



**Universitat
Pompeu Fabra**
Barcelona

TESIS DOCTORAL

**Intercambio de información policial y
protección de datos personales en Europa**

ADN forense en la investigación criminal

Autor

Jordi DOMÈNECH GANAU

Directora de la tesis

Dra. Maribel GONZALEZ PASCUAL

DEPARTAMENT DE DRET

Barcelona, Abril 2022

A Eva

Agradecimientos.

Primero me gustaría agradecer a mi compañera de viaje, Eva, que sin su apoyo y paciencia incondicional no hubiera sido posible finalizar el proyecto que inicié hace más de 10 años y finaliza con este trabajo. Gracias por creer en mí, por los momentos insustituibles que te he robado llevando a cabo este proyecto y por alegrarte conmigo de mi logro y sentirlo como si fuera tuyo.

Por supuesto, también se agradezco a mis padres, que sin la formación académica que me facilitaron y el esfuerzo que hicieron para darme un proyecto de vida, no habría sido posible llegar hasta aquí.

Agradecer la enseñanza proporcionada por los profesores de la Universidad Pompeu Fabra durante el estudio del Master de Ciencias Jurídicas Avanzadas, que me mostraron el camino a seguir para realizar esta tesis. En especial a la Dra. Maribel GONZALEZ PASCUAL quien guió este trabajo, sin los consejos de la cual no habría podido llevarla a término.

A los Mossos de la Unitat del Laboratori Biològic del Cos de Mossos d'Esquadra, por la inestimable ayuda prestada.

A Dani, de la Unitat Central d'Inspeccions Oculars del Cos de Mossos d'Esquadra que con su ayuda se me han abierto muchas puertas a las que llamar y poder resolver dudas.

También agradecer a Tais, Rocio, Morgana y Alberto, compañeros de doctorado, por las cenas que hemos mantenido a lo largo de todos estos años y durante las que nos íbamos apoyando mutuamente para conseguir nuestro objetivo final, el presentar la tesis doctoral. Gracias por ayudarme a conseguirlo.

Y a Angel, que en nuestros viajes, y nuestras largas conversaciones y cafés, me transmitió la confianza en finalizar este proyecto. Ahora le toca a él concluir el suyo.

Finalmente, también va mi agradecimiento a todos aquellos que no menciono, pero que saben qué sin su palabra, presencia o escucha, sin el aporte de tantas personas que estuvieron presentes durante esta experiencia que ha durado varios años, la culminación de este trabajo no hubiese sido posible.

Resumen

El intercambio de información entre los distintos cuerpos policiales favorece la cooperación entre Estados cuando se trata de luchar contra el crimen, pero a veces puede afectar al derecho a la protección de datos de que disponen los individuos. La protección de los derechos de los individuos fortalece la persona frente al interés estatal, pero a la vez, un control demasiado exhaustivo puede entorpecer la investigación.

En este trabajo se da una visión crítica del intercambio de información policial en el seno de la UE, para luego centrarse en el uso del ADN en la investigación policial y en cómo intercambian los datos genéticos los distintos cuerpos policiales a nivel europeo. En el último capítulo se analiza la técnica del *familial search* y la de detección de *características visibles externas* del individuo - EVC -, que son avances de la ciencia genética aplicados a la investigación de delitos y en los que se utiliza la información contenida en el ADN como medio de investigación, a la vez que se estudia la afectación que supone a los derechos de protección de datos y al de la privacidad de las personas el uso de estas nuevas técnicas en el campo de la investigación criminal.

Summary

The exchange of information between the different police forces favors cooperation between States when it comes to fighting crime, but can sometimes affect the right to data protection available to individuals. The protection of the rights of individuals strengthens the person against the state interest, but at the same time, an overly exhaustive control can hinder the investigation.

In this work, a critical vision of the exchange of police information within the EU is given, in order to later operate in the use of DNA in police investigation and in how the different police forces exchange genetic data at a European level. The last chapter analyzes the family search technique and the detection of external visible characteristics of the individual - EVC -, which are advances in genetic science applied to crime investigation and in which the information contained in the DNA is used as a tool of investigation, while studying the impact that the use of these new techniques in the field of criminal investigation has on data protection rights and the privacy of individuals.

Índice

Abreviaturas Utilizadas.....	15
------------------------------	----

CAPÍTULO I

EL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS EN EUROPA

Introducción.....	17
1.- Derecho a la Intimidad y a la Protección de datos.....	19
1.1.- Derecho a la Intimidad.....	19
1.2.- Intimidad versus privacidad.....	23
2.- El Derecho a la protección de datos personales.....	35
2.1.- Un nuevo Derecho.....	35
2.2.- La protección de datos personales en Europa.....	40
2.3.- La protección de datos personales en la jurisprudencia europea.....	46
La Protección de datos personales según el TEDH.....	46
La Protección de datos personales según el Tribunal de Justicia de la Unión Europea - TJUE.....	51
Caso particular de los datos procedentes de las comunicaciones electrónicas.....	55
3.- La protección de datos en las investigaciones policiales.....	60
3.1.- Legislación europea aplicable a la protección de datos en el ámbito de las investigaciones policiales.....	62
3.1.1.- Antecedentes.....	62
3.1.2.- Directiva (UE) 2016/680.....	66
· Definiciones.....	69
- “Datos personales”	70
- “Tratamiento”	74
- “Fichero”	75
- “Responsable” y el “encargado del tratamiento”	76

- “Autoridad competente”	77
4.- Principios aplicables al tratamiento de datos personales en el ámbito de las investigaciones policiales.....	77
4.1.- Principios relativos al tratamiento.....	78
a.1.- Licitud.....	79
a.2.- Leal.....	80
b.- Transparente.....	83
c.- Seguridad.....	86
d.- Limitación de finalidad.....	88
e.- Decisiones individuales automatizadas.....	90
4.2.- Principios relativos a los datos personales.....	91
a.- Exactos.....	91
b.- Pertinentes y no excesivos - minimización de datos -.....	93
c.- Conservados un periodo no superior al necesario.....	94
- Supresión – Derecho al olvido.....	97
d.- Distinción entre diferentes categorías de interesados.....	101
e.- Distinción entre datos personales y verificación de la calidad de los datos personales.....	103
f. - Tratamiento de categorías especiales de datos personales.....	105
4.3.- Derechos del interesado.....	106
a.- Derecho a la información.....	107
b.- Derecho de acceso del interesado a los datos personales.....	108
c.- Derecho de rectificación y supresión de datos personales del interesado.....	110
Conclusiones.....	110

CAPÍTULO II

TRANSMISIÓN DE DATOS PERSONALES EN EL ÁMBITO DE LA COOPERACIÓN POLICIAL INTERNACIONAL

Introducción.....	113
1.- Cooperación policial.....	116

1.1.- Modelos de cooperación interpolicial.....	116
1.2.- Cooperación intergubernamental.....	117
2.- Transmisión de datos personales en el ámbito policial dentro del marco del Consejo de Europa.....	118
2.1.- Convenio 108 y su Protocolo Adicional de 2001.....	118
2.2.- Recomendación (87) 15 del Comité de Ministros.....	123
3.- Transmisión de datos personales en el ámbito policial en el marco de la Unión Europea.....	125
3.1.- Acervo de Schengen.....	125
a.- Acuerdo de Schengen.....	126
b.- Convenio de aplicación del Acuerdo de Schengen – CAAS -	129
- Intercambio de información.....	131
- Centros de Coordinación Policial y Aduanero.....	142
- Vigilancia.....	146
- Persecución en caliente.....	151
- Registro de huéspedes -.....	152
- Información espontánea.....	153
- Sistema de información de SCHENGEN (SIS).....	154
3.2.- Consejo Europeo de Tampere.....	163
3.2.1.- Prevención de la delincuencia en la UE (párrafo 42).....	164
3.2.2.- Equipos conjuntos de investigación - ECI - (párrafo 43)...	165
3.2.3.- Unidad operativa europea de jefes de policía - European Chief of Police Task Force (párrafo 44).....	168
3.2.4.- Academia Europea de Policía (párrafo 47).....	169
3.3.- El Convenio relativo a la asistencia judicial en materia penal entre los estados miembros de la Unión Europea – en adelante Convenio de asistencia mutua de 2000 -	170
3.3.1.- Intervención de las telecomunicaciones.....	172
3.3.2.- Uso de los datos obtenidos en las investigaciones.....	173
3.4.- Tratado de PRÜM.....	174
3.5.- Tratado de la UNION EUROPEA (TUE) y Tratado de Funcionamiento de la UNIÓN EUROPEA (TFUE).....	179

3.6.- Decisión Marco 2006/960/JAI.....	181
3.7.- Directiva 2016/680 del Parlamento Europeo y del Consejo.	182
3.8. - EUROPOL.....	187
4.- Protección de datos personales versus cesión de datos a las autoridades policiales en España.....	195
4.1.- Legislación aplicable.....	195
4.2.- Cesión de datos en investigaciones policiales.....	196
5.- INTERPOL.....	198
Conclusiones.....	201

CAPÍTULO III
ADN FORENSE EN LA INVESTIGACIÓN POLICIAL
LA PROTECCIÓN DE LOS DATOS GENÉTICOS

1. -Nociones de biología celular.....	205
2.- ADN de uso forense.....	208
2.1.- Tipos de ADN utilizados en el ámbito forense.....	214
2.2.- Características del análisis de ADN forense.....	217
3.- Usos del ADN forense.....	220
3.1.- Criminal.....	225
3.2.- Humanitario.....	226
3.3.- Paternidad / Maternidad.....	226
4.- Muestra biológica y perfil genético.....	227
5.- Obtención de las muestras.....	233
5.1. - Muestra dubitada versus indubitada.....	236
5.2.- Obtención de muestras dubitadas.....	237
5.3.- Obtención de muestras indubitadas.....	242
5.3.1.- Con consentimiento del interesado.....	242
5.3.2.- Sin consentimiento del interesado.....	246
a.- Principio de Proporcionalidad.....	247
b. - Principio de razonabilidad.....	252
5.4.- Muestra atribuida.....	256

5.5.- Almacenamiento de las muestras.....	263
6.- Bases de datos de perfiles genéticos.....	269
6.1.- Marco normativo de la introducción de perfiles genéticos en las Bases de datos policiales de ADN en España	271
6.2.- Creación de Bases de datos policiales de ADN en España..	279
6.3.- Bases de datos de ADN de investigación criminal.....	282
6.4.- Sistema CODIS - (Combined DNA Index System) -.....	287
6.5.- Intercambio de perfiles genéticos a nivel internacional.....	291
6.5.1.- Bases de datos internacionales de perfiles genéticos.....	293
6.5.2.- Bases de datos nacionales que están vinculadas o en red. El Tratado de Prüm.....	298
7.- Introducción de perfiles genéticos en las bases de datos.....	303
7.1.- Según el tipo de delito investigado.....	303
7.2.- Situación procesal del donante de la muestra.....	310
7.3.- Cancelación de los datos.....	322
Conclusiones.....	326

CAPÍTULO IV

ADN FORENSE EN LA INVESTIGACIÓN CRIMINAL A LA LUZ DE LA EVOLUCIÓN JURISPRUDENCIAL EN EUROPA: PROPUESTA DE FUTURO.

1.- Introducción.....	333
2.- Búsqueda familiar – familial search - utilizando las bases de datos genéticas policiales.....	340
2.1.- Búsqueda familiar - familial search - usando las bases de datos policiales.....	345
2.1.1.- Búsqueda familiar indirecta.....	345
2.1.2.- Búsqueda familiar directa.....	347
2.1.2.1.- Coincidencia parcial inadvertida.....	348
2.1.2.2.- Coincidencia parcial intencionada.....	349

2.2.- ¿Pueden usarse bases de datos genéticas policiales para llevar a cabo este tipo de <i>familial search</i> ?.....	357
3.- Búsqueda familiar utilizando las bases de datos genéticas no policiales.....	364
3.1.- Tipos de Bases de datos genéticas no policiales.....	365
3.2.- Uso de bases de datos genéticos no policiales para la investigación de delitos graves.....	373
3.3.- Análisis genéticos en masa.....	377
4.- Problemática jurídica en el uso de la <i>familial search</i>	381
4.1.- Datos genéticos.....	383
4.2.- Implicación de distintos laboratorios.....	388
4.3.- Investigación policial que afecta a personas sin relación con el hecho delictivo.....	389
4.4.- El consentimiento informado, ¿es suficiente?.....	396
4.5.- Derecho a no conocer.....	400
4.6.- Uso de bases de datos genéticas policiales.....	403
4.7.- Uso de bases de datos genéticas NO policiales.....	416
4.8.- Destino final de las muestras genéticas.....	423
5.- La regulación de la <i>familial search</i> : propuesta de mejora.....	424
6.- Obtención de las EVC del donante de la muestra: una técnica de investigación genética complementaria y prometedora.....	433
6.1.- Identificación de la zona geográfica de procedencia.....	441
6.2.- Género.....	444
6.3.- Color de los ojos.....	445
6.4.- Color del pelo.....	446
6.5.- Inconvenientes de la obtención de EVC.....	447
6.6.- Ventajas del uso de EVC.....	454
Conclusiones.....	457
CONCLUSIONES GENERALES.....	463
Bibliografía.....	491

Abreviaturas Utilizadas

ADN	Ácido desoxirribonucleico
AIM	Marcadores Informativos de Ancestralidad
art.	Artículo
CAAS	Convenio de Aplicación del Acuerdo de Schengen
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CE	Constitución española
CEDH	Convenio Europeo de Derechos Humanos
CODIS	Combined DNA Index System
CP	Código Penal
DTC	Direct-to-Consumer Genetic Testing
EVC	Externally Visible Characteristics
FJ	Fundamento jurídico
p.	Página
SNP	Single Nucleotide Polymorphism
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STR	Short Tandem Repeats
STS	Sentencia del Tribunal Supremo

TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea
UE	Unión Europea

CAPÍTULO I

EL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS EN EUROPA

Introducción.

El establecimiento en la Unión Europea de un espacio sin fronteras facilita la circulación de personas entre los estados miembros, pero también favorece la delincuencia transfronteriza y el crimen organizado. La eliminación de fronteras va unida a la necesidad de reforzar la cooperación policial entre estados. Los diferentes cuerpos de policía de los distintos países que la forman deben trabajar coordinadamente compartiendo recursos, con rapidez y efectividad. Pero no solo las policías europeas entre sí, sino con las policías del resto del mundo. Hoy en día, un ciudadano comunitario puede despertarse en Roma, comer en Barcelona y dormir en Berlín, sin que nadie registre su documento al pasar la frontera.

Los cuerpos policiales trabajan con distintas bases de datos que les proporcionan la información necesaria para llevar a cabo una investigación criminal. Algunas de estas bases de datos están administradas por los mismos funcionarios que pertenecen al cuerpo policial - de huellas dactilares, personas con antecedentes policiales, perfiles de ADN,.. -; otras, en cambio, pertenecen a Estamentos Públicos, que son creadas y administradas para una finalidad concreta, distinta de la función policial – padrón municipal de habitantes, Registro Mercantil, datos tributarios, tráfico.. -; en cambio, otras bases de datos son privadas – compañías telefónicas, bancos, registros de datos de pasajeros,.. -. Todas ellas son bases de datos susceptibles de ser utilizadas por agentes policiales al llevar a cabo una investigación criminal.

La investigación policial debe estar en equilibrio con los derechos fundamentales de las personas ya que la protección de los derechos individuales fortalece a la persona como individuo frente al estado. Por este motivo deben promulgarse normas reguladoras del derecho a la protección de datos personales. Pero debe tenerse en cuenta que una protección demasiado férrea puede entorpecer las pesquisas de las autoridades policiales y favorecer al delincuente.

El derecho a la protección de datos personales nació a finales del SXIX, como parte del derecho a la intimidad, y a lo largo del SXX y principios del SXXI ha ido evolucionando hasta considerarse un derecho autónomo, principalmente a causa de la evolución del desarrollo de la informática y su aplicación al tratamiento de datos. En el primer capítulo de este trabajo vamos a ver en que consiste este derecho y el trato legislativo que se le da desde la Unión Europea.

1.- Derecho a la Intimidad y a la Protección de datos.

1.1- Derecho a la Intimidad.

Desde los tiempos del ensayo de Warren & Brandeis¹ de 1890, que articularon el *derecho a la intimidad* como el “derecho a estar solo” poniendo límite a las intrusiones de la prensa en la vida privada de las personas, el nuevo derecho pasó de formar parte del ordenamiento jurídico a través de la jurisprudencia al ser reconocido en declaraciones internacionales de derechos², llegándose a integrar en el

¹ WARREN y BRANDEIS, (1890).

² Por ejemplo, el art. 8 del CEDH protege el Derecho al respeto a la vida privada y familiar, así como el domicilio y la correspondencia, al igual que más tarde hizo la *Carta de Derechos Fundamentales* de la Unión Europea del año 2000 - art. 7 - que, a causa de la evolución de las nuevas tecnologías, amplió el término “correspondencia” que utilizaba el Convenio por las “comunicaciones” en general. También está recogido en la Declaración Universal de los Derechos Humanos de 1948 – art. 12 -, Pacto internacional

acervo de derechos de algunas de las Constituciones³ modernas europeas. El diccionario de la Real Academia Española define intimidad como *zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*. El Tribunal Constitucional español reconoce que el concepto *intimidad* – *al igual que el del honor* - son realidades intangibles, la extensión de los cuales vienen determinadas por cada sociedad y por el momento histórico⁴, partiendo “*de la idea originaria del respeto a la vida privada, personal y familiar, que debe quedar excluida del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado*”⁵. A este ámbito pertenecen la inviolabilidad del domicilio y la correspondencia⁶, así como los derechos a la propia imagen y a la intimidad personal - de la que forma parte la intimidad corporal⁷ - y familiar, vinculados estos últimos a la propia personalidad y la dignidad de la persona⁸.

de Derechos Civiles y Políticos de 1966 – art. 17 –, la Convención Americana sobre Derechos Humanos de 1969 – art. 11 -, la Declaración Universal de los Derechos Humanos de 1948 – art. 12 – o en el art. 8 de la Convención Europea de los Derechos Humanos – CEDH – de 1950.

3 El art. 18 de la *Constitución de España*, en el art. 33 de la *Constitución Portuguesa* de 1976, en el art. 14 – inviolabilidad domicilio - y art. 15 – secreto de las comunicaciones – de la *Constitución italiana*, en los art. 10 - el secreto de las comunicaciones postales y las telecomunicaciones – y art. 13 – inviolabilidad del domicilio – de la *Constitución Alemana*.

4 STC 171/1990 de 12 de noviembre.

5 STC 110/1984 de 26 de noviembre, FJ 3.

6 STC 110/1984 de 26 de noviembre, FJ 3.

7 STC 37/1989 de 15 de febrero, FJ 7.

8 STC 231/1988 de 1 de diciembre, FJ 3.

La intimidad es una manifestación y reconocimiento jurídico de una necesidad social del individuo, que debe tener un ámbito reservado e inaccesible a terceras personas. El ser humano necesita que el orden jurídico proteja sus esferas de vida durante toda su existencia; no solo por sí mismo, sino por la sociedad a la que pertenece⁹. El concepto de intimidad no puede ser cerrado; depende del individuo, de la sociedad; tiene un componente subjetivo. REBOLLO DELGADO¹⁰ reconoce tres conceptos de intimidad: **Concepto objetivo:** Atiende a la etimología del concepto en sí, acorde con la definición que da la Real Academia Española o el propio Tribunal Constitucional Español, cuando afirma la *“existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana”*. Así ese derecho *“confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido”*. *“Lo que garantiza el art. 18.1 CE es el secreto sobre nuestra propia esfera de vida personal, excluyendo que sean los terceros, particulares o poderes públicos, los que delimiten los contornos de nuestra vida privada”*¹¹. **Concepto subjetivo:** Se identifica con el

9 EICHLER (1973).

10 REBOLLO DELGADO (2004).

11 STC 159/2009 de 29 de junio, FJ 3; STC 185/2002 de 14 de octubre, FJ 3; STC 93/2013 de 23 de abril, FJ 8.

“*derecho a la autodeterminación informativa*” que significa que el individuo puede ejercer activamente el derecho a controlar los datos que registros públicos o privados tienen almacenados sobre él. Es una facultad propia del individuo derivada de la idea de autodeterminación.

Concepto de la teoría del mosaico: Este es el concepto más reciente e interesante y surge para proteger al individuo de las amenazas que - en particular la informática, y en general las nuevas tecnologías – suponen al derecho a la intimidad del individuo. Esta teoría, formulada por MADRID CONESA¹², afirma que los datos de una persona aisladamente no tienen ningún valor; pero considerados en un conjunto adquieren su significado, al igual que ocurre con las teselas de un mosaico.

Durante una investigación policial se va reuniendo información relativa a una o varias personas, información que puede consistir en números de teléfono, posicionamiento de la antena de telefonía móvil utilizada al realizar una llamada, personas con las que ese individuo se relacionan, direcciones, vehículos, pasos por peajes de autopistas, por citar algunos. Estos datos inicialmente puede parecer que aportan poca información, pero analizándolos en su conjunto pueden permitir conocer que es lo que este individuo ha

¹² MADRID CONESA (1984), p. 45.

estado haciendo un día determinado de su vida, revelando a extraños facetas que podrían pertenecer a la intimidad de las personas.

Si los datos se someten a un tratamiento adecuado con el objeto de obtener un resultado concreto, esos datos se convierten en información¹³.

1.2.- Intimidad versus privacidad.

La intimidad está ampliamente protegida en el ordenamiento jurídico internacional, así como en las distintas constituciones de los países de la UE que otorgan el derecho a la intimidad de las personas el rango de derecho fundamental. No es el caso de la *privacidad*.

El concepto de privacidad (*privacy* en inglés) es demasiado vago, impreciso, confuso y los diferentes conceptos que sobre el término existen, pueden hacer perder su valor legal. Es relativamente sencillo reconocer una lesión en el derecho a la privacidad pero crear un concepto articulado que sea de fácil aplicación resulta más difícil. A esto se le añade el problema que derechos como el de la libertad de expresión, el de la libertad personal o el de la seguridad, que a menudo

13 REBOLLO DELGADO (1998), p. 181.

entran en conflicto con el derecho a la privacidad, son más fáciles de definir, reconocer y proteger.

Como recordaba muy bien el Preámbulo de la derogada Ley Orgánica 5/1992¹⁴, no hace muchos años las fronteras de la privacidad estaban defendidas por el tiempo y el espacio: el primero hacía que el recuerdo se desvaneciera, no permitiendo que se pudiera construir una historia lineal sobre una persona; el segundo dificultaba el tener noticia de los hechos protagonizados por los demás que ocurrían lejos del lugar donde nos encontrábamos.

Durante la segunda mitad del SXX, para definir privacidad tuvo una extensa acogida la teoría *de las esferas* – *Sphärentheorie* – de HUBMAN H.¹⁵: En ella la **esfera íntima** hacía referencia a lo secreto, los sentimientos, los pensamientos, las creencias, etc.. Son noticias que deben permanecer ajenas al resto de las personas y, cuando alguien las difunde sin consentimiento, la esfera es violada. Envolviendo a ésta, estaba la **esfera privada** que protege el ámbito de la vida familiar y personal. Se desea mantener al margen de la injerencia de ciertas personas. La esfera

14 Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal que fue derogada en su día por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

15 DELGADO REBOLLO (1998).

privacidad es más amplia que la **íntima**: mientras la primera “*constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado*”, la segunda hace referencia a la esfera donde se llevan a cabo las facetas más reservadas de la vida de las personas, tales como el domicilio – lugar donde se llevan a cabo sus actos más íntimos – o las comunicaciones que mantiene con las otras personas de su entorno¹⁶. Finalmente, en el exterior y envolviendo las otras dos esferas, se encontraría la **esfera individual** que se refiere a la peculiaridad de la persona (imagen, reputación, datos personales,...). Contiene los elementos que nos diferencian los unos de los otros y hace que seamos singulares. El Tribunal Europeo de Derechos Humanos superó esta teoría al reconocer que el concepto de vida privada también debe comprender un cierto grado de desarrollo de relaciones con otros seres humanos y por tanto no deben excluirse, por ejemplo, las relaciones surgidas de las actividades laborales o profesionales, ya que en la vida diaria de las personas puede resultar difícil distinguir entre lo que pertenece a su

¹⁶ Preámbulo de la derogada Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

vida laboral y lo que no¹⁷. El Tribunal Constitucional Federal Alemán por su parte, acuñó el concepto de la “*autodeterminación informativa*” surgida a partir de la Sentencia del Censo electoral¹⁸ de 1983, según la cual la intimidad no es aislacionismo, sino el control que posee el individuo de “*a quién, qué y con qué ocasión*” éste puede facilitar los datos sobre su persona a un tercero¹⁹. El individuo puede ejercer activamente el derecho a controlar los datos que registros públicos o privados tienen almacenados sobre él.

Por su parte, GARZON VALDES²⁰ da unas definiciones más sencillas de lo que se puede considerar íntimo, privado y público. La ***intimidad*** es el último reducto de la personalidad, donde el individuo es lo que es y cualquier intervención de una persona ajena afecta a la dignidad del individuo como

17 STEDH de 16 de diciembre de 1992. Caso Niemietz c. Alemania, párrafo 29.
En la STEDH de 25 de junio de 1997, Caso Halford c. Reino Unido, el Tribunal pone bajo el paraguas de la protección del Art. 8 de la Convención tanto las llamadas telefónicas realizadas desde el hogar como desde el lugar de trabajo. Ambas están amparadas por el derecho a la privacidad.

18 Ley del Censo de Población de 1983 fue aprobada por el Bundestag el 4 de marzo de 1982 y publicada el 31 de marzo del mismo año. La sentencia del Tribunal Constitucional Alemán anulando parcialmente la ley se puso el 15 de diciembre de 1983. En una época en que el emplazamiento de los misiles era secreto, esta ley obligaba a los ciudadanos a dar gran cantidad de información sobre sí mismos. La sentencia del Tribunal elevó a Derecho Constitucional la facultad que tiene el individuo de determinar “por sí mismo la divulgación y la utilización de los datos referentes a su persona”.

Traducción de DARANAS PELAEZ (1984).

19 REBOLLO DELGADO (1998), p. 161.

20 GARZON VALDES (2003), p. 16 y ss.

ser humano. Es ajena a la intervención de terceros en las acciones que comporta. La **privacidad** es un ámbito reservado a un tipo de relaciones en el que el individuo selecciona sus participantes, donde sus límites vienen impuestos por el contexto social y cultural del individuo. Es una condición necesaria para ejercer la libertad personal. Finalmente, **público**, es el ámbito del individuo al que todas las personas tienen acceso. Si el ámbito personal de un individuo se cubriese con un velo, la zona opaca del velo cubriría lo que este considerara íntimo, el ámbito público sería cubierto con un velo transparente y el ámbito privado se cubriría por un velo con una transparencia relativa, que no permitiera que fuera visto todo.

THOMPSON entiende la *privacidad* en termino de control: la capacidad que tienen los individuos de tener control sobre la información, “controlar las revelaciones sobre uno mismo, y de controlar cómo y hasta qué punto éstas pueden comunicarse a los demás”²¹. Hay que abandonar la idea de privacidad en términos de espacio físico; en el mundo de las tecnologías de la información y de las comunicaciones, la privacidad debe abrirse a nuevas dimensiones. Cuando alguien se conecta a Internet desde su casa, puede revelar datos sobre su persona a miles de usuarios en la red,

21 THOMPSON (2011), p. 29 y ss.

creyendo que tiene el control sobre la cesión de información, cuando realmente ya no la tiene.

SOLOVE²² afirma que la doctrina ha desarrollado numerosos conceptos de privacidad, que se solapan entre sí y que la definen desde distintos ángulos.

Así privacidad se puede definir como:

Derecho a estar solo.

Evitar que personas no deseadas accedan a datos o informaciones sobre uno mismo.

Confidencialidad.

Control sobre la información personal.

Protección de la personalidad, individualidad y dignidad.

Controlar el acceso de terceras persona a las relaciones o a aspectos de la intimidad de una persona.

La privacidad protege al individuo de trastornos que pueden producirse en ciertas actividades, que incluso pueden destruir o inhibir estas actividades.

²² SOLOVE (2008), p. 12.

Siguiendo con este autor²³, son muchas las virtudes de la privacidad hacia el individuo. Esta permite que el individuo pueda reducir las tensiones de la vida diaria generadas por las relaciones sociales, retraerse y descansar, permitiendo momentos de contemplación espiritual o intelectual, de autorreflexión. Así puede desarrollar la libre asociación, la discusión política y la expresión creativa, aspectos que de hacerse públicas de manera temprana y recibir severas críticas podrían causar un daño irreparable.

También tiene sus detractores. Ya los antiguos griegos definían la privacidad negativamente, en términos de carencia, considerándola secundaria frente a la esfera pública, que era lo que realmente importaba en su sociedad. Asumían la privacidad como el espacio necesario que se le debía dar al individuo para que sobreviviera y pudiera participar de la esfera pública²⁴. Otro ejemplo son las sociedades comunales, que carecen de privacidad²⁵ porque reduce el control social que se hacen sus miembros entre sí, favoreciendo así las actividades ilícitas y dificultando el establecimiento de la confianza entre los conciudadanos. En

23 SOLOVE (2008), p. 79 y ss.

24 THOMPSON (2011), p. 26 y ss.

25 En su obra UTOPIÍA (1532), Tomás MORO decía "*Todos, expuestos a las miradas de todos, se entregan al trabajo cotidiano o a un honesto esparcimiento*" (p. 37).

Consultada en <https://biblioteca.org.ar/libros/300883.pdf> (última consulta 18/03/2022).

las sociedades patriarcales, la opresión de las mujeres se lleva a cabo en el seno de la familia cuyas relaciones quedan bajo el paraguas de la privacidad²⁶. La sociedad no entra a valorar lo que ocurre en el seno familiar. También hay autores que piensan que la privacidad va en detrimento de la sociedad, que entra en conflicto con sus valores importantes, como pueden ser la libertad de expresión, la protección de la propiedad privada o la prevención y castigo del crimen. Hay el peligro que la privacidad sea vista como una construcción antisocial.

En esta línea, CATE²⁷ enumeró una serie de costes que la sociedad debe estar dispuesta a pagar para gozar del derecho a la privacidad. Resumidamente, algunos de estos costes son:

- Facilita la distribución de información falsa. O dicho de otro modo, no permite comprobar cierto tipo de información, de manera que si alguien miente en algún aspecto – salud, económico,... - no puede comprobarse.

26 “Los hombres están a cargo de las mujeres debido a la preferencia que Allah ha tenido con ellos, y deben mantenerlas con sus bienes. Las mujeres piadosas obedecen a Allah y a sus maridos, y cuidan en ausencia de ellos [su honor y sus bienes] encomendándose a Allah”. Corán, 4:34.

27 CATE (1997), p.102.

- Protege a la persona que esconde información valiosa²⁸.
- Interfiere de manera significativa en la selección de personal.
- Incrementa el coste de provisión de los bienes y servicios, ya que si se han de hacer comprobaciones, se necesita tener el consentimiento de la persona interesada para hacer solicitudes o que el mismo interesado facilite los datos.

Estas comprobaciones pueden provocar retrasos significativos que afecten al usuario ya que este puede no disponer de los datos que se necesiten en ese preciso momento²⁹.

28 El copiloto del vuelo 9525 de Germanwings estrelló el aparato el 24 de marzo de 2015 en el macizo de Estrop (Francia) estuvo años bajo tratamiento psicoterapéutico por sus tendencias suicidas, cosa que era desconocido por la compañía para la que trabajaba ya que se trataba de información secreta. https://www.ondacero.es/noticias/mundo/copiloto-estaba-baja-medica-habia-ocultado-germanwings-dia-accidente_20150327553e3d9e0cf2a0530b725757.html (última consulta 18/03/2022).

29 Por ejemplo, la consulta de datos sanitarios que en el preciso momento que se necesitan no se puede acceder por la burocracia establecida y el usuario los desconoce.

- Interfiere en la seguridad física de los ciudadanos, además de dificultar la prevención y el castigo del crimen, entra en conflicto con la seguridad nacional.

El no revelar el pasado delictivo de una persona hace que los ciudadanos no se puedan proteger debidamente. ¿A quién no le gustaría saber si la persona que ha contratado para cuidar a la persona mayor de la familia, ha cometido con anterioridad alguna infracción penal en otros domicilios para los que había sido contratada de igual forma?

- También interfiere en el derecho a la libertad de expresión, el de la sociedad que tiene derecho a conocer.

Son numerosos los artículos periodísticos³⁰ que afirman que en la sociedad actual no existe privacidad, que ha muerto, está sitiada o está seriamente amenazada. Aun así, hay personas que, siendo conocedores de los riesgos, no vacilan en facilitar sus datos personales en la red, revelando detalles íntimos de sus vidas privadas, colgando fotografías en redes

³⁰ <https://www.lanacion.com.ar/opinion/la-privacidad-ha-muerto-podemos-seguir-siendo-libres-nid1965126/> noticia del 11/12/2016 (última consulta 18/03/2022).

<http://www.elmundo.es/sociedad/2017/03/19/58cd7462468aebc5428b45ca.html> noticia del 19/03/2017 (última consulta 21/11/2021).

sociales abiertas a todos los usuarios. Todo y que el tratamiento de datos debe ser concebido para servir a la humanidad³¹, lo cierto es que es un activo económico importante en nuestra sociedad. Hoy en día hay mucha información personal repartida por distintos ámbitos: los bancos saben cuánto dinero ganamos y en qué nos lo gastamos, si estamos matriculados en un curso o donde vamos de vacaciones; las compañías telefónicas saben con quién hablamos por teléfono y pueden localizarnos a través de sus repetidores de telefonía; Google sabe que buscamos en Internet y nos puede “aconsejar” para encontrar lo que buscamos; la Administración Sanitaria sabe las veces que nos hemos puesto enfermos los últimos 10 años o si padecemos alguna enfermedad grave.

Atravesamos la que se ha llamado la cuarta revolución industrial, marcada por la convergencia de tecnologías digitales, físicas y biológicas, caracterizada por el uso intensivo de las nuevas tecnologías y la creación de una sociedad digital. Cada vez es más fácil generar, tratar, guardar y transmitir la información; además, es más valiosa la

31 Considerando 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

información recogida digitalmente que la que está en papel, ya que la transmisión es más rápida.

En esta nueva sociedad, el último reducto de protección que le queda a la Privacidad es el Derecho. La ley es la que impide a los gigantes de Internet, bancos, agencias de viajes, compañías de telefonía y a un largo etcétera de empresas, utilizar los datos de los usuarios con otros fines distintos para los que fueron recogidos³², al menos sin el consentimiento del propietario real de la información, que es el propio usuario. Con las nuevas tecnologías no hay refugio para los datos; el simple uso de las propias tecnologías genera información con la que la misma empresa prestadora del servicio puede comerciar.

Pero la ley no debe convertirse en la madriguera del que es perseguido por ella. Si tenemos una sociedad sin fronteras, debemos tener seguridad sin fronteras y los remedios a aplicar deben ser sin fronteras también. Debe haber un equilibrio entre el derecho a la privacidad, la intimidad y la protección de datos por un lado y el derecho a la seguridad pública y a la tutela judicial efectiva por el otro. Se deben disponer de herramientas legales para poder acceder, quirúrgicamente a la información necesaria para luchar eficazmente contra el crimen.

³² SOCIETY et al. (2003) p 5.

2.- El Derecho a la protección de datos personales.

2.1.- Un nuevo Derecho.

La evolución tecnológica ha llevado a desarrollar enormemente las técnicas de recolección y almacenamiento de datos amenazando la privacidad de los ciudadanos. Por poner un ejemplo, los dispositivos móviles que llevamos en el bolsillo permiten saber las personas con las que nos comunicamos habitualmente, el contenido y los destinatarios de los mensajes enviados, el recorrido que hemos realizado a lo largo de un día determinado, las páginas de Internet que hemos visitado y así hasta un largo etcétera. Son pautas de comportamiento que deberían pertenecer a la esfera privada del individuo y a la cual deberían dejar acceder a las personas que el propio usuario autorizara³³. Hace unos años estos datos por separado eran inocuos, difícilmente podían dar una información relevante sobre un individuo concreto. Hoy en día, los avances informáticos y los datos que las distintas empresas y organismos públicos y privados guardan de los ciudadanos, han supuesto para la privacidad una

³³ La STC 292/2000 define el derecho a la protección de datos como “un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso” (STC 292/2000, FJ 7).

amenaza potencial que era desconocida hasta el momento. Han hecho desaparecer las barreras del tiempo y del espacio.

Los datos personales se encuentran almacenados en bases de datos accesibles a través Internet: la clasificación de los participantes en una carrera de fondo comarcal, el currículum personal de una persona que está buscando trabajo, noticias acontecidas hace años o multas de tráfico de un individuo están en la red. Todo ello estará almacenado y visible para todo el mundo hasta que alguien lo borre. La Comisión Europea ha hecho suya esta preocupación y ha decidido regular el “derecho al olvido”³⁴, para que el tiempo pueda seguir siendo una “pequeña” frontera a la privacidad. Pero la barrera del espacio parece haber caído definitivamente, ya que en la era de la comunicación e Internet tenemos conocimiento casi instantáneo de lo que ocurre en el otro lado del planeta.

Por poner un ejemplo de como el tratamiento de datos puede afectar al conocimiento que se puede adquirir sobre los hábitos de una persona, basta citar al TJUE cuando afirma

³⁴ STJUE de 13 de Mayo 2014, Google Spain and Google, C-131/12, EU:C:2014:317.

Posteriormente el derecho al olvido o de “supresión” se incorporó a la legislación europea en el Art 17 del Reglamento (UE) 2016/679, según el cual el interesado tiene derecho a pedir al responsable del tratamiento el borrado de los datos que consten en la base de datos.

que “*estos datos – refiriéndose a los datos de tráfico y de localización de los abonados y usuarios registrados de las compañías telefónicas - considerados en su conjunto, permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan*”³⁵.

Por lo tanto debemos marcar nuevas barreras que delimiten la privacidad, protegiéndola de las herramientas que la hacen más vulnerable: el uso de la informática o, en otras palabras, el tratamiento de los datos. Como dice LUCENA CID³⁶, las redes sociales y otros recursos informáticos asociados a Internet, las nuevas aplicaciones en dispositivos móviles, las bases de datos personales, los sistemas de control de los ciudadanos a través de sofisticados mecanismos para garantizar la seguridad y el orden social, etc. han quebrado los límites de las distintas esferas que separaban la intimidad, la privacidad y lo público, siendo este último la zona que se caracteriza por el libre acceso del resto de las

35 STJUE de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970. Apartado 99.

36 LUCENA CID (2014), p 30.

personas a las decisiones y actividades que realiza el individuo³⁷.

Así como el derecho a la intimidad implica el poder jurídico que tiene el individuo a rechazar intromisiones ilegítimas en su esfera íntima – un derecho de defensa -, el derecho a la protección de datos tiene por objeto preservar la información individual frente al uso incontrolado y no deseado de dicha información por parte de un tercero³⁸. El fundamento de este derecho es la dignidad de la persona y el libre desarrollo de la personalidad.

Siguiendo a REBOLLO³⁹ se pueden distinguir hasta tres generaciones de normas de protección de datos personales:

1.- Durante la *primera generación*, es la administración pública quien dispone de bases de datos y la protección radica sobre el lugar donde se ubica la información físicamente y los accesos permitidos para consultar la información. No se hace referencia a los archivos de datos de carácter privado.

37 GARZON VALDES (2003).

38 REBOLLO DELGADO (1998), p.179.

39 REBOLLO DELGADO& SERRANO PEREZ (2006), p. 23 y ss.

Se crean instituciones encargadas del control del tratamiento que dan cuenta al Parlamento directamente⁴⁰.

2.- En la *segunda generación* se tiene en cuenta la lesión de derechos por parte de individuos ajenos a las instituciones estatales que hacen un uso indebido de los datos personales. Se establecen los principios básicos de tratamiento de datos personales, como son el consentimiento del titular al tratamiento, el derecho de acceso y control o el de informar en el momento de la recogida de los datos de la finalidad de la misma⁴¹.

En una fase posterior, se incide en el tratamiento de datos sensibles – raza, ideología, religión,... -.

