

MOHAMMADI, G. ET AL. "Person identification by using AR model for EEG signals", en Proceedings of 9th International Conference on Bioengineering Technology. Czech Republic, 2006.

MOLINERA MATEOS, J. F. "El control empresarial del correo electrónico. Conflicto de derechos", *Absentismo laboral. Causas. Control y análisis. Nuevas formas. Técnicas para su reducción,* Fundación CONFEMETAL, 2001, pág. 153 y ss.

MONWAR/ GAVRILOVA, "Multimodal biometric system using rank-level fusion approach", *IEEE Transactions on Systems, Man and Cybernetics, Part C: Cybernetics*, 39 (4), 867-878, 2009.

MORA SÁNCHEZ, J. M.: *Aspectos sustantivos y procesales de la tecnología del AND*, Cátedra de Derecho y Genoma Humano – Comares, Bilbao Granada, 2001.

MORDINI, E./ MASSARI, S.: "Body Biometrics and Identity", *Bioethics Journal* vol. 22, nº 9/ 2008, pp488-498.

MORDINI, E./ REBERA, A. P. "Biometrics and Ageing: social and ethical considerations", en FAIRHURST, M. (ed.), *Age Factors in Biometrics Procesing*, 2013, pp39ss.

MORDINI, E./ PETRINI, C. 'Ethical and social implications of biometric identification technology', Ann. Ist Super Sanità 2007, pp. 5–11.

MORDINI, E./ TZSOVARAS, D. (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, 2012.

MORDINI, E. ASHTON, H. "The Transparent Body: Medical Information, Physical Privacy and Respect for th Body Integrity", en MORDINI, E./ TZSOVARAS, D. *Second Generation*, 2012, pp269ss.

MORETON, R./ J MORLEY, "Investigation into the use of photo anthropometry in facial image comparison", *Forensic Science International* 212 (2011) 232.

MORGAN, D./ KROUSE, W. *Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues*, CRS Report for Congress, Febrero de 2005.

MORRIS, E. "What's in a Name? (II)", *The New York Times*, 2012, http://opinionator.blogs.nytimes.com/2012/05/01/whats-in-a-name-part-2/?_r=0

MUND, *C. Biobanks – Data Sources without Limits?,* 3 De octubre de 2005. Disponible en http://www. privacyconference2005.org/fileadmin/PDF/mund_e.pdf

MURON, A./ POSPISIL, J. "The human iris structure and its usages", *Physica*, Elsevier,2000, 39:89-95.

MURRAY, M. "Gait as Total pattern of movement", *American Journal of Physical Medicine*, vol. 46, nº,1, 1967, pp290-332.

MUSAR, N. P.: "Workshop report. Restrictions on the Implementation of the EU Data Protection Directive for Public Interest, security and defense", en *HIDE Newsletter*, vol. 2 (7), 2009.

MUZZY, M.: "UNICEF good practices in integration birth registration into health systems (2000-2009), UNICEF 2010, http://www.unicef.org/protection/Birth_Registration_Working_Paper%282%29.pdf (ultimo acceso julio de 2015).

MYHR, TH. *Regulating a European eID. A preliminary study on a regulatory framework for entity authentication and a pan European ID*, 2005. Disponible en http://porvoo10.net/p10/Thomas_Myhr_report.pdf

NAKAJIMA, K./ MIZUKAMI, Y./ TANKA, K./TAMURA, T. "Footprint-based personal recognition", *IEEE Transactions on Biomedical Engineering* 2000, 47(11): 1534–1537.

NANAVATI, S./ THIEME, M./ NANAVATI, R. *Biometrics. Identity verification in a networked World*, 2002.

NATIONAL BUREAU OF STANDARDS, *Guidelines on the evaluation of techniques for automated personal identification*, Federal Information Processing Standards Publication 48, 1 de abril de 1977.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 'Biometric Testing Program', National Voluntary Laboratory Accreditation Program, updated 23.12.2008, disponible en http://ts.nist.gov/standards/scopes/programs.htm

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, Privacy & Biometrics. Building a Conceptual Foundation, 15 de septiembre de 2006 (update). Disponible en http://www.biometrics.gov/Documents/privacy.pdf

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, Biometrics History 2006. Disponible en http://www.biometrics.gov/Documents/BioHistory.pdf

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, *The National Biometrics Challenge*, 2006. disponible en http://www.biometrics.gov/nstc/publications.aspx

NEETHLING, J.:. "Personality rights: a comparative overview", *Comparative and International Law Journal of Southern Africa*, vol. 38, 2/ 2005, pág. 210-245.

NGUYEN, N. "Chokepoint: Regulating US Student mobility through biometrics", Political Geography, 46, 2015, pp1-10.

NICKEL, C. 'Authentisierung an mobilen Geräten mittels Gangerkennung', DuD 2009, pp.280–283.

NICOLÁS JIMÉNEZ, P. *La protección jurídica de los datos genéticos de carácter personal*, Comares, 2006.

NICOLL, C. 'Concealing and revealing identity on the Internet' en NICOLL, C./PRINS, J/ VAN DELLEN, M. (EDS.), *Digital Anonymity and the Law – Tensions and Dimensions*, The Hague, Asser Press, ITeR, 2, 2003, pp. 99–119.

NICOLL, C./ PRINS, J/ VAN DELLEN, M. (eds.), *Digital Anonymity and the Law – Tensions and Dimension*s, The Hague, Asser Press, ITeR, 2, 2003, 307 p.

NITHIN, M./ MANJUNATHA, B./ PREETHI, D./ BALARAJ, B. 'Gender differentiation by finger ridge count among South Indian population', *Journal of Forensic and Legal Medicine* 2011, pp. 79–81.

NOLDE, N.: "Grundlegende Aspekte biometrischer Verfahren", en NOLDE/ LEGER (ed.) *Biometrische Verfahren* 2002, 20 (21).

NOLDE, V./ L. LEGER (EDS.), *Biometrische Verfahren - Korpermerkmale als Passwort*, DWD Köln 2002.

NORRIS, C./ MCCAHILL, M./ WOOD, D. 'The Growth of CCTV: A Global Perspective on the International Diffusion of VideoSurveillance in Publicly Accessible Space', *Surveillance & Society*, 2004, 2, 110.

NORRIS, C. J. M. (ED.), Surveillance, closed circuit televisión and control, Ashgate, 1998, pp41-65.

NOUWT, S./ DE VRIES, B/ PRINS, C. (EDS.), *Reasonable Expectations of Privacy? Eleven CountryReports on Camera Surveillance and Workplace Privacy*, Den Haag, Asser Press, 2005.

NOWBECK, J./ B. BURGER/ D. FUCHS-TELEK/ M PAVLOSKI, "Adermaoglyphia", *American Journal of Human Genetics*, 2011, 89 (2), p302.

NUFFIELD COUNCIL ON BIOETHICS, *The forensic use of bioinformation: ethical issues*, London,Cambridge Publishers, 2007.

OCDE - WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based Technologies*, 2004.

OCDE Background material on biometrics and enhanced network systems for the security of international travel, Paris, OECD,DSTI/ICCP/REG(2003)3/FINAL, 23 De diciembre de 2004.

OECD, Ministerial Declaration on the Protection of Privacy on Global Networks, 7–9.10.1998.

OFFICE OF TECHONLOGY ASSESMENT – OTA, "Computer-based National Information Systems: Technology and Public Policy Issues", Office of Technology Assessment, Congreso de los Estados Unidos, Washington DC, 1981.