3.- La *tercera generación* nace con la proclamación de la autodeterminación *informativa* por parte del Tribunal Federal Alemán cuando declaró anticonstitucional la “Ley del censo” de 1982. En esas fechas (1 de enero de

40 De esta época son la *Datenschutz* de 1970, ley sobre tratamiento de datos personales del Land de Hesse o la *Bundesdatenschutzgesetz*, Ley Federal de Protección de Datos de 1977, ambas de la República Federal de Alemania.

También la *Data Lag* 1973/289, por la cual Suecia imponía un sistema de registro abierto para publicitar los bancos de datos personales relativo a personas físicas realizado por medios automatizados.

41 De esta época son la *Loi n.º 78-17* du janvier, relative à l’informatique, aux fichiers et aux libertés, adoptada en Francia en 1978 o la *Privacy Act* de 1974 de estados Unidos.

1983) aparece Internet, lo que provoca una evolución técnica de las telecomunicaciones que hace que puedan vulnerarse derechos fundamentales con mayor facilidad. El uso de computadoras se generaliza, al igual que la transmisión de información, con el riesgo a los derechos fundamentales que supone.

A la larga conlleva que los países deban actualizar sus normas de protección de datos – los que las tengan – o crearlas – las que no las tenían⁴².

2.2.- La protección de datos personales en Europa

El principal motivo que inició la preocupación por tutelar la privacidad y la intimidad de los ciudadanos fueron los avances tecnológicos que se iban produciendo en la década de los sesenta⁴³. Ya en la primera Conferencia Internacional de Derechos Humanos que se celebró en Teherán del 23 de abril al 13 de mayo de 1968 para examinar los progresos obtenidos después de 20 años de la promulgación de la Declaración Universal de Derechos Humanos, se alertaba que los descubrimientos científicos y los adelantos tecnológicos podían comprometer los derechos y libertades

42 Responde a esta orientación el Convenio 108 adoptado por la Comunidad Económica Europea en 1981 o la antigua Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

43 ALMUZARA ALMAIDA et al. (2005), p. 33.

de los individuos. En la misma línea, la Resolución 509 de la Asamblea del Consejo de Europa adoptada el mismo año, proponía al Comité de Ministros que se estudiara si, bajo el prisma del artículo 8 del CEDH, la legislación de los estados Miembros protegían el derecho a la privacidad contra las violaciones que podían producirse con el uso de los modernos métodos científicos y técnicos.

El Consejo de Europa siguió preocupándose por la Protección de Datos y en 1973 y 1974 promulgó sendas resoluciones del Consejo que establecían la protección de datos personales en los bancos de datos automatizados del sector público⁴⁴ y en el privado⁴⁵. Con la finalidad de fortalecer la unión de los países que formaban parte del Consejo de Europa y para ampliar la protección del respeto a la vida privada de sus ciudadanos, teniendo en cuenta la circulación de datos de carácter personal a través de las fronteras y la libre circulación de la información, en 1981 se promulgó el **Convenio 108 sobre Protección de Datos del**

44 Resolución 22/1973, de 20 de noviembre, del Consejo de Europa sobre regulación jurídica de los ficheros electrónicos en el sector privado. Consultada en: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830> (última consulta 18/03/2022).

45 Resolución 29/1974, de 29 de noviembre, para establecer pautas ordenadoras del sector público de la informática. Consultada en: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51> (última consulta 18/03/2022).

Consejo de Europa⁴⁶. Dividido en siete capítulos, enumera los principios básicos que debe tener todo tratamiento de datos de carácter personal. Establece además la libre circulación de los datos a través de las fronteras de los estados firmantes con una protección para los datos personales equivalente. Crea también las Autoridades Nacionales en protección de datos. Posteriormente fue ampliado por el **Protocolo de 2001**⁴⁷, donde se abordan cuestiones relativas a las autoridades de control y al flujo transfronterizo de datos personales. El Convenio ha sido ratificado por todos los países del Consejo de Europa, no así el Protocolo⁴⁸.

El Consejo de Europa ha considerado más oportuno legislar la Protección de datos adoptando Recomendaciones⁴⁹ de carácter sectorial, entre las que está la **Recomendación**

46 Convenio n° 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.

47 Protocolo adicional del Convenio núm. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a transferencias de datos firmado en Estrasburgo a 8 de noviembre de 2001. Protocolo disponible en: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Protocolo-adicional-al-Convenio-108-2001.pdf> (última consulta 18/03/2022).

48 Falta por firmar el Protocolo: Azerbaiyán, Malta, San Marino, Eslovenia. Falta por ratificar: Bélgica, Grecia, Islandia, Italia, Noruega, Rusia y Reino Unido.

49 Las Recomendaciones no constituyen instrumentos jurídicos con caracteres de positividad, que permitan ser aplicadas directamente, pero son opciones técnicas, que traducen un consenso de los estados Europeos.

(87)15⁵⁰, emitida por el Comité de Ministros del Consejo de Europa, relativa al tratamiento de los datos personales en el sector de la policía, y sobre la que volveremos más adelante.

Por su parte, la UE desarrolló una amplia labor legislativa en esta materia con la aprobación de la **Directiva 95/46/CE**. Ésta exigió a los estados miembros de la UE que protegieran los derechos y libertades de las personas físicas respecto al tratamiento de sus datos personales⁵¹. Los tres primeros considerandos de la Directiva eran una clara muestra de intenciones. Si se tenía que garantizar la circulación de estos datos entre los miembros de la Unión, los datos y su tratamiento tenían que cumplir una serie de garantías relativas a la calidad de los datos o la legitimidad del tratamiento, a la vez que otorgar una serie de derechos a los interesados.

Con el tiempo, la **Directiva 95/46/CE** fue desarrollada en algunos sectores⁵². No así en el ámbito penal, ya que no era

50 Recomendación n.º R(87)15 del Comité de Ministros del Consejo de Europa a los estados miembros por la que se regula el uso de datos personales en el ámbito policial (adoptada por el Comité de Ministros el 17 de septiembre de 1987).

51 Art. 1 de la Directiva 95/46/CE.

52 - **Transporte de viajeros** - Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

- **Comercio electrónico** - Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

de aplicación en las actividades del estado en materia criminal y, en cualquier caso, al tratamiento de datos que tenían por objeto la seguridad pública, la defensa y la seguridad del estado.

A partir del 25 de mayo de 2018, la **Directiva 95/46/CE** queda derogada por el **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).**

El Reglamento establece que el Derecho de la Unión o de los estados miembros, a través de medidas legislativas, puede limitar el alcance de los derechos del interesado. También obliga a comunicar una violación de la seguridad de sus datos personales al interesado. Esta limitación deberá respetar en lo esencial los derechos y libertades fundamentales y ser una medida necesaria y proporcionada en una sociedad democrática para – entre otros ámbitos - la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales,

incluida la protección frente a amenazas a la seguridad pública y su prevención⁵³.

Por este motivo, en el mismo diario⁵⁴ donde se publicó el Reglamento General de Protección de datos de la UE, se publicó también la **Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016**⁵⁵ que establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales por parte de las autoridades competentes en la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, marcando límites a los derechos de los ciudadanos en el ámbito de la protección de datos con la finalidad de garantizar la adecuada protección de los datos de las víctimas, testigos e investigados por la presunta comisión de delitos a la vez que facilita la libre circulación de datos personales desde la UE a organismos internacionales que luchan contra el crimen, como es el caso de INTERPOL⁵⁶.

53 Art. 23.d del Reglamento (UE) 2016/679.

54 Diario Oficial de la Unión Europea (DUE) nº 119 de 4 de mayo de 2016.

55 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

56 Considerando 25 Directiva (UE) 2016/680.

Si los estados miembros encomiendan a las autoridades competentes en esta materia otras funciones que no necesariamente se lleven a cabo con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, ese tratamiento de datos personales entrará dentro del ámbito de aplicación del **Reglamento (UE) 2016/679**.

2.3.- La protección de datos personales en la jurisprudencia europea.

La Protección de datos personales según el TEDH.

El TEDH considera que la protección de los datos personales juega un papel fundamental en el ejercicio del derecho al respeto de la vida privada y familiar que el art. 8 de la Convención garantiza⁵⁷. El almacenamiento de este tipo de datos entra dentro de su ámbito de protección ya que el término *vida privada* tiene una noción amplia y no es susceptible de una definición exhaustiva. Hace referencia a la integridad física y moral del individuo y, a veces, a su identidad física y social. Abraza elementos como la orientación sexual o la identificación de género o nombre, por citar a algunos⁵⁸. Además, no debe hacerse una distinción entre actividades profesionales o personales; el individuo

57 STEDH de 25 de febrero de 1997. Caso Z. c. Finlandia, párrafo 95.

58 STEDH de 29 de abril de 2002. Caso Pretty c. Reino Unido, párrafo 61.

tiene derecho a desarrollar relaciones con otros seres humanos en cualquier ámbito de su vida y estas quedan amparadas por este artículo⁵⁹.

No todos los datos de carácter personal tienen porqué considerarse relativos a la vida privada de una persona, pero el tratamiento de dichos datos constituirá una injerencia a la vida privada del individuo atendiendo al tipo de información retenida, su naturaleza, la manera en la que estos serán tratados y los resultados que podrán inferirse⁶⁰. Los datos personales forman parte de la esfera de la vida privada del individuo y que éste debe poder decidir libremente sobre ellos. No es que haya nacido el nuevo Derecho a la protección de los datos personales: es que las nuevas tecnologías han experimentado tal avance que han creado nuevas formas de lesión de ciertos Derechos. Se ha creado una nueva necesidad. Además, la protección recae sobre los datos personales automatizados y los no automatizados, ya que ambos modos de tratamiento forman parte del derecho a la vida privada.

Pero éste no es un derecho absoluto. Así, el Convenio permite la injerencia⁶¹ de los poderes públicos en la esfera de

59 STEDH de 26 de marzo 1987. Caso Leander c. Sweden, párrafo 48.

STEDH de 16 de febrero de 2000. Caso Amann c. Suiza, párrafo 65.

60 STEDH de 4 de diciembre de 2008. Caso Marper c. Reino Unido, párrafo 67.

protección de los derechos y limitarlos. Dicha limitación debe cumplir los siguientes requisitos:

1.- Estar prevista por la ley. *“En opinión del Tribunal, las dos condiciones siguientes se encuentran entre las que explican la expresión ‘previstas por la ley’. La primera hace referencia a que la ley tiene que ser lo suficientemente accesible: el ciudadano tiene que disponer de patrones suficientes que se adecúen a las circunstancias de las normas legales aplicables al caso. La segunda condición se refiere a que una norma no puede considerarse ley a menos que se formule con la suficiente precisión que permita al ciudadano adecuar su conducta.”*⁶² Y debe entenderse por ley las disposiciones inferiores al rango legislativo y al "Derecho no escrito"⁶³.

La norma debe prever descripciones detalladas, como por ejemplo sobre el tipo de información que se pueda almacenar, el periodo de tiempo de almacenamiento,

61 El Art. 8 del CEDH, donde está recogido el derecho a la vida privada, es un artículo de dos párrafos. Al igual que los artículos 9 - libertad de pensamiento, de conciencia y de religión -, 10 - libertad de expresión - y 11 - libertad de reunión y de asociación -. En todos ellos el primer párrafo define el derecho y el segundo el cómo puede ser limitado.

62 STEDH de 6 de noviembre de 1980. Caso Sunday Times c. Reino Unido, párrafo 49.

63 STEDH de 24 de abril de 1990. Caso Kruslin c. Francia, párrafo 29.

personas autorizadas a realizar consultas o el acceso del interesado a la información, entre otros⁶⁴.

2.- Ser una medida necesaria en una sociedad democrática para perseguir un fin legítimo. Y la sociedad democrática incluye *“pluralismo, la tolerancia y el espíritu de apertura”*⁶⁵. Debe constituir *“una medida que en una sociedad democrática sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y las libertades de los demás”*⁶⁶.

En este sentido el TEDH da un cierto *margen de apreciación* a cada estado, dándole un cierto poder discrecional para crear las normas, poder que no es ilimitado⁶⁷.

3.- Los límites que se establecen al derecho deben ser proporcionales para los fines perseguidos. “Una

64 STEDH de 4 de mayo de 2000. Caso Rotaru c. Rumanía, párrafo 57.

65 STEDH de 7 de diciembre de 1976. Caso Handyside c. Reino Unido, párrafo 49.

66 STEDH de 6 de septiembre de 1978. Caso Klass y otros c. Alemania, párrafo 39.

67 STEDH de 6 de septiembre de 1978. Caso Klass y otros c. Alemania, párrafo 49.

*restricción a un derecho consagrado por el Convenio debe ser proporcionada al fin legítimo conseguido*⁶⁸.

Así, en lo que respecta al derecho a la protección de datos, el TEDH ha afirmado en varias sentencias que almacenar información relativa a la vida privada de las personas y su posterior publicación está bajo el ámbito de protección del artículo 8.1 del CEDH⁶⁹. La injerencia en el derecho a la protección de datos puede darse en cualquiera de las tres fases que requiere el tratamiento de datos: la fase de obtención de los datos de un individuo particular, la fase de proceso o uso de los datos obtenidos o en la de publicación de los mismos de más allá de lo previsible⁷⁰.

El derecho a la protección de datos personales puede verse limitado también al entrar en conflicto con otros derechos, como el de libertad de expresión o para promover la transparencia en las Administraciones Públicas, por ejemplo. Así un periodista que publica sobre unos hechos que forman parte de una investigación en

68 STEDH de 18 de octubre de 1982. Caso Young, James y Webster c. Reino Unido, párrafo 63.

69 STEDH de 26 de marzo de 1987. Caso Leander c. Suecia, párrafo 48.
STEDH de 16 de febrero de 2000. Caso Amann c. Suiza, párrafos 65 y 69-70.
STEDH de 4 de mayo de 2000. Caso Rotaru c. Rumanía, párrafo 43.
STEDH de 18 de octubre de 2011. Caso Khelili c. Suiza, párrafo 55.

70 STEDH de 2 de septiembre de 2010. Caso Uzun c. Alemania, párrafo 45.

curso en la que se dan datos de personas fácilmente identificables – algo muy común en nuestro país -, o la publicación de subvenciones concedidas por la Administración a personas físicas o jurídicas, pueden afectar el derecho a la protección de datos de las personas aludidas. Consideraciones que se escapan al objeto del presente estudio.

La Protección de datos personales según el Tribunal de Justicia de la Unión Europea - TJUE.

Ante la ausencia de un catálogo de Derechos Fundamentales en los Tratados Constitutivos de la Comunidad Económica Europea, fue el anteriormente llamado *Tribunal de Justicia de Luxemburgo* el que moldeó el sistema de protección de derechos fundamentales partiendo de las tradiciones constitucionales comunes de los distintos estados miembros de la época y de las disposiciones del CEDH.

Inicialmente, el Tribunal no va más allá de la literalidad de los textos constitucionales y se niega a enjuiciar la aplicación del derecho interno de los propios estados ya que su función consiste en dirimir sobre la aplicación de las normas que emanan del Derecho Europeo. Esta fase es conocida como la fase “*inhibicionista*”⁷¹ que acabará a finales de los años 60,

71 LLANO C.H. (2005), p. 130.

reconociendo los derechos fundamentales como parte de los Principios Generales del Derecho Comunitario.

En una segunda fase, Tribunal pasa de inhibirse a constituir: ya que no hay un catálogo propiamente dicho de derechos fundamentales, lo va creando a partir de las tradiciones constitucionales comunes de los estados miembros y de los tratados internacionales para la protección de los Derechos Humanos en los cuales han sido parte o a se han adherido los estados miembros⁷². Este nuevo sistema de protección se va haciendo a “*golpe de sentencia*”⁷³ o de “*construcción de constitución*”⁷⁴, inaugurando esta actividad “*pretoriana*” del Tribunal con la sentencia del caso STAUDER. Éste es a la vez, el primer caso en el que el TJUE resuelve sobre la protección de datos. Hace referencia a si los bonos nominales que se concedían a los beneficiarios de ayuda social – que contenían los datos personales - podía violar su dignidad humana, ya que desvelaban un aspecto de la persona interesada que ésta no deseaba revelar a la sociedad en general. El Tribunal resuelve en el sentido que la “*disposición controvertida no ha revelado ningún elemento que permita cuestionar los derechos fundamentales de la*

72 STJUE de 14 de mayo de 1974, Nold, C-4/73, EU:C:1973:51, párrafo 13.

73 ARENAS RAMIRO M. (2008), p. 117.

74 IGNACIO y ECEIZABARRENA (2014), p. 448.

*persona subyacentes en los principios generales del Derecho comunitario*⁷⁵.

En sentencias posteriores, el TJUE considera que el acceso a los datos personales de los ciudadanos por parte de las autoridades públicas constituye una injerencia al artículo 7 de la Carta relativo al respeto a la vida privada, aunque la injerencia no sea considerada grave e independientemente que los datos en cuestión tengan o no carácter sensible⁷⁶. La simple transmisión y almacenamiento de los datos personales de una autoridad pública ya implica una injerencia a dicho Derecho. A la vez supone también una injerencia al Derecho fundamental de protección de datos personales recogido en el artículo 8 de la Carta, puesto que la mera transferencia de datos personales, su conservación y utilización ya constituye un tratamiento de los mismos⁷⁷.

Las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario. Por ello la normativa *“que conlleve la injerencia debe establecer reglas claras y precisas que regulen*

75 STJUE de 12 de noviembre de 1969, Stauder, C-29/69, EU:C:1969:57, párrafo 7.

76 STJUE de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, párrafo 51.

77 Dictamen del Tribunal de Justicia (Gran Sala) de 26 de julio de 2017. Acuerdo Canadá UE sobre tratamiento y transferencia de datos del registro nombres de pasajeros.

el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas”. Así deberá indicar “en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando que la injerencia se limite a lo estrictamente necesario⁷⁸”.

El Tribunal se ha reafirmado recientemente en esta necesidad de mantener el nivel de protección garantizado en la Carta tal como ha sido interpretada por la jurisprudencia, obligando incluso a los países receptores de datos personales procedentes de la Unión a garantizar un nivel de protección sustancialmente equivalente al garantizado por el Reglamento General de Protección de Datos⁷⁹.

Uno de los factores que influyen en la gravedad de la injerencia es el tipo de datos personales de que se trate. Así por ejemplo, según el Tribunal, la simple conservación de los datos que deben almacenar los proveedores de servicios de comunicaciones electrónicas se considera una injerencia grave, puesto que analizados en su conjunto proporcionan medios para determinar información sensible acerca de los usuarios, como pueden ser hábitos de la vida cotidiana, lugares de residencia permanentes o temporales,

⁷⁸ Dictamen 1/15 del Tribunal de Justicia (Gran Sala) de 26 de julio de 2017, párrafos 139 y 140.

⁷⁹ STJUE de 16 de julio de 2020, Schrems II, C-311/18, EU:C:2020:559, párrafo 178.

desplazamientos, relaciones sociales y círculos sociales que frecuentan⁸⁰. En cambio, si dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas, no estaríamos hablando de una injerencia grave.

Caso particular de los datos procedentes de las comunicaciones electrónicas.

Una herramienta fundamental en las investigaciones policiales de hoy en día es el estudio de los datos asociados a las comunicaciones telefónicas, ya que toda persona que pertenece al mundo delincriminal tiene, al menos, una línea telefónica con la que se pone en contacto con otras personas de su entorno. Todas las conexiones telefónicas dejan un rastro que puede ser estudiado y analizado.

En el ámbito de la prevención, investigación, descubrimiento y persecución del delito, el principio de proporcionalidad exige que una injerencia grave en los derechos fundamentales venga motivada por la lucha contra una delincuencia grave también⁸¹. Por lo tanto, el estudio de la tarificación de una línea telefónica - que incluiría información relativa al número que llama y el que es llamado, duración,

80 STJUE de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartado 99.

81 STJUE de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, párrafo 60.

antena de telefonía desde la que se realiza la llamada además de otros datos - no sería justificable para investigar un delito leve.

Una de las sentencias más importantes del TJUE sobre la protección de datos personales fue la Sentencia de Digital Rights⁸² en la que se derogaba la Directiva 2006/24/CE de 15 de marzo de 2006 ⁸³. El TJUE consideró que era una norma que no cumplía el principio de proporcionalidad por la forma en que el Parlamento Europeo y el Consejo regularon la retención de datos procedentes de las comunicaciones electrónicas – telefonía móvil principalmente -, al tiempo que dejaron un amplio margen de maniobra a los estados para trasponerla a los respectivos ordenamientos jurídicos, a pesar de la grave afectación que tenía sobre los art. 7 y 8 de la Carta. Las medidas de dicha Directiva suponían una injerencia en los derechos fundamentales que superaba lo

82 STJUE de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/2, EU:C:2014:238.

83 La Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Era una herramienta muy útil en la investigación de delitos relacionados con el crimen organizado o el terrorismo. El análisis de los datos que disponen los diferentes operadores de telecomunicaciones es una fuente de información que puede permitir a los agentes que luchan contra estos grupos criminales abrir nuevas líneas de investigación. Pero al igual que se almacenan y ceden a terceros los datos de los presuntos delincuentes, también se almacenan y ceden los datos de todos los ciudadanos que utilizan estos servicios, sin discriminación.

estrictamente necesario. Para que la restricción de los derechos a la privacidad y a la protección de datos personales esté justificada, es necesario que las medidas restrictivas no vayan más allá de lo estrictamente necesario para dar cumplimiento al objetivo de luchar contra la delincuencia grave que deben llevar a cabo los estados. Aún así, el Tribunal avaló la utilización de los datos de telefonía móvil para la lucha contra la delincuencia grave - terrorismo, crimen organizado, delitos graves -.

La anulación de la Directiva 2006/24/CE provocó la retrotracción al ordenamiento jurídico que había anteriormente sobre privacidad y comunicaciones electrónicas, volviendo a poner en vigor la Directiva 2002/58/CE⁸⁴, la cual prevé una serie de garantías que deben ser observadas por los estados miembros a la hora de imponer obligaciones a las compañías que proveen servicios de comunicaciones electrónicas. Dichas garantías se basan en la confidencialidad de las comunicaciones: (1) se prohíbe *la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los*

84 La Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

*usuarios, sin el consentimiento de los usuarios interesados*⁸⁵ y (2) los estados podrán adoptar medidas legales con el propósito de limitar este derecho para, entre otras finalidades, la de prevención, investigación, descubrimiento y persecución de delitos, siempre que dicha limitación *constituya una medida necesaria proporcionada y apropiada en una sociedad democrática*⁸⁶.

El TJUE interpreta la aplicación de la Directiva 2002/58/CE con base en el principio de proporcionalidad y a los derechos de la Carta, de manera que la facultad que tienen los estados de establecer excepciones a los derechos y obligaciones no puede justificar que la excepción a la obligación de garantizar la confidencialidad - de las comunicaciones electrónicas y de los datos asociados a ellas - se convierta en la regla. La restricción de los derechos, en este caso el derecho a la privacidad, debe hacerse de forma excepcional y cuando se cumplan los requisitos establecidos en la legislación⁸⁷. En los asuntos acumulados *La Quadrature du Net y otros*, y en *Orden de abogados francófonos y germanófonos de Bélgica y otros*, el TJUE alega que *el "mero hecho de que se haya adoptado una medida nacional con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del*

⁸⁵ Art 5 de la Directiva 2002/58/CE.

⁸⁶ Art 15.1 de la Directiva 2002/58/CE.

⁸⁷ STJUE de 6 de octubre de 2020, *Privacy International and in joined cases*, C-623/17, EU:C:2020:790, párrafo 59 y 38.

*Derecho de la Unión ni dispensar a los estados miembros de la necesaria observancia de dicho Derecho*⁸⁸.

Por lo que respecta a la *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, a mi juicio, no debería anularse ya que ahora queda promulgada bajo el amparo de la excepción hay recogida en la Directiva 2002/58 /CE, en la que se permite a los estados adoptar medidas limitadoras de Derechos, siempre y cuando sea una *“medida necesaria proporcionada y apropiada en una sociedad democrática”* con el fin de, entre otros, *“la prevención, investigación, descubrimiento y persecución de delitos”*.

Sin embargo, hay algún aspecto que debería ser revisado al no cumplir con el principio de proporcionalidad. Uno de ellos es la gran cantidad de datos de las comunicaciones de un elevado número de usuarios de servicios de telefonía móvil y de internet que son almacenados por las compañías. Otro aspecto es el del período de tiempo de conservación de estos datos. CRUZ VILLARON⁸⁹ vería justificada una

88 STJUE de 6 de octubre de 2020. Asuntos acumulados, La Quadrature du Net / Premier ministre y otros, C-511/18 C-512/18 y C-520/18 EU:C:2020:791.

89 Conclusiones del Abogado General, de 12 de diciembre de 2013, Ponente CRUZ VILLARON, párrafo 147.

retención de datos por un período de tiempo no superior a un año, aunque, el *Verfassungsgerichtshof* austriaco, por ejemplo, considera los seis meses excesivos⁹⁰. Documentos técnicos de la propia UE⁹¹ hablan que con un período de tiempo de seis meses podría ser suficiente. Lo cierto es que debe replantearse o incluso estudiar otros métodos, como pueden ser el *quick freeze*⁹² que plantea el Grupo de Protección de Datos del art. 29⁹³.

3.- La protección de datos en las investigaciones policiales.

La investigación policial, entre otros aspectos, implica el estudio de datos relativos a personas. Pueden ser datos

90 STJUE de 8 de abril de 2014, Digital Rights, C-293/12 y C-594/2, EU:C:2014:238, párrafo 20.

91 Opinión 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf (última consulta 18/03/2022).

92 Quick freeze - no se lleva a cabo un almacenamiento general de los datos, sino que en casos justificados las autoridades policiales piden a los proveedores que almacenen varios datos y posteriormente pueden pedir una autorización que les permita acceder a ellos. VILASAU, M. (2006).

93 Grupo sobre Protección de Datos del Artículo 29. Dictamen 4/2005 sobre la propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE (COM(2005)438 final de 21.09.2005). Adoptado el 21 de octubre de 2005.

procedentes de bases de datos abiertas al público o de internet – Registro de la Propiedad, Registro Mercantil,...-; datos sobre las personas que proceden de las empresas que les prestan servicios – de telefonía, bancarios –, datos obtenidos a través de la misma investigación – balizas de seguimiento, grabaciones de voz y/o imagen – o de la propia policía – bases de datos de antecedentes policiales, fotografías de detenidos, huellas dactilares, perfiles genéticos -, datos procedentes de terceros países obtenidos a través de distintos acuerdos internacionales... Cualquiera de esos datos considerados de forma aislada no tiene porqué indicar un aspecto relevante de la vida privada de un individuo; pero teniendo una visión de conjunto, podría llegar a romper el principio de presunción de inocencia del autor en relación a unos hechos concretos que ha cometido. Y ese es el objetivo de la investigación policial.

El uso de bases de datos informatizadas supone un riesgo añadido al derecho a la intimidad y al de la protección de datos⁹⁴. El uso que hace la policía de la tecnología siempre ha suscitado dificultades en el Derecho Constitucional, especialmente en el campo de los Derechos Humanos. Para

94 Por ejemplo, el acceso indebido de personas a la base de datos o la recolecta de datos para una determinada finalidad, pero que luego serán utilizados para otra. Estos son riesgos sobre los que el Tribunal Constitucional español ya se ha pronunciado - STC 202/1999 de 8 de noviembre, STC 11/1998 de 13 de enero y STC 144/1999 de 22 de julio, por citar algunas.

evitar la vulneración de derechos, la legislación europea ha acotado el uso que puede hacer la policía de los datos que dispone acerca de los ciudadanos y de cómo deben usarse durante las investigaciones policiales.

3.1.- Legislación europea aplicable a la protección de datos en el ámbito de las investigaciones policiales.

3.1.1.- Antecedentes.

Por lo que respecta a la legislación que emana del Consejo de Europa, la primera norma de interés es la **Recomendación (87)15**, en la cual el Consejo toma conciencia de la amenaza a la privacidad que podía suponer el uso indebido del tratamiento automatizado de datos personales en el sector policial y busca el equilibrio entre la lucha contra la delincuencia y el derecho a la privacidad. En ella, el Comité de Ministros del Consejo de Europa recomienda a los estados Miembros aplicar una serie de principios básicos relativos a la recolección, almacenamiento, uso y comunicación de datos personales para fines policiales, y los derechos de acceso, rectificación y reclamación de datos en este tipo de archivos, ya que el propio Convenio 108 sobre protección de datos, prevé la excepción de una serie de principios cuando el tratamiento

de datos personales está destinado a la “represión de infracciones penales”⁹⁵.

En ella se define, por ejemplo, la expresión “fines policiales” refiriéndose a la función que la policía realiza para la prevención y represión de las infracciones penales así como para el mantenimiento del orden público. Los datos recogidos deben ser los necesarios para la prevención de un peligro real o para la represión de una infracción penal, estando sujetos a la legislación nacional ya que el simple almacenamiento de datos por parte de las autoridades policiales constituye una injerencia al derecho a la vida privada de las personas⁹⁶.

La policía puede recopilar y almacenar datos personales sin el conocimiento de los afectados. Pero reconoce el derecho a que estas personas sean informadas, siempre que no perjudique la investigación⁹⁷. Establece la obligación de que la información policial se almacene según su grado de fiabilidad o exactitud y debe distinguirse entre los datos con finalidad administrativa y los datos con finalidad policial.

Reconoce los derechos de acceso, rectificación y cancelación, así como la necesidad de revisión periódica de

95 Art. 9.2 del Convenio 108 sobre protección de datos personales.

96 STEDH de 4 de diciembre de 2008. Caso Marper c. Reino Unido, párrafo 41.

97 Principio 2 de la Recomendación n°. R(87)15.

la información, la creación de una Autoridad Independiente de supervisión y recoge el Principio de Finalidad, por el cual la policía solo puede usar los datos para el fin por el cual fueron recogidos, excepto en casos de investigaciones concretas y con una provisión legal que lo autorice.

La **Decisión Marco 2008/977/JAI**⁹⁸ relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, adoptada por el Consejo de la Unión Europea, debía sustituir la **Recomendación (87)15** y había de suponer una actualización de la protección de datos en el marco policial. Sin embargo, el ámbito de aplicación de esta Decisión Marco era muy reducido y se limitaba solo al tratamiento de los datos personales transmitidos o puestos a disposición entre estados miembros⁹⁹ y a terceros estados o a Organismos Internacionales¹⁰⁰. Dejaba fuera de la aplicación de la Decisión Marco el intercambio de datos realizado en el marco de Europol, Eurojust, el SIS¹⁰¹ y el SIA¹⁰², ni los que permitían a las autoridades de los estados miembros acceder directamente a determinados sistemas de datos de otros

98 Decisión Marco 2008/977/JAI del Consejo de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

99 Considerando 7 Decisión Marco 2008/977/JAI.

100 Art. 13 Decisión Marco 2008/977/JAI.

101 Sistema de Información Schengen.

102 Sistema de Información Aduanera.

estados miembros¹⁰³, ni cuando el tratamiento afectaba a los intereses esenciales de seguridad del estado ni a las actividades específicas de inteligencia en el sector de la seguridad del estado¹⁰⁴. La norma tampoco era aplicable al intercambio de datos personales que las autoridades administrativas, policiales y judiciales tienen a nivel interno.

No recogía un apartado para excepciones o las limitaciones a los derechos o principios esenciales a la protección de datos personales: éstas están en todo el articulado y, numerosas ocasiones, formulado de manera vaga¹⁰⁵.

103 Por ejemplo la transferencia automatizada de perfiles de ADN, de datos dactiloscópicos o registros nacionales de matrículas de vehículos.

104 Art. 1 Decisión Marco 2008/977/JAI.

105 A título de ejemplo cabe citar el art. 6 que permite el tratamiento de categorías especiales de datos – que revelen origen racial o étnico, ideas políticas o religiosas,... - cuando sea «estrictamente necesario y el Derecho nacional establece garantías adecuadas».

En la misma línea se limita el principio de finalidad. Así, el art. 3.1 define el tratamiento de los datos recogidos respecto a los fines para los que fueron recogidos. Pero más adelante se permite el tratamiento para otros fines con conceptos tan vagos como que «*sea necesario para ese otro fin y proporcionado a él*» (art. 3.2.c), en «*otros procedimientos judiciales y administrativos directamente relacionados con la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales*» (art. 11.b) o en caso de «*prevención de amenazas inmediatas y graves a la seguridad pública*» (art. 11.c) por citar ejemplos.

3.1.2.- Directiva (UE) 2016/680.

El mes de mayo de 2016 entró en vigor¹⁰⁶ la Directiva (UE) 2016/680 que derogaba la Decisión Marco 2008/977/JAI. La nueva Directiva se aplica al tratamiento de datos personales *“por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública”*, estableciendo estándares mínimos para el tratamiento de datos personales en el ámbito policial en cada país. Así, a diferencia de la Decisión Marco, ésta se aplica tanto en el tratamiento de datos personales a nivel transnacional como en el ámbito interno de cada estado, por lo que armoniza el régimen legal en este aspecto. Además, al tratarse de una Directiva, el margen de apreciación de los estados se reduce considerablemente.

Aun así, la aplicación de la Directiva se escapa (1) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión – seguridad a nivel nacional de cada uno de los estados - y (2) por parte de las instituciones, órganos u organismos de la Unión. En estos dos campos, la Directiva no se aplica.

¹⁰⁶ España ha sido multada por no haber transpuesto la Directiva. STJUE de 25 de febrero de 2021, Comisión / España, C-658/19, EU:C:2021:138.

Aunque tiene menos excepciones que la Decisión Marco, ello no significa que no las tenga. Si a la primera se le objetaba las numerosas excepciones al principio de finalidad del tratamiento, a la Directiva se le puede recriminar la limitación al derecho de la información y del que más adelante se hablará.

La Directiva debe aplicarse a las personas físicas, independientemente de su nacionalidad o lugar de residencia¹⁰⁷. Pero no debe aplicarse al tratamiento de datos personales en actividades que no estén comprendidas en el ámbito de aplicación del Derecho de la Unión¹⁰⁸ ni en las políticas sobre controles de las fronteras, inmigración y asilo. Dispone que el responsable del tratamiento debe llevar a cabo una evaluación de impacto relativa a la protección de datos cuando exista la probabilidad de que las operaciones de tratamiento entrañen un alto riesgo para los derechos y las libertades de los interesados¹⁰⁹. En cualquier caso, se deben disponer de unos estándares mínimos de seguridad¹¹⁰.

107 Considerando 17 Directiva (UE) 2016/680.

108 Por este motivo no será de aplicación en actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional.

Considerando 14 Directiva (UE) 2016/680.

109 Art. 27.d de la Directiva (UE) 2016/680.

110 Art. 29.2 de la Directiva (UE) 2016/680.

Se establece la responsabilidad del encargado del tratamiento en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. La probabilidad y la gravedad de los riesgos para los derechos y libertades de los interesados deben determinarse en función de la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe determinarse basándose en una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un alto riesgo¹¹¹.

También se establece la figura del delegado de protección de datos¹¹², designado por el responsable del tratamiento, las autoridades de control¹¹³ que deben actuar con total transparencia y ser designadas por cada estado miembro para supervisar la aplicación de la Directiva, así como las funciones que desempeña el Comité Europeo de Protección de Datos¹¹⁴ en relación con el tratamiento de datos en el ámbito de la Directiva.

111 Es un especial riesgo de perjuicio para los derechos y libertades de los interesados.

112 Art. 32 de la Directiva (UE) 2016/680.

113 Art. 41 de la Directiva (UE) 2016/680.

114 Art. 51 de la Directiva (UE) 2016/680. El Comité Europeo de Protección de Datos es creado en el Art. 68 del Reglamento (UE) 2016/679.

· Definiciones

La Directiva (UE) 2016/680 utiliza las mismas definiciones básicas que conciernen al tratamiento de datos personales que las que son recogidas en el Reglamento (UE) 2016/679.

- “datos personales”, “tratamiento”, limitación del tratamiento”, “elaboración de perfiles”, “seudonimización”, “fichero”, “responsable y encargado del tratamiento”, “destinatario”....

Hay dos conceptos que desaparecen de la Directiva cuando se habla del tratamiento de datos personal en el ámbito policial:

- Desaparece el concepto de *tercero*, ya que quien tratará los datos personales siempre será una *autoridad competente*. Entre dichas autoridades competentes se deben incluir autoridades públicas - autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad – y también cualquier otro organismo o entidad en que el Derecho del estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva¹¹⁵. Cuando esta autoridad trate datos con otra finalidad distinta a la de la Directiva, deberá atenerse a lo que dispone el Reglamento.

¹¹⁵ Considerando 11 de la Directiva (UE) 2016/680.

- Desaparece el *consentimiento* del interesado como requisito para que se traten sus datos personales. No es un fundamento jurídico para que las autoridades competentes traten los datos personales, ya que estos serán tratados sin el consentimiento del interesado.

El Reglamento (UE) 2016/679 establece seis motivos por los que el tratamiento de datos será lícito. Uno de ellos es el consentimiento del interesado; otro es que “*el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*” para lo cual es necesario que sea establecido por el derecho de la Unión o del estado miembro¹¹⁶. Por lo tanto, para el tratamiento de datos personales por las autoridades policiales no es necesario el consentimiento del interesado, sino que basta con que lo establezca una norma de la Unión Europea o del propio estado miembro.

- “**Datos personales**”

La Directiva (UE) 2016/680 considera *datos personales* toda información sobre una persona que permita identificar su identidad, directa o indirectamente, “*mediante un*

¹¹⁶ Art. 6.1 del Reglamento (UE) 2016/679.

*identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*¹¹⁷. No es necesario una plena coincidencia entre dato y persona, sino que la identificación debe poder hacerse sin utilizar “*esfuerzos desproporcionados*”¹¹⁸; por tanto, deben tenerse en cuenta los medios de que disponen las personas que quieren identificar dicha persona a partir del dato¹¹⁹.

A modo de ejemplo, se consideran datos personales el nombre y apellidos de una persona, su número de documento de identificación, la fecha de nacimiento, su dirección... También lo serán el número dirección de IP¹²⁰ de un usuario al acceder a la red o el registro de las horas en

117 El Reglamento (UE) 2016/679 ha incluido a la definición que daba el art. 2.a de Directiva 95/46/CE los datos genéticos, a los cuales incluye en los datos personales.

118 Sentencia Audiencia Nacional 1485/2002 (Sala de lo Contencioso Administrativo – Sección 1ª), de 8 de marzo de 2002 (recurso 948/2000).

119 “*Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.*” Considerando 26 del Reglamento (UE) 2016/679.

120 Sentencia del TJUE de 24 de noviembre de 2011, Scarlet Extended, C-70/10, EU:C:2011:771, párrafo 51 y la STJUE de 19 de Octubre de 2016, Patrick Breyer, C-582/14, EU:C:2016:779, Párrafo 49.

que un trabajador en concreto inicia y finaliza su jornada¹²¹, así como las interrupciones que realiza. En el primer caso, el proveedor de Internet, si lo requiere, puede identificar la persona que establece la conexión; en el segundo caso se trata de información que pertenece a una “*persona identificada o identificable*”.

La doctrina del TEDH establece un principio general de protección para los datos personales. A la vez requiere una protección reforzada para los que, dentro de los datos personales, considera que son “*datos sensibles*”. Estos hacen referencia, por ejemplo, a los datos relativos a la orientación sexual de los individuos¹²², a la ideología política o los datos médicos¹²³: afectan directamente al desarrollo de la personalidad del individuo. La Directiva (UE) 2016/680 ha recogido esta doctrina y considera datos personales que merecen especial protección los que “*revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o*

Las direcciones IP son secuencias de números que se asignan a los ordenadores conectados a Internet para que estos puedan comunicarse entre sí a través de esa red.

121 STJUE de 30 de mayo de 2013, Worten – Equipamentos para o Lar, C-342/12, EU:C:2013:355.

122 STEDH de 22 de octubre de 2002. Caso Perkins y R. c. UK.

123 STEDH de 17 de agosto de 1997. Caso M.S. c. Suecia.

datos relativos a la vida sexual o las orientación sexuales de una persona física”.

Será necesario una ley del estado Miembro o de la Unión para que sea lícito el tratamiento de este tipo de datos. También se podrán tratar en caso de que deban protegerse los intereses vitales del interesado o de un tercero o que sean datos que el interesado ya haya hecho públicos anteriormente.

Por su parte, el Reglamento (UE) 2016/679 también considera que este tipo de datos personales merecen especial protección por lo que, de forma general, prohíbe su tratamiento¹²⁴, a diferencia de la Directiva. En el grupo de datos que merecen especial protección, el Reglamento incluye a los datos personales relativos a condenas e infracciones penales¹²⁵, adoptando así la doctrina generada por el TEDH a la vez que cumple uno de los principios básicos¹²⁶ para la protección de datos establecidos en el Convenio 108.

La Directiva 95/46/CE consideraba datos personales los relativos a las personas físicas constituidos por imágenes y

124 Art. 9 Reglamento (UE) 2016/679.

125 Art. 10 Reglamento (UE) 2016/679.

126 Artículo 6 del Convenio 108. Categorías particulares de datos.

sonido¹²⁷. La Directiva (UE) 2016/680 ha matizado esta inclusión creando el concepto de “*datos biomédicos*” que son datos personales obtenidos a partir del tratamiento técnico de “*características físicas, fisiológicas o conductuales de una persona física*” que permitan identificar un individuo y los incluye en la categoría especial de datos personales. Aquí se incluyen las imágenes faciales, las huellas dactiloscópicas y la voz que emite una persona y con la que puede ser identificada.

En el caso de imágenes, la doctrina del TEDH considera que la instalación de cámaras que no graban, de por sí, no da lugar a una interferencia en la vida privada de las personas, aunque dicha instalación no esté habilitada por ninguna ley. Al no grabar, es difícil que esas imágenes se destinen a una finalidad distinta a la que se estarían obteniendo. Además, su efecto es el mismo que si se colocara allí a una persona en el mismo sitio mirando¹²⁸.

- “**Tratamiento**”

El Convenio 108 definió tratamiento *automatizado* como “las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos

127 Considerando 14 de la Directiva 95/46/CE.

128 STEDH de 14 de enero de 1998. Caso Herbecq y otros c. Bélgica.

automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión”¹²⁹. El temor por aquel entonces era el tratamiento automatizado de los datos personales, no los archivos físicos de datos, que no se veían amenazados.

La Directiva 95/46/CE, el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 expandieron la definición de tratamiento e incluyeron las operaciones que no son automatizadas a la vez que añadían más tipos de operaciones a las mencionadas¹³⁰ en el Convenio.

El *tratamiento* abarca desde la recogida de los datos hasta que los datos son destruidos o transmitidos, incluyendo el uso que se hace de los mismos.

- “Fichero”

El Convenio 108 concebía el fichero automatizado, es decir, informaciones que eran susceptibles de ser tratadas de

¹²⁹ Art. 2.c del Convenio nº 108 del Consejo de Europa.

¹³⁰ Art. 2 b de la Directiva 95/46/CE: la recogida, organización, conservación, elaboración, consulta, utilización, comunicación por transmisión, cualquier forma que facilite el acceso a los mismos, cotejo o interconexión, así como su **bloqueo**, supresión o destrucción;

Art. 4 del Reglamento (UE) 2016/679: la **recogida**, registro, **organización**, estructuración, **conservación**, adaptación o modificación, extracción, **consulta**, **utilización**, **comunicación por transmisión**, **difusión o cualquier otra forma de habilitación de acceso**, cotejo o **interconexión**, limitación, **supresión o destrucción**.

forma automatizada. El Reglamento (UE) 2016/679 y Directiva (UE) 2016/680 mantienen la definición de la Directiva 95/46/CE, definiéndolo como un conjunto estructurado de datos personales que sean accesibles utilizando determinados criterios.

Actualmente se entiende como fichero un conjunto organizado de datos, que puede ser informatizado o en soporte papel, y que identifican o permiten identificar a una persona.

- “Responsable” y el “encargado del tratamiento”

El *responsable del tratamiento* será la persona u organismo que determina los fines y medios del tratamiento. Decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales que contiene el fichero. Si son dos o más los responsables que determinan los objetivos y medios utilizados, serán considerados corresponsales del tratamiento, pudiendo ejercer los derechos que le corresponde al interesado frente a cada uno de ellos¹³¹.

El *encargado del tratamiento* será la persona u organismo que lleve a cabo el tratamiento efectivo, a cuenta del responsable.

131 Art. 26 del Reglamento (UE) 2016/679.

Se crea también la figura del *delegado de protección de datos*, que será designado por el responsable del tratamiento según disponga la legislación del estado miembro. Varias autoridades competentes podrán designar un mismo delegado, el cual informará y asesorará al responsable del tratamiento y velará por el cumplimiento de la legislación vigente en cuanto a protección de datos, a la vez que cooperará con la autoridad de control.

- “Autoridad competente”

Es toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública.

4.- Principios aplicables al tratamiento de datos personales en el ámbito de las investigaciones policiales.

El Convenio 108 ya establecía una serie de principios básicos para la protección de datos personales. Estos mismos principios han sido recogidos en el art. 5 del Reglamento (UE) 2016/679 e indican cómo se deben

obtener, tratar y ceder los datos personales de un individuo para así garantizar su derecho a la protección de datos personales. Dado que el derecho a la protección de datos personales no es un derecho absoluto, podrán establecerse restricciones por ley a esta protección siempre que se *“respeten los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática”* ¹³².

Cuando nos referimos al tratamiento de datos personales efectuados por las autoridades policiales, la Directiva (UE) 2016/680 establece sus propios principios, que difieren a los del Reglamento (EU) 2016/679.

Veamos los principios de cada una de las normas.

4.1.- Principios relativos al tratamiento.

a.- Los datos personales deben ser tratados de forma lícita y leal.

El Reglamento (EU) 2016/679 recoge que los datos deben tratarse de forma *leal, lícita y transparente* en relación con el interesado, que debe saber en qué circunstancias han sido recogidos, para así poder ejercer las garantías básicas

¹³² Art. 23 del Reglamento (UE) 2016/679.

procedimentales¹³³ que le correspondan. La recogida, tratamiento y cesión de datos personales debe ajustarse a la ley. No debe engañarse al interesado en cuanto al hecho de que se están recogiendo sus datos personales ni a la finalidad a la que serán destinados. Debe ser una finalidad explícita y legítima, debiendo estar ya determinada en el momento de la recogida.

Por su parte, la Directiva (UE) 2016/680 considera necesario que el tratamiento de los datos personales debe ser *transparente*. Todo y que el concepto no ha sido recogido expresamente en el articulado¹³⁴, en el apartado de los considerandos¹³⁵ sí se requiere que las autoridades policiales lleven a cabo el tratamiento de los datos de forma transparente y solo para los fines que la ley prevea. Los conceptos *licitud* y *lealtad* no tienen el mismo significado que el establecido en el Reglamento (EU) 2016/679.

a.1.- Licitud.-

De acuerdo con la Directiva (UE) 2016/680 “basta con que el tratamiento de los datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y

¹³³ STEDH de 3 de septiembre de 2015. Caso Sõro c. Estonia.

¹³⁴ Art. 4 de la Directiva (UE) 2016/680.

¹³⁵ Considerando 26 de la Directiva (UE) 2016/680.

la protección y prevención frente a las amenazas contra la seguridad pública sea necesario para la Autoridad Competente que lo lleve a cabo y que esté autorizado por una norma del estado miembro o de ámbito europeo para que éste sea considerado lícito. La norma debe establecer los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento”¹³⁶.

Como vemos, en ningún momento se habla del consentimiento del propietario de los datos para que el tratamiento sea lícito. Así, no es necesario que el propietario de los datos de su consentimiento para que éstos sean utilizados por las autoridades policiales.

En cambio, en el Reglamento (EU) 2016/679 la licitud vendrá determinada por el consentimiento del interesado o, a falta de este, por una base legítima establecida conforme a Derecho, clara, precisa y con aplicación previsible para sus destinatarios¹³⁷.

a.2.- Leal.-

Uno de los significados de la palabra leal es fidedigno, verídico, fiel¹³⁸. Por tanto, los investigadores no podrán

¹³⁶ Art. 8 de la Directiva (UE) 2016/680.

¹³⁷ Considerandos 40, 41 y Art. 6 del Reglamento (UE) 2016/679.

¹³⁸ Diccionario de la Real Academia Española.

engañar a una persona para obtener los datos personales que se van a utilizar en una investigación policial. El interesado debe dar la información a los agentes policiales sabiendo la condición de funcionarios policiales que éstos ostentan¹³⁹.

Este apunte tan obvio, plantea un problema cuando se considera la figura del *agente encubierto*. En las últimas décadas ha habido una gran evolución de la delincuencia organizada y los grupos terroristas debido principalmente a la deslocalización de la sociedad y la supresión de fronteras, cosa que ha provocado la aparición de nuevas formas de crimen organizado por lo que las autoridades policiales han tenido que aplicar nuevos métodos de lucha contra él. Una de estas nuevas formas es la figura del agente encubierto, que incluso ha sido abalada por el TEDH, el cual solo exige que la actuación de los agentes encubiertos sea acotada y rodeada de garantías¹⁴⁰.

En el caso español, esta figura está regulada en el art. 282 bis de la LECrim y requiere una autorización, intervención y control judicial del agente que está actuando con una

¹³⁹ Los agentes no deben mentir o hacerse pasar por terceras personas con la finalidad de obtener información de interés. Era una práctica extendida el llamar a una línea telefónica de la cual se desconocía su usuario habitual, diciendo ser empleados de una compañía telefónica, con la finalidad que el interlocutor proporcionará datos personales suyos.

¹⁴⁰ STEDH de 26 de febrero de 2001. Caso Teixeira Castro c. Portugal.

identidad supuesta, falsa e inexistente en la realidad y que ha sido facilitada por el propio Ministerio del Interior. Por tanto, se trata de un engaño legalizado por los poderes públicos, cuya finalidad es la de adquirir la confianza de los miembros del grupo criminal y obtener información que luego podrá ser usada en un proceso judicial en su contra. El agente encubierto, desempeñando su función, entrará en el domicilio de los investigados con su consentimiento – viciado –, mantendrá conversaciones en la que éstos le facilitaran información – direcciones, números de teléfono, datos personales,... - e incluso podrá llegar a realizar determinados actos relacionados con la actividad delictiva de la organización criminal.

Hay autores como DEL POZO PEREZ o EXPOSITO LOPEZ que consideran que la actuación del estado, a través de los agentes encubiertos es lícita, ya que actúan bajo el amparo de la ley y es una fórmula que se utiliza “*para la averiguación de conductas especialmente graves y lesivas para el conjunto de la sociedad incluso para la propia seguridad de los cimientos que sostiene nuestro estado de Derecho*”¹⁴¹. Durante toda la investigación, el agente encubierto está bajo control jurisdiccional y cuando estas actuaciones pueden afectar a los derechos fundamentales, el agente deberá

141 DEL POZO PEREZ M. (2006), p. 286.

solicitar del órgano judicial competente las autorizaciones correspondientes¹⁴².

Es cierto que el legislador europeo está de acuerdo con la utilización de estas técnicas de investigación¹⁴³, pero es difícil entender por qué en la Directiva (UE) 2016/680 no se ha postulado de una forma más clara a favor de esta técnica de investigación tan útil y ampliamente aceptada en la lucha contra el crimen organizado y la cual está directamente enfrentada con la *lealtad* en la forma de obtener la información.

b.- Transparente.

El *principio de transparencia* exige que toda información y comunicación relativa al tratamiento de los datos personales sea fácilmente accesible y comprensible, y que se utilice un lenguaje sencillo y claro. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento¹⁴⁴. Al interesado se le debe facilitar la forma de acceder al responsable del tratamiento para así ejercer los derechos que le son propios. También se le debe facilitar

142 EXPÓSITO LÓPEZ L. (2015), p. 258.

143 Considerando 26 de la Directiva (UE) 2016/680.

144 Considerando 39 del Reglamento (UE) 2016/679.

información referente al periodo de tiempo que serán guardados los datos, los datos personales de los interesados que se ven afectados, la finalidad del tratamiento, las consecuencias del hecho de no facilitar los datos – en caso que sea un requisito legal o contractual – y si con sus datos se van a elaborar decisiones individualizadas automatizadas así como la importancia y las consecuencias que puede suponer dicho tratamiento para el interesado¹⁴⁵.

Pero, ¿qué datos deben de ser facilitados al interesado?. Con los sistemas informáticos existentes actualmente, los algoritmos predictivos cada vez más potentes y la facilidad con la que determinados usuarios los facilitan a través de Internet – adquiriendo productos por ejemplo -, el sistema puede llegar a obtener datos o conclusiones que el interesado no ha facilitado o que incluso puede llegar a desconocer¹⁴⁶.

145 Art. 13.2 del Reglamento (UE) 2016/679.

146 Se da el caso de un padre que conoció del embarazo de su hija a través de una empresa de e-comercio que le enviaba cupones de descuento por correo para adquirir productos para bebés. Esta empresa descubrió que las mujeres embarazadas acostumbran a consumir cantidades mayores de lo habitual de 25 productos - lociones o suplementos dietéticos - que analizados conjuntamente pueden determinar si una mujer está embarazada.

Noticia obtenida en:

<https://www.netquest.com/blog/es/blog/es/padre-descubre-embarazo-hija-targeting>. (última consulta 18/03/2022).

La ONU insta a la creación de mecanismos nacionales de supervisión independientes y efectivos¹⁴⁷ para mejorar la transparencia para proteger el derecho a la protección de datos, opinión que secunda el TEDH¹⁴⁸; este último añade también la publicación de informes periódicos¹⁴⁹ como otro método para incrementar la transparencia en general.

La *Autoridad de Control* ha de contribuir a la transparencia de los tratamientos de datos que se efectúen en el estado miembro¹⁵⁰. La transparencia se consigue con la cesión de información hacia el interesado; de esta manera el Derecho de transparencia y información están estrechamente ligados.

Como ya se ha dicho, el articulado de la Directiva (UE) 2016/680 no exige que el tratamiento de los datos personales sea transparente en el sentido que sí lo exige el Reglamento (UE) 2016/679. Según la Directiva, se debe informar al interesado de: la identidad del responsable del tratamiento, la existencia de la operación de tratamiento, los fines del tratamiento, el derecho a presentar una reclamación y el derecho a solicitar al responsable del tratamiento el acceso a

147 La resolución 68/167 de la Asamblea General “El derecho a la privacidad en la era digital” A/RES/68/167 (18 de diciembre de 2013), disponible en: <http://www.un.org/es/comun/docs/?symbol=A/RES/68/167>. (última consulta 18/03/2022).

148 STEDH de 13 de octubre de 2015. Caso de Szabó y Vissy c. Hungría.

149 STEDH de 22 de noviembre de 2012. Caso de telegraaf media nederland landelijke media b.v. y otros c. Holanda.

150 Considerando 63 de la Directiva 95/46/CE.

los datos personales, su rectificación o supresión, o la limitación de su tratamiento. Toda esta información, genérica, podrá ser facilitada a través la página web de la autoridad competente¹⁵¹.

La información que se facilita es genérica. Así, una persona que conste en una base de datos policial, por ejemplo en el *Sistema d'Informació de la policia de la Generalitat de Persones Físiques (SIP PF)*¹⁵² del Cos de Mossos de Esquadra, podrá conocer la finalidad del tratamiento y los destinatarios que los reciben, incluso si son terceros países. Pero las autoridades policiales no le facilitaran las veces que sus datos han sido consultados o en que bases de datos policiales han sido incluidos.

¹⁵¹ Considerando 42 de la Directiva (UE) 2016/680.

¹⁵² ORDRE IRP/435/2009, de 2 de Octubre, por la cual se regulan los ficheros que contienen datos de carácter personal gestionados por la Secretaria de Seguridad y por la Dirección General de la Policía del Departament d'Interior, Relacions Institucionals i Participació: Annex II.

c.- Seguridad.

Se debe garantizar la seguridad de los datos personales. Se tomarán las medidas apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados para evitar la destrucción accidental o no autorizada, la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados. Las medidas a adoptar pueden ser tanto físicas como lógicas.

Son el responsable y el encargado del tratamiento los que deben aplicar medidas técnicas – como puede ser el cifrado de los datos - y organizativas para garantizar un nivel de integridad y confidencialidad adecuados¹⁵³.

Tanto la Directiva como el Reglamento obligan al responsable del tratamiento a llevar a cabo una “*evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales*” cuando sea previsible que dicho tratamiento suponga un “*alto riesgo para los derechos y libertades de las personas físicas*”¹⁵⁴. Ello significa que debe hacerse una descripción de las operaciones previstas durante el tratamiento, evaluar los riesgos para los derechos y libertades de los interesados, establecer medidas para

153 Considerando 60 de la Directiva (UE) 2016/680.

154 Art. 27 de la Directiva (UE) 2016/680.

hacer frente a estos riesgos, las garantías y los mecanismos de protección.

En caso de violación de la seguridad del fichero de datos personales, el responsable del tratamiento debe notificarla a la autoridad de control. Si los datos proceden de otro estado miembro, la notificación debe realizarse también al responsable del tratamiento de ese estado¹⁵⁵.

Por otro lado, *“cuando sea probable que la violación de la seguridad de los datos personales vaya a dar lugar a un alto riesgo para los derechos y libertades de las personas físicas”* el responsable del tratamiento debe comunicarlo al afectado. Si dicha comunicación supone un esfuerzo desproporcionado, puede hacerse a través de una comunicación pública. Los estados tienen la facultad de limitar esta comunicación si pueden obstaculizar o causar perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales o procedimientos oficiales o judiciales.

d.- Limitación de finalidad.

Al igual que se exige en el Reglamento (UE) 2016/679, los datos personales con los que trabajan las autoridades

155 Art. 30 de la Directiva (UE) 2016/680.

policiales deben ser recogidos para unas *finalidades determinadas, explícitas y legítimas, y no ser tratados de forma incompatible*¹⁵⁶ con la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública¹⁵⁷. Si se lleva a cabo un tratamiento de datos personales posterior o se modifica la finalidad inicial para la que los datos fueron recopilados, esta nueva finalidad no puede ser incompatible con la original.

Así, la Directiva UE 2016/680 permite que las autoridades policiales traten los datos personales prescindiendo del consentimiento del interesado. Se requiere que sean recogidos para una finalidad concreta que debe estar establecida por una norma del estado miembro.

Si es necesario tratar los datos para una finalidad distinta a la que fueron recogidos, deben darse dos circunstancias:

- Que sea amparado por una norma de la Unión o del estado miembro.

¹⁵⁶ Art. 4 de la Directiva (UE) 2016/680.

¹⁵⁷ Considerado 29 de la Directiva (UE) 2016/680.

- Que sea un tratamiento necesario y proporcional para esta nueva finalidad.

Para comprobar si la nueva finalidad es compatible con la finalidad inicial, deberá tenerse en cuenta la relación entre el objetivo inicial y el final, el contexto en el que se han recogido los datos personales, la naturaleza de los datos personales de que se trate, las consecuencias que pueda conllevar a los interesados el tratamiento posterior o si existen unas garantías adecuadas para este nuevo tratamiento¹⁵⁸.

e.- Decisiones individuales automatizadas¹⁵⁹.

El interesado también tiene derecho a que una decisión que produzca efectos jurídicos negativos sobre él o le afecten significativamente, no se base únicamente en un tratamiento automatizado, salvo que estén autorizadas por el Derecho de la Unión o del estado miembro y la ley prevea garantías apropiadas. Al menos se le debe de garantizar la intervención humana durante el tratamiento.

Se pueden incluso tratar categorías especiales de datos personales si se toman las medidas adecuadas para salvaguardar los derechos y libertades y los intereses

158 Art. 6.4 del Reglamento (UE) 2016/679.

159 Art. 11 de la Directiva (UE) 2016/680.

legítimos del interesado. Por contra, queda prohibido también, desde el ámbito policial, la discriminación de personas físicas elaborando perfiles basados en categorías especiales de datos personales.

4.2.- Principios relativos a los datos personales.

a.- Exactos.

Los datos personales a utilizar deben ser *exactos* y, si fuera necesario, actualizados. No deben contener fallos, estar incompletos o inducir a errores¹⁶⁰. Se tendrán que adoptar las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados¹⁶¹. Se deben corregir los factores que puedan introducir datos personales inexactos en el sistema y reducir al máximo el riesgo de error. La corrección se debe efectuar en el momento que se recojan, cuando sean tratados o cuando sean transmitidos. La inclusión de datos erróneos o no veraces en las bases de datos policiales, más cuando están sujetas a procesamientos automáticos, podría suponer una injerencia al artículo 8 de la Convención¹⁶².

160 ARENAS RAMIRO M. (2006), p. 320.

161 Art. 4.1, apartados b, c y d de la Directiva (UE) 2016/680.

162 STEDH de 18 de octubre 2011. Caso *Khelili c. Suiza*.

El interesado tendrá derecho a la rectificación de los datos personales inexactos con respecto a los fines para los que se tratan o, en su caso, a que se completen los datos personales que sean incompletos¹⁶³.

La falta de consentimiento del interesado para el tratamiento de datos - cuya consecuencia es que desconoce que sus datos están en una base policial - sumado a la limitación del derecho a la información a la que están sujetos, producen una limitación de las fuentes de obtención de información sobre el interesado, haciendo que las autoridades policiales tengan que hacer un esfuerzo a la hora de actualizar sus datos. Ello provoca que en ciertas ocasiones la información no sea precisa y se produzcan retrasos en la investigación. Para evitarlo debería haber una interrelación entre distintas bases de datos que provocara un flujo de los datos desde las bases más fiables hacia el resto.

En el caso español, por ejemplo, las bases de datos judiciales y policiales no están interconectadas. De esta manera, acabadas las diligencias policiales y enviadas al órgano judicial, éste lleva a cabo la instrucción y, cuando la finaliza, envía las actuaciones a enjuiciar. El órgano judicial competente dictará sentencia que podrá ser condenatoria o absolutoria. El resultado de dicha sentencia no hace el

163 Art. 16 del Directiva (UE) 2016/680.

camino inverso, por este motivo el cuerpo policial, al no saber el resultado de la sentencia, no puede actualizar sus bases de datos en la misma dirección. Así, en las bases de datos policiales hay numerosas personas con antecedentes policiales que deberían estar cancelados porque han resultado absueltos después de un juicio o no han llegado siquiera a juicio. Debido a la falta de comunicación entre los dos estamentos, si el interesado no lo solicita expresamente, los datos contenidos en las bases de datos policiales no se modificarán hasta que se cumpla el periodo de prescripción establecido por ley.

b.- Pertinentes y no excesivos - minimización de datos -.

Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados. Los datos personales deben tratarse solo si es necesario y, de ser así, tratar solo los estrictamente necesarios. De esta manera, la Administración pública en un boletín oficial, por ejemplo, debe hacer público solo los datos necesarios para identificar al infractor, como el número de DNI en el caso español; no sería necesario poner el nombre, apellidos, la dirección...

Los datos personales solo deberán ser objeto de tratamiento si la finalidad que se persigue no puede lograrse

razonablemente por otros medios. Serán lo adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que han de ser tratados¹⁶⁴.

c.- Conservados un periodo no superior al necesario.

Al igual que en el Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 establece que debe haber un periodo de tiempo durante el cual los datos han de ser conservados y que no debe ser superior al necesario para los fines para los que son tratados. El TEDH exige que el interesado tenga la posibilidad real y efectiva de borrar los datos no exactos que le conciernan¹⁶⁵. Son los propios estados miembros los que fijan el plazo de supresión para los datos personales que hayan quedado obsoletos¹⁶⁶.

Esta cláusula abre una ventana a que los datos no sean borrados nunca dado que las autoridades policiales son reacias al borrado de datos de sus bases de datos y, por regla general, no se suelen borrar si no se solicita expresamente¹⁶⁷. Los datos personales deberían dejar de ser de interés para las autoridades policiales cuando ya no son

164 Art. 5.1 Reglamento (UE) 2016/679.

165 STEDH de 5 de febrero de 2009. Caso Brunet c. Francia.

166 Art. 5 de la Directiva (UE) 2016/680.

167 Esto lleva aparejado el problema de la inexactitud de los datos: cuanto más antiguos son los datos, más riesgo de que sean inexactos.

exactos. Pero no es el caso: aún así, pueden proporcionar una información policial útil.

En el caso de las bases de datos que contienen los antecedentes policiales de las personas detenidas por los distintos cuerpos policiales españoles – hay que recordar que cada cuerpo tiene su propia base de datos – el responsable del tratamiento revisará la necesidad de conservar, limitar o suprimir los datos personales cada tres años como máximo. Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurren ciertos factores u que hagan necesario el mantenimiento del tratamiento de los datos¹⁶⁸.

Un ejemplo de periodo extremadamente largo de conservación de los datos se da en el caso de personas que han sido condenadas en sentencia firme por cualquier delito contra la libertad e indemnidad sexuales. A efectos de prevención y con la finalidad de hacer posible su seguimiento y control, el legislador español ha creado el **Registro Central de Delincuentes Sexuales en el Registro Central de Penados**¹⁶⁹. En él se incluye la información penal relativa a

¹⁶⁸ Art. 8 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

¹⁶⁹ Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia.

estas personas, con las consecuencias a nivel social que ello conlleva¹⁷⁰. El régimen de cancelación de la inscripción se establece en función de la edad de la víctima y la del condenado, pero en el caso que la víctima sea menor de edad, la duración de la inscripción se amplía hasta los 30 años, constituyendo una medida para la protección de la infancia y la adolescencia, y que “*no se opone a los principios de proporcionalidad, necesidad o re-inscripción*”¹⁷¹.

A toda persona que comete un delito sexual se le impondrá una pena o una medida de seguridad, si es el caso. Además, independientemente del tipo subjetivo del autor y de su peligrosidad o de sus posibilidades de reincidencia se le inscribirá en dicho registro. A mi entender, parece que la única finalidad de conservar los datos de estas personas durante tanto tiempo es por el mero hecho de tenerlos inscritos en una base de datos y evitar así una presunta *reiteración delictiva tan habitual en los tipos de delitos sexuales*¹⁷² y no parece tener una finalidad de protección

170 Por ejemplo el art. 13.5 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil que obliga a obtener un certificado negativo del Registro Central de Delincuentes Sexuales a quien pretenda el acceso y ejercicio a las profesiones, oficios y actividades que impliquen contacto habitual con menores.

171 Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales.

172 Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales.

hacia el menor. La inscripción se le impondrá al condenado independientemente de las circunstancias personales del sujeto o de si es capaz de no ser peligroso para la sociedad.

En mi opinión, que transcurran 30 años desde que se extinguió la pena impuesta a una persona para que sus datos sean borrados del Registro Central de Delincuentes Sexuales me parece un periodo excesivo. La inscripción en el Registro debería ser una medida de seguridad y como tal, ser aplicada por un Juez o Tribunal en base a unos informes técnicos. Las características del autor o su comportamiento después de la comisión de cumplir la pena, por ejemplo, deberían tenerse en cuenta para valorar el periodo de tiempo que debe permanecer dicha inscripción en el registro.

Pero sorprendentemente, el TEDH no considera que sea desproporcionado el almacenar los datos personales de las personas condenadas como autores de delitos sexuales graves durante un máximo de 30 años, ya que se debe tener en cuenta el fin perseguido y el interés público en relación con el interés privado de la persona en cuestión¹⁷³.

173 STEDH de 17 diciembre de 2009. Gardel c. Francia, párrafo 69.
STEDH de 17 diciembre de 2009. Caso B.B. c. Francia.
STEDH de 13 octubre de 2005. M.B. c. Francia.

- Supresión – Derecho al olvido.

Con las nuevas tecnologías, y especialmente en Internet, con los tratamientos automatizados de datos o el big-data no se implementa lo suficiente el borrado de datos antiguos. Hay el peligro que estos datos se vayan acumulando en la red de manera que las personas se conviertan en prisioneras de su propio pasado.

Al igual que los antecedentes penales o las sanciones disciplinarias en el ámbito administrativo caducan, los datos que se disponga de un individuo en un archivo han de poder caducar y ser borrados del sistema. Por ejemplo, el Código Penal español¹⁷⁴ cancela los antecedentes penales en función de la gravedad del delito siendo 10 años el tiempo máximo que debe transcurrir desde que se extingue la responsabilidad penal hasta que se cancelan los antecedentes penales, siempre y cuando no se hayan cometido de nuevos.

En 2012, el TJUE consciente de la necesidad de implementar el derecho al olvido, obligó al gestor de un motor de búsqueda y que considera “*responsable del tratamiento*” – en este caso a Google Inc. - a eliminar “*en la lista de resultados obtenida como consecuencia de una búsqueda efectuada a*

¹⁷⁴ Art 136.1 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

partir de su nombre, de vínculos a páginas web, publicadas legalmente por terceros y que contienen datos e información verídicos relativos a su persona” si dicha información “es inadecuada, no es pertinente, o ya no lo es, o es excesiva en relación con los fines del tratamiento en cuestión realizado por el motor de búsqueda”¹⁷⁵. Pero esta sentencia solo afectó a la función del motor de búsqueda de internet, no a la información en sí, y requiere que se analice cada caso para determinar si el interés del público en la información de ese individuo debe prevalecer sobre el derecho de respeto a la vida privada y de protección de datos personales; deberían analizarse la naturaleza de la información, su antigüedad y la sensibilidad a esta información en la vida privada de la persona¹⁷⁶. Además, solo establece que el motor de búsqueda debe desvincular el nombre de la persona de la información en sí, pero no obliga a que ésta última sea borrada de internet. Dicha información podrá ser consultada

¹⁷⁵ El 5 de marzo de 2010, el Sr. C. G. presentó ante la AEPD una reclamación contra un periódico de gran difusión y contra Google Spain y Google Inc. Esta reclamación se basaba en que, cuando un internauta introducía el nombre del Sr. C.G. en el motor de búsqueda de Google, obtenía como resultado vínculos hacia dos páginas del periódico en cuestión, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. C.G., el cual alegaba que ese asunto había sido resuelto hacía años.

STJUE de 13 Mayo 2014, Google Spain and Google, C-131/12, EU:C:2014:317, párrafo 94.

¹⁷⁶ ALVAREZ RIGAUDIAS C. (2014), p. 116.

a partir de otros parámetros de búsqueda, pero no a partir del nombre de la persona en cuestión.

La Comisión Europea y las distintas agencias de protección de datos han regulado el *derecho al olvido o a la supresión* como una proyección del derecho a la protección de datos. Así, en el Reglamento (UE) 2016/679, los interesados tienen derecho a que sus *datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento, se oponen a dicho tratamiento o hayan sido tratados ilícitamente*¹⁷⁷. La Directiva (UE) 2016/680 contempla el derecho a la supresión de una forma similar.

Pero el derecho a la supresión de los datos no es, ni mucho menos absoluto, y las excepciones a la supresión de los datos que se recogen en una u otra norma, no son las mismas. Así, el Reglamento (UE) 2016/679 autoriza al responsable del tratamiento no suprimir los datos para ejercer el derecho a la libertad de expresión, el de información, de interés público en el ámbito de la salud pública o con fines de archivo en interés público, de investigación científica o histórica o fines estadísticos.

¹⁷⁷ Art. 17.1 Reglamento (UE) 2016/679.

En cambio, la Directiva (UE) 2016/680 permite que las autoridades policiales conserven los datos para *(1) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; (2) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; (3) proteger la seguridad pública; (4) proteger la seguridad nacional; (5) proteger los derechos y libertades de otras personas*¹⁷⁸. Son requisitos muy amplios.

En la Directiva (UE) 2016/680, las limitaciones al derecho a la supresión son las mismas que impone al derecho de acceso a los datos que se están tratando sobre el individuo, no así en el Reglamento (UE) 2016/679. De ello se deduce que la Comisión es consciente de que la información con la que trabajan las autoridades policiales es esencial para desarrollar su trabajo con eficacia y coloca obstáculos para dificultar que los ciudadanos puedan conocer la información con la que tratan dichas autoridades y a que ésta sea suprimida, aunque sean datos inexactos o ya no sean útiles para la función para la que fueron recogidos. Las bases de datos policiales pueden guardar datos personales durante años. Por norma general, si la eliminación de los datos no se solicita, estos no serán borrados y serán almacenados

¹⁷⁸ Art. 16.4 Directiva (UE) 2016/680.

durante un tiempo ilimitado ya que no hay ningún sistema de borrado automático y debe hacerse caso a caso.

d.- Distinción entre diferentes categorías de interesados

Como novedad, la Directiva dispone que, cuando sea posible, los responsables del tratamiento deben establecer diferentes categorías de interesados. Así deben distinguir entre:

- a) Sospechosos de haber cometido o ir a cometer una infracción penal;
- b) personas condenadas por una infracción penal;
- c) víctimas de una infracción penal o posibles víctimas;
- d) terceras partes – testigos, personas de contacto, informadores, personas asociadas a las anteriores... - .

La reciente Ley Orgánica 7/2021, de 26 de mayo ya hace esta distinción, “*en la medida de lo posible*”.

El Cuerpo Nacional de Policía dispone del fichero **PERPOL** de gestión de antecedentes de las personas de interés policial. En él se inscriben las personas que tienen “órdenes de búsqueda vigentes o cesadas, que hayan sido detenidas o se haya demostrado su implicación en hechos delictivos o

sobre las que haya recaído alguna resolución judicial; también los conceptuados policialmente como delincuentes activos y cadáveres sin identificar”¹⁷⁹. Este fichero separa las víctimas y terceras partes de las personas sospechosas o detenidas.

Pero en ficheros de datos personales que poseen la Guardia Civil (**INTPOL**)¹⁸⁰, la Policía de la Generalitat-Mossos d’Esquadra (**SIP PF**)¹⁸¹ y en otros del Cuerpo Nacional de Policía (**GATI**) no se hace tal distinción. Las bases de datos se nutren de toda la información que contienen los atestados policiales, las denuncias penales, administrativas y otros hechos de interés policial.

En una misma base de datos se incluye el amplio espectro de personas que se ven implicadas en una actuación policial sin que se haga distinción de los motivos que provocan la inclusión en dichas bases de datos. Además, hay que tener un cierto nivel de acceso a la base de datos para determinar el motivo de la inclusión en dicha base. Un agente que

¹⁷⁹ Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior.

Fichero 25 del ámbito del Cuerpo Nacional de Policía.

¹⁸⁰ Orden INT/1202/2011, de 4 de mayo.

Fichero 25 del ámbito de la Guardia Civil.

¹⁸¹ Orden IRP/435/2009, de 2 de octubre, por la que se regulan los ficheros que contienen datos de carácter personal gestionados por la Secretaria de Seguretat y por la Direcció General de la Policia del Departament d’Interior.

Anexo II. Ámbito sistemas de información de la Policía de la Generalitat-Mossos d’Esquadra.

consulta esta base de datos puede determinar si a la persona le constan antecedentes policiales o no, pero no si se trata de una víctima, una tercera persona implicada en un hecho penal o de una persona sospechosa de cometer un ilícito.

e.- Distinción entre datos personales y verificación de la calidad de los datos personales¹⁸².

Se debe distinguir entre datos personales basados en hechos y los basados en apreciaciones personales. Como acertadamente apunta ciertos autores¹⁸³ el almacenamiento de datos por categorías parece una excepción al principio de exactitud, ya que permite almacenar datos inexactos y no precisos. Solo hay que separarlos con una “etiqueta” de los datos que son exactos.

En una materia tan sensible como la información que consta en las bases de datos policiales, abogamos por una interrelación de las bases de datos de las distintas autoridades competentes, que tienen como finalidad la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas

182 Art. 7 de la Directiva (UE) 2016/680.

183 REBOLLO DELGADO, L. y SERRANO PEREZ, M. M. (2006) p. 131.

contra la seguridad pública, para de este modo obtener mayor exactitud de los datos.

Hay que tener en cuenta que muchas investigaciones se inician a partir de hechos o datos que no están corroborados, basándose en fuentes confidenciales de información¹⁸⁴, observaciones de los agentes, deducciones de los propios agentes o de otros actores de la investigación y si se parte de datos imprecisos o erróneos es perder tiempo y dinero. Aún así, es necesario que dicha información obre en poder de las autoridades policiales y que esté inscrita en las bases de datos ya que una investigación consiste en corroborar una hipótesis de trabajo la cual, por propia definición, no es un dato exacto. Al finalizar la investigación, la hipótesis se podrá convertir – o no - en un hecho corroborado.

f. - Tratamiento de categorías especiales de datos personales¹⁸⁵.

En el ámbito de aplicación de la Directiva, se permite procesar datos relativos al *“origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera*

¹⁸⁴ Persona que facilita información a las autoridades policiales, ya sea regularmente o de forma esporádica sobre actividades delictivas.

¹⁸⁵ Art. 10 de la Directiva (UE) 2016/680.

unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales”; para ello se requiere que sea estrictamente necesario y que el derecho de la Unión o del estado Miembro lo contemple en su legislación.

Este tratamiento se permitiría también para proteger los intereses vitales de una persona física o que el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

En el Estado español, hay bases de datos policiales que contienen este tipo de información. Así por ejemplo, el fichero “*Sistema d'Informació de la Policia de la Generalitat de Persones Físiques (SIP PF)*”¹⁸⁶ de la Policía de la Generalitat-Mossos d'Esquadra contiene datos relativos a la raza de las personas o el fichero ADN - HUMANITAS datos relativos a perfiles genéticos¹⁸⁷.

4.3.- Derechos del interesado.

Cuando las Autoridades policiales limiten los derechos del interesado deben hacerlo siguiendo una normativa que *debe*

¹⁸⁶ Orden IRP/435/2009, de 2 de octubre. Anexo II. Ámbito sistemas de información de la Policía de la Generalitat-Mossos d'Esquadra.

¹⁸⁷ Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior.

Fichero 4 del ámbito del Cuerpo Nacional de Policía.

establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida garantizando que la injerencia se limite a lo estrictamente necesario siguiendo la interpretación dada por el TJUE y el TEDH.

El interesado puede ejercer sus derechos a través del control correspondiente previsto en la legislación o, en caso de no quedar satisfecho, acudir a la tutela judicial.

a.- Derecho a la información.

Cada estado miembro debe disponer la forma en la que la información ha de ser facilitada al interesado, así como en qué ha de consistir esta información. Como mínimo, le ha de ser facilitado:

- La identidad del responsable del tratamiento y los datos de contacto del delegado de protección de datos – si existe -.
- La finalidad del tratamiento, así como los destinatarios o las categorías de destinatarios de los datos personales.
- Los derechos que le corresponden (reclamación delante la autoridad de control, acceso, rectificación, supresión o limitación).

En ciertos casos establecidos por ley, se le debe informar de la base jurídica en que se fundamenta el tratamiento de los datos, el plazo de tiempo que se conservaran así como las categorías de destinatarios de los datos personales, en particular en cuando se trate de terceros países u organizaciones internacionales. Cuando los datos hayan sido recabados sin conocimiento del interesado, se le podrá facilitar más información.

Así y todo, la información que debería ser facilitada en estos casos puede ser retrasada, limitada o puede incluso no ser facilitada si ello conlleva “*que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales*”¹⁸⁸. Por lo tanto, la última palabra la tendrá siempre la autoridad policial. Algunos autores¹⁸⁹ consideran que no es proporcional la previsión que hace la Directiva a la excepción del derecho que tiene el titular a ser informado del uso de sus datos. La limitación del derecho por *simples indagaciones*, parece permitir la exclusión del derecho a ser informado sin indicio alguno. O que se puedan obstaculizar *procedimientos oficiales* indican que fácilmente puede obviarse el derecho que tiene el interesado a ser informado¹⁹⁰.

188 Art. 13 de la Directiva (UE) 2016/680.

189 OUBIÑA BARBOLLA S. (2015), p 104.

190 Art. 13 de la Directiva (UE) 2016/680.

Además, tampoco se determina el plazo de tiempo que tienen las autoridades para informar.

b.- Derecho de acceso del interesado a los datos personales.

Los estados miembros deberán *confirmar* al interesado si están tratando o no sus datos personales y, en caso afirmativo, debe facilitarle información relativa a:

La finalidad y base jurídica del tratamiento, los destinatarios del tratamiento, el plazo de tiempo durante el cual los datos personales serán tratados, los derechos que le asisten, así como los datos que son objeto de tratamiento y de donde proceden¹⁹¹.

La limitación del derecho de acceso es la misma que la del derecho a la información. El derecho a la información se ejerce sobre el tratamiento y el de acceso versa sobre los datos personales que se ven sometidos a dicho tratamiento¹⁹².

¹⁹¹ Art. 14 de la Directiva (UE) 2016/680.

¹⁹² Se podrá limitar el derecho de acceso (art. 15.1 de la Directiva (UE) 2016/680).

- a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;
- b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;
- c) proteger la seguridad pública;
- d) proteger la seguridad nacional;

En caso de limitar el derecho de acceso, el responsable del tratamiento deberá informar al interesado que se le deniega el acceso y de que tiene derecho a interponer reclamación delante de la autoridad de control o a un recurso judicial.

c.- Derecho de rectificación y supresión de datos personales del interesado.