OFFICE OF THE PRIVACY COMMISSIONER, Approval of the Biometrics Institute Privacy Code, Australia, 19 Julio 2006, 24 p.disponible en www.Biometricsinstitute.org

OHM, P. 'Broken Promises of Privacy: Responding to the surprising failure of anonymization', UCLA Law Review 2010, pp. 1701–1777.

OLOGUNDE, R. "Plastic Surgery and the biometric ePassport: implications for facial recognition", *Journal of Plastic Surgery and Hand Surgery*, 2014.

OPPONG, M. "Mehr Sicherheit durch biometrische Daten in Ausweispapieren?", en *Liberal. Vierteljahresheft für Politik und Kultur*, 3/2005,pp24 a 27.

ORTEGA, M./ L. BRODO/ M. BICEGO/ M. TISTARELLI, "Measuring changes in face appearance through aging", Computer Vision and Pattern Recognition Workshops, Florida, 2009, pp107-113.

OUWERKERK, M./ F. PASVEER, G. LANGEREIS, "Unobtrusive Sensing of Psychophysiological Parameters: Some Examples of Non-Invasive Sensing Technologies", Vol. 8 of Philips Research Book Series, Dordrecht, The Netherlands: Springer, 2008, pp. 163–193.

PAGE, C./ CAMPBELL, R./ COGGESHALL, S./ GILLESPIE, E./ JOHNSON, R./ OLSON, M./ PERKINS, P. *Demystifying Big Data: A Practical Guide To Transforming The Business of Government Microsoft*. Washington, DC, disponible en: http://www-304.ibm.com/industries/publicsector/fileserve?contentid=239170.

PAGE, M./ TAYLOR, J./ BLENKIN, M. "Uniqueness in the forensic identification Sciences- -Fact or fiction?", *Forensic Science International* 206, 2011, 12–18.

PALANIAPPAN, R./ KRISHNAN, S. M. "Identifying individuals using ECG beats", en Proceedings of the International Conference Signal Processing Communication, 2004, 569–572. Bangalore. ISBN: 0-7803-8674-4.

PARANJAPE, R./ ET AL. "The electroencephalogram as a biometric", *Proceedings of the Canadian Conference on Electrical and Computer Engineering*. 2001. doi: 10.1109/CCECE.2001.933649

PARK, U./ ROSS, A./ JAIN, A. "Periocular biometrics in the visible spectrum: A feasibility study", *Proceedings of the BTAS*, Washington, DC, 2009.

PARKER, T. 'Are we protected? The Adequacy of Existing Legal Frameworks for Protecting Privacy in the Biometric Age', *Ethics and Policy of Biometrics*, Lecture Notes in Computer Science, Berlin, Springer, 2010, pp. 40–46.

PARLAMENTO ALEMÁN (Deutsche Bundestag): Drucksache 16/ 161, 2005, preguntas de la fracción DIE LINKE sobre la seguridad de los documentos de viaje que incluyen biometría.

PARLAMENTO FRANCÉS - ASSEMBLEE NATIONALE (France). *Révolution numérique et droits de l'individu: pour un citoyen libre et informé. Rapport d'information par la mission d'information commune sur les droits de l'individus dans la révolution numérique*. 2011.

PARLAMENTO FRANCÉS. Office Parlementaire d'évaluation des choix scientifiques et technologiques, Rapport sur lesméthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre, CABAL, CH. (ED.), Assemblée National N° 938, Sénat, N° 355, 2003.

PARLAMENTO FRANCÉS. Office Parlementaire d'évaluation des choix scientifiques et technologiques, Rapport sur la valeur scientifique de l'utilisation des empreintes génetiques dans le domaine judiciaire, Cabal, Ch. (ed.), Assemblée National N° 3121, Sénat, N° 364, 2001.

PARMELEE, A. H.: "Infant crying and neurologic diagnosis", *J. Pediat*, 1962, 801-802.

PARZIALE, G./ RIENER-HOFER, R. "Biometrie und EU. Identifizieren mit Maß und Chip", Ecolex-Beotrag.

PARZIALE, G./ RIENER-HOFER, R.:"Biometrie: Begriff und Diskussionsstand"*Juridikum* 2004, 91.

PASCAL, G./ EDINGER, A.: *Nouvelle Enciclopédie Bordas*, vol. II, 1989.

PASCUAL, E.: *Configuración jurídica de la Dignidad humana en la jurisprudencia del Tribunal Constitucional*, Bosch, 2009.

PATO, J./ MILLETT, L. (eds.), *Biometric Recognition: Challenges and Opportunities*, National Research Council, 2010.

PAYE, J.-C.: *Global War on Liberty*, Telos Press, 2007.

PEACOCK, C./ GOODE, A./ BRETT, A. "Automatic forensic face recognition from digital images", *Sci Justice*, 2004 jan-Mar, 44 (1), 29-34.

PEEPLES, E. F./ L. K. DIXON/ W. R. BUSS, "Genetic analysis of the pina of the human ear: sex differences in collage age adults", *J. Heredity*, 1985: 76 (5), 390-2.

PERELLÓ DOMENECH, I.: "El principio de proporcionalidad y la jurisprudencia constitucional", *Revista Jueces para la Democracia*, nº 28, marzo 1997, 69.

PÉREZ GIL, J./ GONZÁLEZ LÓPEZ, J. J. "Cesión de datos personales para la investigación penal. Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal", *Diario La Ley*, nº 7401, 13 de mayo de 2010.

PÉREZ HERRERO, D. A./ P. CORTIJO, "Pasaporte electrónico de segunda generación: España en la autopista de los documentos de viaje", REVISTA DINTEL, octubre/noviembre 2010, 132.

PETERMANN, T./ SAUTER, A.: "Biometrische Identifikationssysteme. Sachstandsbericht", *TAB Arbeitsbericht* nº 76, 2002.

PFITZMANN, A/ BORCEA-PFITZMANN, K. 'Identitätsmanagement und informationelle Selbstbestimmung',enRossnagel, A. (ed.), Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung, Baden-Baden, Nomos, 2006, 83–91.

PHILIPS, J. ET AL. 'An introduction to the Good, the Bad & the Ugly Face Recognition: Challenge Problem', National Institute of Standards & Testing, 2011, disponible en http://www.nist. gov/itl/iad/ig/upload/05771424.pdf

PHILLIPS, P./ SCRUGGS, W./ O'TOOLE, A./ FLYNN, P./ BOWYER, K./ SCHOTT, C/ SHARPE, M. FRVT 2006 and ICE 2006 Large - Scale Results, 2007, 56 p. Disponible en http://www.face-rec.org/ vendors/frvt2006andice2006largescalereport.pdf

PIECHULECK, A. "Empfehlung für Unternehmen zum Schutz personenbezogener biometrischer Daten", *Workshhop IT-Sicherheitsmanagement*, 2008, p8-9.

PIERRE-BEAUSSE, C. *La Protection des Données Personnelles*, Luxemburg, Promoculture, 2005.

PINO, G. "The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights", en M. VAN HOECKE. F. OST (eds.).*The harmonization of private law in Europe*, Oxford: Hart Publishing, 2000, pp235 y ss.

PINO, G.: *Il diritto all'identità personale: interpretazione costituzionale e creatività giurisprudenziale*, Il Mulino, Bolonia, 2003.