Cuando el interesado ejerce el derecho de acceso a sus datos personales, se le debe informar de a quién se debe solicitar la rectificación o supresión de sus datos personales, así como la limitación de tratamiento. Y el responsable del tratamiento debe rectificar o completar los datos que el interesado le comunique e informar a los destinatarios de la transmisión de los datos, a no ser que el interesado tenga dudas sobre la exactitud de los mismos o se deban conservar a efectos probatorios.

En cambio, el Reglamento (UE) 2016/679 obliga al responsable del tratamiento a limitar el tratamiento de los datos cuando el interesado impugne la exactitud de los mismos¹⁹³.

e) proteger los derechos y libertades de otras personas.
193 Art. 18.a del Reglamento (UE) 2016/679

Conclusiones.

El derecho a la privacidad nace a finales del siglo XIX en los Estados Unidos como el “derecho a estar solo” poniendo límite a las intrusiones ajenas en la vida privada de las personas. En los 60 y 70 del siglo pasado, a medida que la sociedad va teniendo conciencia del valor que tienen los datos personales, se empieza a regular específicamente este aspecto, llegándose a crear un derecho autónomo.

Los datos personales pertenecen al individuo y éste los cede bajo unas condiciones. La protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitadas de sus datos personales queda englobada en el derecho general de protección de la persona y debe determinar por sí mismo la divulgación y la utilización de los datos¹⁹⁴.

Las nuevas tecnologías permiten un tratamiento de los datos de forma masiva de manera que es posible conocer aspectos de la vida de un individuo a partir de datos aparentemente inocuos. Las autoridades son conscientes de este aspecto y tratan de proteger a los ciudadanos del abuso que puede ejercer el sector privado o la propia administración pública pero, por otro lado, debe proteger el principal que recurso de

¹⁹⁴ Sentencia del Tribunal Constitucional Federal Alemán de 15/12/1983 que declara inconstitucional algunos aspectos de la Ley del Censo de 31/03/1982.

que disponen las autoridades policiales para luchar contra el crimen: la información, gran parte de ella formada por datos personales.

El cuerpo legislativo relativo a la protección de datos ha ido adaptándose a los avances científicos que se han producido en este campo por un lado y a las necesidades que ha ido experimentando la sociedad al ver que dicho avance científico ha supuesto una merma del derecho a la privacidad de los individuos. Por este motivo se han desarrollado una serie de derechos que varían en función de quien hace el tratamiento de los datos. Así, si los datos personales van a ser utilizados por las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales los derechos van a ser más restrictivos que si van a ser utilizados por otras entidades del sector público o privado que tengan otras finalidades.

CAPÍTULO II

TRANSMISIÓN DE DATOS PERSONALES EN EL ÁMBITO DE LA COOPERACIÓN POLICIAL INTERNACIONAL

Introducción.

En los últimos tiempos, numerosos países y organizaciones internacionales han dirigido parte de sus esfuerzos hacia la lucha contra la delincuencia transfronteriza provocando la creación, a lo largo del tiempo, de una gran amalgama de acuerdos bilaterales y multilaterales, tratados internacionales, compromisos y resoluciones. Algunos de ellos hacen referencia a distintas formas de cooperación, como pueden ser tratados de extradición o de reconocimiento de sentencias. Otros, en cambio, se centran en la lucha contra ciertas categorías específicas de crímenes, como el terrorismo, el tráfico internacional de sustancias estupefacientes o la trata de seres humanos, por citar

algunos. Unos se articulan a nivel judicial y otros, en cambio, a nivel policial. Los instrumentos internacionales de cooperación son tantos y tan variados que sería una ardua tarea entrar en el estudio detallado de todos ellos y no es el objetivo de este trabajo.

En este capítulo, haremos un estudio de las formas de cooperación policial en Europea que lleva aparejada la transmisión de información, y por ende datos personales, entre los distintos cuerpos policiales. La Unión Europea ha desarrollado un cuerpo normativo mucho más extenso que el del Consejo de Europa.

A lo largo de una investigación, la policía trabaja con información que, posteriormente, parte de ella se convertirá en datos, de los cuales, una parte más pequeña podrán informatizarse en bases de datos donde se almacenaran para posibles usos futuros. Éste es un proceso que se retroalimenta. Así, una parte del análisis de la información consiste en analizar datos, que proporcionaran nueva información que servirá para obtener nuevos datos, los cuales, analizados otra vez producirán más información y así hasta la resolución del caso - si se consigue -. Durante todo el proceso de una investigación se produce el intercambio de información.

Antes de adentrarnos en este capítulo, debemos distinguir entre dos principios que rigen la transmisión de información entre dos entidades, en este caso estados, y que poseen marcadas diferencias¹⁹⁵:

- principio **pull**: el estado que requiere la información tiene línea directa con la base de datos, de manera que recoge de ella toda la información que necesita.

- principio **push**: el estado interesado en la información hace una petición hacia el estado que la posee, requiriendo los datos que necesita, de manera que la otra parte hará una selección de dicha información y la transmitirá.

En este segundo principio se basa el intercambio de datos entre las distintas autoridades policiales. Cada una de ellas tiene sus propias bases de datos y si alguna otra autoridad requiere la información, ésta debe solicitarla y la otra le facilitará exclusivamente la información que necesite. La Unión Europea ha diseñado unos procedimientos legales que permiten el intercambio de información de forma relativamente ágil entre distintos países cuando se lucha contra la delincuencia organizada. En éste capítulo vamos a analizar los distintos convenios y tratados que permiten este intercambio policial de datos.

¹⁹⁵ GUTWIRTH et al. (2009).

1.- Cooperación policial.

Siguiendo el esquema propuesto por JOUBERT y BEVERS¹⁹⁶ hay diversos modelos de cooperación policial internacional. Distintas personas luchando contra los mismos delitos – que no necesariamente mismos delincuentes – y en distintos países, con lo que supone en cuanto a herencia cultural y diversidad de ordenamientos jurídicos, han desarrollado diversas formas de cooperación policial.

1.1.- Modelos de cooperación interpolicial.

La policía, como organización, tiene un fuerte componente de equipo que a veces llega a traspasar fronteras. Los agentes de policía, entre sí, se dan el tratamiento de colegas. Esta cooperación puede cristalizar en acuerdos entre los distintos cuerpos policiales que, dependiendo del grado de formalidad que se les confiera, podrían distinguirse entre acuerdos formales o informales.

Cooperación policial informal.

Esta vendría dada por los acuerdos que tienen los distintos agentes policiales entre sí. Las convenciones policiales, las asociaciones de policías, los cursos de formación, además

¹⁹⁶ JOUBERT y BEVERS (1996) p. 27 y ss.

de para intercambiar experiencias, sirven para intercambiar tarjetas de presentación con números de teléfono a los que recurrir cuando es necesaria una información concreta sobre un determinado asunto.

Otro ejemplo de este tipo de cooperación policial lo encontramos en los contactos que pueden tener entre sí agentes que cubren a ambos lados una misma frontera. Además de trabajo, comparten los delitos a resolver y los delincuentes que los cometen. Las fronteras crean y atraen delitos y delincuentes. Es habitual que los agentes compartan información entre sí de manera informal.

Cooperación policial formal.

El paradigma de este modelo de cooperación ha sido, hasta hace unas décadas, **Interpol**, organización de la que se habla al final de éste capítulo.

1.2.- Cooperación intergubernamental.

En éste tipo de cooperación hay varios modelos que dan una estructura formal a los acuerdos a los que llegan los distintos gobiernos. Por citar algunos, están el *Convenio Europeo de Extradición* de 1957 y el *Convenio Europeo de Asistencia Judicial en Materia Penal* de 1959, promovidos ambos por el

Consejo de Europa en materia de cooperación jurídica penal. Los dos son instrumentos multilaterales en materia de asistencia penal en Europa.

2.- Transmisión de datos personales en el ámbito policial dentro del marco del Consejo de Europa.

2.1.- Convenio 108 y su Protocolo Adicional de 2001.

El Convenio 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, fue abierto a la firma en Estrasburgo, y actualmente está ratificado por 41 países¹⁹⁷.

En su objeto de garantizar el derecho a la vida privada de cualquier persona física - protección de datos - el art. 12 regula el flujo transfronterizo de datos personales entre los países firmantes del Convenio. Así, utilizando la excusa de la protección de la vida privada, un estado parte del tratado no podrá prohibir o someter a una autorización especial la transmisión de datos personales a otra parte del Convenio. Hay libre circulación de datos personales entre los países firmantes del Convenio.

¹⁹⁷ https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=P7JN8uYf (última consulta 18/03/2022).

A diferencia de la legislación de la Unión Europea, el Convenio 108 no hace distinción de ámbitos de aplicación, ya que debe aplicarse tanto a los flujos transfronterizos de datos entre empresas del sector privado como para datos utilizados por las autoridades policiales en la investigación de delitos.

Del Convenio solo forman parte los estados y no se permite a las organizaciones internacionales entrar en él.

- Transmisión de datos personales entre un estado que forma parte del Convenio 108 a otro que no forma parte de él.

El Convenio recoge una excepción según la cual, si los datos personales a transferir tienen una protección especial en el estado emisor, deben tener una **protección equivalente** también en el estado receptor. Se podrá denegar la transmisión si la parte receptora ha de transferir los datos personales a un estado no parte del Tratado, si el objetivo de la transmisión es el de burlar la legislación.

El Convenio 108 fue ampliado por el **Protocolo adicional de 2001**¹⁹⁸ en el que se regula la transmisión de datos personales a un estado que no sea parte del Convenio. En él

¹⁹⁸ Protocolo adicional de 2001 al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos.

se rebajan las condiciones de la transferencia de los datos ya que se pasa de exigir una protección *equivalente* en el Convenio, a un “**adecuado nivel de protección**”.

a.- Para los estados parte del Convenio que no forman parte de la Unión Europea, el Protocolo adicional establece que sea el derecho interno de cada país el que evalúe el nivel de protección de datos del país receptor¹⁹⁹.

b.- Para los estados pertenecientes a la Unión Europea, es la Comisión la encargada de determinar si un tercer país o territorio garantiza un nivel adecuado de protección, calificación que puede ser obtenida también por una organización internacional.

Para ello, la Comisión tendrá en cuenta:

- el respeto de los derechos humanos y las libertades fundamentales en general y la legislación sobre protección de datos en particular que tenga dicho estado u organización, así como los derechos exigibles y efectivos de los interesados.
- la existencia de una autoridad o autoridades independientes de protección de datos.

¹⁹⁹ Art. 2.2 del Protocolo adicional de 2001 al Convenio.

- los compromisos internacionales asumidos que deriven de convenios o instrumentos jurídicamente vinculantes con carácter general y, en particular, en relación con la protección de los datos personales²⁰⁰.

La Comisión tomará la decisión de si existe un adecuado nivel de protección mediante un *acto de ejecución*²⁰¹, el cual deberá ser revisado al menos cada 4 años. Cuando un país es declarado adecuado se podrán transferir datos desde los estados miembros de la Unión Europea sin necesidad de ningún tipo de trámite o autorización especial²⁰².

Si la Comisión no ha adoptado una decisión sobre si el estado en cuestión o la organización internacional disponen de un adecuado nivel de protección, se podrán transferir datos si se *disponen de las garantías apropiadas*²⁰³. En este caso deberá darse uno de los dos requisitos²⁰⁴:

200 Art. 36 de la Directiva (UE) 2016/680.

201 Procedimiento regulado en el art. 5 del Reglamento (EU) 182/2011 del Parlamento Europeo y del Consejo de 16 de febrero de 2011 por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión.

202 En esta página web puede consultarse la lista de países que tienen un adecuado nivel de protección de datos: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (última consulta 18/03/2022).

203 Cabe notar que la Directiva (UE) 2016/680 utiliza el término garantías *apropiadas*, mientras que el Reglamento (UE) 2016/679 – art. 46 – utiliza el de garantías *adecuadas*, para lo que es necesario unos requisitos más exigentes.

204 Art. 37 de la Directiva (UE) 2016/680.

- Ese estado haya aportado garantías apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante. Se pueden tener en cuenta, por ejemplo, acuerdos de cooperación celebrados entre Europol o Eurojust y terceros países que permitan el intercambio de datos personales²⁰⁵.
- El responsable del tratamiento haya evaluado todas las circunstancias que concurren en la transferencia de datos personales y hayan llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales. De usar esta opción se debe comunicar a la autoridad de control²⁰⁶ y documentar los datos de la transferencia.

Finalmente, en caso de no disponer de ninguno de los dos requisitos anteriores – no tener garantizado un nivel adecuado de protección ni disponer de la garantías adecuadas – la transferencia de datos podrá realizarse para proteger intereses vitales de una persona o legítimos del interesado, para prevenir la amenaza grave e inmediata para la seguridad pública de un estado o en casos individuales. En

²⁰⁵ Considerando 71 de la Directiva (UE) 2016/680.

²⁰⁶ La autoridad de control está creada en los art. 51 i ss del Reglamento (UE) 2016/679. Es una autoridad pública independiente que supervisa la aplicación de la Directiva (UE) 2016/680 y será creada según estipula el Reglamento (UE) 2016/679. Cada estado miembro puede disponer que sea una o varias las autoridades con esta responsabilidad.

este caso también debe documentarse la transferencia de datos personales por si lo requiere la autoridad de control²⁰⁷.

Si una autoridad competente considera que la transferencia a una autoridad competente del tercer país - que carece de las garantías anteriores - resulta ineficaz o inadecuada, sobre todo porque no pueda efectuarse dentro de plazo, para casos particulares y específicos, puede transferir directamente los datos personales a destinatarios establecidos en ese país si considera que ninguno de los derechos y libertades fundamentales del interesado en cuestión son superiores al interés público que precise de la transferencia de que se trate²⁰⁸.

2.2.- Recomendación (87) 15 del Comité de Ministros²⁰⁹.

El Convenio 108 prevé una serie de excepciones a lo dispuesto en el propio convenio respecto a la calidad de los datos, a sus categorías particulares y a las garantías que dispone la persona a la que conciernen los datos en cuestión²¹⁰. En aras de "*protección de la seguridad del estado, de la seguridad pública, para los intereses*

207 Art. 38 de la Directiva (UE) 2016/680.

208 Art. 39 de la Directiva (UE) 2016/680.

209 Recomendación (87) 15 del Comité de Ministros a los estados Miembros regulando el uso de datos personales en el sector policial, de fecha 17 de septiembre de 1987.

210 Art. 5, 6 y 8 del Convenio 108.

*monetarios del estado o para la represión de infracciones penales*²¹¹ el Comité de Ministros del Consejo de Europa estableció la Recomendación (87)15 que equilibra el derecho a la privacidad de los individuos con el interés de la sociedad a luchar y prevenir la delincuencia y mantener el orden público en una sociedad democrática.

La transferencia de datos entre distintos cuerpos policiales debe realizarse solo para fines policiales y siempre que haya un legítimo interés entre ellos en el marco de sus respectivas competencias.

Se permite la comunicación de datos a otros organismos públicos no policiales en casos particulares, como que haya una obligación o autorización a la cesión de datos, que lo autorice la autoridad supervisora o que sea indispensable para el cumplimiento de las funciones de dicho organismo, siempre que el tratamiento de los datos no sea incompatible con el procesamiento original.

También se podrán transmitir si, la cesión de los datos, ha sido autorizada por el interesado - o se presume su consentimiento - o sea necesario para prevenir un serio e inminente peligro. Finalmente, la cesión de datos a partes privadas podrá realizarse en caso de que haya una

²¹¹ Art. 9.2.a. del Convenio 108.

obligación o autorización a dicha cesión, que lo autorice la autoridad supervisora o el propio interesado - o se presuma su consentimiento - o sea necesario para prevenir un serio e inminente peligro.

A nivel internacional, la comunicación de datos policiales debe ser realizada, exclusivamente, entre los diferentes cuerpos policiales. Se debe llevar a cabo si existe una provisión legal de ámbito nacional o internacional y, de no existir, se llevará a cabo para prevenir un serio e inminente peligro o para reprimir delitos graves²¹².

3.- Transmisión de datos personales en el ámbito policial en el marco de la Unión Europea.

3.1.- Acervo de Schengen.

Tal como reza el anexo del Protocolo de Schengen, forman parte del acervo de Schengen: el **Acuerdo de Schengen**, el **Convenio de aplicación del Acuerdo de Schengen – CAAS** - y las **Decisiones del Comité Ejecutivo** creado por este último. Hoy en día, este acervo normativo se ha integrado en el de la Unión Europea a partir del Tratado de Amsterdam²¹³ de 1997, que puso énfasis en definir la Unión

²¹² Art. 5 de la Recomendación (87)15.

²¹³ Tratado de Amsterdam por el que se modifican el Tratado de la Unión Europea, los Tratados constitutivos de las Comunidades Europeas y

como un espacio de libertad, seguridad y justicia. De esta manera los estados que forman parte de la UE se integraron en el espacio Schengen. Ello ha supuesto que el Comité Ejecutivo creado por el CAAS haya sido sustituido por el Consejo de la Unión, así como el control parlamentario y jurisdiccional de los actos llevados a cabo, de manera que los ciudadanos que vean vulnerados sus derechos por estos actos puedan recurrir delante del Tribunal de Justicia de la Unión Europea o a las instancias jurisdiccionales nacionales que les correspondan.

A continuación expongo brevemente los dos primeros conjuntos normativos.

a.- Acuerdo de Schengen.

El Consejo Europeo reunido en Fontainebleau, el 25 y 26 de junio de 1984 adoptó una serie de orientaciones respecto a la implementación de la cooperación europea, entre las que había la supresión de formalidades fronterizas relativas a aduana y policía en la circulación de personas.

determinados actos conexos, el 2 de octubre de 1997 en Amsterdam y que entró en vigor el 1 de mayo de 1999.

Posteriormente, los estados que formaban parte de BENELUX, Francia y Alemania²¹⁴ firmaron el **Acuerdo de Saarbrücken**, - también conocido como el **Acuerdo de Schengen de 1985** - donde dieron un primer paso encaminado a la supresión de sus fronteras, a la vez que instaban a reforzar la cooperación entre las autoridades policiales en el ámbito de la prevención y la investigación²¹⁵, para luchar conjuntamente contra el crimen.

El acuerdo en sí es una declaración de intenciones de las medidas a aplicar para conseguir el objetivo de la supresión total de todos los controles y las formalidades entre las fronteras comunes.

Los 33 artículos de que consta hacen referencia a:

- Medidas aplicables a corto plazo:

214 Actualmente el espacio Schengen está formado por: Austria, Bélgica, Rep. Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Noruega, Polonia, Portugal, Eslovaquia, Eslovenia, España, Suecia, Suiza y Liechtenstein.

215 Art. 18 del Acuerdo entre los Gobiernos de los estados de la Unión Económica de Benelux, la República Federal de Alemania y la República Francesa sobre la abolición gradual de los controles en sus fronteras comunes. - Acuerdo de Saarbrücken o Acuerdo de Schengen de 1985 -.

Después de la firma del Tratado de Amsterdam en 1997, el acuerdo fue incluido en el acervo de la UE.

<http://www.jus.uio.no/english/services/library/treaties/02/2-07/schengen-agreement-1985.xml#history> (última consulta 18/03/2022).

Están encaminadas a facilitar la circulación de personas, vehículos particulares, transporte profesional y de mercancías por carretera, transportes ferroviarios y fluviales entre las fronteras comunes. Coordina las políticas de visados. Preocupa la delincuencia, por lo que se insta a que las autoridades aduaneras y policiales colaboren en la lucha contra la criminalidad, en especial contra el tráfico ilícito de sustancias estupefacientes y de armas, inmigración ilegal, fraude fiscal, aduanero y contrabando, así como los movimientos irregulares de capitales.

- **Medidas aplicables a largo plazo:** Los países firmantes deberán transferir los controles de las fronteras internas a las externas, armonizando legislación en lo referente a la concesión de visados y deberán llegar a acuerdos en lo relativo a la cooperación policial y judicial para combatir más eficazmente la criminalidad. También se exponen medidas encaminadas a la armonización de impuestos indirectos y de mejora en el transporte internacional de mercancías.

b.- Convenio de aplicación del Acuerdo de Schengen – CAAS -.

El 14 de Junio de 1985 estos países firman el **CAAS**, que entró en vigor el 26 de marzo de 1995. En él se regula la normativa relativa al cruce de fronteras exteriores²¹⁶ y los sistemas de visados comunes, identificando los estados que son responsables de estudiar las solicitudes de asilo²¹⁷. La abolición de los controles fronterizos hizo que se implementaran medidas relativas a la cooperación policial entre los distintos estados. Además de regular la cooperación judicial y policial, introduce sencillos mecanismos de cooperación judicial – cursar comisiones judiciales, hacer notificaciones por correo, ampliación de la asistencia judicial -.

El título III hace referencia a la cooperación transfronteriza en el ámbito policial y judicial en materia penal. El primer capítulo habla de la cooperación policial. Los capítulos segundo, tercero, cuarto y quinto tratan de la asistencia

²¹⁶ A raíz de los atentados de París de 2015, desde el 7 de abril de 2017 entró en vigor la modificación del Reglamento 2016/399 del Código de Fronteras Schengen, que aplica controles de identidad obligatorios para comunitarios en las fronteras exteriores de la UE. Ello significa consultar las bases de datos europeas – SIS II, BDSN o las bases de datos de Interpol – para evitar que se usen documentos sustraídos, extraviados o invalidados con el fin de ocultar la verdadera identidad. Anteriormente, los ciudadanos europeos solo eran sometidos a controles mínimos para verificar la validez del documento identificativo de viaje que presentaban.

²¹⁷ Modificado por el Convenio de Dublín de 2003.

judicial en materia penal, aplicación del principio “*non bis in ídem*”, la extradición y sobre la ejecución de sentencias penales. Los dos últimos capítulos tratan de las sustancias estupefacientes y de las armas de fuego y municiones.

Los títulos IV y VI versan sobre la creación del Sistema de información de Schengen (SIS) y sobre la protección de datos de carácter personal. El resto de títulos hacen referencia a la supresión de controles en las fronteras interiores y circulación de personas, al transporte y circulación de mercancías, a la creación de un comité ejecutivo para la aplicación del convenio y a las disposiciones finales.

Dado el objeto de este trabajo, es necesario centrarse en el **Título III**, relativo a la **Policía y Seguridad** donde se exponen las medidas acordadas encaminadas a mejorar la cooperación policial. Todo y que a nivel operativo son medidas que resultan muy eficientes, el uso de algunas de ellas de manera arbitraria podría menoscabar el derecho a la protección de datos de los ciudadanos.

- Intercambio de información.

Se permite que los servicios de policía “*se presten asistencia para prevenir e investigar hechos delictivos*”²¹⁸. El CAAS establece el compromiso de asistencia mutua entre los respectivos servicios policiales, siempre que (1) se respetara la legislación nacional, (2) la solicite un órgano competente, (3) para prevenir e investigar delitos, (4) que el derecho nacional no reserve la solicitud a las autoridades judiciales y (5) que las autoridades policiales requeridas no deban aplicar la coacción para ejecutar la solicitud.

Cuando sea necesario aportar esta información como prueba, debe ser autorizado por la autoridad judicial del estado de donde se obtiene. La información – petición y respuesta – será intercambiada a través de las oficinas **SIRENE** – de las cuales hablaremos más adelante – o, en caso de urgencia, directamente a las autoridades competentes del estado afectado. En las regiones fronterizas se podrá regular acuerdos entre los ministros competentes²¹⁹.

218 Art. 39 CAAS.

219 Por ejemplo entre España y Francia hay firmado el Convenio de Cooperación Transfronteriza en materia policial y aduanera (1998), conocido también como en Convenio Blois.

Pero la información que las autoridades policiales disponen de sus propios ciudadanos es distinta en cada país, como consecuencia de los distintos ordenamientos jurídicos y cuando se intercambia la información esta disparidad normativa no siempre se tiene en cuenta, pudiendo haber desproporcionalidad en la información en cuanto a la cantidad y calidad de los datos transmitidos.

Esta falta de homogeneidad y de concreción puede provocar problemas no solo prácticos sino también de disfrute de los derechos. Problemas cuya solución es bastante evidente pero para la que sería precisa una fuerte voluntad política de convergencia de las legislaciones nacionales, particularmente difícil en materia policial y penal. Sin embargo, esta resistencia de los estados a llegar a acuerdos respecto de la información de la que disponen los cuerpos policiales supone un serio revés para el ejercicio de los derechos. Dos son quizá los casos más claros, desde la perspectiva española, de vulneración de derechos de algunos colectivos por la diversidad de la información puesta a disposición de los cuerpos policiales: los problemas derivados de la Sexual Offences Act y los boletines policiales mensuales con información acerca de los carteristas o *pickpockets*.

1.- Sexual Offences Act.

En virtud de la conocida *Sexual Offences Act* de 2003, las personas condenadas por delitos sexuales en el Reino Unido están obligadas a comunicar - entre otros datos – el domicilio en el que reside habitualmente²²⁰. El periodo durante el cual deben hacer la comunicación varía en función del tiempo de condena. Así, para condenas inferiores a 6 meses de prisión la comunicación debe realizarse durante siete años; en cambio, para condenas superiores a los 30 meses la comunicación será durante tiempo indefinido²²¹.

Cuando una de estas personas obligadas a notificar abandona el Reino Unido por un periodo igual o superior a 3 días debe comunicarlo a las autoridades policiales británicas. Ello significa que si esta persona se va una semana de vacaciones a la costa española, por ejemplo, debe comunicar a las autoridades policiales de su país el hecho del viaje y el lugar donde se alojará, al menos, la primera noche.

En situación similar se encuentran las personas con antecedentes de delitos sexuales cometidos en los Estados Unidos o Australia. Las autoridades policiales de sus países informan - a través de Interpol – a las autoridades de destino

²²⁰ Art. 83 *Sexual Offences Act* 2003.

²²¹ De por vida sería un término más ajustado.

de los viajes que hacen estas personas. En esta comunicación se facilitan los datos de filiación de la persona, la fecha de llegada y de salida a dicho país, el lugar donde se va a hospedar – si se conoce -, una breve descripción de los hechos que cometió para ser condenado y la pena que le fue impuesta. Les muestra su pasado como convicto.

De esta manera, las autoridades policiales de destino tendrán conocimiento que una persona con antecedentes de delitos sexuales, y que habitualmente reside en otro país, irá a su localidad a pasar unos días y sus datos serán grabados en las bases de datos policiales. Es indiferente si el motivo del viaje es de placer con la familia o viaja solo o por negocios.

Cuando las autoridades policiales españolas tienen conocimiento – a través de SIRENE, Interpol o Europol - de la presencia en España de una persona con antecedentes penales o policiales en el extranjero por delitos contra la libertad e indemnidad sexuales, darán de alta un control específico en la Base de Datos de Señalamientos Nacionales (BDSN), haciendo las comprobaciones oportunas relativas a las condiciones de viaje y estancia. Cualquier incumplimiento o desvío “sensible” de las condiciones de viaje o estancia prevista, deberá ser comunicada a las autoridades de

procedencia de la comunicación²²². Como respuesta a la solicitud de colaboración, las autoridades policiales españolas redactan un informe en el que se hace constar la actividad que ha tenido dicho individuo en nuestro país: cuando ha llegado, cuando ha partido, el lugar o lugares en los que se ha hospedado y si ha habido algún incidente con esta persona, que no tiene que ser necesariamente de carácter sexual. Si se le identifica en la vía pública, al constar sus datos en las bases de datos policiales, se le abrirá un incidente en el que se hará constar dicha identificación y sus circunstancias.

Todo ello significa que, en la comisaría de policía de referencia en la que se investiguen los delitos de ámbito sexual, pueden tener una fotografía de dicho individuo extranjero colgada en la pared como persona candidata a investigar en caso de haber algún delito sexual en la zona y sus datos constaran en las bases de datos policiales españolas como potencial delincuente sexual, hasta que estos sean borrados.

222 SES 1/2015 - Instrucción de la Secretaria de estado de Seguridad núm. 1/2015, sobre medidas policiales a adoptar para un mejor control de individuos condenados o detenidos por delitos contra la libertad e indemnidad sexuales de los menores, modificada por la Instrucción de la Secretaria de estado de la Seguridad núm. 8/2016.

En cambio, al lado de la misma comisaria puede tener su domicilio habitual una persona de otra nacionalidad con antecedentes de ámbito sexual en España y pasar completamente inadvertido para las autoridades policiales. El motivo que se argumenta en la Instrucción SES 1/2015 es el alto riesgo de reincidencia que presentan los delincuentes condenados por delitos contra la libertad e indemnidad sexuales, por lo cual se precisa de herramientas eficaces para proteger a los menores de estas personas. Pero parece que solo son peligrosos los delincuentes sexuales procedentes de estos países y no los del resto de países, ni tampoco los residentes en el propio país.

La legislación española referente a los delincuentes sexuales es distinta respecto de los países mencionados. El Legislador español ha creado el **Registro Central de Delincuentes Sexuales**²²³ en el Registro Central de Penados, a los solos efectos de prevención y con la finalidad de hacer posible su seguimiento y control a nivel judicial de *“quienes hubieran sido condenados en sentencia firme por cualquier delito contra la libertad e indemnidad sexuales, así como por trata de seres humanos con fines de explotación sexual, incluyendo la pornografía”* y al cual tienen acceso jueces, fiscales y policía judicial que trabajen en este ámbito. Se trata

²²³ Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales.

de una base de datos no pública en la que debe quedar registrado el acceso de cualquier persona a ella.

Podría afirmarse que hay una clara discriminación entre los ciudadanos que han cometido este tipo de delitos dependiendo del país en el que se ha cometido. Así, un británico que haya cometido un delito de origen sexual en España y que, una vez cumplida la pena, vuelva a su país, las autoridades policiales británicas no recibirán ningún aviso de las autoridades policiales españolas informándoles del hecho del viaje y el lugar a donde se dirigirá, ya que éstas últimas no disponen de dicha información. Es más, no se les comunicará los antecedentes policiales/penales que pueda tener este sujeto en nuestro país.

En España cualquier persona condenada en sentencia firme por cualquier delito contra la libertad e indemnidad sexuales debe ser inscrita en el Registro Central de Delincuentes Sexuales y la consulta de datos debe hacerse a requerimiento, por lo que las autoridades británicas deberían hacer una solicitud para consultar oficialmente los datos del registro, caso de querer algún tipo de información al respecto.

Las autoridades policiales españolas, a mi juicio, y con la excusa de salvaguardar la libertad e indemnidad sexuales de los menores, llevan a cabo una actuación desproporcionada y discriminatoria contra las personas procedentes de estos países y que tienen antecedentes policiales o judiciales de delitos sexuales – aunque no se hayan cometido contra menores -. A las personas procedentes de otros países con similares antecedentes no se les exige ninguna comunicación. Así, si en un determinado país los agresores sexuales no son puestos bajo una vigilancia policial discreta, cuando en ese país existe una persona que sí se encuentra bajo vigilancia en su país, dicha vigilancia debería cesar hasta que regresara a su lugar de origen.

Si el Tribunal Europeo de Derechos Humanos extiende la protección del derecho a la vida privada a los aspectos relacionados con la identidad personal tales como el nombre, la integridad física y moral o la fotografía²²⁴ de una persona, más aún deben protegerse el acceso a los antecedentes penales desfavorables. A mi juicio, las autoridades españolas deberían obviar este tipo de información procedente de estos países, absteniéndose de llevar a cabo cualquier acción que menoscabe el derecho a la privacidad de estos individuos.

²²⁴ STEDH de 7 de febrero de 2012. Caso Von Hannover c. Alemania, párrafo 95.

2.- Los Pickpockets – carteristas -.

En el marco de Europol, periódicamente se lleva a cabo una reunión de distintos cuerpos policiales europeos en la que se trata el problema de los carteristas a escala continental²²⁵. Es obvio que las policías europeas deben aunar esfuerzos para luchar contra este tipo de crimen callejero, más cuando se trata de grupos de personas que están organizados y tienen gran movilidad dentro del espacio Schengen. En una de estas reuniones se llegó al acuerdo de compartir información relativa a personas que cometen este tipo de delitos en los ámbitos territoriales de actuación de cada policía.

La información se comparte de la siguiente manera: cada cuerpo policial redacta en un formato consensuado un informe en el que constan informaciones relevantes sobre personas que cometen este tipo de delitos y que se desea transmitir. Estos informes son enviados a una lista de correos electrónicos de los distintos participantes en las reuniones y que posteriormente son distribuidos internamente dentro del cuerpo policial entre las diversas unidades que luchan contra este tipo de delitos.

²²⁵ Más información sobre la última conferencia llevada a cabo del 7 al 9 de diciembre de 2015 en el enlace de Europol: <https://www.europol.europa.eu/events/international-pickpocketing-gangs-conference> (última consulta 14/03/2022).

En la práctica, entre la información que se comparte hay la siguiente:

- Fotografías o fotoprinters de personas sospechosas, de la cual se desconoce la identidad y que ha cometido un hurto de un objeto valioso, por ejemplo, un reloj.

- Fotografías o fotoprinters de una persona de la que no se tiene ningún dato, con la finalidad de si averiguar si algún cuerpo policial tiene información sobre su identidad. Se desconoce el hecho delictivo concreto que ha llevado a cabo.

- Datos de filiación de una persona con fotografía actualizada y relación de los hechos cometidos en el país emisor del informe.

En ciertos casos los individuos que realizan este tipo de delitos son menores de 18 años, lo que conlleva que, al tratarse de únicamente de información policial, ciertos cuerpos policiales no tienen inconveniente en facilitar filiación y fotografías de menores de edad. Este hecho entra en contradicción, por ejemplo, con la legislación española en la que los registros policiales donde consten la identidad y otros datos que afecten a la intimidad de los menores serán de carácter estrictamente confidencial y no podrán ser

consultados por terceros²²⁶. Solo pueden acceder a estos datos las personas que participan en la investigación del delito en cuestión o las que autoricen expresamente el Juez de Menores o el Ministerio Fiscal. La difusión de los datos de filiación de menores en el sí de un cuerpo policial, sin que el menor estuviera involucrado en la investigación, no se ajustaría a la legalidad del estado español.

Salvando la problemática que puede suponer el dar difusión de datos de filiación y fotografías de menores de 18 años, en realidad, la finalidad del intercambio de información es la difusión de datos de personas que hacen hurtos en el territorio europeo. Ello supone hacer difusión de personas que, por su aspecto, no son residentes de ese país. Así por ejemplo, las policías suizas hacen difusión de personas que por sus rasgos étnicos no corresponden con el estándar suizo tradicional.

Por otra parte, la información efectiva que se transmite es la de ciertos hechos delictivos concretos. Suelen ser fotoprinters de centros comerciales de personas no identificadas que nunca va acompañada de información relativa a la investigación en la que se ha llegado a la conclusión – o simplemente se ha intuido – que se trata de

226 Art. 2.3 del Real Decreto 1774/2004, de 30 de julio, por el que se aprueba el Reglamento de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

un grupo criminal organizado con movilidad geográfica a nivel europeo.

Igual que un cuerpo policial hace difusión de los autores de ciertos delitos entre los agentes de una determinada zona, que dependerá del tipo de delito y del lugar donde se haya cometido, la información que se intercambian en estos boletines de pickpockets tiene la misma finalidad pero a nivel europeo. Ello supone que miles de agentes en la Unión Europea pueden disponer de los datos de filiación de estas personas por el simple hecho de haber cometido hurtos del tipo carterista y tener unos rasgos étnicos determinados.

El intercambio directo de información entre unidades policiales de distintos países llega a provocar un intercambio de datos que realmente no debería producirse. En definitiva, el intercambio de información debe ser concreta, precisa y ajustarse a las necesidades de las autoridades policiales de los distintos estados implicados.

- Centros de Coordinación Policial y Aduanero.

El CAAS también ha previsto que las regiones fronterizas puedan regular acuerdos en materia de seguridad para reforzar la cooperación policial transfronteriza. Así, se han

creado los **Centros de Coordinación Policial y Aduanero** entre países que comparten fronteras terrestres.

En el caso de España y Francia existen 4 de estos centros, que fueron abriéndose a partir de la aplicación del Tratado de Blois²²⁷. Por su parte, Francia tiene abiertos seis centros más a lo largo de su frontera terrestre. Con Portugal, España ha abierto cinco centros²²⁸.

Actualmente hay más de 40 centros de cooperación en funcionamiento entre las fronteras comunes de países vecinos. Algunos de estos centros son multilaterales, como por ejemplo el de Heerlen, entre Holanda, Bélgica y Alemania. En otros casos, se han creado con países que no

²²⁷ En virtud del Convenio de cooperación transfronteriza en materia policial y aduanera entre el Reino de España y la República Francesa (Blois, 7 de julio de 1998). BOE núm. 224 de 18 de septiembre de 2003, se han creado los centros de La Jonquera/Le Perthus, Les/Melles-Pont de Roi, Canfranc y Hendaya.

Las policías autonómicas están en los Centros que territorialmente les corresponde. Así, la Policía de la Generalitat-Mossos d'Esquadra está presente en los centros a partir de la Resolución de 27 de septiembre de 2007 de la Secretaría Técnica, en cumplimiento del artículo 1 del Convenio de Blois. La Policía de la Generalitat-Mossos d'Esquadra se integró en el Centro del Pertús el 7 de enero de 2008 i en el de Melles el 28 julio de 2008. La Ertzaintza se integró en el de Hendaya el marzo del 2010.

²²⁸ Acuerdo entre el Reino de España y la República Portuguesa sobre cooperación transfronteriza en materia policial y aduanera, hecho «ad referendum» en Évora el 19 de noviembre de 2005. En la actualidad, hay cinco **Centros de Cooperación Policial y Aduanera (CCPA)** hispano-portugueses, dos en territorio español en Tuy/Valença do Minho (Pontevedra) y Cayas/Elvas (Badajoz), y tres en territorio portugués en Vilar Formoso-Fuentes de Oñoro (Salamanca), Castro Marim/Ayamonte (Huelva) y Quintanilha/Alcañices (Zamora).

forman parte de la UE, como por ejemplo los dos que tiene España con Marruecos (Algeciras y Tánger) o el que existe entre la frontera de Rumanía y Ucrania.

Los Centros de Coordinación Policial y Aduanero han de permitir favorecer el buen funcionamiento de la cooperación policial transfronteriza entre los estados que forman parte. De las funciones que tienen asignadas destacan las siguientes:

- Recogida, análisis, intercambio y difusión de información que sea útil para la cooperación policial transfronteriza, en particular para la lucha contra la delincuencia transfronteriza, la inmigración irregular, los tráficos ilícitos y para prevenir las amenazas contra el orden público.
- Coordinación de acciones de cooperación entre los estados fronterizos. Por ejemplo coordinando medidas conjuntas de vigilancia en la zona fronteriza (patrullas mixtas).
- Ayuda a la preparación y soporte de las vigilancias (art. 40 CAAS) y persecución transfronterizas (art. 41 CAAS).
- Readmisión de extranjeros en situación irregular.

Cada Centro de Coordinación Policial y Aduanero tiene un coordinador²²⁹ para cada estado miembro que lo forma. En el caso español, esta figura se va alternando cada 3 años entre el Cuerpo Nacional de Policía y la Guardia Civil. En el caso de Francia, el coordinador es fijo para un cuerpo policial según qué Centro de Coordinación se trate. Así por ejemplo, el centro de Le Perthus es coordinado por un Comisario de División de la Policía Nacional Francesa y el de Melles lo es por un Teniente Coronel de la Gendarmerie Nationale.

Las consultas policiales más habituales que se llevan a cabo hacen referencia a antecedentes policiales y aduaneros, permisos de conducir o titularidad de vehículos, comprobación de domicilios en los respectivos sistemas, verificación de documentos, fotografías o huellas, información sobre alertas respectivas o información básica que es contenida en atestados. Si alguna unidad policial española hace una petición de este estilo a las autoridades francesas, pero referente a un objetivo italiano, el cuerpo policial francés hace suya la petición y la envía al Centro de Coordinación que tienen las autoridades policiales francesas

²²⁹ Los cuerpos policiales y aduaneros autorizados a desarrollar funciones en los Centros de Coordinación Policial y Aduanero en el lado español son: el Cuerpo Nacional de Policía, la Guardia Civil, el Departamento de Aduanas e Impuestos Especiales de la Agencia Estatal de Administración Tributaria del Ministerio de Economía y Hacienda, Mossos d'Esquadra y Ertzaintza. Por la parte francesa están: Police Nationale, Gendarmerie Nationale y Douanes et droits indirects.

con las autoridades policiales italianas para que les remitan la respuesta, que hace el camino inverso.

- Vigilancia.²³⁰

El Tratado autoriza que, en el marco de una investigación judicial, los agentes policiales que están vigilando a una persona que presuntamente haya participado en un delito que pueda dar lugar la extradición, puedan continuar esa investigación en territorio de otro estado contratante, si hay una petición de asistencia judicial previa. Por lo tanto, se requiere que la (1) investigación verse sobre un delito en el que pueda aplicar la extradición²³¹, (2) que haya cometido o participado en el delito, (3) existencia de una investigación judicializada y (4) solicitud de asistencia judicial previa debidamente presentada y canalizada a través de la oficina SIRENE.

230 Art. 40 CAAS.

231 Art. 1.1. del Convenio Europeo de Extradición, hecho en París el 13 de diciembre de 1957: *“Darán lugar a la extradición aquellos hechos que las Leyes de la parte requirente y de la parte requerida castiguen, bien con pena privativa de libertad o medida de seguridad privativa de libertad cuya duración máxima sea de un año por lo menos bien con pena más severa. Cuando en el territorio de la parte requirente se hubiere pronunciado condena a una pena o se hubiere infligido una medida de seguridad, la sanción impuesta deberá tener una duración de cuatro meses cuando menos”*.

Si se trata de razones particularmente urgentes y para una serie de delitos graves²³², la vigilancia puede proseguir siempre que lo autorice la otra parte y que se solicite asistencia judicial. Si en cinco horas no hay autorización o la respuesta es negativa, la vigilancia debe cesar. Pero hay muchos puestos fronterizos sin cámaras o que no están guardados por lo que no se puede detectar la entrada de los vehículos que realizan el seguimiento ni el momento exacto en el que se cruza la frontera.

Pero más difícil es controlar cuando cesa la vigilancia. Y ¿qué hacer con los datos obtenidos hasta ese momento en el país extranjero?. Esos datos serán incorporados a la investigación policial, y en caso de carecer de autorización, no podrán ser judicializados.

Los agentes que efectúan la vigilancia podrán llevar su arma reglamentaria – salvo que la otra parte decida expresamente lo contrario – pero no podrán arrestar al sospechoso, ni lo van a poder interrogar, ni tampoco entrar en lugares donde el

²³² Art. 40.7 CAAS. Entre ellos se encuentra el homicidio, la extorsión, la violación o el secuestro.

público no tenga acceso²³³. En caso de ver un delito flagrante podrían actuar como un ciudadano común de ese país.

La investigación pasará a ser tutelada por las autoridades policiales del estado en cuyo territorio se realiza la vigilancia y los agentes de donde procede la investigación colaboraran en ella, incluso en los procedimientos judiciales.

La ley únicamente habla de la vigilancia, pero ¿y la escucha?, ¿pueden escucharse conversaciones mientras se están haciendo las vigilancias?. Cabe entender que, en cuanto hay la autorización requerida para continuar la vigilancia en un país firmante, deberán atenerse a la legislación de dicho país.

Lo mismo ocurre con los dispositivos de vigilancia y seguimientos. Hoy en día es muy habitual complementar los seguimientos con estos dispositivos y para los que, en algunos estados como el español, se requiere autorización judicial para su instalación. Si una persona a la que se está vigilando - objetivo - abandona el país con uno de estos

²³³ Los agentes habilitados en el estado español para cruzar la frontera son funcionarios del Cuerpo Nacional de Policía, de la Guardia Civil y de la Administración de Aduanas. Recogido en el instrumento de ratificación del acuerdo de adhesión al CAAS - BOE núm. 81 de 5 de abril de 1994 -.

El 5 de noviembre de 2021 se llevó a cabo la 44 Junta de Seguridad de Catalunya en la cual se habilita al Cos de Mossos d'Esquadra para hacer vigilancias transfronterizas, homologándolos a cualquier policía europea.

dispositivos y se requiere continuar el seguimiento en otro estado parte, en la solicitud de continuación del seguimiento deberá constar el uso de este dispositivo durante el seguimiento en ese país. En caso de negarse el uso del dispositivo, éste debería ser apagado y se volvería a conectar cuando se tuviera la constancia que ha regresado al territorio del país de origen.

Si el objetivo de la vigilancia no regresara al país de inicio, y a los solos efectos de retirar el dispositivo, éste podría ser utilizado para ser localizado y retirado. Los dispositivos normativizados de vigilancia y seguimiento que disponen las Fuerzas y Cuerpos de seguridad del Estado permiten la desconexión y posterior conexión del dispositivo, de manera que toda señal de posicionamiento del aparato queda reflejada en las evidencias generadas.

El uso de dispositivos de geolocalización acoplados a vehículos, el procesamiento y el uso de los datos obtenidos, supone una vulneración de la vida privada de las personas y, como tal, debe estar prevista por ley²³⁴. Por lo tanto, si la legislación del territorio al que ha accedido el vehículo monitorizado no autoriza explícitamente el uso de estos dispositivos, no podrían utilizarse.

234 STEDH de 28 de marzo de 2014. Caso Ben Faiza c. Francia.

El CAAS aboga también por el uso de la *entrega vigilada*²³⁵, que consiste en que las autoridades policiales y judiciales permitan que ciertas partidas de sustancias ilícitas, así como los equipos de procesamiento o los precursores químicos, puedan circular por el territorio de un estado bajo la vigilancia de la autoridad o sus agentes del país por donde circula, con la finalidad de descubrir la identidad de las personas que participan en la comisión del delito. La decisión de permitir la entrega corresponde a las autoridades de cada país²³⁶ y debe ser llevada a cabo de acuerdo con el derecho interno de cada estado por el que circule la partida en cuestión, el cual tendrá el control de la operación²³⁷. Los estados miembros deben permitir en sus territorios esta diligencia en el marco de una investigación penal respecto de delitos que puedan dar lugar a la extradición.

235 Puede ser considerada una especialización de la vigilancia y es una medida utilizada en la lucha contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas, contemplada en el art. 73 del CAAS, en el apartado del convenio dedicado a la lucha contra el tráfico de estas sustancias.

236 El CAAS ha sido pionero en hacer que se examinen técnicas de investigación poco desarrolladas en algunos de los estados del territorio Schengen, como por ejemplo la Decisión del Comité Ejecutivo de 28 de abril de 1999 relativa a los principios generales en materia de retribución de confidentes y personas infiltradas o los principios generales en materia de retribución de confidentes y personas infiltradas que dictó la Decisión del Grupo Central el 22 de marzo de 1999.

237 Art. 12 del Convenio celebrado por el Consejo de conformidad con el artículo 34 del tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los estados miembros de la unión europea.

- Persecución en caliente.

Como medidas compensatorias a la supresión de controles interiores, el CAAS permite a los agentes de un estado cruzar la frontera y continuar la persecución en el país vecino sin que haya habido una autorización previa²³⁸. Para ello se requiere que los agentes hayan sorprendido a la persona perseguida en la comisión de un delito²³⁹ flagrante, no hayan podido advertir de la entrada en el territorio a causa de la urgencia o dichas autoridades no hayan podido personarse en el lugar para proseguir la persecución. A más tardar en el momento de cruzar la frontera, los agentes actuantes deberán recurrir a las autoridades competentes que podrán solicitar la interrupción de la persecución o hacerse ellos cargo de la misma.

En el caso que las autoridades locales no pudieran actuar con rapidez, los agentes que llevan a cabo la persecución en el país vecino no podrán detener al individuo; están autorizados a retenerlo hasta que llegue la policía competente en el territorio que es la que lo detendrá. Para

²³⁸ La persecución solo puede llevarse a cabo durante unos kilómetros determinados. Las fuerzas policiales españolas pueden adentrarse hasta 10 km en territorio francés y 50 km en territorio portugués.

²³⁹ Art. 41.4 CAAS. Los delitos en los que se puede aplicar son los mismos que en el caso de proseguir la vigilancia con carácter de urgencia. A estos hay que sumarles en caso de fuga a raíz de un accidente con resultado de muerte o heridas graves.

ello podrán realizar un registro de seguridad al sospechoso y retirarle los objetos de interés, pudiéndole poner las esposas para su traslado delante de las autoridades competentes.

Realmente no existe una clara diferencia entre una retención o la detención de un individuo. En este caso la diferencia se hace menor ya que a los agentes extranjeros se les permite poner las esposas, cachear y trasladar de lugar al sospechoso, todo ello con la finalidad de ponerlo a disposición de las autoridades locales. Los agentes habilitados en el estado español para llevar a cabo estas acciones son también funcionarios del Cuerpo Nacional de Policía, de la Guardia Civil y de la Administración de Aduanas²⁴⁰.

- Registro de huéspedes²⁴¹ -

El CAAS crea un registro de huéspedes en el seno de cada país firmante. Los establecimientos de hospedaje deben pedir a sus huéspedes que cumplimenten y firmen las fichas de declaración en las que deben justificar su identidad. Si viajan en familia o en grupo de viaje solo será necesario registrar una persona. Las fichas o los datos que contienen

²⁴⁰ Desde el 1 de julio de 2020, la Ertzaintza y el Cos de Mossos d'Esquadra están autorizados a cruzar las fronteras en estos casos. No se contempla que esta función pueda ser asumida por las Policías Locales de los municipios fronterizos.

²⁴¹ Art. 45 CAAS.

serán transmitidas a las autoridades policiales que las utilizarán para (1) prevenir peligros, (2) perseguir delitos o (3) averiguar el paradero de personas desaparecidas o víctimas de accidentes.

En la legislación española este registro viene regulado por la LO 4/2015 de 30 de marzo de protección de la seguridad ciudadana, y que trata el hospedaje como una actividad relevante para la seguridad ciudadana, como lo son también el transporte de personas, comercio o reparación de objetos usados, compraventa de joyas y metales o la venta de productos químicos peligrosos a particulares, por citar algunas.

Este fichero es muy útil para las tareas de investigación policial, pero es muy fácil sortearlo. Solo está obligado a identificarse una persona por habitación, de manera que si se viaja en grupo o en familia, la persona de interés podría no quedar registrada en la base de datos.

- Información espontánea²⁴².

Una de las partes, respetando su legislación nacional, podrá comunicar a otra, sin que ésta lo solicite, información que

242 Art. 46 CAAS.

crea importante para ayudar a reprimir o prevenir infracciones o peligros para el orden o la seguridad pública.

La vía normal de comunicación será a través de las oficinas SIRENE aunque, en caso de urgencia, la comunicación podrá efectuarse directamente a las autoridades de policía interesadas, sin obviar la comunicación a las oficinas SIRENE.

Información de este tipo puede ser intercambiada directamente también, fuera de los canales de comunicación establecidos por CAAS. Si la información hace referencia a infracciones penales o a sanciones administrativas recurribles a las autoridades judiciales, ésta puede ser transmitida sin que haya habido una solicitud previa²⁴³.

- Sistema de información de SCHENGEN (SIS).

Se trata de un sistema de información común que permite a las autoridades responsables de los estados integrantes del espacio Schengen intercambiar datos sobre determinadas categorías. Consta de una parte nacional en cada estado miembro (N-SIS) y una unidad de apoyo técnico, situada en Estrasburgo (C-SIS). Los estados miembros suministran

²⁴³ Art. 7 Convenio relativo a la asistencia judicial en materia penal entre los estados miembros de la Unión Europea.

datos al sistema a través de las redes nacionales N-SIS conectadas al sistema central C-SIS. La información no será transferida a ningún sistema informático para su consulta ni se descargará parte de ella.

El SIS fue creado de conformidad con lo dispuesto en el título IV del CAAS²⁴⁴, pero con vistas a la ampliación de la Unión Europea y *“aprovechar los últimos progresos en el ámbito de las tecnologías de la información y permitir la introducción de nuevas utilidades”*, en el año 2001²⁴⁵ se inició el desarrollo de una segunda generación, el SIS II. Posteriormente²⁴⁶, determinados operadores – entre los que había Europol y Eurojust – acordaron mejoras en la búsqueda de datos, modificando la información a introducir y la creación de las oficinas SIRENE²⁴⁷.

244 Las conclusiones del Consejo Europeo de Laeken de 14 y 15 de diciembre de 2001, y en particular los puntos 17 (cooperación entre servicios especializados en la lucha contra el terrorismo) y 43 (Eurojust y cooperación policial en el marco de Europol), así como el plan de acción de 21 de septiembre de 2001 contra el terrorismo, hacen referencia a la necesidad de ampliar el SIS y mejorar su capacidades.

245 Reglamento (CE) 2424/2001 del Consejo de 6 de diciembre de 2001 sobre el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II).

246 Decisión 2005/211/JAI del Consejo de 24 de febrero de 2005 relativa a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo.

247 El CAAS no incluyó inicialmente las oficinas SIRENE (Supplementary Information Request at the National Entry). La Decisión 2005/211/JAI del Consejo añadió el punto 4 al artículo 92 del CAAS.

SIS II.

En la actualidad, el SIS II tiene su base jurídica en el Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo de 28 de noviembre de 2018²⁴⁸, en lo que respecta a la cooperación judicial en materia penal y cooperación judicial, y en el Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo de 28 de noviembre de 2018²⁴⁹ en lo que respecta a políticas sobre controles en las fronteras, asilo e inmigración.

En esta base de datos se introducen señalamientos de personas y objetos que, en caso de ser localizados, debe emprenderse una acción determinada solicitada por el estado que emite el requerimiento, que asumirá la responsabilidad de la información contenida en el sistema central respecto de su N-SIS II. Así, al introducir el nombre de una persona o el número de bastidor de un vehículo, por ejemplo, y obtener un *“hit”*, se llevará a cabo una determinada acción sobre ellos,

248 Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo de 28 de noviembre de 2018 relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n° 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión.

249 Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el CAAS y se modifica y deroga el Reglamento (CE) n° 1987/2006.

como puede ser una detención de la persona o la aprehensión del vehículo en cuestión.

En el sistema se pueden introducir dos categorías de datos, de los cuales se hará constar la siguiente información:

Personas: Como mínimo se deberá informar del apellido, fecha de nacimiento, conducta a observar y motivo de la inscripción, pero pueden añadirse más datos que ayuden a identificar al sujeto²⁵⁰. Así se pueden introducir elementos de identificación biométrica en las descripciones como por ejemplo huellas dactilares y palmares, como también de imágenes faciales y perfiles de ADN, haciendo uso de las disposiciones del tratado de Prüm sobre el acceso mutuo transfronterizo en línea a las bases de datos nacionales.

En cuanto al motivo de la inscripción, se debe añadir información relativa a la autoridad informadora, las posibles conexiones con otras descripciones introducidas en el SIS II y el tipo de delito.

Los señalamientos hacen referencia a personas buscadas a efectos de entrega, al amparo de una Orden de Detención Europea²⁵¹, personas desaparecidas que deban ser puestas

²⁵⁰ Art. 22 Reglamento (UE) 2018/1862.

²⁵¹ Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre

bajo protección (para su propia protección o prevenir amenazas) o que se haya de determinar su paradero (adultos o menores)²⁵², con requerimientos en procedimientos judiciales, investigadas, víctimas o testigos de los que es necesario averiguar su domicilio²⁵³. Pueden darse de alta también señalamientos de personas no admisibles en un estado miembro²⁵⁴.

Objetos: El sistema diferencia distintas categorías de objetos: vehículos a motor, embarcaciones y aeronaves; remolques, caravanas, contenedores, motores fuera borda, equipos industriales; armas de fuego; documentos oficiales (vírgenes o no), certificados y placas de matrícula o valores mobiliarios y medios de pago que hayan sido robados, sustraídos, extraviados o anulados; billetes de banco.

El motivo del señalamiento es la localización del objeto para incautarlo o usarlo como prueba en el proceso penal²⁵⁵; la

Estados miembros.

La **orden de detención europea (ODE)** es un procedimiento judicial simplificado y transfronterizo de entrega a efectos de enjuiciamiento o de ejecución de una pena o de una medida de seguridad privativas de libertad. Las órdenes de detención europeas emitidas por las autoridades judiciales de cualquier país de la UE son válidas en todo el territorio de la Unión Europea. La orden de detención europea viene funcionando desde el 1 de enero de 2004. Ha sustituido a los dilatados procedimientos de extradición que solían existir entre países de la UE y al que hacía referencia el SIS.

252 Capítulo VII del Reglamento (UE) 2018/1862.

253 Capítulo XIV del Reglamento (UE) 2018/1862.

254 Art. 24 del CAAS.

255 Art. 38 del Reglamento (UE) 2018/1862.

autoridad que lo localice, se pondrá en contacto con la autoridad emisora del señalamiento para decidir sobre las medidas a adoptar.

A las personas y a los objetos se les podrá dar de alta un **control específico**²⁵⁶ o una **vigilancia discreta**²⁵⁷. La actuación que se requiere es que en caso de localización en un control policial, se transmita información relativa al lugar en el que se localiza, personas y objetos con los que se desplaza, los itinerarios y los destinos de viaje, las personas que acompañan al sujeto o los ocupantes del vehículo y las circunstancias en las cuales hayan sido encontrados el sujeto o el vehículo. Los señalamientos se conservaran el tiempo estrictamente necesario, debiéndose revisar periódicamente en función del motivo de su introducción en el sistema.

Los datos pueden ser consultados por las autoridades competentes en controles fronterizos y en las

256 Art. 99.5 del CAAS. **Control específico:** las personas, vehículos y objetos podrán ser registrados con arreglo al Derecho nacional. Si la ley de ese estado no lo permite el control específico se convertirá automáticamente, para dicha parte contratante, en vigilancia discreta.

257 Art. 99.4 del CAAS. **Vigilancia discreta o control discreto:** Los agentes de policía pueden recoger y transmitir información relativa a la persona o el vehículo hayan sido encontrados, al lugar, el momento o el motivo de la verificación; al itinerario y destino del viaje; a las personas que acompañan al interesado o los ocupantes, al vehículo utilizado, a los objetos transportados, y sobre las circunstancias en las que los hayan encontrado. Todo ello de manera discreta.

comprobaciones policiales y aduaneras realizadas dentro del país.

Europol y Eurojust tienen derecho a acceder a los datos contenidos en el SIS II. En caso de obtener un “*hit*”, lo deben comunicar al estado emisor del señalamiento. En lo que se refiere a Eurojust, solo tendrán acceso los miembros nacionales y sus asistentes²⁵⁸.

El sistema N-SIS II en España se encuentra en la Secretaría de Estado de Seguridad del Ministerio del Interior y tienen acceso: Dirección General de la Policía, Dirección General de la Policía de la Guardia Civil, Servicio de Vigilancia Aduanera, Asuntos Consulares, Policías Autonómicas y Policías Locales, Dirección General de Tráfico, Jueces y Magistrados²⁵⁹.

Oficinas SIRENE.

La base de datos nacional **N-SIS** se crea a cuenta y riesgo de la parte nacional del SIS de cada estado miembro e incluye una oficina **SIRENE** que está abierta las 24 h de los 365 días del año. Estas oficinas son organismos de

258 Art.48 y 49 del Reglamento (UE) 2018/1862.

259 Orden INT/2287/2014, de 25 de noviembre, por la que se modifica la Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior.

cooperación que se encargan del intercambio de información (peticiones y difusiones) entre los estados miembros así como supervisar, complementar y verificar las alertas sobre las diferentes categorías de personas y objetos integrados en el SIS II. Cuando hay una coincidencia, dan respuesta en menos de 12 h.

En el caso español, la oficina SIRENE está integrada en la estructura de la Dirección General de la Policía del Cuerpo Nacional de Policía, dentro de la División de Cooperación Internacional, en las que también están integradas la Oficina Central Nacional de Interpol y la Unidad Nacional de Europol.

Así, los distintos cuerpos policiales del estado español, cada vez que llevan a cabo una consulta en sus respectivas bases de datos, están consultando el contenido de tres bases de datos simultáneamente:

1.- La base de datos propia de cada cuerpo policial.

2.- Una base de datos común a todos ellos, la denominada **Base de Datos de Señalamientos Policiales (BDSN)** en los que se dan de alta los señalamientos policiales y judiciales a nivel nacional. Los distintos cuerpos dan de alta los requerimientos policiales que consideran oportuno. Por su parte, la autoridad judicial envía sus propias solicitudes de

alta de requerimientos judiciales a las distintas policías – normalmente la que lleva la investigación sobre los hechos – las cuales insertan el señalamiento judicial en la BDSN.

3.- La **base de datos SIS II**, en las que están registrados los señalamientos de las distintas policías europeas.

Cada estado designará a una autoridad que, respetando el derecho nacional, se encargue de ejercer un control independiente sobre el fichero de la parte nacional del SIS II y comprobara que el tratamiento y la utilización de los datos no atentan contra los derechos de los ciudadanos. A su vez, se crea una Autoridad de Control Común (ACC) encargada del control de la unidad de apoyo técnico del SIS que vela por la correcta ejecución del sistema²⁶⁰.

En el estado español, la Agencia Española de Protección de Datos ejerce el control sobre el SIS y su director nombra los representantes españoles en la ACC²⁶¹.

260 Art. 114 y 115 del CAAS.

261 Art. 7 del Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

3.2.- Consejo Europeo de Tampere²⁶².

Los días 15 y 16 de octubre de 1999 se celebró en Tampere (Finlandia) una sesión especial del Consejo Europeo donde se adoptaron una serie de orientaciones y prioridades políticas en aras de convertir la Unión Europea en un espacio de libertad, seguridad y justicia. Esto requería reforzar la lucha contra la delincuencia organizada y transnacional grave de manera que los delincuentes no pudieran aprovecharse de las diferencias existentes entre los sistemas judiciales de los estados miembros.

Así, en este Consejo se promovió la aplicación de una serie de directrices políticas y objetivos concretos. Entre ellos estuvo reforzar el papel de **Europol** y crear **Eurojust**, una unidad integrada por fiscales, magistrados y agentes de policía de competencia equivalente, cedidos temporalmente por cada estado miembro y que deberían coordinar las fiscalías nacionales, colaborar con la red judicial europea y apoyar las investigaciones penales en los casos de delincuencia organizada²⁶³.

Insta a que las autoridades nacionales se centren en la lucha de sectores que se consideran de especial importancia, tales

²⁶² http://www.europarl.europa.eu/summits/tam_es.htm#c (última consulta 14/03/2022).

²⁶³ Párrafos 45 y 46 del Consejo Europeo de Tampere.

como la delincuencia financiera (blanqueo de capitales, corrupción, falsificación del euro), el tráfico de drogas, la trata de seres humanos, la delincuencia de alta tecnología, el delito ecológico y la delincuencia económica grave.

En cuanto a la cooperación policial se refiere, se articularon una serie de mecanismos para sacar el máximo provecho de la cooperación entre las autoridades de los estados miembros al investigar la delincuencia transfronteriza en cualquier estado miembro. Estos mecanismos se desarrollaron durante la siguiente década.

3.2.1.- Prevención de la delincuencia en la UE (párrafo 42).

Debe desarrollarse el intercambio de mejores prácticas entre los estados de la Unión, reforzar la red de autoridades nacionales competentes en materia de prevención del delito, la cooperación entre los organismos nacionales competentes, siendo las principales prioridades la delincuencia juvenil, la urbana y la relacionada con las drogas.

3.2.2.- Equipos conjuntos de investigación²⁶⁴ - ECI - (párrafo 43).

En el Tratado de Amsterdam ya se instaba a Europol a facilitar, apoyar y estimular la coordinación y ejecución de acciones específicas de investigación entre sus miembros. Entre éstas estaba la creación de **equipos conjuntos de investigación - ECI** - que incluyan representantes de Europol²⁶⁵. Más adelante, en el Consejo Europeo de Tampere, se hizo un llamamiento para que se hiciera efectiva esta creación²⁶⁶.

Los **ECI** se crean oficialmente en el Tratado de Lisboa²⁶⁷, instando a Europol a realizar funciones de coordinación, organización y para que se lleven a cabo investigaciones y actividades operativas²⁶⁸.

264 Inicialmente fueron regulados por la Decisión Marco 2002/465/JAI del Consejo, de 13 de junio de 2002, sobre equipos conjuntos de investigación, hasta que entró en vigor el Convenio celebrado por el Consejo de conformidad con el artículo 34 del tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los estados miembros de la unión europea.

España firmó el Convenio en 29/05/2000 y entró en vigor el 23/08/2005.

265 Art. K2.2 del Tratado de Amsterdam.

266 Se veía como una herramienta efectiva para la lucha contra el tráfico de drogas, la trata de seres humanos y la lucha contra el terrorismo. Párrafo 43 del las Conclusiones de la Presidencia del Consejo de Tampere celebrado el 15 y 16 de Octubre de 1999.

267 Art. 69.g del Tratado de Lisboa.

268 Art. 88.2.b del TFUE.

La creación de los ECI están regulados por el *Convenio relativo a la asistencia judicial en materia penal entre los estados miembros de la Unión Europea* - del cual se habla en el siguiente punto - y serán creados por las autoridades competentes con un fin y período de tiempo determinados para llevar a cabo investigaciones penales en uno o más de los estados miembros que formen el equipo²⁶⁹. Se formarán en investigaciones difíciles y complejas, que requieran muchos medios a la vez que afectan a varios estados miembros o cuando sea necesaria una coordinación concertada y coordinadas entre los distintos países integrantes.

Será dirigido por una autoridad competente de un estado miembro del ECI bajo la legislación del país en el que se hallen, permitiendo que actúen los agentes de otros estados que sean integrantes del ECI. De esta manera, policías de varios países que trabajen en el mismo ECI, podrán actuar como si estuvieran bajo una misma jurisdicción y podrán compartir la información entre los miembros del equipo conjunto de conformidad al derecho interno del país de cada miembro, dentro de los límites de las competencias atribuidas. La información que intercambian los distintos integrantes del ECI podrá ser utilizada (1) para la finalidad

²⁶⁹ Art. 13 Convenio relativo a la asistencia judicial en materia penal.

para la que fue creado el ECI, (2) para otras investigaciones penales si el estado del que proviene la información lo autoriza, (3) para evitar una amenaza grave e inmediata para la seguridad pública y (4) para otros fines, si se acuerda en el momento de creación del ECI²⁷⁰.

En el caso del estado español, se considera la autoridad competente a la Audiencia Nacional, cuando la investigación recaiga sobre los delitos cuyo enjuiciamiento corresponda a dicho órgano jurisdiccional y el Ministerio de Justicia en el resto de casos, siempre que participen en el ECI miembros de las carreras judicial o fiscal. Cuando no participen lo será el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad. En este segundo caso, significa que los ECI estarán integrados por miembros de la Guardia Civil y/o del Cuerpo Nacional de Policía y, si se considera necesario, se podrá compartir información con los Cuerpos de Policía Autonómicos²⁷¹.

270 El art. 5.h de la Ley 11/2003, de 21 de mayo, que regula los equipos conjuntos de investigación penal en el ámbito de la Unión Europea - RCL 2003\1341 – estipula que en el acuerdo de constitución del ECI se debe reflejar el régimen de la información obtenida durante la investigación.

271 Disposición adicional tercera de la Ley 11/2003, de 21 de mayo, que regula los equipos conjuntos de investigación penal en el ámbito de la Unión Europea.

3.2.3.- Unidad operativa europea de jefes de policía - European Chief of Police Task Force (párrafo 44).

Su objeto es intercambiar, en cooperación con Europol, experiencia, mejores prácticas e información sobre las tendencias de la delincuencia transfronteriza, así como de contribuir a la planificación de acciones operativas.

La primera reunión tuvo lugar los días 7 y 8 de abril de 2000 en Lisboa, bajo el nombre de "*Informal meeting of Chief Police Officers*". Inicialmente se trataba de reuniones de debate de altos funcionarios policiales, pero no tenía base legal ni formaba parte de ningún órgano del Consejo. Aún así, en los años siguientes, se llevaron a cabo diversas operaciones propiamente dichas, algunas de las cuales fueron muy exitosas²⁷².

Los Jefes de Policía han creado los **COSPOL**²⁷³ que son equipos de trabajo multinacionales formados para llevar a cabo una investigación concreta y que está dirigido por un país afectado directamente por esa problemática que a la vez es el responsable de dirigir las operaciones.

²⁷² En mayo de 2005 se llevó a cabo una operación a nivel de toda la UE contra la pornografía infantil en la que participaron cientos de policías de Suecia, el Reino Unido, Dinamarca, Francia, los Países Bajos, Malta, Noruega y Polonia. BRADY (2007).

²⁷³ Comprehensive Operational Strategic Planning for the Police.

Un ejemplo de ello fue el proyecto **CIRCAMP**²⁷⁴, monitorizado por la policía de Dinamarca, dirigido a la lucha contra la distribución o posesión de material pornográfico infantil y que se llevó a cabo en 22 países, efectuándose más de 100 detenidos²⁷⁵. Otros grupos creados han sido para luchar contra el terrorismo, tráfico de drogas sintéticas, cocaína, heroína o inmigración ilegal, por citar algunos.

3.2.4.- Academia Europea de Policía (párrafo 47).

Establece la **Academia Europea de Policía - CEPOL** ²⁷⁶ para la formación de funcionarios policiales de rango superior, abierta a las autoridades de los países candidatos. Se convino que la Escuela empezaría como una red de centros nacionales de formación de los funcionarios policiales de rango superior ya existentes, sin excluir la creación ulterior de una institución permanente y que servirían de base. En 2005 se instauró la sede en Bramshill (Reino Unido)²⁷⁷. Desde el 1 de julio de 2016, la CEPOL ha pasado a denominarse oficialmente **«Agencia de la Unión**

²⁷⁴ COSPOL Internet Related Child Abuse Material Project, del que formaban parte Noruega, UK, Bélgica, Dinamarca, Estonia, Finlandia, Francia, Irlanda, Italia, Letonia, Malta, Holanda, Polonia e Interpol.

²⁷⁵ <https://www.europol.europa.eu/newsroom/news/joint-action-in-22-european-countries-against-online-child-sexual-abuse-material-in-internet> (última consulta 14/03/2022).

²⁷⁶ Se estableció en virtud de la Decisión 2000/820/JAI, de 22 de diciembre de 2000.

²⁷⁷ Art. 4 de la Decisión 2005/681/JAI, de 20 de septiembre que anuló la Decisión 2000/820/JAI.

Europea para la Formación Policial»²⁷⁸ y ha trasladado su sede a Budapest (Hungria).

Ha dejado de ser una escuela de formación de funcionarios de rango superior, para llevar a cabo actividades de formación destinadas a las autoridades con funciones policiales de los estados miembros.

En el estado español, la Secretaria de Estado de Seguridad actúa como Unidad Nacional de la Agencia²⁷⁹.

3.3.- El Convenio relativo a la asistencia judicial en materia penal entre los estados miembros de la Unión Europea – en adelante Convenio de asistencia mutua de 2000 - .

En 1959 se firma en Estrasburgo el **Convenio Europeo de Asistencia Judicial en materia penal** en el que los países firmantes – miembros del Consejo de Europa - se comprometen a prestarse mutuamente una amplia asistencia judicial en los procedimientos relativos a infracciones cuya represión sea de la competencia de las autoridades judiciales

²⁷⁸ Reglamento nº 2015/2219 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015.

²⁷⁹ Real Decreto 146/2021, de 9 de marzo, por el que se modifican el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, y el Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

de la parte requirente. Un procedimiento a seguir será a través de *Comisiones Rogatorias* en el caso de realizar actuaciones de instrucción o transmitir piezas probatorias, expedientes o documentos. También regula la notificación de documentos procesales y resoluciones judiciales, comparecencia de testigos, peritos y procesados.

En el estado español²⁸⁰ se consideran autoridades judiciales las estrictamente judiciales²⁸¹. En cambio en Dinamarca, Noruega o Suiza, por citar algunos, se incluyen a altos mandos policiales.

El Convenio de asistencia mutua de 2000²⁸² - celebrado por el Consejo de la Unión Europea - firmado en Bruselas el 29 de mayo de 2000 - viene a complementar el anterior del Consejo de Europa y tiene como principal objetivo reforzar y agilizar la cooperación entre los estados miembros de la Unión Europea. Posteriormente, en 2001 el Consejo adoptó un Protocolo Adicional al Convenio dirigido,

280 Modificación de la Declaración de España relativa al artículo 24 del Convenio Europeo de asistencia judicial en materia penal, hecho en Estrasburgo el 20-4-1959 (RCL 1982\2423).

281 Los Jueces y Tribunales de la jurisdicción ordinaria; los Secretarios Judiciales; los miembros del Ministerio Fiscal; las autoridades judiciales militares; los Jueces Togados y Tribunales militares y los Secretarios Relatores de la Jurisdicción Militar.

282 Convenio celebrado por el Consejo, de conformidad con el artículo 34 del Tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los estados miembros de la Unión Europea, hecho en Bruselas el 29-5-2000.

fundamentalmente, a la lucha contra el blanqueo y la corrupción.

Como ya hemos visto en apartados anteriores, en él se tratan solicitudes de determinadas formas específicas de asistencia judicial. Se regulan las entregas vigiladas, los equipos conjuntos de investigación, las investigaciones encubiertas o el traslado temporal de detenidos para fines de investigación.

3.3.1.- Intervención de las telecomunicaciones²⁸³.

El Tribunal Europeo de Derechos Humanos considera que las comunicaciones telefónicas, postales y, por extensión las telemáticas, están comprendidas en las expresiones de “*vida privada*” y de “*correspondencia*” recogidas en el art. 8.1²⁸⁴ del Convenio Europeo de Derechos Humanos.

En el *Convenio de asistencia mutua de 2000* se regula a nivel internacional esta importante herramienta de investigación²⁸⁵. Una autoridad competente del estado miembro requirente podrá cursar a otra autoridad competente

²⁸³ La intervención de las telecomunicaciones están también reguladas en el Capítulo V de la Directiva 2014/41/UE, de 3 de abril, relativa a la Orden Europea de Investigación (OEI) en materia penal, en el que se hace hincapié en los aspectos relativos al auxilio técnico de otros estados miembros y las notificaciones que deben llevarse a acabo en estados donde se encuentre la persona, pero de los que no se necesita el apoyo técnico.

²⁸⁴ STEDH de 6 de septiembre de 1978. Caso Klass y otros c. Alemania, párrafo 41.

²⁸⁵ Título III del Convenio de asistencia mutua de 2000.

del estado miembro requerido una solicitud de intervención, grabación y ulterior transmisión de la grabación de la telecomunicación al estado miembro requirente. La solicitud que se le haga al estado requerido deberá incluir un resumen de los hechos, de manera que le permita decidir si él mismo habría adoptado la medida solicitada en un caso nacional de características similares.

Si no se requiere la ayuda técnica del estado de donde se encuentra el sujeto en cuestión, el estado que lleva a cabo la intervención debe informar al estado donde se encuentra el sujeto que se está llevando a cabo dicha intervención. La información debería llevarse a cabo antes que el sujeto llegue al nuevo país y, si no es posible, en cuanto se tenga conocimiento de su llegada. El estado requerido podrá autorizar que prosiga la intervención o pedir el cese de la misma²⁸⁶.

3.3.2.- Uso de los datos obtenidos en las investigaciones²⁸⁷.

Los datos de carácter personal obtenidos a partir de las investigaciones llevadas a cabo en el marco del *Convenio de*

²⁸⁶ A no ser que haya acuerdo entre los estados de utilizar dicha información. (Art. 20).

²⁸⁷ Art. 23 del Convenio relativo a la asistencia judicial en materia penal entre los estados miembros de la Unión Europea.

asistencia mutua de 2000 podrán ser utilizados por el estado miembro al que se hayan transmitido para que sean utilizados en los procedimientos judiciales y administrativos relativos a dichas investigaciones. También podrán ser utilizados para otras finalidades si el estado transmisor lo autoriza – pudiendo auditar el uso que se ha hecho de los datos transmitidos - o el propietario de los datos da su consentimiento. En todo caso, se refiere a los datos transmitidos de un estado a otro estado, no a los datos que se han obtenido en el propio estado y no es necesaria su transmisión.

3.4.- Tratado de PRÜM

Optando por utilizar mecanismos que están fuera del Derecho Comunitario²⁸⁸, siete estados miembros de la Unión Europea firmaron el ***Tratado de Prüm***²⁸⁹ en la ciudad que lleva el mismo nombre el 27 de mayo de 2005. Como se creó

288 El Derecho Comunitario prevé la denominada “**cooperación reforzada**”, procedimiento permite que un número mínimo países de la UE - actualmente son 9 - establecer una integración o cooperación avanzada en un ámbito de las estructuras europeas sin la participación de los demás países de la UE.

El TFUE permite que para instar medidas encaminadas a la cooperación policial entre estados se utilice este procedimiento, cuyo proceso se contempla en el art. 329 i ss. del TFUE.

289 El nombre completo es *Tratado entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal.*

al margen del marco institucional de la Unión Europea, este tratado fue muy criticado²⁹⁰ - algún autor lo ha definido como un tratado de origen “*bastardo*”²⁹¹-. Entre sus críticos se hallaba el Supervisor Europeo de Protección de Datos²⁹².

Tiene la finalidad de reforzar la cooperación transfronteriza y en particular el intercambio de información entre las partes firmantes, que se lleva a cabo aplicando el **Principio de Disponibilidad**, según el cual *"el agente de los servicios de seguridad de un estado miembro de la Unión que necesite información para llevar a cabo sus funciones debe poder obtenerla de otro estado miembro, y que las autoridades de los servicios de seguridad del estado miembro que tenga dicha información deben ponerla a su disposición para el fin declarado, teniendo en cuenta las necesidades de las investigaciones pendientes en dicho estado miembro"*²⁹³.

La primera parte del Tratado hace referencia al acceso a la información que deben contener las bases de datos de ADN no codificante y a las de datos dactiloscópicos que los países

290 “*El Tratado de Prüm se negoció y se adoptó de una forma muy poco transparente y sin un control democrático serio (los parlamentos nacionales sólo participan en el proceso de ratificación y el Parlamento Europeo sólo participa actualmente a través de una consulta sobre el proyecto de Decisión del Consejo)*”; fragmento extraído de la Comisión de Libertades Civiles Justicia y Asuntos de Interior 2007.

291 MARTÍNEZ PÉREZ y POZA CISNEROS (2013).

292 El Dictamen se publicó en el DOUE serie C 116, de 17.5.2006.

293 Considerado 4 de la Decisión JAI/615/2008 de 23 de junio de 2008.

contratantes se obligan a crear. Pero el intercambio de información, por lo que respecta a las bases de datos de ADN solo podrá realizarse para investigar delitos; en cambio, la búsqueda de coincidencias dactilares entre las bases de datos podrá llevarse a cabo en caso de prevención y persecución de delitos. El intercambio de información se realiza a través de *puntos de contacto nacionales* designados por las partes contratantes que se regirán por la ley nacional aplicable de cada país.

El Tratado también permite el intercambio de datos de registro de matriculación de vehículos en caso de prevención y persecución de delitos, perseguir infracciones de competencia judicial/fiscal y para prevenir amenazas contra la seguridad o el orden público y la transmisión de información de datos no personales - tanto a petición como por iniciativa propia - en caso de grandes eventos de alcance transfronterizo, especialmente en actos deportivos. En caso que se presuma que una persona pueda cometer un delito o que pueda ser una amenaza, relacionado con el evento, se podrán facilitar sus datos al estado en cuestión. En caso de terrorismo y para casos concretos, también se autoriza la transmisión de informaciones y de datos personales.

El Tratado también establece otras formas de cooperación policial. Así, permite la formación de patrullas conjuntas²⁹⁴ entre agentes de las partes contratantes con el objeto de prevenir delitos, amenazas para la seguridad y el orden público, además de crear los "air marshals"²⁹⁵. Atribuye a agentes de países contratantes facultades para actuar en territorios que forman parte del Tratado bajo la condición que debe llevarse a cabo en presencia de agentes del estado del territorio en cuestión. En caso de urgente necesidad, también pueden cruzar fronteras sin requerir la autorización previa de dicho estado²⁹⁶ al que se le debe notificar dicho cruce. Para prevenir e investigar delitos, las partes contratantes permiten prestar asistencia recíproca previa petición y en el marco de sus respectivas competencias.