POLEMI, D. *Informe ETS Biometrics para la Comisión Europea*: Biometric techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the áreas where they are most applicable, Institute of Communcation and Computer Systems. National Technical University of Athens, 1997

POLZEHL, T./ A SCHMITT, F METZE, M WAGNER, "Anger recognition in speech using acoustic and linguistic cues", *Speech Communication*, 2011.

POPESCU-BODORIN, N./ V. E. BALAS, I M MOTOC, "The Biometric Menagerie – A Fuzzy and Inconsistent Concept", *5th Int Conf Soft Computing and Application*s (Szeged, HU), 2012, pp1-9.

POULOS, M./ ET AL. "On the use of EEG features towards person identification via neural networks", *Medical Informatics & the Internet in Medicine*, 2001. doi: 10.1080/14639230118937.

POULOS, M./ ET AL. "Person identification from the EEG using nonlinear signal classification", *Methods of Information in Medicine* 2002, 41: 64–75.

POULOS, M./ ET AL. "Parametric person identification from EEG using computational geometry", *en Proceedings of the 6th International Conference on Electron, Circuits and System* (ICECS'99), 1999. doi: 10.1109/ICECS.1999.813403.

POULOS, M./ ET AL. "Person identification via the EEG using computational geometry algorithms", en *Proceedings of the Ninth European Signal Processing*, Rodas, 1998, 2125–2128.

POUSSON, A. : "Domicile et identité. Je t'aime, moi non plus'", en J. POUSSON-PETIT (ed.). *L'identité de la personne humaine. Étude de droit français et le droit compare*, Bruylant, 2002, pp529 y ss.

PRABHAAKAR, S./ PANKANTI, S./ JAIN, A. K. "Biometric Recognition: Security and Privacy Concerns", *IEEE SECURITY & PRIVACY*, 2003.

PRABHU, G./ POORNIMA, S. "*Minimize Search Time through Gender Classification from Multimodal Biometrics*", *Procedia Computer Science* 50 (2015), 289-294.

PREITE, G. *Il riconoscimento biometrico. Sicurezza versus privacy*, Ed Uni Service, Trento, 07, pp 47 yss.

PRINS, C. "Making our Body Identify for US: Legal implications of Biometric Technologies", *Computer Law & Security Report*, 1998/ 14, pp159-165.

PRIVACY INTERNATIONAL, *Statewatch, European Digital Rights*, An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents, 2004.

PROBST, T.: "Anonymität und Pseudoanonimität bei biometrischen Identifikationsverfahren"en BÄUMLER, H./ VON MUTIUS, A (eds.), A*nonymität im Internet. Grundlagen, Methoden und Tools Zur Realisierung eines Grundrechts*, Braunschweig, Wiesbaden, 2003, pp179-190.

PROBST, T.:"Biometrie aus datenschutzrechtlicher Sicht", en NOLDE, V./ LEGER, L. (eds.), *Biometrische Verfahren, Körpermerkmale als Passport. Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identification*, Köln, 2002.

PROCTOR, R. (1988): "From Anthropologie to Rassenkunde", en *Bones Bodies, Behaviour*, STOCKING, G. W. (ed.) Madison, University of Wisconsin.

PRUZANSKY, S. "Pattern-matching procedure for automatic talker recognition", *Journal of the Acoustical Society of America,* 1963, 35, p354–358.

PUHLL, R.M./ HEUERL, C. A. "The stigma of obesity: A review and update", Obesity, *2009*. doi: 10.1038/oby.2008.636. B

PÜHRINGER, S.: *Biometrische Daten im Datenschutzrecht,* 2008.

PÜHRINGER, S.: *Biometrische Daten im Datenschutzrecht*, Seminar Privates und öffentliches Informatikrecht und Rechtsinformatik, Salzburg, 2008.

PUNIE, Y. *A social and technological view of Ambient Intelligence in Everyday Life: What bends the trend?,* Sevilla, DG JRC IPTS, Technical Report, EUR 20975 2003. Sumario ejecutivo disponible en http://ftp.jrc.es/EURdoc/20975-ExeSumm.pdf y segunda version disponible en http://www.idate.fr/fic/revue_telech/410/CS57_PUNIE.pdf

PURTOVA, N. *Property Rights in Personal Data: A European Perspective*, Oisterwijk, BOXPress, 2011.

QIU, X./ S. SUN AND T. TAN, 'Global Texture Analysis of Iris Images for Ethnic Classification',enD. Zhang and A. Jain (Eds.), Advances in biometrics: international conference, Hong Kong, ICB, 2006, pp. 411–418.

RAMENZONI, L. L./ Sergio R.P. LINE, „Automated biometrics-based personal identification of the Hunter-Schreger bands of dental enamel", *Proceedings of the Royal Society B* (2006), 273, p1155-1158.

RAMUS, S.J./ EICHENBAUM, H. "Neural correlates of olfactory recognition memory in rat orbitofrontal cortex", *Journal of Neuroscience* 2000, 20: 8199–8208.

RAND, A. *The Fountainhead*, Bobbs-Merril, New York, 1943 (1969.

RANNENBERG, K./ ROYER, D./ DEUKER, A. (eds.), *The Future of Identityenthe Information Society -Challenges and Opportunities*, Dordrecht, Springer, 2009.

RASHID, R .A. "Security system using biometric technology: design and implementation of voice recognition system (VRS)", *IEEE Int Conf Comput Commun Eng*, 2008, 898–902. doi:10.1109/ICCCE.2008.4580735

RATHA, N. 'Privacy Protection in High Security Biometrics Applications', en A. KUMAR AND D. ZHANG (eds.), *ICEB* 2010, LNCS 6005, pp. 62–69.

RATHA, N./ CONNELL, J/ BOLLE, R. 'Enhancing security and privacy in biometrics-based authentication systems', *IBM Systems J.*,2001, pp. 614–634.

RATHGEB, C./ UHL, A./ WILD, P. *Iris Biometrics. From Segmentation to Template Security*, Springer, 2013.

RATTANI, A./ FRENI, B./ MARCIALIS G./ ROLI, F. "Template update methods in adaptative biometric systems: A critical review", *Advances in Biometrics*, vol LNCS 5558, 2009, pp847-858.

REBERA, A. P./ MORDINI, E.: "Biometrics and Ageing", en M. FAIRHURST, *Age Factors*, 2013.

Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, O. J. 2006 L 381, 28.12.2006.

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), O. J. 2006 L 381, 28.12.2006.

Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, O. J. L 142, 06.06.2009.

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 Julio de 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, O. J. L 218, 13.08.2008.

Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 Enero de 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Border Code, O. J. L 35, 4.02.2009.

REID, P. *Biometrics for Network Security*, Upper Saddle River, N J., Prentice Hall PTR, 2004.

REJMAN-GREENE, M. 'Privacy Issues in the Application of Biometrics: a European Perspective',en Wayman, J./ Jain, A./ Maltoni, D/ Maio, D. (eds.), Biometric systems: Technology, Design, and Performance Evaluation, New York, Springer, 2005, pp. 335–359.

REJMAN-GREENE, M. (ed.), *Roadmap for Biometrics in Europe to 2010*, BioVision, 15 de octubre de 2003. Disponible en http://oai.cwi.nl/oai/asset/4057/04057D.pdf

REJMAN-GREENE, M. "Privacy Issues in the Application of Biometrics: a European Perspective", en WAYMAN ET ALTERE, *Biometric Systems*, 2005, p356.

RENGAMANI, H./ P KIMARAGURU/ R. CHARAKRABOIL,/ R. RAGHAU RAO, "The Unique Identification Number Project: Challenges and Recommendations", en A. KUMAR/ D. ZHANG(ed.), *Ethics and policy of Biometrics*, 2010, pp146, ss.

REYES GARCÍA, C. A./ O: F. REYES-GALAVIZ, S. D. CANO-ORTIZ, ET ALT, "Soft Computing Approaches to the Problem of Inant Cry Classification with Diagnostic Purposes", en P. MELIN/ J. KACOZRZYK/ W. PEDRYCZ (eds.), *Soft Computing for Recognition Based on Biometrics*, Springer, 2010.

RICANEK, K./ G. MAHALIGAM/ A. MIDORI/ R. W. VORDER, "Human face ageing: a perspective analysis from anthropometry and biometrics", M. FAIRHURST (ed.), *Age Factors*, pp93ss.

RICOEUR, P.: *Oneself as another*, Chicago: University of Chicago Press, 1992.

RICOEUR, P."La personne et la référence identifiant", en *Soi-même comme un autre*, Ed. du Seuil, 1990, pp39-54. También distingue entre *mismidad* y *self*, *idem* e *ipse*, el CCNE en su Avis nº 98 "Biométrie, donnés identifiants et droits de l'homme", 2007.

RIENER-HOFER, "Vermessen? Die neuen Pass- und Visabestimmungen für die USA nach 9/11", *Juridikum* 2003, p118 y ss.

RIERA, A./ S. DUNNE/ I. CESTER/ G. RUFFINI, "Electrophysiological Biometrics: Opportunities and Risks", MORDINI/ TZOVARAS (eds.), *Second Generation Biometrics*, Springer, 2012, pp154ss.

RIERA, A./ ET AL. "STARFAST: A wireless wearable EEG/ECG biometric system based on the ENOBIO sensor", *Health Proceedings of the 5th International Workshop on Wearable Micro and Nanosystems for Personalised Health,* 2008.

RIERA, A./ ET AL. "Unobtrusive biometric system based on electroencephalogram analysis", *Hindawi Journal of Advances in Signal Processing 2008*. doi: 10.1155/2008/143728.

ROBINS, G. *Proportion and Style in Ancient Egyptian Art*, University of TexasPress, Austin, 1994.

ROBINSON, N./ GRAUX, H./ BOTTERMAN, M/ VALERI, L. *Review of the European Data Protection Directive*, Cambridge, Rand, 2009. Disponible en http://www.ico.org.uk/upload/ documents/ library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

ROCKWELL, M.: Can Voice Recognition Answer the Call?, *Wireless Week*, 10 (10), 2004, pp21-23.

RODOTÁ, S.: "Democracia y protección de datos", *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciciembre 2003), pp15 y ss.

ROIG, A.: "Comentario jurisprudencial. Derecho público y tecnologías de la información y la comunicación (TIC)", Revista Catalana de Dret Públic, núm. 35, 2007, p1 y ss.

ROMEO CASABONA, C. "Predictivity, genetic tests and insurance law", *Revista de Derecho y Genoma Humano*, Nº 31, 2009, PAGS. 107-124.

ROMEO CASABONA, C. M. (ed.), *Bases de datos de perfiles de ADN y criminalidad*, Catedra de Derecho y Genoma-Comares, Granada, 2003.

ROMEO CASABONA, C. M. (ed.), *Caracteristicas biológicas, personalidad y delincuencia*, Catedra de Derecho y Genoma-Comares, Granada, 2003.

ROMEO CASABONA, C.: "Los perfiles de ADN en el proceso penal: novedades y carencias del derecho español", *Estudios de Derecho Judicial*, pags. 411-476.

ROMEO CASABONA, *The Legal and Ethical Aspects related to the Project of the Human Genome*, Pontificia Academica Scientiarum, Cittá del Vaticano, 1995.

ROSE, N/ C. NOVAS, "Biological Citizenship", en Glbal assemblages. Technology, politics, and ethics as anthropological problems, v. Collier, S,/ Ong, A. Blackwell, 2005, pp439-463.

ROSENBERG, A. "Automatic speaker recognition: a review", *Proc. IEEE*, 1976, 64(4), 475–487.

ROSENBLATT, Brain-fingerprinting technologies, CCN 2008.

ROSS, A./ JAIN, A. *Hand geometry*, published at the site of Michigan State University, Department of Computer Science and Engineering, disponible en http://www.cse.msu.edu/rgroups/biometrics/hand_geometry.html

ROSS, A./ SHAH, J/ JAIN, A. 'From template to Image: Reconstructing Fingerprints from Minutiae Points', IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics, 2007, pp. 544–560,disponible en http://ieeexplore.ieee.org/xpl/login. jsp?tp=&arnumber=4107560&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all. jsp%3Farnumber%3D4107560

ROSS, A./ SHAH. J./ JAIN, A.K. (2007) From template to image: reconstructing fingerprints from minutiae points. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4):544–560.

ROSSNAGEL, A. (ed.), *Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung*, Baden-Baden, Nomos, 2006.

ROTTER, P. (ed.), *Large - scale Biometrics Deployment in Europe: Identifying Challenges and Threats*, JRC Scientific and Technical Reports, European Commission JRC – IPTS, Seville, 2008.

ROWLAND, D./ MACDONALD, E. *Information technology law*, London, Cavendish, 2005.

ROWNELL, K./ R. PUHL. "Stigma and discrimination in weight management and obesity", The Permanente Journal 2003, 7(3): 21–23.

RUDOLPH, T./ LINZMAJER, M. "Big Data im Handel", *Marketing Review St. Gallen*, 10/2014,
RUIZ RUIZ, R. "La ponderación en la resolución de colisiones de derechos fundamentales. Especial referencia a la jurisprudencia constitucional española", en *Revista Telemática de Filosofía del Derecho*, nº 10, 2006/2007, pp. 53-77.

RULE, J. "*Social control and modern social structure",* en Rule, J./ Lane, A. *Private lives and public surveilance: Social Control in the Computer Age*, Schocken Books, New York, 1974, pp. 314-15

RULE, J. B. *Privacy in Peril. How we are sacrificing a fundamental right in exchange for security convenience*, Oxford University Press 2007.

RULE, J. B.: *Privacy in Peril. How we are sacrificing a fundamental right in exchange for security convenience*, Oxford University Press 2007.

RULE, J./ GREENLEAF, G. (eds.), *Global Privacy Protection. The First Generation*, Cheltenham (U.K.) – Northampton (Mass. U.S.A.), Edward Elgar, 2010.

RÜSEN, J. "History and Utopia", *HISTOREIN*, vol. 7, 2007, pp1-10. MANUEL, F. E. "Toward a Psychological History of Utopias", *Daedalus*, vol. 94, 2/ 1965, pp293 y ss.

RUTTY, G. N./ ABBAS, A./ CROSSING, D. "Could earprint identification be compterised", and Ilustrated proof of concept paper", International Journal of Legal Medicine, vol 119, nº6, 2005, pp335-343.

SABOROWKSI, M. "Die Pluripotenz der Biodaten. Beobachtungen zu einem Verwertungsgeschehen", en T. POTTHAST/ B. HERRMANN/ U. MÜLLER (eds.), *Wem gehört der menschliche Körper?*, Mentis, Paderborn, 2010, pp367-368.

SABOROWKSI, M. "Die Pluripotenz der Biodaten. Beobachtungen zu einem Verwertungsgeschehen", en POTTHAST, T./ HERRMANN, B./ MÜLLER, U. (eds.), *Wem gehört der menschliche Körper?*, Mentis, Paderborn, 2010, p380.