El capítulo VII está dedicado a la protección de datos personales, consciente "*en particular de que la transmisión de datos de carácter personal a otra parte Contratante requiere que en la parte Contratante receptora se garantice un nivel adecuado de protección de datos*"²⁹⁷ la cual, como mínimo, debe ser equivalente a la que proporciona el Convenio 108 sobre Protección de Datos y el Protocolo

294 Art. 24 Tratado de Prüm.

295 Art. 17 Tratado de Prüm: Escoltas de seguridad en los vuelos.

296 Art. 25 Tratado de Prüm.

297 Considerandos del Tratado de Prüm

Adicional de 8 de noviembre de 2001²⁹⁸ y que se atenga a la Recomendación n.º R (87) 15. Los estados firmantes deben velar por la exactitud, la actualidad y el borrado de los datos cuando dejen de ser necesarios o hayan transcurrido los plazos máximos establecidos en el derecho nacional del estado transmitente.

En el Consejo de Justicia y Asuntos de Interior del 15 de febrero de 2007 se acordó integrar partes del Tratado de Prüm en el ordenamiento jurídico de la UE que se llevó a cabo con la promulgación de la **Decisión JAI/615/2008** y la **Decisión JAI/616/2008**. Entre la parte integrada se encuentra la relativa a los perfiles de ADN, las bases de datos dactiloscópicas, registros de matriculación de vehículos, acontecimientos importantes, medidas de prevención de atentados terroristas y otras formas de cooperación entre estados. También incluye una declaración de respeto a los derechos fundamentales²⁹⁹ y a la protección de datos³⁰⁰.

298 Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001.

299 Considerado 22 de la Decisión JAI/615/2008 de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

300 Capítulo VI de la Decisión JAI/615/2008 de 23 de junio de 2008.

3.5.- Tratado de la UNION EUROPEA (TUE) y Tratado de Funcionamiento de la UNIÓN EUROPEA (TFUE).

El objetivo de la Unión Europea es construir un espacio de libertad, seguridad y justicia, con ausencia de controles sobre las personas en las fronteras interiores y en el que se respeten los derechos fundamentales. Para ello la Unión se esfuerza en la prevención de la delincuencia, del racismo y la xenofobia y debe tomar medidas de coordinación y cooperación entre autoridades policiales y judiciales, a la vez que debe aproximar normas penales y de reconocimiento mutuo de resoluciones judiciales en materia penal de los estados miembros. También permite que los estados miembros, por su parte, puedan adoptar formas de cooperación y coordinación en esta materia entre ellos.

Para mejorar la cooperación policial entre países miembros de la UE, el Parlamento Europeo y el Consejo podrán tomar medidas relativas a:

a) La recogida, almacenamiento, tratamiento, análisis e intercambio de información entre las autoridades competentes de los estados miembros, en los que se incluyen los servicios de policía, de aduanas y otros servicios con funciones coercitivas especializados en la prevención y

en la detección e investigación de infracciones penales. Parte de estas medidas se realizan a través de Europol.

b) el apoyo a la formación, así como la cooperación para el intercambio de personal, los equipos y la investigación científica policial;

c) las técnicas comunes de investigación relacionadas con la detección de formas graves de delincuencia organizada.

Estas medidas deben ser tomadas por unanimidad dentro del Consejo, previa consulta al Parlamento Europeo. Para evitar bloqueos normativos, el TFUE contempla el mecanismo de la **cooperación reforzada**³⁰¹ y del cual la adopción del **Tratado de Prüm** es un ejemplo. Pero no se puede utilizar para legislar sobre materias de competencia exclusiva de la Unión, ni para aumentar competencias, debiendo seguir los pasos que regula el art. 329 y ss. del TFUE.

Los estados Miembros que lo soliciten pueden unirse al mecanismo creado cuando lo deseen.

³⁰¹ Regulado en el Título IV del TUE y en el Título III del TFUE.

3.6.- Decisión Marco 2006/960/JAI³⁰².

Otro de los mecanismos puestos en marcha para mejorar la coordinación policial, fue la instauración del “*principio de disponibilidad*” del cual se ha hablado anteriormente. En el Programa de La Haya, que se adoptó en el Consejo Europeo del 4 y 5 de noviembre de 2004, se recogían las prioridades de la Unión destinadas a reforzar el Espacio de Libertad.

Una primera aproximación a la puesta en marcha de este principio está en la **Decisión Marco 2006/960/JAI³⁰³** donde se establecen “*las normas en virtud de las cuales los servicios de seguridad de los estados miembros puedan intercambiar de forma rápida y eficaz la información e inteligencia disponibles para llevar a cabo investigaciones criminales u operaciones de inteligencia criminal*”³⁰⁴. Éste es un instrumento jurídicamente vinculante que enuncia qué tipo de información es intercambiable, los mecanismos de petición y regula las condiciones y los plazos de entrega de

302 Decisión Marco 2006/960/JAI del Consejo de 18 de diciembre de 2006 sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los estados miembros de la Unión Europea.

303 Fue incorporada al ordenamiento jurídico español a través de la Ley 31/2010 de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los estados miembros de la Unión Europea y la Ley Orgánica 6/2010, de 27 de julio, complementaria de la anterior, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los estados miembros de la Unión Europea.

304 Considerando 8 de la Decisión Marco 2006/960/JAI.

la información. Llama la atención el uso policial de la información facilitada por otro estado, pero no así el uso judicial, ya que se debe pedir el consentimiento de dicho estado para presentar dicha información ante un tribunal.

En 2007, el Supervisor Europeo para la Protección de Datos Peter Hustinx³⁰⁵ ya reconoció que el principio de disponibilidad por si solo no bastaba, que era necesario acompañarlo de medidas legislativas adicionales para que el intercambio entre autoridades judiciales y policiales fueran efectivas. Una parte de estas funciones se llevan a cabo a través de los sistemas de información de Europol, del cual hablaremos más adelante.

³⁰⁵ Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía (Europol), publicado en el Diario Oficial de la Unión Europea el 27/10/2007.

3.7.- Directiva 2016/680 del Parlamento Europeo y del Consejo³⁰⁶.

En esta Directiva se establecen las normas que deben seguir las autoridades competentes en lo que respecta al tratamiento de los datos personales "*con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública*" garantizando a la vez el intercambio de estos datos³⁰⁷.

El apartado que la Directiva dedica a los principios y a los derechos del interesado ya ha sido tratado en el capítulo anterior.

En el capítulo V se trata la transmisión de datos personales a terceros países u organizaciones internacionales en este ámbito. Debe darse entre autoridades públicas competentes en esta materia según el Derecho del estado miembro. Si los datos provienen de un tercer país, es necesario que éste de

³⁰⁶ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

³⁰⁷ Art. 1 y 2 de la Directiva (UE) 2016/680.

la autorización para que sean transmitidos. Si no hay tiempo para obtenerla, a fin de prevenir una amenaza inmediata y grave para la seguridad pública o para los intereses fundamentales de un estado miembro o de un tercer país, se podrían transmitir también los datos personales, debiendo informar a la autoridad responsable de dar la autorización.

La transferencia de datos personales se llevará a cabo dependiendo del tipo de tratamiento que da el ordenamiento jurídico del país receptor a la protección de datos personales. Pueden darse tres supuestos:

1.- La Comisión ha emitido una Decisión de Adecuación³⁰⁸.

La Comisión ha constatado que el ordenamiento jurídico del país receptor ofrece un nivel adecuado de protección a los datos personales, similar al que se da en los países de la Unión Europea. Para ello debe tenerse en cuenta el estado de derecho, el respeto a los derechos humanos, la legislación y jurisprudencia relativa a la protección de datos, la transferencia ulterior a terceros países u organizaciones internacionales y los derechos de que gozan los interesados.

También tendrá en cuenta la existencia de una autoridad

308 Art. 36 de la Directiva (UE) 2016/680.

Países que gozan de esta calificación: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Faroe, Andorra, Israel, Uruguay, Nueva Zelanda, Estados Unidos - entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU -. Fuente: AEPD.

independiente en materia de protección de datos, así como los compromisos internacionales asumidos u otras obligaciones jurídicamente vinculantes del tercer país en relación con la protección de datos.

Una *Decisión de Adecuación* no significa que el tercer país garantice un nivel idéntico de protección de datos personales al que tiene la Unión Europea sino que exige "*que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión*"³⁰⁹.

La Decisión permite la transferencia de datos personales entre estados miembros de la UE con terceros estados sin que tengan que aportar otras garantías ni condiciones. Asimila las transmisiones de datos dentro de la Unión³¹⁰.

2.- Disponer de las garantías apropiadas³¹¹.

Si el tercer estado u organización internacional no dispone de una Decisión de Adecuación emitida por la Comisión, se le podrán transmitir los datos si dispone de las garantías

309 STJUE de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650.

310 [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2017\)7&lang=es](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2017)7&lang=es) (última consulta 14/03/2022).

311 Art. 37 de la Directiva (UE) 2016/680.

apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante o el responsable del tratamiento haya evaluado todas las circunstancias que concurren en la transferencia de datos personales y haya llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales.

En este segundo caso, se deberá informar a la autoridad de control y deberá documentarse la transferencia.

3.- Excepciones³¹².

En caso que el estado u organización internacional no estuviera incluida en ninguno de los dos apartados anteriores, la transferencia de los datos puede llevarse a cabo únicamente en caso de proteger los intereses vitales de personas o los intereses legítimos del interesado - si lo provee el estado miembro que transfiere los datos personales -, para prevenir una amenaza grave e inmediata para la seguridad pública de un estado miembro o de un tercer país o, en casos individuales, para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

³¹² Art. 38 de la Directiva (UE) 2016/680.

La autoridad competente de la transmisión deberá determinar si el interés público de la transferencia prevalece sobre los derechos del interesado. Obviamente la transferencia de datos deberá documentarse y ponerse a disposición de la autoridad de control.

También pueden transferirse directamente datos personales a destinatarios establecidos en terceros países en casos particulares y específicos, siempre que se cumplan las condiciones establecidas en el art. 39 de la Directiva 2016/680.

3.8. - EUROPOL.

Los Tratados de la Unión hacen referencia a la Oficina Europea de Policía - **Europol**³¹³ -, organismo con capacidad jurídica propia en la que los órganos policiales que forman parte pudieran intercambiar información entre ellos. Así, en 1995 se estableció *Convenio de Europol*³¹⁴ que creó el marco legal para la creación de la futura Oficina Europea de Policía, cuya función era la de mejorar la eficacia de los servicios de policía encargados de prevenir y luchar contra el *terrorismo, el tráfico de estupefacientes, de material nuclear y*

313 Art. 88 de la Directiva (UE) 2016/680.

314 Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995.

radioactivo, las redes de inmigración clandestina, la trata de seres humanos y el tráfico de vehículos robados en los que haya indicios de una estructura delictiva organizada y que afecte a dos o más estados miembros. En 2009³¹⁵, se modificó el objetivo de la organización y se hizo una primera ampliación de la lista de delitos sobre los que puede actuar respecto de la pactada en el 1995 incluyendo también los delitos conexos³¹⁶. En 2016 se promulgó el Reglamento (UE) 2016/794³¹⁷ con el que se amplió nuevamente la lista de delitos en los que Europol es competente³¹⁸.

315 Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía (Europol).

316 Anexo II - Tráfico ilícito de estupefacientes, actividades ilícitas de blanqueo de capitales, delitos relacionados con materiales nucleares o sustancias radiactivas, tráfico de inmigrantes clandestinos, trata de seres humanos, delincuencia relacionada con el tráfico de vehículos robados, homicidio voluntario, agresión con lesiones graves, tráfico ilícito de órganos y tejidos humanos, secuestro, retención ilegal y toma de rehenes, racismo y xenofobia, robo organizado, tráfico ilícito de bienes culturales, incluidas las antigüedades y obras de arte, fraude y estafa, chantaje y extorsión, violación de derechos de propiedad industrial y falsificación de mercancías, falsificación de documentos administrativos y tráfico de documentos administrativos falsos, falsificación de moneda, falsificación de medios de pago, delito informático, corrupción, tráfico ilícito de armas, municiones y explosivos, tráfico ilícito de especies animales protegidas, tráfico ilícito de especies y variedades vegetales protegidas, delitos contra el medio ambiente, tráfico ilícito de sustancias hormonales y otros factores de crecimiento.

317 Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo.

318 El anexo II, además de los delitos incluidos en el 2009, añade: robo y hurto con agravantes, delitos contra los intereses financieros de la Unión, operaciones con información privilegiada y manipulación del mercado, la contaminación procedente de buques, abusos sexuales y explotación sexual, incluido el material sobre abuso de menores y la captación de menores con

Europol está formada por agencias de seguridad de corte **militar** – Guardia Civil o Cuerpo de Carabineros de Italia -, de corte **policial** – Cuerpo Nacional de Policía o la Policía Federal de Alemania -, **servicios de inteligencia** – Cuerpo de Finanzas de Italia o Departamento de Policía Financiera de Letonia - y servicios de **protección de fronteras** - Dirección Adjunta de Vigilancia Aduanera española o el Servicio Central de Investigaciones de Aduanas alemán -. Las agencias de seguridad que forman parte de Europol se convierten en emisoras a la vez que receptoras de información, ya que la Oficina es el ente transmisor de la información, que se lleva a cabo a través de las denominadas unidades nacionales, sin perjuicio de los tratados bilaterales que puedan tener los países entre sí. Estas unidades pueden compartir la información con otras unidades a iniciativa propia para que sean utilizadas por las agencias de seguridad de otros países o por la propia Europol, o la compartirán previa solicitud de alguna unidad interesada.

Una de las funciones iniciales de Europol era la de *“facilitar el intercambio de información entre los estados miembros y recoger, compilar y analizar informaciones y datos para ser utilizadas por las agencias de seguridad”*. Estas funciones

finés sexuales, genocidio, crímenes de lesa humanidad y crímenes de guerra.

han sido ampliadas en 2016, de modo que ahora debe *”elaborar evaluaciones de las amenazas, análisis estratégicos y operativos e informes generales de situación”*. Además, se le permite *“participar en equipos conjuntos de investigación, así como proponer su creación”*. Los funcionarios de Europol, recopilan y analizan la información que facilitan los estados miembros, la tratan y la hacen utilizable para sus propias investigaciones y para crear inteligencia que será distribuida al resto de países miembros para hacer frente a actividades terroristas o a organizaciones criminales. En cambio no podrá *“aplicar medidas coercitivas en la realización de sus tareas”*³¹⁹.

Intercambio de información.

Europol tenía capacidad jurídica para firmar convenios con estados terceros con el objetivo de transferir datos a estos países y a organizaciones internacionales para cumplir sus funciones, pero con el Reglamento de 2016 debe ceñirse a lo dispuesto en la Directiva (UE) 2016/680³²⁰.

El intercambio de información entre agencias de seguridad a través de las bases de datos de Europol permite cumplir el **principio de disponibilidad** de manera que la información

319 Art. 4 del Reglamento (UE) 2016/794.

320 Art. 25 del Reglamento (UE) 2016/794.

circula de forma ágil y segura entre los distintos miembros que la forman. La información se almacena en el **Europol Information System (EIS)** y se intercambia a través de la **Secure Information Exchange Network Application (SIENA)**, una plataforma de intercambio rápido de información operativa y estratégica de manera que permite unir funcionarios de enlace, analistas, estados miembros y terceras partes con las que Europol tiene convenio. Desde que empezó a funcionar SIENA, las agencias de seguridad pueden acceder directamente a la información sin necesidad de pasar por la unidad de enlace. A partir de 2010, se ha brindado acceso a SIENA a unidades especializadas como son las unidades de información al pasajero (PIU), unidades de inteligencia (UIF), equipos de búsqueda activa de fugitivos (ENFAST) o unidades de lucha contra el terrorismo³²¹ y a diversos socios con los que coopera³²².

Todos los datos nuevos insertados en el **EIS** se comparan automáticamente con la información existente en él (por ejemplo, nombres, números de teléfono, direcciones de correo electrónico, ADN, armas de fuego, etc.). Además, toda

³²¹ <https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena> (última consulta 14/03/2022).

³²² Eurojust, Interpol, Australia, Canadá, Noruega, Suiza y los Estados Unidos. Puede consultarse en el Informe general sobre las actividades de Europol de 2010. https://www.europol.europa.eu/sites/default/files/documents/es_europolreview.pdf (última consulta 14/03/2022).

la información proporcionada es cotejada automáticamente con los demás repositorios operativos de Europol.

La información está estructurada en códigos que permiten establecer su fiabilidad a la vez que aportan información relativa a la fuente – fiabilidad, veracidad, autenticidad – y a la confiabilidad – si es precisa o si el funcionario la puede corroborar o no -.

Pero Europol no es solamente un mero transmisor de la información; dado que no tiene capacidad ejecutiva en el terreno, con ella hace inteligencia, análisis operativos, informes de situación, análisis de tendencias, informes-evaluación de la amenaza, así como también informes de situación y tendencias. Puede almacenar datos referentes a investigaciones relativas a crímenes de su competencia, como son información sobre los autores o sospechosos, posibles testigos, perjudicados - o que puedan serlo - y acompañantes, incluidos los delitos conexos, así como personas que pueden facilitar información³²³. Estos ficheros deben gozar de un alto nivel de seguridad desde el principio hasta después de finalizar el juicio penal que se produjera con la finalidad de preservar la identidad de las víctimas, testigos o facilitadores de la información, ya que de otra

323 Anexo II del Reglamento (UE) 2016/794.

forma las vidas de dichas personas podrían estar en serio peligro.

Cuando sea estrictamente necesario para la finalidad de los ficheros, se permite el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la afiliación sindical y el tratamiento de datos relacionados con la salud o la vida sexual³²⁴.

En 2020 los Ministros de Interior de la Unión instaron a la Comisión a que revisara el mandato de Europol para mejorar el tratamiento de grandes conjuntos de datos, con la finalidad de reforzar la lucha antiterrorista y el extremismo violento³²⁵. Así, la Comisión Europea tiene previsto ampliar el poder de tratamiento de datos que actualmente posee Europol, motivo por el cual, en diciembre de 2020 se publicó una propuesta de modificación del Reglamento 2016/794 ya que desde su aplicación, las tareas operativas de la agencia han cambiado sustancialmente debido a la constante evolución de la seguridad, con amenazas cambiantes y cada vez más complejas. Por este motivo *“Europol debe disponer de las*

324 Art. 30 del Reglamento (UE) 2016/794.

325 Declaración conjunta de los ministros de Interior de la UE sobre los recientes atentados terroristas en Europa de noviembre de 2020.

<https://www.consilium.europa.eu/es/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/> (última consulta 14/03/2022).

capacidades y herramientas necesarias para apoyar eficazmente a los estados miembros en la lucha contra la delincuencia grave y el terrorismo". Uno de los campos a reforzar será el apoyo que dará Europol a los estados en el análisis de conjuntos de datos grandes y complejos, abordando la dificultad que los macrodatos plantean a las autoridades policiales³²⁶.

Algunos autores afirman que con Europol finalizaron los intercambios informales de información entre las autoridades policiales de los distintos países europeos, ya que se creó una estructura para reglar el intercambio de datos³²⁷. En mi opinión, Europol ha ayudado a crear vínculos personales entre las distintas autoridades policiales creando los canales de comunicación formal, pero la comunicación informal no solo sigue existiendo sino que se ha incrementado, dado que se han incrementado también los contactos personales. Así, cuando la comunicación de datos se establece entre integrantes de distintas agencias investigadoras de manera informal, desaparecen los controles de garantías de los que

326 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación, de fecha 09/12/2020.

<https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0796&from=EN#footnoteref9> (última consulta 14/03/2022).

327 JIMÉNEZ SÁNCHEZ, F. (2015), p. 99.

sí gozan la transmisión de datos formales, con los peligros de menoscabos de derechos fundamentales que ello puede conllevar.

Una muestra de ello se da en los **Equipos Conjuntos de Investigación** de los que se ha hablado anteriormente y que Europol incentiva. Estos se crean con un fin determinado y un periodo de tiempo limitado para llevar a cabo investigaciones penales en uno o más de los estados miembros que hayan creado el equipo³²⁸. Una vez creado el equipo, sus miembros comparten la información de las bases de datos en lo que respecta la finalidad del equipo conjunto, pero también se puede compartir información relativa a otros casos que nada tienen que ver con los del equipo; y esa relación tiende a mantenerse en el tiempo. Cuanta mayor es la información que se comparte, mayor es el tiempo que perdura la relación profesional. Este tipo de trasvase de información carece de cualquier control ya que la información se transmite sin intermediarios y raras veces queda registrada, más allá de quedar almacenado el e-mail en el que se ha transmitido.

³²⁸ Art. 1 de la Decisión Marco 2002/465/JAI del Consejo, de 13 de junio de 2002.

4.- Protección de datos personales versus cesión de datos a las autoridades policiales en España.

4.1.- Legislación aplicable.

La Constitución Española limita “*el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*”³²⁹. Para tal fin se promulgó la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal que fue modificada por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD). Con la entrada en vigor del Reglamento 2016/679 y de la Directiva 2016/680, el parlamento español promulgó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que anuló la anterior.

4.2.- Cesión de datos en investigaciones policiales.

¿Deben las empresas privadas y las Administraciones Públicas ceder a la policía los datos de que disponen legalmente para una finalidad distinta a la que han sido recabados, sin que el propietario de los datos sea conocedor

³²⁹ Art. 18.4 CE

de tal cesión? Según la la *Ley Orgánica 7/2021, de 26 de mayo, que transpone la Directiva 2016/680* al ordenamiento jurídico español, *"las Administraciones públicas, así como cualquier persona física o jurídica, deben proporcionar a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el artículo 549.1 de la Ley Orgánica 6/1985, de 1 de julio y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal"*. El interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora³³⁰.

En cambio, respecto de la cesión de datos por parte de las Administraciones Públicas, habrá que atenerse a lo que dispone la ley de creación de la base de datos en cuestión ya que si hay una norma con rango de ley que habilite la cesión,

³³⁰ Art. 7 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

esta exige del consentimiento del interesado. Así, por ejemplo, la cesión a otra administración de los datos contenidos en la base de datos del padrón de habitantes de un municipio está contemplada en la Ley Reguladora de las Bases de Régimen Local³³¹.

5.- INTERPOL.

Nace en 1914 durante el Primer Congreso Internacional de Policía Criminal celebrado en Mónaco donde tuvieron representación 24 países. Su función es la de conectar las fuerzas policiales de los distintos países que la forman entre sí, facilitando información sobre delitos y delincuentes, así como apoyo técnico de diversa índole.

331 Art. 16.3 de la Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local, redactado conforme a lo establecido en la Ley Orgánica 14/2003, de 20 de noviembre, de 20 de noviembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, dispone que *“los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública”*.

Actualmente está formada por miembros de 194 países³³². La Secretaria general se halla en Lyon y el Complejo Mundial en Singapur. Dispone de siete oficinas regionales³³³ además de representación ante la Unión Africana, la Unión Europea y las Naciones Unidas. Cada país “*designa como Miembro de la Organización a cualquier organismo oficial de policía cuyas funciones están comprendidas en el marco de las actividades de la Organización*”³³⁴.

Interpol dispone de 19 bases de datos propias entre las que destacan las bases de datos con información sobre individuos, huellas dactilares, perfiles genéticos, reconocimiento facial, bienes robados - como pasaportes, vehículos a motor, obras de arte, embarcaciones -, comparación de datos balísticos o armas³³⁵. Los países van alimentando dichas bases de datos de forma voluntaria.

332 Organización Internacional de Policía Criminal. www.interpol.int/Member-countries/World (última consulta 14/03/2022).

Interpol Madrid está integrada por funcionarios de las distintas escalas pertenecientes al Cuerpo Nacional de Policía, expertos en análisis de información, idiomas, derecho y protección de datos de carácter personal. Junto con ellos, en sus oficinas, se encuentran agregados de otros cuerpos policiales, tanto de la Guardia Civil como de las policías autonómicas (Mossos d’Esquadra, Ertzaintza y Policía Foral de Navarra), con objeto de mejorar la coordinación policial interestatal.

333 Argentina, Camerún, Costa de Marfil, El Salvador, Kenia, Tailandia y Zimbabue.

334 Art. 4 del Estatuto de la organización internacional de policía criminal – Interpol aprobado por la Asamblea General de la Organización en su 25ª reunión (1956 - Viena).

335 Pueden consultarse en <https://www.interpol.int/es/Como-trabajamos/Bases-de-datos/Nuestras-19-bases-de-datos> (última consulta 14/03/2022).

Tratamiento de datos en INTERPOL.

En 1974 la Asamblea General aprobó la Resolución núm. AGN/43/RES/1 sobre el “*Carácter confidencial de la información*” en el que se pide insistentemente “*que al intercambiar informaciones las OCN y la Secretaria General tengan en cuenta el respeto a la vida privada de las personas y limiten estrictamente la comunicación de informaciones a los servicios de represión y a las autoridades judiciales competentes en materia penal*”.

Interpol se rige por el **Reglamento sobre el Tratamiento de Datos (RDT)** que fue aprobado por la Asamblea General en 2011 y entró en vigor en julio de 2012. Además la organización dispone de la **Comisión de Control de Ficheros** que puede emitir decisiones vinculantes y dictámenes en asuntos relacionados con el tratamiento de los datos de carácter personal y de un funcionario encargado de la protección de datos en la Secretaria General.

Respetar los principios generales de la protección de datos como son el de la limitación de la finalidad (art. 10), la licitud (art. 11), la calidad de los datos (art. 12), la transparencia (art. 13), la confidencialidad (art. 14) y la seguridad (art. 15), así como el derecho de los individuos a acceder, rectificar y

eliminar sus datos que consten en las bases de datos de Interpol (art. 18). Los datos pueden ser tratados fuera del ámbito de la organización si tal tratamiento es necesario y se realiza con fines policiales (art. 16.1).

También se contemplan garantías adicionales, como son los plazos de conservación (art. 49), restricciones de acceso (art. 58) y la verificación de la exactitud y pertinencia de los datos (art. 63).

El reglamento además dispone de un título completo – Título IV - en el que se definen los niveles de control sobre los datos, los instrumentos y las medidas de control establecidas.

Conclusiones.

Para que la libertad de circulación de personas y bienes en la Unión Europea no sea un campo abonado donde prolifere la criminalidad internacional, es necesario disponer de mecanismos que hagan posible que la lucha policial y judicial contra el crimen organizado, terrorismo y la comisión de delitos graves sea eficiente. Entre las personas que se desplazan, hay individuos que aprovechan el cambio de país

para delinquir, convencidos de que cuando lo abandonen, su historial delictivo no les seguirá. Otros residen en un país y se desplazan a otro durante un período de tiempo relativamente corto para delinquir y regresar a su país para disfrutar el botín.

La UE ha creado una serie de estructuras legislativas que permiten que el intercambio de información entre las distintas autoridades policiales sea eficiente y rápido. Los cuerpos policiales pueden consultar las bases de datos de policías de otros países cuando lo necesiten, compartir información e incluso, llevar a cabo operaciones en un territorio que no es el suyo. Pero, a veces, estos canales de intercambio de información no son utilizados solamente para investigar delitos graves, el crimen organizado o el terrorismo. Se aprovechan para transmitir cualquier tipo de información.

En aras de la coordinación policial se llevan a cabo encuentros de autoridades policiales de distintos países, estableciéndose relaciones personales que son provechadas para el intercambio de información *peer-to-peer* en ámbitos específicos. Es una de las ventajas que tienen los encuentros en foros policiales internacionales. Pero no es aceptable que cuerpos policiales de distintos países compartan información relativa a delitos leves como hurtos o estafas, cuando no hay

indicios suficientes de la existencia de una organización criminal, por ejemplo. No deberían utilizarse los instrumentos creados en estos foros para llevar a cabo la difusión europea de este tipo de información. En sus investigaciones, las autoridades policiales trabajan, básicamente, con información que obtienen de distintos canales, uno de ellos la cooperación entre distintas unidades policiales, cuerpos policiales de un mismo país o cuerpos policiales de países distintos. Por lo que el intercambio de información procedente entre autoridades policiales siempre va existir. Pero la información que manejan es lo suficientemente sensible y puede afectar seriamente al derecho a la intimidad y a la protección de datos de un individuo, por lo que deberían establecerse ciertos controles tanto de buena praxis como normativos. Cuando las autoridades policiales de un país soliciten información a las de otro país, éste debe facilitar exclusivamente la información solicitada. Dicha información podrá ser utilizada durante una investigación, pero no deberá ser utilizada en un procedimiento judicial si no ha sido contrastada y con el consentimiento explícito del estado que la ha facilitado, que significará que ha sido obtenida respetando los derechos fundamentales de las personas implicadas.

La UE ha creado instrumentos legales muy útiles para luchar contra la delincuencia transnacional, pero no debería olvidar que ha de instar a los estados a armonizar su legislación penal. La disparidad legislativa existente entre los diferentes estados en materia policial y penal puede provocar un tratamiento policial distinto entre individuos que han cometido un mismo hecho. Así por ejemplo, está más controlado un agresor sexual que ha delinquirido en el Reino Unido y que se encuentra de paso en el estado español, que el que ha realizado el mismo delito en España. Las autoridades policiales españolas deberán informar a las autoridades policiales inglesas del comportamiento de este individuo en nuestro país. En cambio, a los delincuentes sexuales que han delinquirido en España no se les hace ningún seguimiento de esta índole³³⁶.

A mi juicio hay que valorar muy positivamente el cuerpo normativo creado en la UE para la lucha contra el crimen en el ámbito de la UE, todo y las pequeñas disyunciones que se han detectado. Este es el camino que debe seguirse en la cooperación policial europea, mientras no se dote a Europol de más competencias y se convierta en una fuerza policial real en todo el ámbito de la Unión.

³³⁶ En España, cuando se considera que un agresor sexual pueda reincidir una vez cumplida la condena y ya ha sido puesto en libertad, la Fiscalía puede ordenar a la policía algún tipo de seguimiento a esta persona durante un corto período de tiempo. Pero son casos excepcionales.

CAPÍTULO III

ADN FORENSE EN LA INVESTIGACIÓN POLICIAL

LA PROTECCIÓN DE LOS DATOS GENÉTICOS

1. -Nociones de biología celular.

Las molécula de ADN, principalmente, se hallan en el núcleo de la célula; pero también las hay en otros orgánulos celulares como las mitocondrias o en los cloroplastos. En ella se encuentra toda la información que necesita un organismo para desarrollar sus funciones y poder vivir. En todas las células de un individuo las cadenas ADN son idénticas pero no así entre individuos, ya que existen pequeñas variaciones entre sí que hacen que el ADN de cada individuo sea único. La ciencia forense ha aprovechado esta circunstancia y ha desarrollado técnicas en las que al comparar dos cadenas de ADN puede establecerse si proceden de un mismo individuo. Para realizar estos cálculos, no es necesario analizar toda la cadena; con analizar pequeños fragmentos y aplicar las reglas de la probabilidad es suficiente.

Antes de entrar en los usos del ADN forense, debemos recordar algunos conceptos biológicos que nos permitan entender cómo funciona esta técnica.

La molécula de ADN es un polinucleótido³³⁷ formado por dos cadenas de nucleótidos con un esqueleto de pentosas – molécula de cinco carbonos - y grupos fosfatos que adopta una estructura enrollada de doble hélice. Los cuatro nucleótidos se van repitiendo a lo largo de una de las cadenas de forma desigual, siendo la otra cadena una copia antiparalela de la primera. La manera como estén distribuidos los nucleótidos constituye el código genético, que una vez replicado en otras partes de la célula darán lugar a los aminoácidos que, posteriormente, formaran las proteínas. Cuando la célula eucariota³³⁸ se divide, el ADN que está en el núcleo se agrupa formando los cromosomas.

El **gen** es una secuencia lineal de nucleótidos que contiene la información esencial para una función específica en la célula y que ocupa un lugar determinado - denominado *locus* - en el **cromosoma**. Este lugar será el mismo para todas las células que componen un individuo. Al conjunto de genes de una especie se le conoce como genotipo. En las células

337 Las bases que forman los nucleótidos son la Adenina (A), Guanina (G), Citosina (C) y Timina (T)

338 Las células **eucariotas** se diferencian de las **procariotas** por tener el material genético en el núcleo, el cual está separado por una membrana.

eucariotas - entre las que se encuentran las células que forman el cuerpo humano - el ADN se halla en el **núcleo** de la célula – ADN nuclear – y en las **mitocondrias**³³⁹ - ADN mitocondrial -.

Las células sexuales son los denominados **gametos** y contienen la mitad de la carga genética de una célula no sexual. La unión que resulta de dos de ellas después de la **fecundación** se denomina **zigoto**, y contendrá la mitad de la carga genética del progenitor masculino y la mitad de la del femenino. La fecundación se lleva a cabo en el gameto femenino u **óvulo**, de manera que el gameto masculino o **espermatozoide** cede, exclusivamente, su carga genética y el óvulo aporta su carga genética y el resto de elementos celulares necesarios para el desarrollo de la nueva célula. El cigoto humano está formado por 23 pares de cromosomas (46) así que un cromosoma procede de un progenitor y su par del otro.

Por lo tanto, el núcleo celular del cigoto resultante de la unión de dos células sexuales llevará un 50% de la carga genética del progenitor masculino y la otra mitad de la de su

³³⁹ Es un orgánulo celular recubierto por una membrana que se encuentra en el citoplasma celular. Se halla en la mayoría de las células eucariotas todo y que su número puede variar en función del tipo de célula de que se trate. Según la *teoría endosimbiótica*, las mitocondrias serían células procariotas que hace millones de años fueron devoradas por los antepasados de las células eucariotas y desde entonces ambas viven en simbiosis.

progenitor femenino. Pero la carga genética será distinta entre su descendencia dado que el material genético que portan los espermatozoides es distinto entre ellos porque la distribución se hace al azar.

2.- ADN de uso forense.

Los nucleótidos que puede llegar a contener una célula formando parte de su ADN es de unos 3000 millones; un gen puede estar formado desde unos 3000 nucleótidos hasta más de 100.000. Se estima que el cuerpo humano tiene unos 30.000 genes de los cuales unos 18.000 codifican proteínas³⁴⁰ y que representan el 1 o 2 % del ADN que contiene la célula. El resto corresponde al **ADN no codificante** y que se distingue del **ADN codificante** en que el primero no tiene información para sintetizar proteínas. Éstas son regiones cromosómicas sin expresión genética, aquellas de cuya capacidad para determinar alguna propiedad funcional del individuo no se tiene constancia³⁴¹.

340 <https://genotipia.com/curiosidades-del-genoma-humano/> (última consulta 14/03/2022).

341 Definición sobre la *parte no codificante del ADN* que da el art. 2 de la Decisión 2008/616/JAI del Consejo de 23 de junio de 2008 relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

El ADN no codificante, al no verse expuesto a la presión evolutiva, admite niveles de variación mayores que el ADN codificante. Una variación de bases en el segundo puede suponer una malformación que ponga en riesgo los descendientes de este individuo, haciendo que la selección natural decida sobre la idoneidad del cambio producido; éste hecho no sucede con el ADN no codificante por lo que la mutación se transmite a las generaciones futuras.

El ADN que se usa en la investigación forense es el ADN no codificante, del cual se extrae una serie de fragmentos - **marcadores** - ubicados en distintas cromosomas. Se trata de pequeñas regiones formadas por unos 100 - 500 nucleótidos compuestos por una unidad de 4 - 5 nucleótidos que se van repitiendo en tándem a lo largo de dicha región durante un determinado número de veces (Short Tandem Repeats - STRs) y que presentan una alta variabilidad entre los individuos. Cuanto mayor es el número de marcadores que se estudian, menor es la probabilidad³⁴² que dos individuos tengan el mismo número de repeticiones en todos los fragmentos estudiados.

³⁴² Hay una probabilidad de 1 entre 10^9 que dos individuos tengan el mismo número de STR en todos los fragmentos estudiados. Cuanto mayor sea el número de fragmentos estudiados, menor es la probabilidad de error en el análisis.

Los marcadores que se estudian en un análisis de ADN – actualmente - carecen de información relativa a las características genéticas del individuo. Pero con los avances científicos en ciencia genética, no se puede descartar que en un futuro los fragmentos de ADN considerados “basura” y que actualmente se utilizan para determinar el perfil genético de un individuo estén asociados con información relativa a enfermedades, rasgos de comportamiento o a sus características físicas. De darse este caso, deberían cambiarse los marcadores genéticos y utilizarse otros³⁴³ de los que no hubiera constancia de su implicación genética. Los distintos marcadores componen el perfil de ADN de la muestra analizada y representan el conjunto de características identificativas de la parte no codificante de ese ADN; su representación es la de un código alfanumérico o numérico³⁴⁴.

El Consejo de la Unión Europea establece un estándar europeo mínimo de 12 marcadores³⁴⁵ - conocidos como **ESS**

343 Resolución del Consejo de 30 de noviembre de 2009 relativa al intercambio de resultados de análisis de ADN (2009/C 296/01).

344 Definición de perfil de ADN que da el art. 2 de la Decisión 2008/616/JAI del Consejo de 23 de junio de 2008.

345 Resolución del Consejo de 30 de noviembre de 2009 relativa al intercambio de resultados de análisis de ADN (2009/C 296/01).

Con el fin de determinar la frecuencia alélica de cada marcador en la población española, han participado los cinco laboratorios de genética forense representados en la **Comisión Técnica Permanente de la Comisión Nacional para el Uso Forense del ADN** y pertenecientes al Cuerpo Nacional de Policía, Guardia Civil, Ertzaintza, Mossos de Esquadra e Instituto

- que deben ser analizados en el ADN nuclear. En España, la base de datos nacional de ADN - Denominada SDIS - State DNA Index System - almacena 23 marcadores, entre los que se encuentran los doce del ESS.

Un ejemplo de resultado de un análisis genético para cuatro muestras es el siguiente:

STR ¹ Autosòmics i Amelogenina	MOSTRA 11id	MOSTRA 9	MOSTRA 5	MOSTRA 4 (barreja d'ADN)
D10S1248	15/16	15/16	14/15	15/16/17
vWA	18/20	18/20	18	17/18/20
D16S539	11	11	13	11/12
D2S1338	17/24	17/24	17/22	17/24/25
Amelogenina	X	X	X/Y	X/Y
D8S1179	13/15	13/15	14/15	13/15
D21S11	29/30	29/30	30	28/29/30
D18S51	15/16	15/16	14/15	14/15/16/17
D22S1045	15/16	15/16	11/15	11/15/16/17
D19S433	12/14	12/14	14.2/15.2	12/13/14
TH01	6/7	6/7	6/8	6/7/8
FGA	22/23	22/23	22	19/22/23
D2S441	11/14	11/14	10/14	11/14
D3S1358	15/16	15/16	17/19	15/16
D1S1656	15.3/16.3	15.3/16.3	13/15.3	13/15.3/16.3
D12S391	17/21	17/21	18/21	17/21/23
SE33	17/30.2	17/30.2	14/27.2	17/19/30.2

Por ejemplo, el primer marcador **D10S1248**, significa que en el locu S1248 del cromosoma 10, para la muestra **11id** hay 15 repeticiones en un alelo³⁴⁶ y 16 en el otro alelo. Los alelos provienen de cada uno de los progenitores, pero no puede

³⁴⁶ Nacional de Toxicología y Ciencias Forenses.

saberse si la madre dio el de 15 o el de 16 repeticiones. Su distribución es aleatoria en toda la cadena. En cambio en el marcador **D16S539**, locu S539 del cromosoma 16, ambos alelos tienen 11 repeticiones; así tanto el que cedió el padre como el de la madre tenían 11 repeticiones.

La muestra 11id y la muestra 9 tienen los mismos marcadores. Ello significa que hay una coincidencia **entre perfiles**. Dicha coincidencia se valora estadísticamente: no se puede afirmar tajantemente que ambas muestras provienen del mismo individuo, sino que a partir de cálculos estadísticos se determina qué probabilidad hay que ambas muestras provengan de un mismo donante. Así, a partir de datos empíricos se determina la frecuencia en la que se halla un determinado alelo en la población de referencia³⁴⁷ - en este caso la española - y se aplica a cada marcador. Finalmente se hace el cálculo para todos los marcadores.

En el caso del perfil genético de la muestra 11id, sería necesario examinar el perfil genético de mil trillones de

³⁴⁶ Alelo - Son las distintas formas que puede tener un mismo gen y que produce manifestaciones concretas de ese gen. Cada par de alelos se ubica en el mismo lugar del cromosoma.

³⁴⁷ La probabilidad que un individuo de la población determinada - en este caso España - tenga en el locus D10S1248 15 repeticiones en un alelo y 16 en el otro es de 0,2060 y 0,1250 respectivamente.

Datos obtenidos en la página:

<https://www.mjusticia.gob.es/ca/ministerio/organismos-entidades/instituto-nacional/comision-nacional-para-forense/comision-tecnica-permanente>

(última consulta 14/03/2022).

personas para localizar otro individuo que tuviera el mismo perfil genético de la muestra 11id, de lo que se deduce que el donante de la muestra 11id y la muestra 9 es el mismo. Las probabilidades de coincidencias están del orden de billones o trillones.

En cambio, entre el perfil genético de la muestra 11id y la muestra 5 hay varias diferencias. Ello significa que no proceden del mismo donante.

Finalmente, la muestra 4 es una mezcla de dos o más donantes, ya que hay hasta cuatro alelos con distintas repeticiones en diversos locus. Como el ADN de los distintos donantes se ha mezclado no se puede saber que alelo pertenece a una muestra y cual pertenece a otra. En este caso, la única manera de poder discernir los distintos perfiles genéticos que forman la mezcla es comparándolo con otro perfil. Así la muestra 11id sería uno de estos donantes, dado que las repeticiones de sus locus son iguales a repeticiones que se dan en la muestra 4.

El estudio de perfiles genéticos son análisis de datos estadísticos. Puesto que no está permitido – ni es viable - analizar toda la cadena de ADN, se analizan fragmentos de

esta cadena y se tratan estadísticamente; así, cuantos más marcadores se analicen más preciso será el resultado.

2.1.- Tipos de ADN utilizados en el ámbito forense.

- ADN Nuclear

Se encuentra en el núcleo de la célula y su composición es única para cada individuo. Todas las células del cuerpo - excepto los gametos - tienen la misma carga genética nuclear. Los métodos de análisis genéticos permiten determinar con exactitud si un resto biológico en el que se ha localizado ADN nuclear pertenece a un individuo concreto.

El análisis de este tipo de ADN es el más utilizado en investigación criminal, todo y que el 99,9 % del genoma humano es igual entre todos individuos. Se han identificado unos 3 millones de localizaciones donde existen diferencias en las bases de ADN de los humanos.

- ADN Mitocondrial - ADNmt.

Las células del cuerpo humano pueden albergar cientos de mitocondrias, dependiendo del tipo de célula que se trate y del individuo en cuestión, provocando la existencia de miles de moléculas de ADNmt por célula. Esto permite realizar el

estudio en casos en los que el material genético se encuentra en mal estado o que no haya una cantidad suficiente de material genético nuclear a analizar. También es importante para el análisis de los pelos cuando carecen de bulbo raquídeo, ya que es en él donde se encuentran las células.

La reproducción de las mitocondrias en el interior de la célula es de forma asexual e independiente de la reproducción de la célula. Así la mitocondria "madre" tendrá la misma carga genética que la de las mitocondrias "hijas". Cuando se forman las células sexuales del cuerpo, el óvulo llevará las mitocondrias del progenitor femenino y, durante el proceso de la fecundación, el espermatozoide únicamente depositará su carga genética. Por lo tanto, las mitocondrias del cigoto resultante serán del progenitor femenino, de manera que las mitocondrias del individuo resultante llevarán ADNmt de éste. Así, el ADNmt de los hijos será el mismo en todos e igual al de la madre y, el de ésta, igual al de su madre, y así sucesivamente. Se hereda como un bloque de madre a hijos e hijas de forma *matrilineal*.

El análisis del ADNmt permite establecer una línea familiar que no estará formada por miles, sino por millones de individuos en todo el mundo, de manera que su análisis

puede ser utilizado como línea de investigación, pero no será determinante para establecer el individuo que dio origen a un determinado material genético.

- Cromosoma Y.

El cromosoma Y³⁴⁸ determina el sexo en la mayoría de los mamíferos ya que posee un gen que es el responsable de la masculinización del embrión.

El ser humano tiene 23 pares de cromosomas, siendo un único par el que determinará el sexo del embrión. Así en las mujeres, este par está formado por dos cromosomas XX y en los hombres está formado por el par XY. Durante el proceso de formación de las células sexuales, este par de cromosomas no presentan una recombinación genética total de manera que cada espermatozoide tiene un único cromosoma X o un único cromosoma Y, de la misma manera que un óvulo tendrá un único cromosoma X. En la concepción del embrión es el espermatozoide quien controla el sexo genético del cigoto dependiendo de si el espermatozoide que fecunda lleva el cromosoma X o el Y. De esta manera el cromosoma Y pasa íntegramente a su prole masculina.

³⁴⁸ Es uno de los cromosomas humanos más pequeños, con un tamaño de aproximadamente 60 millones de pares de bases y solo tiene unos 20 genes, a diferencia del cromosoma X que tiene miles de genes.

Así, al igual que ocurre con el ADNmt respecto de la línea genética femenina, el análisis de ADN del cromosoma Y permite identificar una línea genética masculina, ya que la descendencia masculina llevará el mismo cromosoma Y que el padre y éste la misma que sus hermanos masculinos y el de su propio padre. Se hereda en bloque de padres a hijos masculinos.

El análisis genético de este cromosoma es interesante en los casos en que hay mezcla de ADN's masculino y femenino en la muestra, y el segundo es muy superior. Así, en las investigaciones por delitos sexuales donde en las muestras genéticas recogidas hay mezcla de células femeninas de la víctima con esperma u otras células del autor - masculino -, puede quedar enmascarado el perfil genético del asaltante ya que en el análisis del perfil se obtiene una amplificación de la muestra mayoritaria, que en muchos casos es la femenina. La identificación del cromosoma Y en este tipo de muestras permite corroborar la participación de uno o varios hombres en el hecho, así como establecer una línea de investigación. No servirá para individualizar al autor.

2.2.- Características del análisis de ADN forense.

a.- Universal en un mismo individuo.

Independientemente del lugar del cuerpo del individuo de donde procedan las células que se analizan, el resultado será el mismo para cada sujeto. Con el análisis forense del ADN de la saliva se obtendrá al mismo resultado que si se analiza una gota de sangre o de piel.

Las muestras indubitadas de ADN se suelen obtener de la saliva del sujeto a través de un raspado bucal con una torunda de algodón. En el lugar de los hechos, las muestras de ADN se obtienen de los lugares más variopintos: desde restos de sangre o semen, pelos, huesos o dientes. Pero también de restos de saliva en una cinta americana cortada con los dientes, cepillos de dientes, cuellos de camisas, pantalones y un largo etcétera. Los nuevos métodos de análisis permiten obtener ADN de muestras que cada vez contienen menor carga genética.

b. - Estabilidad en el tiempo.

El ADN es materia orgánica y, como tal, se degrada. Pero ciertas condiciones de humedad, temperatura y luz permiten su conservación durante largos periodos de tiempo³⁴⁹. Por este motivo el interior de los huesos o de los dientes son

³⁴⁹ Se ha conseguido obtener muestras de ADN del interior de los dientes de momias egipcias de 1800 años de antigüedad.
<https://www.lavanguardia.com/cultura/20180118/4477192626/el-adn-resuelve-el-misterio-de-estas-momias.html> (última consulta 14/03/2022).

lugares en los que esta molécula tarda más degradarse y es más estable.

En casos de catástrofes aéreas, por ejemplo, en el que los cuerpos están mutilados y en muchos casos, carbonizados, pueden encontrarse células con el ADN intacto que permiten la identificación del cuerpo.

Son muchos los casos en los que, gracias al análisis de indicios recogidos del lugar del crimen con restos de ADN, han podido determinar muchos años después la inocencia de los que inicialmente fueron juzgados y condenados³⁵⁰.

c.- Diversidad en la especie humana.

Todos los seres humanos tenemos el ADN distinto los unos de los otros. Se transmite de padres a hijos de acuerdo con los postulados mendelianos. Por tanto, una mitad de la carga genética corresponde al padre y la otra mitad a la de la madre. A la vez, esta mezcla es distinta entre hermanos ya que los genes que un padre o una madre transmite a cada

³⁵⁰ Por ejemplo el caso de James BAIN, que fue condenado a cadena perpetua en 1974 por violación y asesinato de un niño de 9 años en el estado de Florida. Cuando en 2009 se analizó el ADN del semen que se había encontrado en la ropa del menor se comprobó que no había sido el asesino. BAIN fue puesto en libertad después de haber pasado 35 años en prisión por un crimen que no había cometido.

Puede consultarse en <https://www.innocenceproject.org/cases/james-bain/> (última consulta 14/03/2022).

uno de los miembros de su descendencia son distintos³⁵¹ entre sí. La combinación genética es aleatoria.

d.- Fiabilidad. Probabilidad estadística.

La probabilidad de coincidencia de dos muestras escogidas al azar que no estén relacionados genéticamente variara en función de si se trata de perfil genético obtenido ADN nuclear, mitocondrial o del cromosoma Y. La fiabilidad de la prueba depende del número de marcadores que se comparen - a mayor número, mayor fiabilidad -, de cuán frecuentes son esos marcadores en la población estudiada y de si se tiene a los dos progenitores o no.

3.- Usos del ADN forense.

Este capítulo versa en el uso en la investigación criminal que tiene el ADN forense. Pero hay que romper un mito del uso del ADN forense en la investigación criminal: localizar un perfil genético de una persona en la escena de un crimen, no indica *per se* la culpabilidad de ese individuo. Por poner un ejemplo, si el lugar de los hechos es el domicilio del presunto

³⁵¹ Excepto en los gemelos univitelinos, que comparten el mismo ADN. Proceden de un mismo óvulo y espermatozoide ya que en una fase muy inicial del embrión, sus células se dividen para dar lugar a dos embriones distintos que comparten una misma placenta.

autor, localizar su perfil genético allí puede resultar penalmente irrelevante.

La localización de un perfil genético en un indicio determinado indica que, presuntamente³⁵², el donante ha estado en contacto con ese objeto o lugar. Será la investigación policial/judicial que se lleve a cabo, la que determinará si es una prueba concluyente, si es indiciaria o incluso irrelevante. La relevancia penal que tiene el indicio biológico a la hora de determinar la culpabilidad de una persona vendrá determinada por la investigación y la decidirá el juez o el tribunal.

El primer factor que debe determinar la investigación es averiguar cómo ha llegado el perfil biológico de la persona en cuestión a ese indicio. Por norma general, el hallazgo del perfil biológico en ese lugar indicará que la persona que dejó la muestra ha estado en contacto directo con dicho indicio. Pero no deben descartarse otros supuestos:

- *Contaminación*. Las muestras biológicas deben manipularse con sumo cuidado para evitar la contaminación con material biológico procedente de las personas que participan en el

³⁵² Podría darse el caso de aparecer perfil genético de una persona en un lugar en el que nunca ha estado. Sería el caso, por ejemplo, de una persona u objeto que se mancha de sangre de otra persona y, cuando va a otro lugar, quedan restos de esa sangre. Se trata de contaminación por transferencia.

proceso. Los agentes de la policía científica que recogen las muestras en el lugar de los hechos, los que las trasladan al laboratorio o los propios técnicos del laboratorio que las analizan pueden dejar rastro de su propio ADN o el de otras personas. Para detectar este tipo de contaminación, los agentes y técnicos que participan de este proceso introducen sus propios perfiles genéticos en las bases de datos policiales. La coincidencia de un perfil genético con el de algún técnico del laboratorio o agente policial que haya manipulado las muestras, indicaría la contaminación de la muestra.

- *Transferencia secundaria*. Los restos biológicos pueden transportarse de un lugar a otro con solo el mero contacto. Así, si el autor de un homicidio se mancha los zapatos con sangre de la víctima, cuando suba a un vehículo para huir del lugar de los hechos, puede dejar rastro de esa sangre en la alfombrilla de dicho vehículo por transferencia. Las nuevas técnicas de análisis de ADN hace que pueda obtenerse un perfil genético con muestras cada vez menores.

Las nuevas técnicas de laboratorio de análisis de ADN permiten obtener un perfil genético a partir de muy pocas células. Si por transferencia secundaria se transmite un puñado de células de una persona a otra y luego, ésta las

deposita en un objeto, el análisis de los restos biológicos obtenidos en dicho objeto podrían dar un resultado erróneo. Hay estudios que demuestran que después de dos minutos de contacto mano a mano entre dos personas, cuando seguidamente éstas han utilizado un cuchillo, se ha dejado muestra biológica que corresponde al otro individuo y que ha podido ser detectada³⁵³.

Una vez se determina que hay una relación directa entre la muestra biológica y su localización en ese indicio concreto - y no proviene de un error o una transferencia secundaria - la investigación criminal debe analizar la relevancia del indicio respecto del hecho criminal. En este aspecto es determinante, por ejemplo, el lugar concreto donde se ha localizado dicho indicio, cuantas personas pueden tener acceso al lugar, si la persona a la que pertenece la muestra tiene acceso a él, además de otros aspectos de esta índole.

Perfil genético sobre un indicio relevante.

El hallazgo de una huella dactilar del presunto autor manchada con la sangre de la víctima por sí solo podría servir para condenar a una persona por un crimen: indicaría que ha tocado el cuerpo de la víctima ensangrentado y luego ha dejado la huella lofoscópica. En el caso de indicios

353 CALE C.M. et al. (2016).

biológicos no es tan claro. La muestra biológica podría haberse dejado en ese lugar antes que la sangre de la víctima. Por eso es tan importante la investigación criminal que se lleva cabo. Así la localización de perfil genético del autor sobre la ropa de la víctima o el de la víctima sobre la ropa del autor, puede no ser relevante penalmente si la persona a la que pertenece el perfil genético tiene una explicación para ello.

Perfil genético sobre un indicio no relevante.

Puede establecer líneas de investigación. Localizar el perfil genético de una persona en un vaso indicará que esa persona ha estado en contacto con el vaso. Si ese vaso estaba en un domicilio, nos dirá que esa persona ha estado en el domicilio; a partir de aquí se puede iniciar una investigación. Esa persona podría ser el autor, amiga del autor, ser un testigo presencial o, simplemente, conocer a los implicados.

Como podemos ver, el objetivo de una investigación criminal es identificar las personas relacionadas con un hecho criminal y establecer la relación que tienen con él, ya sea víctima, autor o testigo. Para esta finalidad, el estudio de los perfiles genéticos es una herramienta muy útil, más que el

estudio de las huellas dactilares. El autor puede dejar rastro en la escena del crimen, pero también puede llevarse algún indicio sin que sea consciente.

Actualmente, los usos del ADN forense son los siguientes:

3.1.- Criminal.

La primera vez que se utilizó la “huella digital” para identificar a una persona fue en 1985, donde fue usada para establecer relaciones de parentesco entre menores que solicitaban la ciudadanía británica alegando ser descendientes de ciudadanos británicos³⁵⁴. La primera aplicación para resolver un caso de homicidio se dio en Leicestershire (Reino Unido) un año más tarde, donde la policía investigaba los asesinatos y violación de dos niñas ocurridos con dos años de diferencia en la misma zona. Los análisis genéticos permitieron exonerar a una persona que afirmó ser el asesino de una de ellas y consiguió identificar el verdadero autor de los dos homicidios³⁵⁵.

354 JEFFREYS et al. (1985)

355 <https://www.theguardian.com/uk-news/2016/jun/07/killer-dna-evidence-genetic-profiling-criminal-investigation> (última consulta 10/11/2021).

3.2.- Humanitario.

El uso humanitario del ADN forense es muy útil en la búsqueda e identificación de desaparecidos, de cadáveres no identificados y de restos cadavéricos. El I Convenio de Ginebra³⁵⁶ ya tiene en cuenta la importancia que para el ser humano significa la identificación de las personas heridas o muertas. El manejo de éstas personas, sea o no en combate, son tareas humanitarias. Los cuerpos policiales son los encargados de llevar a acabo la identificación de cadáveres y restos cadavéricos sin identificar y la búsqueda de personas desaparecidas. Para ello, utilizan las bases de datos de perfiles genéticos de ámbito criminal, pero de manera limitada.

3.3.- Paternidad / Maternidad.

La prueba de paternidad / maternidad permite determinar el vínculo familiar entre dos personas. En la procreación humana, al basarse en la reproducción sexual, el hijo tiene la mitad de la carga genética de la madre y la mitad del padre. Además, de la madre el barón compartirá el cromosoma X y

356 El art. 16 del I Convenio de Ginebra del 12 de agosto de 1949 reza "*Las partes en conflicto deberán registrar, tan pronto como sea posible, toda la información adecuada para identificar a los heridos, a los enfermos y a los muertos de la parte adversaria caídos en su poder*".

del padre, el cromosoma Y. La hija compartirá un cromosoma X de la madre y el cromosoma X del padre.

Podría llevarse a cabo un estudio a partir de las muestras de los padres de uno de los progenitores.

4.- Muestra biológica y perfil genético.

La Directiva (UE) 2016/680 define el término **datos genéticos** como "*datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de la persona física de que se trate*". Los datos genéticos están incluidos en las categorías especiales de datos personales³⁵⁷. Pero estos datos no contienen solamente información relativa a la persona física: en ellos también hay información sobre sus parientes cercanos, de sus progenitores y de sus descendientes. Por tanto, una infracción al derecho a la *intimidad genética* no afecta únicamente a la persona de la que proviene la muestra, sino que también afectará a sus familiares biológicos. Todo y tratarse de ADN no codificante, la información que facilitan estos datos permiten identificar o hacer identificable de forma inequívoca a un individuo.

³⁵⁷ art. 3.12 y art. 10 de la Directiva (UE) 2016/680.

El **perfil genético** obtenido a partir de una muestra biológica se encuentra codificado en una secuencia de números y letras; la identificación del individuo solo se produce si hay una coincidencia con otro perfil de la base de datos. Sin esa coincidencia, los datos numéricos no tienen ningún sentido.

Esta forma de pensar llevó al Tribunal Supremo a afirmar que la toma de muestras de ADN mediante frotis bucal afecta *levemente* al derecho a la intimidad cuando se hace a efectos meramente identificativos llegando a comparar la reseña dactilar o fotográfica con la reseña genética³⁵⁸. En dicha sentencia se sitúa el núcleo de la protección en el momento de la recogida de la muestra, argumentando que solo se utilizaba una pequeña parte de la cadena de ADN que carecía de valor genético.

A mi juicio, el hecho de que el perfil genético contenga datos personales únicos sobre un individuo en cuestión y que éstos puedan ser almacenados para ser tratados de manera automática, hace que su análisis pueda ir más allá de la simple identificación muestra/individuo ya que en el ADN celular de cada individuo no solo se encuentra las características genéticas de ese sujeto, sino que también contiene las de sus ancestros y las de sus descendientes. Aunque el perfil genético consista en una serie de números

358 STS 709/2013 de 10 octubre, FJ segundo.

que por si solos carecen de todo sentido y que se han obtenido de fragmentos de ADN que forman parte del denominado "ADN basura" dado que no contendrían información codificante, el tratamiento automatizado puede ir más allá de la "*identificación neutra de un individuo*" ya que permite que se lleven a cabo búsquedas familiares³⁵⁹ a través de identificar relaciones genéticas entre individuos³⁶⁰ o determinar el origen étnico del donante de la muestra³⁶¹.

Como se ha dicho anteriormente, el mero almacenamiento de datos genéticos de una persona supone una interferencia a su vida privada. Por lo tanto, deben ser considerados datos personales altamente sensibles y entran dentro de la protección de l'art. 8 del CEDH. La retención sistemática de material genético por parte de las autoridades de un país, es

359 STEDH de 4 de Diciembre de 2008. Caso Marper c. Reino Unido, párrafo 77.

360 Se han dado casos de identificación de asesinos y delincuentes sexuales a partir de ADN localizado en la escena del crimen y, una vez tratado y obtenido su perfil genético, éste ha sido introducido en bases de datos de los EEUU y se han localizado a los familiares del autor. A través de ellos se ha llegado al autor material. La noticia en:

<https://www.technologyreview.es/s/10333/la-detective-que-encuentra-asesinos-desde-casa-con-adn-de-su-familia> (última consulta 10/11/2021).

361 En 2015 se detuvo el asesino de **Eva Blanco** ocurrido el 10 de abril de 1997. La investigación se basó en el perfil de ADN que se obtuvo de una muestra del presunto autor hallado en el cuerpo de la víctima. Los análisis determinaron que el autor era de origen norteafricano por lo que se investigaron todos los ciudadanos de éste origen que en la época vivían en la comarca. Así, se llegó al hermano del asesino y, posteriormente, a éste.

La noticia en: https://elpais.com/politica/2015/10/01/actualidad/1443719863_809928.html (última consulta 10/11/2021).

lo suficientemente intrusivo como para considerarlo una interferencia en la vida privada de una persona. Creo que no se puede comparar la información que contiene una muestra biológica con la que contiene una huella dactiloscópica o una fotografía.

El resultado del análisis de una muestra biológica no será el mismo si se hubiera llevado a cabo hace 30 años que si se realiza actualmente. En aquella época los análisis eran más rudimentarios, al igual que los resultados, y solo se obtenía un perfil genético que consistía en un código alfanumérico que permitía una identificación neutra del individuo. En los próximos años, es de esperar que las técnicas de análisis de ADN - que se abordan en el último capítulo - vayan más allá de la mera identificación y permitan extraer otras características. En todos los casos, la muestra biológica seguirá siendo la misma.

En cambio, una huella dactilar o una fotografía aporta la misma información actualmente que la que aportaba antaño. El estudio de las crestas dactilares no podrá servir para ir más allá de la mera identificación, a pesar del tiempo transcurrido. Por lo tanto, el grado de protección jurídica a la que se someta a las muestras biológicas debe ser superior al de las huellas dactilares o de las fotografías.

En el uso del ADN forense en la investigación criminal, deben distinguirse tres etapas:

1.- Obtención de las muestras. Puede verse afectada la *intimidad corporal* del donante.

- En esta fase es relevante la situación procesal del donante de la muestra: si está detenido, investigado o es un testigo o víctima.
- Bajo que supuestos legales se obtiene la muestra biológica: si el donante da su consentimiento, se lleva a cabo bajo requerimiento judicial o se trata de una muestra abandonada.
- Bajo que supuestos puede obtenerse una muestra biológica de una persona.
- Diferenciar entre si se conoce la identidad del donante de la muestra o, por el contrario, procede de un escenario en el que es necesario identificar la persona de la que procede dicha muestra.

Respondiendo a las cuestiones planteadas podremos conocer bajo qué condiciones legales una muestra biológica podrá transformarse en un perfil genético apto para ser

utilizado legalmente en una investigación criminal, es decir, se transformara en un código alfanumérico con significado científico y efecto jurídico.

2.- Análisis de las muestras biológicas en el laboratorio para obtener el perfil genético del donante de la muestra.

El perfil genético se obtiene aplicando un kit comercial a la muestra biológica que permitirá extraer unos marcadores concretos. En función del tipo de kit comercial se obtendrá una determinada información genética sobre el individuo.

En esta etapa se ve afectada la intimidad genética de la persona.

3.- El perfil genético debe introducirse en una base datos para que pueda ser comparado con otros perfiles de donantes conocidos o desconocidos. Esto producirá un resultado que puede ser penalmente relevante. Esta etapa afecta a la *autodeterminación informativa* del individuo.

- Bajo que base legal pueden almacenarse perfiles genéticos.
- Como funcionan dichas bases de datos y como funciona el intercambio de datos, que a la larga es la

clave del éxito: a mayor número de perfiles genéticos en la base de datos, mayor probabilidad de identificar el donante de un perfil genético determinado.

- Bases de datos que permiten el intercambio de información a nivel nacional e internacional.

Todas estas cuestiones serán las que trataremos a continuación.

5.- Obtención de las muestras.

El ADN está presente en todas las células del cuerpo humano. En una investigación policial es muy importante localizar restos biológicos que contengan ADN. Dichas muestras pueden extraerse directamente del cuerpo de un sujeto, para lo cual será necesaria una intervención corporal, o una vez ya se ha separado del cuerpo. En el segundo caso, el sujeto del que procede puede estar identificado o no.

Los restos biológicos que contengan ADN pueden agruparse en 6 grandes bloques:

Sangre.

Semen - Habitual en agresiones sexuales. Si el agresor es espermático - no tiene espermatozoides - o se ha esterilizado con la técnica de la vasectomía, no se localizarán restos de ADN.

Células epiteliales - Se encuentran en lugares donde ha habido rozamiento con la piel del individuo del que se quiere obtener el perfil genético (guantes, cuello de camisa,...)

Saliva - Es de donde se obtiene la mayoría del ADN indubitado.

Cabellos - Es importante que los cabellos conserven raíz, ya que es donde hay una cantidad importante de células. La fibra del cabello carece de ADN nuclear, pero sí posee ADN mitocondrial.

Musculatura - Se utiliza en casos de desastres naturales, explosiones, incendios... Son las partes del cuerpo humano que tardan más en degradarse en este tipo de situaciones.

Huesos - Se utiliza en casos en que el cadáver está muy descompuesto. Se recogen los huesos más largos del cuerpo o los dientes.

Las posibilidades técnicas del análisis de muestras de ADN dependen, en gran medida, de la calidad de la muestra, de su naturaleza, pero también de su recogida y posterior envío al laboratorio. Son diversos los casos en los que la contaminación de la muestra ha anulado su utilidad el día del juicio³⁶².

Identificar muestras biológicas encontradas en el lugar de los hechos a través del ADN solo nos lleva a concluir que el individuo en cuestión ha estado en contacto con el lugar u objeto en el que se encontró su muestra biológica. Pero ello no resta importancia a la investigación que se debe llevar a cabo y será la que determinará si esa persona puede ser considerada autor o no. Así por ejemplo, si se está investigando un homicidio ocurrido en el domicilio del presunto autor, quizás, las muestras biológicas localizadas en el lugar de los hechos aportaran poca carga de prueba y esta deberá llevarse a cabo por otros medios. En cambio, si esa muestra procede de una cinta adhesiva con la que fue atada la víctima, su valor incriminatorio puede ser elevado.

Hasta la entrada en vigor de la Directiva (UE) 2016/680 y el Reglamento (UE) 2016/679 las muestras biológicas no eran consideradas un dato de salud en *stricto sensu*. Aunque no lo

³⁶² <https://www.elmundo.es/sociedad/2015/10/08/56162b9a268e3ea6698b45a0.html> (última consulta 14/03/2022).

recoge expresamente el articulado, el considerando 24 de la Directiva afirma que deberían incluirse entre los datos personales relacionados con la salud. En la legislación española, ni la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, ni la Ley de Enjuiciamiento Criminal incluyen las muestras biológicas en la categoría de datos personales, por lo que las deja en un vacío legal. Además la legislación española no regula qué debe hacerse con las muestras biológicas una vez se ha extraído el perfil genético. La única alusión a ellas se hace en la Ley Orgánica 10/2007, de 8 de octubre³⁶³, cuando traslada toda la responsabilidad a la autoridad judicial en cuanto a su conservación.

5.1. - Muestra dubitada versus indubitada.

Las muestras pueden ser **dubitadas**, lo que significa que se desconoce la identidad de la persona de la que procede la muestra, o **indubitadas**, las cuales proceden de un sujeto del cual se le conoce la identidad.

Las primeras proceden del lugar de los hechos y son los vestigios biológicos que ha dejado el autor en la escena del crimen o en el cuerpo de la víctima, o de un cadáver sin

363 Art. 5.1

identificar, por ejemplo. La investigación que lleve a cabo la policía se centrará en identificar la persona que dejó dicha muestra. Se puede tratar de manchas de semen, sangre o saliva; pero también de los restos biológicos que hay en una taza de café acabada de utilizar, un cepillo de dientes o un pañuelo.

Las segundas, las indubitadas, proceden de una persona que está plenamente identificada y que en la investigación tendrá un rol determinado, que será el de autor, víctima, familiares de víctimas o testigos y cuyas muestras serán comparadas con las muestras dubitadas.

5.2.- Obtención de muestras dubitadas.

La recogida de este tipo de muestras dependerá del material de que se trate - sangre, semen, pelos, huesos,... -. Así, si se trata de una mancha de sangre húmeda, se recogerá con una torunda estéril y se dejará secar. Si la sangre está seca, se raspará la mancha y las raspaduras se recogerán en un sobre de papel.

Son dos los escenarios principales en los que se obtendrán éste tipo de muestras:

Escenario del crimen.

En la legislación española, la policía judicial o, en su caso, el médico forense - ambos por delegación del juez instructor - deben recoger las huellas y vestigios biológicos durante la inspección que lleven a cabo y que ayuden al esclarecimiento del hecho que se está investigando³⁶⁴, para evitar su desaparición, destrucción o contaminación. Éstos son enviados al laboratorio para su análisis, con la finalidad de obtener indicios que permitan identificar el autor. Puede darse el caso que la muestra biológica proceda de un objeto que ha sido recogido y almacenado con otra finalidad.

El perfil genético desconocido encontrado en el lugar donde se ha cometido un delito grave³⁶⁵, será introducido en la base de datos policial de identificadores obtenidos a partir del ADN

364 Es una de las funciones de las Fuerzas y Cuerpos de Seguridad, según el art. 11.1.g de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. También se recoge en el Art. 282 y 326 de la Ley de Enjuiciamiento Criminal y en la Disposición Adicional Tercera de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

365 Entendiendo por graves (arts. 13 y 33 CP) aquellos cuya pena en abstracto sea pena grave por exceder de una determinada duración (5 años si se tratare de pena de prisión). En todo caso, se podrán introducir los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados. Art. 3 de la Ley Orgánica 10/2007, de 8 de octubre.

de las Fuerzas y Cuerpos de Seguridad del Estado, y será cotejado con los perfiles genéticos obtenidos en otros escenarios - y que todavía no han sido identificados - y con los perfiles genéticos indubitados y que consten en la base de datos.

Los análisis de los indicios localizados se realizarán cuando la autoridad judicial los "*considere absolutamente indispensables para la necesaria investigación judicial y la recta administración de justicia*"³⁶⁶. El resultado de esta prueba puede ser concluyente, haciendo variar el peso específico de las otras. La fiabilidad de los análisis genéticos hace que se convierta siempre en una prueba "*absolutamente indispensable*". De esta manera, siempre que del lugar de los hechos de un delito grave se encuentren indicios biológicos, por regla general, éstos serán analizados. Así, atendiendo a motivos económicos, solamente cuando los análisis son muy costosos o deben ser realizados por laboratorios externos, será requerida una autorización judicial para efectuar dicho análisis.

La ley ampara que las muestras biológicas recogidas en la escena del crimen³⁶⁷ puedan ser utilizadas durante un proceso penal. De todas maneras, se trata de muestras que

366 Art. 363 de la Ley de Enjuiciamiento Criminal.

367 Art. 326 de la Ley de Enjuiciamiento Criminal.

han sido abandonadas - voluntaria o involuntariamente - por el autor de los hechos y para la averiguación del delito y el descubrimiento del delincuente la policía judicial puede recogerlas del lugar de los hechos y analizarlas sin necesidad de una autorización judicial³⁶⁸.

Si las muestras han sido abandonadas, las expectativas de privacidad del dueño de la muestra en relación a los elementos inculpatorios que puedan obtenerse no son razonables. No se debe esperar que la policía no recoja unos indicios que cualquier otra persona recogería y los utilizaría para investigar el ilícito penal³⁶⁹. La recogida en sí de la muestra dubitada del lugar de los hechos no debe suponer ningún problema legal, sino más bien en la ingente cantidad de información que se puede llegar a obtener a partir de los datos genéticos. A medida que la ciencia genética está avanzando cabría reconsiderar los tipos de análisis a los que se verá sometida dicha muestra. Un análisis de perfil genético para comprobar si dos muestras pertenecen a una misma persona no invade de la misma manera la intimidad de una persona que si esa misma muestra se somete a un proceso de *familial searching* o de localización de ancestros.

³⁶⁸ STS 1190/2009 de 3 de diciembre, STS 701/2006 de 27 de junio, STS 949/2006 de 4 de octubre y STS 1267/2006 de 20 de diciembre.

³⁶⁹ Ver la Sentencia de US Supreme Court California v. Greenwood, U.S. 35, de 11 de enero de 1988. Se puede consultar en <https://supreme.justia.com/cases/federal/us/486/35/> (última consulta 22/03/2022).

En el siguiente capítulo vamos a profundizar en este tipo de análisis y las afectaciones que suponen al derecho a la protección de datos y a la intimidad del sujeto al que pertenece la muestra que se analizará.

Por este motivo cabría empezar a replantearse que tipo de análisis pueden ser sometidas las muestras dubitativas que han sido recogidas de la escena del crimen. En mi opinión, deberían conservarse, al menos, hasta que prescriba el delito.

Identificación de cadáveres.

Cuando de un cadáver no se obtiene una impresión dactilar lo suficientemente buena como para poderlo identificar o hay sospechas que las impresiones dactilares no serán de suficiente calidad, durante la autopsia se extraerán muestras biológicas para obtener perfil genético. En cadáveres que se encuentran en buenas condiciones se extrae sangre en papel secante. También se puede extraer un fragmento de músculo de una zona profunda mejor conservada, el muslo por ejemplo, para evitar así posibles contaminaciones. De éste se obtendrá el perfil genético que se usará para la identificación del cuerpo. Si hay dudas sobre su conservación, se pueden extraer piezas dentales.

En casos de desastres naturales, accidentes aéreos, explosiones, incendios, cuerpos mutilados, o similares se utiliza la parte de la que se disponga para obtener muestras de ADN; normalmente suelen ser los huesos o dientes, ya que ofrecen mayor resistencia a la destrucción.

5.3.- Obtención de muestras indubitadas.

La técnica con la que se recogen las muestras a personas vivas no se diferencia entre testigos, personas sospechosas/detenidas o familiares de personas desaparecidas. Por norma general se obtendrá muestras de células procedentes de epitelio bucal, dado que es una práctica menos invasiva que la extracción de sangre o tejidos. Consiste en frotar la cara interna de la mejilla unas veinte veces con hisopos³⁷⁰ estériles en seco. Por sistema se obtendrá la muestra por duplicado: un hisopo se frotará en la mejilla interior derecha y un segundo hisopo en la mejilla interior izquierda, para detectar posibles contaminaciones y errores en la toma de muestras.

5.3.1.- Con consentimiento del interesado.

La legislación española diferencia claramente entre la obtención de muestras para extraer perfil genético en las que

³⁷⁰ Bastoncillo acabado en una punta de algodón.

se requiere de un acto de intervención corporal, de las que no se precisa incidir en la esfera privada del individuo para obtenerlas. Si la toma de muestras y/o fluidos requiere de la colaboración activa del sujeto, como es el abrir la boca para realizar el *frotis bucal*, es necesaria la colaboración del investigado, por lo que "*el consentimiento de éste actuará como verdadera fuente de legitimación de la injerencia estatal que representa la toma de tales muestras*"³⁷¹. Para que el consentimiento sea válido debe ser libre y voluntario, excluyendo de esta manera la lesión de la intimidad del sujeto. Ello significa que se le ha de facilitar toda la información previa para que éste sea un *consentimiento informado*³⁷². En el caso de una investigación criminal, equivale a informar al sujeto de como debe facilitar la muestra biológica para que se extraiga su perfil genético y que éste será utilizado en una diligencia de investigación cuya finalidad es la de esclarecer unos hechos delictivos. El perfil será comparado con muestras obtenidas en un hecho delictivo concreto, a no ser que acceda expresamente a que sea comparado con perfiles procedentes de hechos pasados o futuros, en cuyo caso el perfil genético será incluido en las bases de datos policiales de ADN. De ésta forma quedaría

371 STS 767/2013 de 25 de septiembre.

372 STC 37/2011 de 28 de marzo, FJ 5.

salvaguardado el derecho a la intimidad del donante de la muestra³⁷³

Todo y que el procedimiento de obtención de la muestra es independiente del rol jurídico de la persona en la investigación, deben establecerse una serie de garantías para que constituya una prueba válida. Así, en el derecho español la jurisprudencia distingue si la persona está detenida o no.

Los Estados miembros pueden establecer en su legislación el hecho de que el interesado dé su consentimiento para que sus datos genéticos puedan ser tratados en el marco de una investigación penal³⁷⁴, independientemente de su situación procesal, y dichas muestras serán válidas en cualquier país de la Unión Europea.

- Persona no detenida.

Si se tiene que obtener muestra de una persona que no se encuentra detenida, indistintamente si está siendo investigada o no por unos hechos presuntamente delictivos, la recogida de la muestra puede llevarse a cabo con el mero consentimiento de la misma, el cual actúa como fuente de

373 STC 135/2014 de 8 de septiembre, FJ 4.

374 Considerando 35 de la Directiva (UE) 2016/680.

legitimación de tal injerencia. Así, en un acta se hará constar que la persona requerida da su consentimiento libre y expreso para la recogida de muestras biológicas mediante un frotis bucal (dos muestras) con la finalidad de realizar análisis y estudios de ADN no codificante. De esta manera se pueden identificar perfiles genéticos del requirente y excluirlo de la investigación criminal³⁷⁵ o, por el contrario, afirmar su participación en ellos. Los identificadores obtenidos no serán compartidos con otros cuerpos policiales, ni deben inscribirse en la base de datos a nivel nacional.

Las muestras deberían ser eliminadas cuando ya no sean necesarias para el cumplimiento de la finalidad para la que fueron recogidas, todo y que la legislación española deja en manos del juez la destrucción de oficio. También cuando la persona interesada haga uso de su derecho de acceso, rectificación y cancelación, que conlleva la eliminación del perfil genético del fichero y de la muestra biológica.

Pero si resulta que la persona que ha facilitado las muestras biológicas tiene algún tipo de responsabilidad penal en los hechos, y estos se ajustan a los requisitos establecidos en la legislación para la inscripción en las bases de datos de ADN, el perfil genético del individuo será inscrito en ellas.

³⁷⁵ Por ejemplo al tratarse de contaminaciones no deseadas.

La revocación del consentimiento por parte del interesado no producirá efectos retroactivos. Por lo tanto, una prueba de coincidencia genética obtenida a partir de la comparación de una muestra genética facilitada por una persona de manera libre y espontánea podrá ser utilizada ante un tribunal.

- Persona detenida.

El consentimiento informado debe ser dado en presencia letrada si el imputado se halla detenido. En cambio, no será necesario su consentimiento si no es necesario ese acto de intervención corporal y la toma de muestras puede hacerse a partir de restos o excrecencias abandonadas por el propio imputado³⁷⁶. Más adelante entraremos en ello.

5.3.2.- Sin consentimiento del interesado.

Para delitos graves³⁷⁷ y si concurren acreditadas razones que lo justifiquen, el Juez de Instrucción³⁷⁸ podrá acordar, en resolución motivada, la obtención de muestras biológicas del *sospechoso* que resulten indispensables para la determinación de su perfil de ADN³⁷⁹.

³⁷⁶ STS 685/2010 de 7 de julio y STS 827/2011 de 25 de octubre.

³⁷⁷ *Id.* 14

³⁷⁸ En caso de tratarse de un menor de edad, debe ser el Juez de Menores el que dé dicha la autorización. Disposición adicional tercera de la Ley Orgánica 10/2007.

³⁷⁹ Art. 363 de la Ley de Enjuiciamiento Criminal.

En caso de llegar a este extremo, cabría definir más detalladamente el concepto de *sospechoso*. El término de persona sospechosa puede recaer en un individuo que podría ser objeto de una detención³⁸⁰ por los hechos investigados, pero también sobre una persona en la que recaen meras sospechas. ¿Cuándo una persona puede empezar a ser considerada sospechosa de un hecho?

Sí que parece claro que una persona que no es sospechosa, por ejemplo una víctima o un testigo, no puede ser obligada a dar muestras biológicas para obtener el perfil genético.

En otro orden de cosas, dado que se limitarán derechos fundamentales de los ciudadanos, deben seguirse dos principios que vestirán de racionalidad a la decisión que tome la autoridad judicial.

a.- Principio de Proporcionalidad.

Se trata de establecer unos límites a la acción que debe llevar a cabo la Administración. Aplicando el principio de proporcionalidad debe establecerse un equilibrio entre dos opciones contrapuestas y debe escogerse una opción que efectúe una adecuada ponderación entre el interés público - castigar al delincuente y evitar su reincidencia - y el interés

³⁸⁰ A tenor de lo dispuesto en los art. 490 y 492 de la Ley de Enjuiciamiento Criminal.

individual, que asegura la protección de derechos fundamentales.

La *doctrina filosófica del doble efecto*³⁸¹ puede ser una forma de aplicación del principio de proporcionalidad. Según esta doctrina:

- *el acto en sí debe ser indiferente*. Aplicándolo al tema que nos ocupa, la obtención de la muestra y el escrutinio genético que se lleva a cabo son actos en sí insignificantes. La obtención de la muestra se lleva a cabo introduciendo un hisopo en la boca y el escrutinio genético lo hace una máquina, no suponiendo ningún efecto sobre la persona que en su día facilitó la muestra.