SACKS, M. J. "Forensic identification: From a faith-based ''Science'' to a scientific science", *Forensic Science International* 201 (2010) 14–17

SAENZ, R. 'Primary care of infants and young children with Down syndrome', American Family Physician 1999, pp. 381–390, disponible en http://www.aafp.org/afp/990115ap/381.html

SALAZAR-TEJEDA, P./ MELIN, P/ CASTILLO O. 'A New Biometric Recognition Technique Based on Hand Geometry and Voice Using Neural Networks and Fuzzy Logic', en CASTILLO, O. ET AL. (eds.), *Soft Computing for Hybrid Intel. Systems*, Springer, Berlin-Heidelberg, 2008, pp. 170–186.

SALVI, F./ CHIANDOTTO B. (eds.): *Biometria. Principi e metodi per studenti e ricercatori biologi*. Piccin Editore, Padova 1978.

SALVI, M./ Y MORDINI, E (eds.): W*orkshop on Ethical and Social implications of biometric identification technology: towards an international approach*, European Commission – Science and Society (2005).

SAMAL, S./ IYENGAR, P. "Automatic recognition and analysis of human faces and facial expressions: a survey", *Pattern Recognition*, 25, 65–77, 1992.

SAMMUT, C./ SQUIRES, B. "Automatic speaker recognition: anapplication of machine learning", en *Proceeding of the 12th international conference on machine learning*, 1995 doi: 10.1.1.54.7372

SÁNCHEZ BARRILAO, J. F. "Identificación documental de Nacionales y Extranjeros (Comentario a la STC 13/ 2001, de 29 de enero)", *Revista Española de Derecho Constitucional*, año 22, nº 64, 2002, pp217 y ss.

SÁNCHEZ VIGIL, J. M./ FERNÁNDEZ FUENTES, B.: "La fotografía como documento de identidad", *Documentación de las Ciencias de la Información*, 2005, vol 28, pp189-195.

SÁNCHEZ-REILLO, R./ SÁNCHEZ-AVILA, C./ GONZÁLEZ-MARCOS, A. "Biometric Identification througy Hand Geometry Measurements", IEEE Transactionson Pattern Analysis and Machine Intelligence, vol 22/10, 2000, pp1168ss.

SANDOR, G. K./ T. P. MCGUIRE/ L. P YLINKONTIOLA/ W. S. SERLO/ P. M. PIRTTINIEMI, "Management of facial asymmetry", *Oral and Maxillofaxial Surgery of Clinics of North America*, 2007, 19, pp395-422.

SAUNDERS, K. M./ ZUCKER, B. "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act", *Cornell Journal of Law and Public Policy*, 1999/8, pp661-663.

SCHAAR, P. (ed.), *Biometrie und Datenschutz – Die vermessene Mensch, Actas Symposium des Bundesbeauftragten fúr den Datenschutz und die Informationsfreiheit*, 27 de junio de 2006, publicado en 2007, Berlin.

SCHEMER, B. "Risk of Profiling and the Limits of Data Protection Law", en Custers, B./ Calders, T./ Schermer, B./ Zarsky, T. (eds.), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Springer, 2013, pp139-140

SCHNEIDER, J. *Ultrasonic Sensors for Capturing Lifescan of Fingerprint Biometrics*, 13 p. http://www.ultra-scan.com/Portals/16/Schneider%20%20Ultrasonic%20Fingerprint%20Sensors.pdf

SCHNEIDER, W. (1982): "Toward the impact of the Human Race: The history of eugenics in Modern France", en *Journal of Modern History*, vol. 54, n. 2 Jun 1982, pp.268-291.

SCHÖNBERGER, V. 'Strands of Privacy: DNA databases and informational privacy and the OECD Guidelines', en D. LAZER (ed.), *The Technology of Justice: DNA and the Criminal Justice System*, disponible en http://www.ksg.harvard.edu/dnabook/

SCHROECK, M./ SHOCKLEY, R./ SMART, J./ ROMERO-MORALES, D./ TUFANO, S.*: Analytics: The real-world use of big data.* New York, USA: Somers. 2012.

SCHUMACHER, A/ UNVERRICHT, K. 'Rechtliche und gesellschaftliche empfehlungen zur Gestaltung Biometrischer Systeme. Gemäss ISO/IEC Technical Report TR 24714-1', *DuD* 2009, pp. 308–312.

SCHÜMACHER, G. "Behavioural Biometrics: Emerging Trends and Ethical Risks", en MORDINI, E./ TZOVARAS, D. (eds.), *Second Generation*, p216.

SCHUMACHER, G. (ed.), *Biometrics for Border Control – A Roadmap for Europe-*, Best Network, 2012.

SEPD - EDPS, E*DPS comments on the Communication COM(2010) 311 final from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports*, Julio de 2010.

SEPD - EDPS, *Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission related to the "Fingerprint recognition study of children below the age of 12 years*", 25.7.2011 (Case 2011–0209).

SEPD - EDPS, *Opinion on the amended proposal for a Regulation of the European Parliament and of the Council*

on the establishment of 'EURODAC' for the comparison of fingerprints, 5.09.2012.

SEPD - EDPS, Opinion on the data protection reform package, 7.3.2012.

SEPD - EDPS, The EDPS Video-surveillance Guidelines, Brussels, 2010.

SEPD EDPS, Opinion 20 December 2007 on the communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96, O. J. C 101, 23.4.2008, pp. 1–12.

SEPD- EDPS, Opinion on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS), O. J. C 97, 25.4.2006, pp. 6–10.

SETHI, I. K. : "Biometrics", en STRANDBURG, K. J./ RAICU, D. S. *Privacy and Technologies of Identity. A Cross-Disciplinary Conversation*, Springer, 2006, pp117-134.

SFORZA, C./ FERRARIO, V. F. "Soft-tissue facial anthropometry in three dimensions: from anatomical landmarks to digital morphology in research, clinics and forensic anthropology", *JASS, Journal of Anthropological Sciences*, vol. 84 (2006).

SFORZA, Chiarella/ FERRARIO, Virgilio F. "Soft-tissue facial anthropometry in three dimensions: from anatomical landmarks to digital morphology in research, clinics and forensic anthropology", JASS, *Journal of Anthropological Sciences*, vol. 84 (2006), pp97-98.

SHAMIR, L./ LING, S./ RAHIMI, S./ FERRUCCI, L./ GOLDBERG, I. G. "Biometric identification using knee X-rays", *International Journal of Biometrics* 2009, 1(3): 365–370.

SHANE, B. USA today, 25 nov 2012. Palm Scanners get thumbs up in schools and hospitals.

SHERLOCK, R./ MORREY, J. D. *Ethical issues in biotechnology*. Lanham: Rowman &Littlefield. 2002.

SHONIREGUN, C./ CROSIER, S.: *Securing Biometrics Applications*, 2007.

SIMITIS, S.: "Hat der Datenschutz noch in Zukunft?", *RDV 2007*, pp143ss.

SIMITIS,D: "Zur Internationalisierung des Arbeitsnehmerdatenschutzes – Die Verhaltensregeln der Internatiionalen Arbeitsorganisation", en HANAU, P./ HEITHER, F./ KÜHLING, J. (ed.), *Richterliches Arbeitsrecht, Festschrift für Thomas Dieterich*, Beck, München, 1999

SIROVICH, L./ KIRBY, M. "Low-dimensional procedure for the characterization of human faces", *J. Optical Soc. Am.*, 1987, 4, 519–524.

SKULER, M. "Finger and Palm Prints: A Window on Your Health", Glamour, 1984.

SOLOVE, D. *The digital person. Technology and Privacy in the Information Age*, New York, New York University Press, 2004.

SOLOVE, D. *The future of reputation: gossip, rumor, and privacy on the internet*, New Haven, Yale University Press, 2007.

SOLOVE, D. *Understanding Privacy*, Cambridge (Massachusetts, U.S.A.), Harvard University Press, 2008.

SONG, S./ OHNUMA, K./ LIU, Z./ MEI, L./ A. KAWADA/ MONMA, T. "Novel biometrics based on nose pore recognition", *Optical Engineering* 2009, 48(5): 57204.

SPENCER, F. (ed.), *History of Physical Anthropology: an Encyclopedia*, vol I, 1997, voz *Anthropometry* y voz *Bertillon*. JAIN, A. K./ FLYNN, P./ ROSS, A. A. (eds.), *Handbook of Biometrics*, Springer 2007.

SPENCER, F. (ed.), *History of Physical Anthropology: an Encyclopedia*, vol I, 1997, voz *Anthropometry*.

SPENCER, F. (ed.), *History of Physical Anthropology: an Encyclopedia*, vol I, 1997.

SPROKEREEF, A. C. J./ DE HERT, P.: "Ethical Practicce in the use of biometric identifiers within the EU", *Journal of Law, Science and Policy*, 3, 2/2007, pp. 177-201.

SPROKKEREEF, A. 'The Introduction of Biometrics in the Netherlands: An Evaluation Under Data Protection and Administrative Law',en VAN DER HOF S/ GROOTHUIS, M. (eds.), Innovating Government. Normative, Policy and Technological Dimensions of Modern Government, The Hague, Asser, 2011, pp. 217–228.

STACEY, R. B. "Report on the erroneous fingerprint individualization in the Madrid train bombing case", *Forensic Sci. Commun.* 1 (2005) 7.

STANHAM, P.: "Issues and Concerns in Biometrics IT Security", en H. BIGDOLI (ed.), *Handbook of Information Securiy*, J. Wiley and Sons, New York, 2006, pp471-501.

STEVENS, K./ WILLIAMS, C./ CARBONELL, J./ WOODS, B. "Speaker authentication and identification: a comparison of spectrographic and auditory presentation of speech material*", J. Acoust. Soc. Am*., 1968, 44, 596–607.

STIGLER, S. M. "The Problematic Unity of Biometrics", *Biometrics* (Journal), 2000, p654.

STIGLER, S. M.: "Galton and Identification by fingerprints", en *Statistics on the Table*, Harvard University Press, 1999, pp131-189.

STRASSER, P. *Verbrechermenschen. Zur kriminalwissenschaftlichen Erzeugung des Bösen*, ediciónd e 2005 (original de 1948), Kap. II („Der Mythos als Wissenschaft"), 41 ff.

STRASSER, P. "Biometrie – ein Schritt in die Überwachungsdemokratie?", SCHAAR, P. (ed.), *Biometrie Und Datenschutz – Die vermessene Mensch*, 2007.

SUÁREZ ESPINO, M. L.: *El derecho a la intimidad genética*, Marcial Pons, Madrid, 2008.

SURVEILLANCE STUDIES NETWORK: *Memorandum by SURVEILLANCE STUDIES NETWORK*, en House of Lords (UK) –Select Committee on the Constitution. Part 1. Borders, *Citizens and Immigration Bill Report*, 2009.

SUTROP, M. 'Ethical Issues in Governing Biometric Technologies',en A. Kumar and D. Zhang(eds.), ICEB 2010, LNCS 6005, pp. 102–114.

SUTROP, M./ LASS-MIKKO, K. "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics", *Review of Policy Research* vol. 29, nº 1/2012, pp21ss.

SWABEY, M.A./ BEEBY, S.P./ BROWN, A. D./ CHAD, J. E. "Using Otoacoustic emission as biometric", *Proceedings of ICBA*, Hong Kong 2004, LNCS, vol. 3072, pp. 600–606.

SWIFT, B./RUTTY, G. N. "The Human Ear", *J. Forensic Sci*, Kan 2003, vol 48, nº 1, pp153 y ss.

SZAJERKA, T./ JUREK, B./ JABLECKI, J. "Transplanted fingerprints: a preliminary case report 40 months post transplant", *Transplant Proc 2010*, Nov 42 (9), 3553-55.

TABOR, Z./ KARPISZ, D./ WOJNAR, L./ KOWALSKI, P. "An automatic recognition of the frontal sinus in x-ray images of skull", *IEEE Transactions on Biomedical Engineering* 2009, 56(2): 361–368.

TAO, D./ LI, X./ WU, X. ET AL. "Analysis and Gabor features for gait recognition", *IEEE Transactions on Pattern Analysis and Machine Intelligence* 2007, 29(10): 1700–1715.

TAPIA BUENO, S. G. ""La protección jurídica de los Datos Biométricos en la Comunidad Europea", Revista de Derecho Informático, nº 84, julio de 2005, pp1ss.

TAYLOR, K. "Age progression: Growth", en K. T. TAYLOR (ed.) *Forensic Art and Illustration*, Boca Raton, pp235-249

TEIXEIRA, T./ JUNG, D./ DUBLON, G. /SAVVIDES, A. *PEM-ID: Identifying People by Gait-Matching using Cameras and Wearable Accelerometers*, 2009, p.3.

TELETRUST DEUTSCHAND, G. LASSMAN, *Bewertungskirterien zur Vergleichbarkeit Biometrischer Verfahren*, 2002.

TELETRUST DEUTSCHLAND e.V. *Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren*, 2006.

THIERER, A./ WAYNE CREWS (ed.), *Who Rules the Net. Internet Governance and Jurisdiction*, Cato Institute, 2003, xxiii-xviii.

THOMAS, R. (Information Commissioner), *A Report on the Surveillance Society*, publicado por el ICO, Gobierno del Reino Unido, 2006.

THORPE, J./ VAN OORSCHOT, P.C./ SOMAYAJI, A. "Pass-thoughts: authenticating with our minds", *Proceedings of the 2005 Workshop on New Security Paradigms*, doi.acm.org/10-1145/1146269.1146282:14

TISTERELLI, M./ BICEGO, M./ GROSSO, E. "Dynamic face recognition: from human to machine vision", *Image Vision Comput.* 27 (3) (2009) 222–232.

TOPPING, A./ KUPERSCHMIDT, V./ GORMLEY, A. *Method and apparatus for the automated identification of individuals by their beds of their fingernails*, U.S. Patent No. 5751835, 1998.

TORPEY, J: *The invention of the Passport: Surveillance, Citizenship and the State*, Cambridge University Press, 1999.

TOUCHENT, D. 'La mise en oeuvre d'un système de badgeage par empreintes digitales dans l'entreprise', *La*

Semaine Juridique Entreprise et Affaires n°35, 15.12.2005, pp. 1337–1339.

TOWLE, Holly K.: "Identity Theft: Myths, Methods and New Law", Rutgers Computer and Technology Journal, vol 30, 2/ 2004, pp237 y ss.

TRAURING, M. "Automatic comparison of finger-ridge patterns", *Nature*, 1963, 197, 938–940.

TRAURING, M. "On the automatic comparison of finger-ridge patterns", *Hughes Laboratory Research Report* 1961, n. 190.

TRUCCO, L. *Introduzione allo Studio dell'identitá individuale nell'ordinamento costituzionale italiano*, Giappicheli, Torino, 2004.

TRUCHE, P./ FAUGÈRE, J.-P./ FLICHY, P. *Administration électronique et protection des données personnelles – Livre Blanc*, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000100/0000.pdf, pp 31 y ss.

TUREK, J.: "An Industry Group Viewpoint: Biometrics", SIA News, agosto de 2004, pp20ss.

TURK, M./ PENTLAND, A. "Eigenfaces for Recognition", Journal of Cognitive Neuroscience, Vol. 3, 1, 1991, pp71ss.

TURN, R./ SHAPIRO, N./ JUNCOSA, M. *Privacy and security in centralized vs. decentralized databases*, Santa Monica, Calif. Rand Corp. 1975.

UHL, A./ WILD, P. "Footprint-based biometric verification", *Journal of Electronic Imaging*, 2008, 17: 11016.

UK COMPUTING RESEARCH COMMITTEE*: Memorandum by UK COMPUTING RESEARCH COMMITTEE*, en House of Lords (UK) – Select Committee on the Constitution. Part 1. Borders, *Citizens and Immigration Bill Report*, 2009, pp145 y ss.

ULUDAG, U./ ROSS, A./ JAIN, A, K. "Biometric template selection and update: a case study in fingreprints", Pattern *Recognition*, vol 31, nº 7, 2004, pp1533-1542.

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG -HOLSTEIN, Positionspapier zum Antiterrorgesetz der Bundesregierung, 7 de diciembre de 2001.

URRUELA MORA, A. *Imputabilidad penal y anomalía o alteración psíquica*, CDGH - Comares, Bilbao-Granada, 2003.

URRUELA MORA, A.: "La actual discusión sobre las bases genéticas de la criminalidad", en C. M. ROMEO CASABONA (ed.), *Características Biológicas, Personalidad y Delincuencia*, Cátedra de Derecho y Genoma Humano – Comares, Bilbao – Granada, 2003, pp131ss.

US DEFENSE SCIENCE BOARD TASK, Report on Defense Biometrics, 2007.

US GAO, *Using Biometrics for Border Security*, Washington, 2002, p50.

US GOVERNMENT ACCOUNTABILITY OFFICE-GAO, *Using Biometrics gor Border Security*, pp46-47 y US GAO, Registered traveller Program Policy and Implementation Issues, Washington, 2002.

VALENCIA CABALLERO, L. *Metodología para elaborar reconstrucciones faciales empleando gráficos computarizados trimensionales*, Tesis doctoral, Universidad de Granada, 2007, pp60-61.

VAN ALSENOY, B./ KINDT, E./ DUMORTIER, J. 'Privacy and Data Protection Aspects of e-Government Identity Management',envan der Hof S/ Groothuis, M. (eds.), Innovating Government. Normative, Policy and Technological Dimensions of Modern Government, The Hague, Asser, 2011, pp. 251–282.

VAN BLARKOM RE, G./ BORKING, J/ OIK, J. (eds.), *Handbook of Privacy and Privacy – Enhancing Technologies – The case of Intelligent Software Agents*, The Hague, College Bescherming Persoonsgegevens, 2003. Disponible en: t http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

VAN DEN BROEK, E. L. "Beyond Biometrics", *Procedia Computer Science* 1, 2010, 2511–2519.

VAN DEN BROEK, E. L./ SCHUT, M. H./ WESTERINK, J. H. D. M./TUINENBREIJER, K. "Unobtrusive Sensing of Emotions (USE)", *Journal of Ambient Intelligence and Smart Environments* 1 (3), 2009, 287–299.

VAN DEN BROEK, E. L./ WESTERINK, J. H. D. M. "Considerations for emotion-aware consumer products", *Applied Ergonomics* 40 (6), 2009, 1055–1064.

VAN DER PLOEG, I. 'Genetics, biometrics and the informatization of the body', *Ann Ist Super Sanità* 2007, pp. 44–50.

VAN DER PLOEG, I. 'Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications', en VAN DER HOF S/ GROOTHUIS, M. (eds.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government*, The Hague, Asser, 2011, pp. 29–40.

VAN DER PLOEG, I. "The illegal body: 'Eurodac' and the politics of biometric information", Ethics and Information Technology 1: 295-302, 1999.

VAN DER PLOEG, I. *Ethical Brief on Biometrics & Embedded Technology*, Hide, 2009.

VAN DER PLOEG, I. "Identity, biometrics and behavior predictability", RISE. European multistake-holder Conference on Ethics and Governance of Biometrics and Identification Technologies, 2010. www.riseproject.eu

VAN DER PLOEG, P: *The Machine Readable Body. Essay on Biometrics and the Informatización of the Body*, Shaker, 2005.

VIELHAUER, C.: *Biometric User Authentication for IT Security. From Fundamentals to Handwriting*, Springer, 2006.

WALKER, G. DE Q. (1986), "Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal", CIS – Centre for Independent Studies, Policy Report, Vol. 2 No. 1.

WANG, J./ HU, W./ WANG, Z./ CHEN, Z. "Human Identification and Gender Recognition from Bozing", en SUN/ LAI/ ET ALT (eds.), *Biometric Recognition*, 2011, p1952ss.

WANG, L./ GENG, X. *Behavioral biometrics for human identification: Intelligent applications*, Hershey: Medical Information Science Reference, 2009.

Wasz-Höckert, O/ Lind, J./ Vuorenkoski, V/ Partanen, T./ Valanne, E. "The infant cry a spectrographic and auditory analysis", *Clinics in Devel Medicine*, 29, 1968.

WATNER, C./ MCELROY, W. (eds.), *National Identification Systems. Essays in Opposition*, McFarland, 2004.

WAYMAN, J. 'A Definition of "Biometrics"', en WAYMAN, J. (ed.), *National Biometric Test Center Collected Works 1997 – 2000*, San Jose State University, 2000, pp. 21–25, disponible en http://www.engr.sjsu.edu/biometrics/nbtccw.pdf

WAYMAN, J. 'Fundamentals of Biometric Authentication Technologies', en WAYMAN, J. (ED.), *National Biometric Test Center Collected Works 1997 – 2000*, San Jose State University, 2000, pp. 1–20.

WAYMAN, J. (ed.), *National Biometric Test Center Collected Works 1997 – 2000*, San Jose State University, 2000.

WAYMAN, J. L.: "Biometric Identification and the Financial Services Industry", en *National Biometric Center: Collected Works*, 1998, p. 263ss. www.engr.sjsu.edu/biometrics/nbtccw.pdf.

WAYMAN, J./ JAIN, A./ MAIO, D. "An Introduction to Biometric Authentication Systems", en WAYMAN, J./ JAIN, A./ MALTONI, D./ MAIO, M. (eds,), *Biometric Systems. Technology, Design and Performance Evaluation*, Springer, 2008.

WAYMAN, J./ JAIN, A./ MALTONI, D/ MAIO, D. (eds.), Biometric systems: Technology, Design, and Performance Evaluation, New York, Springer, 2005.

WAYMAN, J.L.,"Large-scale civilian biometric systems - issues and feasibility", *Proceedings of the CardTech/SecureTech Government*, 1997, Washington DC, http://www.engr.sjsu.edu/biometrics/nbtccw.pdf.

WAYMANN, J. L. "Technical testing and evaluation of biometric identification devices", en *Biometrics Personal Identification in a Networked Society*, Kluwer, Dordrecht, 1999, pp343-368.

WAYNE CREWS jr, C. "Human Bar Code. Monitoring Biometric Technologies in a Free Society", *Policy Analysis*, nº 452, 2002, pp. 1 y ss.

WEBER, K."Privacy invasions. New technology that can identify anyone anywhere challenges how we balance individuals' privacy against public goals", EMBO Rep 2006, nº especial 7, pp36-39.

WECHSLER, H. "Biometric Security and Privacy Using Smart Identity Management and Interoperability: Validation and Vulnerabilities of Various Techniques", *Review of Policy Research*, vol. 29, 1/ 2012, pp78-79.

WECHSLER, H./ LI, F. "Biometrics and Robust Face Recognition", *Biometrics and Forensics*, 2014, p193.

WECHSLER, H. "Biometric Security and Privacy Using Smart Identity Management and Interoperability: Validation and Vulnerabilities of Various Techniques", *Review of Policy Research*, vol. 29, 1/ 2012, pp63-89.

WEICHEND, S,/ TIENIU, T. "Automated biometric-based personal identification", *PNAS*, USA 96 (1999), pp11065-11066.

WEICHERT, T.: "Biometrie im Spannungsfeld von Persönlichkeitsschutz und Strafverfolgung – Chancen und Risiken", en *Biometrie – Chancen un Risiken, 14. Landesdelegiertentag des BDK*, celebrado en Frankfurt am Main, editado por Bund Deutscher Kriminalbeamter, Landesverband Hessen, 2004, pp36 a 38.

WEICHERT, T.: *Datenschutzrechtliche Anforderungen an den Einsatz Biometrischen Verfahren bei Ausweispapieren*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), 2005.

WEISER, B. *Can Fingerprints Lie? Yes*, New York times, 31 de mayo de 2004 (caso René Ramón Sánchez).

WELLBROK, R. „Datenschutzrechliche Aspekte des Aufbaus von Biobanken für Forschungszwecke", en *MedizinRecht*, 2/ 2003, pp. 77 a 82.

WERRO MILLER, B. J. F.: "The right to inform v. the right to be forgotten: A transatlantic clash", en COLOMBI CIACCHI. Ch. GODT. P. ROTT. L. J. SMITH (eds.). *Liability in the Third Millenniu*m. Georgetown Public Law Research Paper No. 2. Baden-Baden.

WESTIN, A. F.: "Social and Political Dimensions of Privacy", Journal of Social Issues, vol. 59, nº 2, 2003, pp.431-453.

WESTIN, A. F.: *Privacy and Freedom*, Athenum, New York, 1967.

WHITE, C. "The TSA Registered Traveller Program", *Biometrics Consortium Conference*, CTO, Daon, 2006.

WILDES, R. P. "Iris recognition: an emerging biometric technology", *Proc. IEEE*, 85(9), 1348–1364, 1997

WINKLER, M.: "Rechtliche Rahmenbedingungen für Biometrische Systeme. Biometrie und Datenschutz", *ZK-Spezial*, 2009, pp. 3-5.

WINSTON, M/ EDELBACH, R. *Society, Ethics, and Technology*, Cengage Learning, 2013.

WINSTON, R. *What makes me me?,* Dorling Kindersley, London, 2004.

WOLF, P.: "De l'authentification biométrique", *Securité des system d'information*, nº 46, octubre de 2003.

WOODARD, J. D./ FLYNN, P.J. "Finger surface as a biometric identifier", *Computer Vision and Image Understanding*, 2005, 100(3): 357–384.

WOODWARD, J. D. "The law and use of biometrics", EN JAIN AK, FLYNN P, ROSS AA (eds.) *Handbook of Biometrics.* Springer, New York, 2008.

WOODWARD, J./ ORLANS, N/ HIGGINS, P. *Biometrics: Identity assurance in the Information Age*, Berkley, Osborne, 2003.

WOODWARD, J./ WEBB, K./ NEWTON, E./ BRADLEY, M./ RUBENSON, D. ET AL. Army biometric applications: identifying and addressing sociocultural concerns, RAND, Santa Monica, CA, 2001.

WOODWARD. J. D. "Biometrics: Privacy's Foe or Privacy's Friend", *Proceedings of the IEEE,* vol. 85, nº9, Septiembre de 1997, pp1480ss.

WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-Based Technologies*, OCDE, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy 2003.

WRIGHT, D/ DE HERT, P. (eds.), *Privacy Impact Assessment*, Springer, 2012.

WYLIE, M. "An Artificial Nose that Can Sniff out Terrorists? It May Not Be Sci-Fi", *Newhouse News Service*, 2003.

XU, H. *Spectral Minutiae Representations for Fingerprint Recognition*, Enschede, Gildeprint, 2010.

YAGER, N./ T. DUNSTON, "The biometric menagerie", *IEEE transactions on Pattern Analysis and Machine Inteligence,* vol 32, 2010, pp220-230.

YAMPOLSKY, R./ GOVINDARAJU, V. *Behavioural biometrics: A survey and classification*, International Journal of Biometrics, 2008 1(1): 81–113.

YAN, P./ BOWYER, K. W. "Biometric recognition using 3D ear shape", *IEEE Transactions on Pattern Analysis and Machine Intelligence* 2007, 29(8): 1297–1308.

YANG, W. "Application of voice recognition for mobile E-commerce security", *IEEE3rd Pacific-Asia conference on circuits, communications and system*, 2011, pp 1–4. doi: 10.1109/PACCS.2011.5990286

YESHI, *Biometrics*, en MITCHAN (ed.), *Encyclopedia of Science and Technology Ethics*, vol. 4, Thomson-Gale, Farmington, 2005, pp205ss.

YOKOTA, M. "Head and facial anthropometry of mixed-race US Army male soldiers for military design and sizing: A pilot study", *Applied Ergonomics* 36 (2005), pp379-383.

YOUSEFI-NOORAIE, R./ MORTAZ-HEDJRI, S. 'Dermatoglyphic asymmetry and hair whorl patterns in schizophrenic and bipolar patients', *Psychiatry Research* 2008, pp. 247–250.

YUE, F./ ZUO, W./ ZHANG, D./ LI, B. 'Fast palmprint identification with multiple templates per subject', en *Pattern Recognition Letters* 2011, pp. 1108–1118.

ZAMIR, A./ DELL'ARICCIA-CARMON, A./ ZAKEN, N./OZ, C. "The Israel DNA database – The establishment of a rapid, semi-automated analysis system", *Forensic Science International: Genetics*, 6, 2012, 286-289.

ZHANG, D, *Automated biometrics: technologies and systems,* Hardbound, Boston, 2000.

ZHANG, D. "Biometrics technologies and applications", en *Proceedings of 1st international conference on image and graphics*. Tianjin, 2000 China, pp 42–49.

ZHANG, D./ SONKA, M. (eds.), *Medical Biometrics*, Springer 2010.

ZHANG, D./ JING, X/ YANG, J, *Biometric image discrimination technologies*, Idea group Inch publications, Hershey, 2006.

ZHANG, D./ LU, G. 3 D *Biometrics. Systems and Applications*, Springer. 2013.

ZHANG, J./ YAN, Y./ LADES, M. "Face recognition: eigenface, elastic matching and neural nets", *Proc. IEEE*, 1997, 85(9), 1423–1436.

ZITTRAIN, J. *The future of the Internet and how to stop it*. New Haven: Yale University Press, 2008.

Universitat d'Alacant
Universidad de Alicante