- *Se acepta que la decisión produzca un efecto negativo, si éste se produce de forma involuntaria, no buscada*. Durante el escrutinio genético se puede desvelar información relativa a terceras personas ajenas a los hechos. El efecto negativo podría venir del mal uso de esta información.

- *La acción por sí misma debe producir efectos positivos*. Cuando se compara el material genético se

381 <https://plato.stanford.edu/entries/double-effect/> (última consulta 14/3/2022).

abren - o cierran - líneas de investigación que pueden determinar la resolución del caso.

- *Los efectos positivos de la acción deben compensar sobradamente los efectos negativos que pudieran producirse.*

Según el Tribunal Constitucional³⁸², para que se cumpla el principio de *proporcionalidad* deben darse tres condiciones:

- Juicio de idoneidad. La medida propuesta es *susceptible de conseguir el objetivo propuesto*. Comparando el ADN de las muestras biológicas encontradas en el lugar de los hechos con las del perfil genético del interesado se podrá establecer si la primera procede del segundo sin ningún género de dudas.

- Juicio de necesidad. No exista otra medida más moderada para la consecución de tal propósito con igual eficacia.

- Juicio de proporcionalidad en sentido estricto. Si con la aplicación de dicha medida se obtiene más beneficios para el interés general que perjuicios sobre

382 STC 207/1996 de 16 de diciembre, FJ 4

otros bienes. Para llevar a cabo el análisis de ADN, como se ha dicho anteriormente, solo se usan las partes no codificantes de la cadena, haciendo que el resto de la cadena, los datos genéticos, sean irrelevantes penalmente; de hecho no se llegan a analizar. Por tanto, es el método menos invasivo a la intimidad personal. Según el mismo Tribunal, la realización de los análisis de ADN respeta el principio de proporcionalidad³⁸³.

Cuando a un individuo se le extrae una muestra biológica con la finalidad de obtener el perfil genético para que sea comparado con otros perfiles genéticos se le pueden estar vulnerando diferentes derechos personales. Nos estamos refiriendo a los datos genéticos, por lo que se produce una vulneración del derecho a la protección de datos personales. También se vulneran el derecho a la privacidad y al de la integridad física, entre otros. Pero no solo se vulnera el derecho de la persona de la que se obtiene la muestra, si no que también se ve afectado el derecho de los individuos que están relacionados genéticamente con ella. Así, sus familiares biológicos, como pueden ser padres, abuelos, hermanos, primos,.... también pueden ver mermado sus derechos ya que la muestra biológica obtenida contiene

383 STC 199/2013 de 5 de diciembre. FJ 11.

información relativa a la genética de estas personas. Y no solo de los familiares actuales, sino también de sus antepasados. Secretos familiares como infidelidades, incestos, adopciones,... están ocultos en nuestro ADN y podrían salir a la luz de manera involuntaria al ser revelado el perfil genético.

Estos derechos individuales deben confrontarse con el derecho que tiene los ciudadanos a la seguridad pública y a poder desplegar sus propios derechos como ciudadanos y como individuos en la sociedad. Los gobernantes tienen la obligación de preservar los derechos de los ciudadanos.

No debe olvidarse la necesidad que tiene la sociedad de que las autoridades eviten la comisión de cualquier delito y, en caso de que se haya producido, que identifiquen y detengan el autor para que pueda recibir el castigo correspondiente. A mayor gravedad del delito, mayor será la necesidad social de identificar al responsable y detenerlo, de manera que se le pueda aplicar la pena que el código penal impone por el delito cometido. A mi juicio, éste debe ser uno de los criterios para modular la proporcionalidad a la hora de actuar sobre un individuo para obtener su perfil genético: la gravedad del delito.

Trasladando el dilema de la proporcionalidad al uso de los datos genéticos debemos preguntarnos hasta qué punto el código genético de un grupo de personas relacionadas genéticamente puede ser interrogado en aras de identificar y detener un delincuente para que pague por el delito cometido y, en caso de reincidencia, que la investigación que se cierna sobre él sea más efectiva. Evidentemente debería haber un punto óptimo en el que la información genética de algunos individuos pudiera ser utilizada en investigaciones relativas a ciertos delitos en aras de salvaguardar la seguridad pública y los derechos del resto de los ciudadanos.

b. - Principio de razonabilidad.

El segundo principio que la autoridad judicial debe sopesar a la hora de extraer el perfil genético de una persona, es el de la razonabilidad. La decisión debe ser coherente, equilibrada y aceptada por la comunidad.

La extracción de perfiles de ADN del interesado está contemplado por la ley y su finalidad - identificar autores de ilícitos penales - debe confrontarse con los medios empleados para la obtención de la muestra biológica, por un lado, y la introducción de dicho perfil en la base de datos para ser contrastado, por otro.

Si el investigado niega su colaboración en el acto de intervención corporal para obtener las muestras, el juez *"podrá imponer la ejecución forzosa de tal diligencia mediante el recurso a las medidas coactivas mínimas indispensables, que deberán ser proporcionadas a las circunstancias del caso y respetuosas con su dignidad"*³⁸⁴. Pero la Ley de Enjuiciamiento Criminal no especifica si se puede recurrir al uso de la fuerza física si fuera necesario o ese precepto indica una amenaza de denuncia por desobediencia a la autoridad judicial³⁸⁵.

Si no aporta una justificación o explicación suficiente, dicha negativa nunca equivaldrá a la negativa que tiene a no declarar³⁸⁶ y no se tendrá en cuenta en la valoración de la prueba. Puesto que es una prueba que no reporta ningún menoscabo físico y la valoración de dicha prueba puede ser tanto inculpatoria como exculpatoria, todo y no ser probatoria, *"conectado con el resto de la prueba puede reforzar las conclusiones obtenidas por el órgano juzgador"*³⁸⁷. En cambio, en el Derecho Civil español la *"negativa injustificada a someterse a la prueba biológica de paternidad o maternidad permitirá al tribunal declarar la*

384 Art. 520.2bis.6.c de la Ley de Enjuiciamiento Criminal.

385 Art. 556 del Código Penal.

386 STEDH de 17 de diciembre de 1996. Caso Saunders c. Reino Unido, párrafo 69.

387 Apartado 3.5 de la STS 107/2003 de 4 de febrero.

filiación reclamada, siempre que existan otros indicios de la paternidad o maternidad y la prueba de ésta no se haya obtenido por otros medios"³⁸⁸.

Según el Tribunal Supremo, la autorización judicial de ningún modo puede legitimar actos violentos o de compulsión personal con la finalidad de obtener dicha muestra³⁸⁹. Pero el Tribunal Constitucional parece ser un poco más laxo en esta afirmación, con lo que se abre un interesante debate.

Todo y que la Constitución Española no prevé la posibilidad de limitar el ejercicio de los derechos a la integridad física y a la intimidad³⁹⁰, el Tribunal Constitucional no entiende que sean derechos absolutos y éstos pueden ceder ante determinados supuestos previstos por ley. Así pues, el derecho a la intimidad corporal del que todo individuo disfruta, puede ceder ante una resolución judicial dictada en aras de identificar vestigios de un presunto delito en el marco de una investigación penal. Será así siempre y cuando dichos vestigios no puedan ser obtenidos de otro modo³⁹¹,

³⁸⁸ Art. 767.4 Ley de Enjuiciamiento Civil.

³⁸⁹ Aparado 2.1 de la STS 685/2010 de 7 de julio.

³⁹⁰ Como sí lo hace el CEDH en relación al derecho a la vida privada y familiar

³⁹¹ Aplica el vigésimo tercer principio que recoge el Proyecto de reglas mínimas de las Naciones Unidas para la administración de la Justicia Penal: "*Toda intervención corporal está prohibida salvo que se cuente con el consentimiento del afectado. Sin embargo y sólo cuando no exista otro medio para descubrir el presunto delito, la autoridad judicial podrá acordarla, atendida la gravedad del mismo y la falta de peligro para la salud del afectado.*"

que esté amparada por ley y que no se obtengan imponiendo un trato degradante a la persona³⁹². Ello nos lleva a que dicha resolución judicial debe estar especialmente motivada y ser idónea, necesaria y proporcional en relación con un fin constitucionalmente legítimo³⁹³.

A mi juicio, a la pregunta de si es posible utilizar la fuerza física para obtener muestras biológicas de un imputado debe responderse que sí: para ello es necesario una resolución judicial motivada que precise las muestras a tomar, el método que se debe utilizar y, en caso necesario, hacer un uso de la fuerza física razonable y estrictamente necesaria. Dado que se actuará coercitivamente sobre un individuo, dicha coerción no puede ser arbitraria y bajo ningún concepto degradante. Podrían aplicarse métodos poco invasivos, como por ejemplo, aplicar una cinta adhesiva en alguna parte del cuerpo del individuo para que cuando sea arrancada, se arranque con ella células epiteliales. La fuerza a aplicar sería la necesaria para inmovilizar al sujeto.

En cambio la doctrina no lo tiene tan claro. La obligación que se impone al investigado a que coopere facilitando muestras biológicas, algunos autores lo ven como un trato inhumano y degradante y opinan que puede ver vulnerado su derecho a

392 STC 37/1989 de 15 de febrero.

393 MARTIN PATOR J. (2013), p. 213

no declararse culpable³⁹⁴ y que de su negativa a facilitar las muestras no se puede derivar ninguna consecuencia negativa en su contra³⁹⁵. Además, la obligación que impone el art. 118 CE de colaboración con la justicia, no puede exigir una colaboración activa en la realización de actos que puedan inculpar a un sujeto³⁹⁶.

5.4.- Muestra atribuida.

Para la investigación de delitos graves, la policía judicial puede obtener muestras y fluidos del sospechoso, detenido o imputado. Si para la toma de estas muestras se requiere inspecciones, reconocimientos o intervenciones corporales, se necesitará el consentimiento del afectado o autorización judicial, tal como se ha explicado en los puntos anteriores. Pero existe una tercera vía por la que la Policía Judicial puede obtener el perfil genético de una persona y es la de recoger restos biológicos abandonados por dicho sujeto.

Al tratarse de toma de muestras que están separadas del cuerpo, no se vulnerarían ni el derecho a la integridad física ni a la intimidad corporal. El Tribunal Supremo admite que "*la Policía Judicial puede recoger restos genéticos o muestras biológicas abandonadas por el sospechoso sin necesidad de*

394 art. 24 de la CE.

395 JAEN VALLEJO (2004), p. 122 y 123.

396 KAPPLER (2011), p. 72.

autorización judicial". De esta manera, una colilla tirada por el sospechoso se trata de una "*res nullius*" y puede ser recogida por la policía para que la utilice como un instrumento para investigar delitos³⁹⁷. Es más, incluso estando detenido el investigado, la policía judicial puede recoger los vestigios biológicos que éste tira o utiliza, siempre y cuando el abandono no se haya producido utilizando sobre él violencia física o moral alguna, ni haber sido objeto de engaño. Así, se puede dar la circunstancia que un detenido que ha negado su consentimiento para que se le extraiga una muestra biológica, se le puede vigilar y esperar a que deseche algún objeto en el cual haya dejado restos biológicos que puedan ser analizados. El Tribunal Constitucional entiende que se dan circunstancias excepcionales que justifican esta acción dado que, todo y que constituye una injerencia en el derecho fundamental a la intimidad, persigue un fin constitucionalmente legítimo - la investigación de un delito - y goza de cobertura legal³⁹⁸. Incluso el TEDH avala esta práctica cuando "*está destinada a vincular a una persona determinada con un delito concreto que se sospecha que ha cometido*", pero no permite su conservación en una base de

397 Apartado 3 de la STS 179/2006 de 14 de febrero. Pero también en la STS 685/2010 de 7 de julio, STS 1190/2009 de 3 de diciembre, STS 701/2006 de 27 de junio, STS 949/2006 de 4 de octubre y STS 1267/2006 de 20 de diciembre.

398 Al respecto véase la STC 199/2013 de 5 diciembre.

datos para consultas futuras³⁹⁹. Por tanto, es necesario que ese individuo esté siendo investigado por un delito concreto y el perfil genético obtenido solo podrá compararse con las muestras biológicas de ese hecho.

Ésta es una importante y útil herramienta de investigación. Así, cuando la policía dispone de un perfil de ADN encontrado en el lugar de los hechos y hay una o varias personas sospechosas, existe la opción de obtener el perfil genético de las personas sospechosas y compararlo con las muestras encontradas. Si no se quiere poner en alerta al sospechoso, una diligencia de investigación habitual a la que se recurre es hacerle vigilancias y seguimientos hasta que se le ve tirar o abandonar algún objeto que pueda tener restos biológicos con material genético, el cual será analizado y cotejado con la muestra hallada en el lugar de los hechos. Los objetos que se suelen recoger son vasos de un bar de donde el sujeto objeto bajo investigación los haya utilizado para beber, colillas, pañuelos, restos de comida,... Utilizando esta técnica, el sujeto de interés no es consciente que está siendo investigado y, quizás, si se descartara su participación en los hechos, podría no llegarlo a saber nunca.

399 STEDH de 4 de diciembre de 2008. Caso Marper c. Reino Unido, párrafo 100.

La muestra atribuida debe ser tratada como una muestra dubitada y debe servir solamente como línea de investigación. El Tribunal Supremo⁴⁰⁰ considera que la recogida de muestras indubitadas debe hacerse con todas las garantías legales dado que el acto tendría carácter probatorio puesto que debe acreditarse la pertinencia de la muestra a esa persona en concreto, lo cual puede resultar difícil en las muestras atribuidas. Así, en el análisis de laboratorio de éste tipo de muestras se puede hallar más de un perfil genético o que haya habido un error con el objeto en cuestión y en él no se encuentre el perfil del sospechoso, sino el de otra persona. Por poner un ejemplo, en una taza de café recogida de un bar, puede haber restos genéticos de la persona de interés, pero también del camarero que la sirvió en la mesa, del que hizo el café o del que secó la taza. Por tanto, los resultados obtenidos a partir de muestras atribuidas deben ser tratadas como indiciarias.

Así, una vez se ha confirmado que el perfil genético de la muestra atribuida coincide con las muestras obtenidas en el lugar de los hechos, se debe obtener una muestra indubitada del sujeto objeto de investigación con todas las garantías legales – ello es con consentimiento o autorización judicial -, para volver a compararla con la del lugar de los hechos.

400 Las STS 501/2005 de 19 de abril y STS 1311/2005 de 14 de octubre.

La obtención de perfiles genéticos a partir de este tipo de muestras no está exento de polémica. Así, las autoridades policiales pueden utilizar estratagemas para conseguir una muestra biológica de una persona que, por ejemplo, se ha negado a facilitar una muestra biológica a las autoridades. Nada impide introducir el perfil genético obtenido de esta forma en las bases de datos policiales como muestra dubitada y compararla con los obrantes en el sistema para después borrarlo. Todo y que el TEDH no critica el uso de argucias⁴⁰¹ por parte de la policía para luchar contra actividades criminales de manera más efectiva, parece que este método no debería ser la tónica general.

Por otro lado, el tratar los objetos que se van a analizar para extraer un perfil genético a una persona como “abandonados” no parece muy acertado, ya que es imposible que una persona no vaya dejando rastro de su ADN a lo largo de su vida cotidiana. Es imposible que un individuo vaya recogiendo todos los objetos que ha ido utilizando a lo largo del día y que pueden contener muestras biológicas suyas⁴⁰². Eso supondría, por ejemplo, ir a comer a un

401 "*Although the Court by no means excludes its being legitimate for the police to use stratagems in order, for instance, to counter criminal activities more effectively*". STEDH de 5 de febrero de 2002. Čonka c. Bélgica, párrafo 41.

El Tribunal hace referencia a que la policía belga citó a una serie de personas para rellenar un formulario en una comisaria y una vez allí los detuvieron.

402 La popstar Madonna contrata un equipo para esterilizar su camerino después de cada actuación para evitar dejar objetos de los que se pueda obtener ADN.

restaurante y salir de él con todos los elementos de cubertería utilizados o no utilizar nunca ningún objeto de un solo uso y tirarlo a la basura, previamente debería desinfectarse. Y si tenemos en cuenta los pelos o los restos de piel seca que van cayendo del cuerpo a lo largo de la vida sin ser conscientes, hacen de ello una tarea prácticamente imposible.

Si una persona quiere que nadie sepa que contiene su teléfono móvil o sus registros informáticos, los puede proteger con contraseña, borrarlos o destruir el hardware que los contiene. En cambio, con las muestras biológicas que vamos perdiendo y dejando en el camino solo cabe la destrucción. No hay otra forma de ocultar nuestro código genético más que destruyendo dichas muestras, de las cuales no somos conscientes de ir dejando. Por lo tanto, los seres humanos no tenemos otra opción que ir “*abandonando*” ADN en distintos sitios a lo largo de la vida, existiendo la posibilidad que cualquier persona lo pueda obtener.

Por eso, en mi opinión, es discutible que una muestra abandonada por un individuo y recogida para estudiar su contenido biológico, pueda ser tratado de la misma manera

<https://www.mirror.co.uk/3am/weird-celeb-news/madonna-appoints-dna-team-sterilise-907641> (última consulta 14/3/2022).

que el que tira una bolsa de basura. La recogida de la muestra en sí debe ser legal y es a lo que la ley se refiere cuando hace referencia a que la Policía Judicial puede recoger objetos abandonados por el sospechoso o en la escena del crimen, pero estas muestras deberían tener una protección especial en cuanto a la información genética que puedan contener. En ellas hay información sensible de la persona investigada y de sus familiares biológicos, y dado que se van a vulnerar derechos fundamentales creemos que dicha diligencia debería llevarse a cabo bajo la tutela judicial⁴⁰³.

Las autoridades policiales actuarán de urgencia para salvaguardar la muestra biológica del sujeto, que la recogerán cuando el sujeto la abandone. Pero el análisis de dicha muestra debería llevarse a cabo bajo la autorización judicial. Posteriormente, cuando la investigación lo permita, debería obtenerse una muestra indubitada para realizar el análisis y poder confirmar el resultado obtenido con la muestra atribuida. De esta manera se salvaguardaría también el hecho de que el abogado del interesado no estuviese presente durante ningún momento de esta

⁴⁰³ Hay autores que mantienen esta opinión. Por ejemplo Juan José López Ortega, en "La tutela de la intimidad genética en la investigación penal. A propósito de la STC 199/2013 y de la SAP Sevilla 650/2013" en el libro "*ADN forense: problemas éticos y jurídicos*" CASADO M. y GUILLEN M. (2011) p. 110.

diligencia. Resulta poco coherente que el abogado de un detenido o un imputado esté presente cuando éste deba dar su consentimiento para extraerle una muestra genética y en cambio, no sea necesario para dar validez al análisis de una muestra obtenida subrepticamente del investigado, sin que ni él mismo interesado tuviera conocimiento.

De esta manera se blindaría el acceso a la información genética de las personas al cual solo se podría acceder con consentimiento del interesado, en los casos permitidos por la ley o por autorización judicial. La información que contienen las muestras biológicas acerca de un individuo es lo suficientemente importante como para mantenerla salvaguardada y evitar que se haga un mal uso.

5.5.- Almacenamiento de las muestras.

En la sentencia *S. y Marper c. Reino Unido*, el TEDH considera que la conservación y tratamiento de muestras biológicas - cuya finalidad es la obtención de perfiles genéticos - y la de los propios perfiles genéticos en sí, suponen una intromisión en la vida privada en los términos que recoge el art. 8 del CEDH. Por un lado, las muestras biológicas contienen información sensible relativa a una persona, entre la que hay información sobre su salud y la de

su familia biológica. Por otro lado, aunque el perfil genético esté compuesto de datos numéricos y contenga menos información que las muestras en sí, dicha combinación numérica permite ir más allá de la simple identificación neutra de un individuo ya que pueden obtenerse datos referentes a componentes étnicos o familiares, por ejemplo.

La información genética no es de ningún modo comparable con la información que se puede obtener a partir del estudio de las huellas dactilares de un individuo. Los lofogramas son comparados mediante una codificación numérica también, pero solo pueden servir para identificar a un individuo cuando es comparado con otras huellas dactilares de otro individuo, nada más. De la información obtenida no se puede extraer ningún dato más de otros individuos con los que esté relacionado familiarmente, por muchas combinaciones que se hagan con la huella dactilar.

En cambio, la información que puede proporcionar una muestra genética es enorme: datos de salud, de parentesco, características físicas,... toda la información referente al individuo están en ellas. Por este motivo, siguiendo con *Marper*, dado que se produce una intromisión en la información genética de un individuo no se puede producir un almacenamiento de más datos de los necesarios para el

propósito que se busca, ni éstos deben ser almacenados por un periodo de tiempo excesivo.

La finalidad de analizar las muestras biológicas **indubitadas** es la de obtener un perfil genético identificador de un individuo que será introducirlo en las bases de ADN policiales y se confrontará con perfiles genéticos anónimos para encontrar coincidencias. Así, una vez obtenido el perfil genético de una muestra indubitada, la conservación física de la muestra en sí - el hisopo - parece no tener sentido. Por tanto, todos los hisopos obtenidos de un individuo, tenga el rol que tenga en el proceso judicial, una vez analizados deberían ser destruidos.

Cuando se trata de muestras biológicas **dubitadas** obtenidas en el lugar de los hechos, la cosa cambia. Como se verá en el siguiente capítulo, las técnicas de análisis de ADN están avanzando a gran velocidad. Lo que actualmente sería un análisis para cuerpos policiales con elevados presupuestos, en pocos años pueden resultar económicamente asequibles para una investigación en cuerpos policiales con presupuestos más modestos. Así, volviendo a analizar dichas muestras se podrían obtener nuevos marcadores genéticos respecto de una misma muestra. Los marcadores genéticos han ido cambiando a lo largo de la historia de la genética

forense y cada vez puede obtenerse más información de una muestra con posteriores análisis; por ejemplo, si se analizan más marcadores, puede realizarse una búsqueda familiar más eficiente u obtener algunos rasgos étnicos o familiares que, cuando tuvieron lugar los hechos, no eran técnica o económicamente viables. De esta manera, se puede conocer el color del pelo o de los ojos de la persona que dejó restos biológicos en el lugar del crimen, elementos que pueden ayudar en la investigación policial tendente a identificar el autor. Una vez el donante de la muestra dubitada se convierte en muestra indubitada - porque el autor ha sido identificado - y el procedimiento penal lo permite, dicha muestra debería ser destruida para evitar la vulneración de derechos fundamentales. En el siguiente capítulo se abordan distintos tipos de análisis que pueden realizarse a las muestras genéticas y la limitación de ciertos derechos fundamentales que pueden suponer dichos análisis, si no se toman medidas legales al respecto.

La ley española da la potestad a la autoridad judicial a pronunciarse sobre la conservación de las muestras biológicas⁴⁰⁴. Sin distinguir si se trata de muestras dubitadas o indubitadas, la LO 10/2007 delega en el juez el pronunciamiento sobre el destino final de las muestras que

404 Art. 5.2 de la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN

están incluidas en su causa, cosa que raras veces sucede. En realidad, suele ser el propio laboratorio quien decide el tiempo que serán conservadas las muestras una vez analizadas y, seguramente, esta decisión no se tomará siguiendo parámetros de derechos fundamentales.

Los laboratorios acreditados que obtienen perfiles genéticos individualizados de las muestras biológicas, extraen de ella una muestra alícuota que será la analizada para obtener el perfil genético. Como se realizan decenas de análisis a la vez, cada muestra alícuota se coloca en uno de los pocillos de una placa. Las diferentes muestras que contiene la placa no tienen por qué guardar ninguna relación entre sí: suelen proceder de personas detenidas por distintos delitos o de distintos asuntos y son almacenadas todas juntas. De manera que las placas con las muestras ya analizadas, son congeladas y conservadas hasta que el laboratorio propietario de la muestra decide la destrucción de toda la placa. No hay ninguna autoridad independiente que vele por el tiempo que estas muestras deben ser almacenadas ni comprueban su destrucción. A mi juicio, se trata de una flagrante vulneración del art. 8 del CEDH, ya que el solo hecho de producirse la retención sistemática de material celular una vez obtenido el perfil genético del individuo, se

puede considerar una intromisión en el ámbito de este artículo⁴⁰⁵.

Una vez analizadas las muestras indubitadas y obtenido el perfil genético del individuo, el laboratorio debería destruirlas en un corto período de tiempo y no debería almacenarlas⁴⁰⁶. No tiene sentido la conservación de las muestras, ya que carecen de utilidad. En caso que la persona propietaria del perfil indubitado alegara que hubiera algún error en el análisis de la muestra, siempre podría ceder una nueva muestra para llevar a cabo los contra-análisis.

El ENFSI⁴⁰⁷ aconseja que la destrucción debe llevarse a cabo de manera verificable, incluyendo el motivo de la destrucción. Debe destruirse las muestras con sus alícuotas, los perfiles genéticos obtenidos y su electroferogramas⁴⁰⁸.

En el caso de muestras dubitadas, sí que es interesante conservar la muestra de la que se obtiene el perfil ya que, en

405 STEDH de 7 de diciembre de 2006. Van Der Velden c. Holanda.

406 Así queda recogido también en el art. 21.c de la Declaración Internacional sobre los Datos Genéticos Humanos de 16 de octubre de 2003 "*Los datos genéticos humanos, datos proteómicos humanos y muestras biológicas utilizados en medicina forense o en procedimientos civiles sólo deberían estar disponibles durante el tiempo necesario a esos efectos, a menos que la legislación interna compatible con el derecho internacional relativo a los derechos humanos contenga una disposición en contrario.*"

407 ENFSI - European Network of Forensic Science Institutes – organismo fundado en 1995 con el objeto de mejorar el intercambio de información en el campo de las ciencias forense a nivel europeo.

408 ENFSI (2017).

caso de identificar a quien pertenece, una de las partes del proceso podría solicitar un contra-análisis. Dichas muestras biológicas deben conservarse hasta la prescripción del delito, por lo que el dato obtenido a partir de ellas también. Más allá de éste periodo, no tendría sentido su conservación. Así, durante este periodo de tiempo - que puede durar décadas para delitos graves - las técnicas de investigación pueden mejorarse y abaratare. Por ejemplo, puede realizarse una *family search* - técnica que será analizada en el próximo capítulo - para lo cual, con toda probabilidad, será necesario realizar otro tipo de análisis para obtener otros marcadores con los que trabajar.

6.- Bases de datos de perfiles genéticos.

Como se ha comentado anteriormente, el TEDH ha afirmado en varias sentencias que almacenar información relativa a la vida privada de las personas está bajo el ámbito de protección del artículo 8.1 del CEDH⁴⁰⁹. Así, según este Tribunal, la injerencia de los poderes públicos en el derecho a la protección de datos debe cumplir los siguientes requisitos:

- 1.- Estar prevista por la ley.

409 Ver nota 61 del Capítulo 1.

2.- Ser una medida necesaria en una sociedad democrática para perseguir un fin legítimo.

En este sentido, el TEDH otorga un cierto margen de apreciación a cada estado, dándole poder discrecional para crear las normas.

3.- Los límites deben ser proporcionales para los fines perseguidos. *“Una restricción a un derecho consagrado por el Convenio debe ser proporcionada al fin legítimo conseguido”*⁴¹⁰.

Las bases de datos deben establecerse a partir de un régimen legal que esté *"de acuerdo con la ley"*. Según la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea, y en referencia a las bases de datos policiales, los principios fundamentales para tal fin son⁴¹¹:

1.- la creación de poderes policiales debe ser publicada y accesible al público;

410 STEDH de 18 de octubre de 1982. Caso Young, James y Webster c. Reino Unido, párrafo 63.

411 STEDH de 24 de enero de 2019. Caso Catt c. Reino Unido, párrafo 87.

STEDH de 2 de septiembre de 2008. Caso Landen c. Suecia, párrafo 51.

STJUE de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 19.

STJUE de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartados 54 y 55.

2.- se requieren salvaguardas claras y de acceso público para garantizar que la interferencia no ocurra de manera arbitraria, inapropiada o innecesaria;

3.- debe haber criterios claros y accesibles que permitan a las personas, cuyos datos personales se almacenan, asegurar su eliminación, incluso mediante una revisión independiente;

4.- se debe eliminar la información relacionada con aquellos que no son sospechosos de actividad criminal.

6.1.- Marco normativo de la introducción de perfiles genéticos en las Bases de datos policiales de ADN en España ⁴¹².

En España, la introducción y almacenamiento de perfiles genéticos en bases de datos policiales viene determinado por tres normas:

1.- Código Penal.

⁴¹² La información técnica utilizada para redactar esta parte del capítulo procede del "Manual técnico de procedimiento del sistema de gestión nacional de identificadores obtenidos a partir de ADN (SIGENI) editado por el Ministerio del Interior." La versión utilizada es la 7.1.

Una de las consecuencias accesorias que establece el Código Penal español a la comisión de un delito es el almacenamiento en bases de datos de perfiles genéticos de **personas condenadas**.

Dicho almacenamiento puede ser por dos vías⁴¹³:

- por la *comisión de ciertos delitos graves: delito grave contra la vida, la integridad de las personas, la libertad, la libertad o indemnidad sexual, de terrorismo, o cualquier otro delito grave que conlleve un riesgo grave para la vida, la salud o la integridad física de las personas.*

- la existencia de un peligro relevante de reiteración delictiva atendiendo a *las circunstancias del hecho, antecedentes, valoración de su personalidad o de otra información disponible.*

Así, atendiendo al delito cometido o existiendo un peligro relevante de reiteración delictiva, el juez o tribunal podrá acordar la toma de muestras biológicas del condenado y la realización de análisis para la obtención de identificadores de ADN e inscripción de los mismos en la base de datos policial.

413 Art. 129.bis de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

2.- Registro Central de delincuentes sexuales.

La Ley 26/2015 de 28 de julio, de modificación al sistema de protección de infancia y adolescencia crea el Registro Central de delincuentes sexuales en el Registro Central de Penados y en el Registro Central de Sentencias de Responsabilidad Penal de los Menores en el cual se incorporaran los "datos relativos a la identidad y perfil genético (ADN) de las personas condenadas por los delitos contra la libertad e indemnidad sexuales, en los que incluyen la agresión y abuso sexual, acoso sexual, exhibicionismo y provocación sexual, prostitución y explotación sexual y corrupción de menores".

Dichas bases de datos son gestionadas por la Secretaria de Estado de Justicia y no entran en el ámbito de estudio de este trabajo.

3.- Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

Esta ley amplia enormemente el rango de personas que deben ceder sus datos genéticos para que sean incorporados en las bases de datos policiales de perfiles genéticos. Si las dos normas anteriores se referían a

personas condenadas, es decir, que han pasado un procedimiento judicial, esta ley permite que se introduzcan perfiles de personas que sean consideradas "sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada"⁴¹⁴.

La consideración que tiene la persona en el proceso durante la instrucción policial, suele estar bajo el criterio del instructor del atestado policial, que es un agente de policía. Éste (1) decidirá el grado de implicación que tendrá un individuo en relación a los hechos y (2) realizará una primera tipificación penal de los hechos. Bajo estos dos criterios, dicho instructor decidirá si se debe extraer una muestra biológica de un individuo para obtener su perfil genético e introducirlo en la base de datos policial. Por tanto, la LO 10/2007 deja en manos policiales la decisión de extracción de la muestra y la inclusión en la base de datos genéticos, decisión que se toma en un estado inicial de la investigación policial y que, en

⁴¹⁴ Art. 3 de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN

la mayoría de casos, ocurre antes que empiece la instrucción judicial.

Un segundo aspecto que se le puede discutir a la ley, es la consideración que tiene la persona en relación al delito sobre el cual se le pide su perfil genético. Una primera consideración es la de *imputado*, que la ley define como "*persona sobre la que tan sólo recaen meras sospechas y por ello resulta investigado, pero respecto de la cual no existen suficientes indicios para que se le atribuya judicial y formalmente la comisión de un hecho punible*"⁴¹⁵. Por otro lado, el concepto de *detenido* también está claro. Una definición puede ser el de una persona que ha sido privada provisionalmente de la libertad por orden de la autoridad competente.

Más lagunas presenta la consideración de **sospechoso**, que el diccionario de la RAE utiliza las expresiones "*imaginar algo por conjeturas fundadas*" o "*considerar alguien como posible*" para definirlo. Así, no se requieren los requisitos legales que se precisa para ser considerado detenido o investigado. Hay que tener en cuenta que la persona sobre la

⁴¹⁵ Definición de imputado que se encuentra en el preámbulo de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta ley sustituye el concepto de *imputado* por el de *investigado* o *encausado*, dependiendo del momento procesal en que se encuentre la persona.

que recaen "*meras sospechas*" sería un *investigado* o *encausado* - aplicando la nueva nomenclatura -. Por tanto, un sospechoso es un concepto mucho más amplio que podría incluso ser definido en negativo: si una persona no es inocente, puede ser considerado sospechoso. Más rápido, seguro y fiable que comprobar coartadas es realizar pruebas de ADN - si se dispone de la muestra genética del presunto autor, claro -. De esta manera todos los habitantes de un pueblo pueden ser considerados sospechosos y se puede realizar pruebas de ADN a todos los vecinos.⁴¹⁶

Un agente policial puede sospechar de una persona en relación al delito investigado y ésta será considerada sospechosa. La condición de sospechoso puede desaparecer sin que quede siquiera reflejado en el procedimiento policial o judicial. Así, cuando se haya realizado las pruebas de ADN a una persona y se compruebe que no tiene nada que ver con el delito, dejará de ser considerada sospechosa. Ésta es una condición ampliamente utilizada por las autoridades policiales, de manera que bajo la excusa de cualquier sospecha se le puede solicitar a una persona que facilite una muestra

416 "*Someten a un análisis de ADN a todos los hombres de un pueblo para resolver un asesinato de 1996*" publicado en ABC. https://www.abc.es/internacional/abci-someten-analisis-todos-hombres-pueblo-para-resolver-asesinato-1996-201911260943_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F (última consulta 14/3/2022).

biológica para que se extraiga el perfil genético. La sospecha puede ser, por ejemplo, ser vecino de una víctima o pertenecer a su mismo círculo social.

Al tratarse de gestiones policiales que no han dado un resultado positivo para la investigación, no suelen reflejarse en el atestado policial y, por tanto, el juez puede no tener conocimiento de todos los análisis de ADN realizados. A mi criterio, cualquier actuación de este tipo sobre una persona bajo la consideración de sospechoso, debería ponerse en conocimiento de la autoridad judicial para que de esta manera abale la actuación del instructor policial o, de lo contrario, la enmiende. Así el juez podrá comprobar la fundamentación de las sospechas y decidir si el perfil genético debe permanecer o, por el contrario, ser borrado de la base de datos.

Cuando el 2010 la Comisión Nacional para el uso forense del ADN aprobó el contenido mínimo de las actas de recogida de muestras biológicas para el análisis de ADN que utilizan la Cuerpos y Fuerzas de Seguridad del Estado en las que se deja constancia del consentimiento de la persona a la que se le recoge la muestra, se excluyó expresamente la figura del *sospechoso* en el formulario⁴¹⁷. Así, la recogida de muestras

417 Ministerio de Justicia (2012), p. 18

biológicas se hace a las personas que se les da el rol de investigado/detenido durante la investigación policial.

Bajo mi criterio, sería más razonable comparar el perfil genético del investigado/detenido con las muestras dubitadas del caso concreto en el que tiene uno de estos roles de forma que, si resultara condenado, el perfil genético se inscribiría en la base de datos; por contra, si resultara absuelto o sobreseído el caso, el perfil sería eliminado. Así lo establece la Recomendación del Consejo de Europa R (92)⁴¹⁸.

Finalmente, con base en la LO 10/2007, también podrán inscribirse en las bases de datos policiales el perfil genético de las personas que han expresado su consentimiento para tal efecto, además de los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas.

Sorprende que esta ley no haga referencia a las personas condenadas por delitos graves, aunque ya está contemplado en el Código Penal, pero hubiera sido una buena ocasión para evitar la dispersión de normas. Tampoco hace referencia

⁴¹⁸ Art. 8 de la Recomendación núm. 1 (1992) del Comité de Ministros del Consejo de Europa a los estados miembros, sobre la utilización del análisis de ácido desoxirribonucleico (ADN) dentro del marco de la administración de justicia penal.

a los datos que ya están introducidos en la base de datos con anterioridad a la entrada en vigor de la ley.

Los ficheros que contengan este tipo de datos deberán someterse a la Directiva 2016/680 explicada en el capítulo anterior, dado que son datos que pertenecen a personas identificables. Pero hasta que la muestra dubitada no se convierta en una muestra indubitada, es decir, que sea identificada, algunos principios de la protección de datos no podrán ser aplicados. Por ejemplo, no se podrá adjudicar la condición de titular de derechos a ninguna persona. De esta manera nadie puede ejercer el derecho de cancelación o supresión de los datos, el de rectificación, información o de acceso, ya que la ley solo habilita al interesado y éste es desconocido.

6.2.- Creación de Bases de datos policiales de ADN en España.

Con la firma del Tratado de Prüm, España se comprometió a "*crear y mantener ficheros nacionales de análisis del ADN para los fines de la persecución de los delitos*" mediante "*una consulta automatizada de los perfiles de ADN*"⁴¹⁹. Así el año 2007 se crea en España la Base de datos policial sobre

419 Art. 1 y 2 del Tratado de Prüm.

identificadores obtenidos a partir del ADN⁴²⁰ que integra las bases de datos que tenían en esa época las Fuerzas y Cuerpos de Seguridad (FCS) relativas a investigación y averiguación de delitos y las de identificación de restos cadavéricos o de averiguación de personas desaparecidas. Depende de la Comisión Nacional para el uso forense del ADN⁴²¹, órgano que a su vez depende de la Secretaria de Estado del Ministerio del Interior, de manera que su control queda al margen de la Agencia Estatal de Protección de Datos.

En estas bases de datos se inscribirán:

- Los perfiles genéticos obtenidos de los sospechosos, detenidos o imputados de delitos graves⁴²², tanto los procedentes de muestras genéticas halladas en la escena del crimen - dubitados -, como las muestras indubitadas y las atribuidas.

420 Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

421 Art. 3 del Real Decreto 1977/2008, de 28 de noviembre, por el que se regula la composición y funciones de la Comisión Nacional para el uso forense del ADN.

422 Art. 3.1.a de la Ley Orgánica 10/2007 - Se trata de delitos que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados.

- Los perfiles genéticos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas y que sólo podrán ser utilizados en la investigación para la que fueron obtenidos.
- Perfiles genéticos de los cuales se dispone el consentimiento expreso del interesado que autoriza a la inclusión en la base de datos.

Se fusionaron las distintas bases de datos policiales de ámbito criminal y las de ámbito humanitario. De esta manera se creó⁴²³ el **INT-SAIP** (para asuntos de interés criminal) e **INT-FÉNIX** (para asuntos de personas desaparecidas y cadáveres sin identificar) a la que aportan datos las siguientes instituciones:

- Comisaria General de Policía Científica del Cuerpo Nacional de Policía.
- Servicio de Criminalística de la Guardia Civil.
- División de Policía Científica del Cos de Mossos d'Esquadra.
- Unidad de Policía Científica de la Erztaintza.

⁴²³ Orden INT/177/2008 de 23 de enero por la que se modifica la Orden INT/3764/2004 de 11 de Noviembre por la que se adecúan los ficheros informáticos del Ministerio del Interior que contienen datos de carácter personal a la Ley Orgánica 15/1999 de 13 de Diciembre de protección de Datos de Carácter Personal y se crean nuevos ficheros cuya gestión corresponde a dicho Ministerio.

- División de Policía Científica de la Policía Foral de Navarra.
- Instituto Nacional de Toxicología y Ciencias Forenses.

6.3.- Bases de datos de ADN de investigación criminal. LDIS - Local DNA Index System - y SDIS - State DNA Index System -.

Cada una de las instituciones mencionadas anteriormente inscribe los perfiles de ADN procedentes de las muestras biológicas analizadas por sus respectivos laboratorios homologados en su servidor local, también conocido como LDIS. Los perfiles son cotejados de forma sistemática, utilizando el software CODIS - Combined DNA Index System - en busca de coincidencias. La gestión del fichero corresponde a la institución donde está instalado, a la vez que será la propietaria y responsable de la veracidad de los datos introducidos a los efectos de la L.O. 3/2018, de 5 de diciembre, la L.O. 10/2007, de 8 de octubre y la L.O. 7/2021, de 26 de mayo.

Cuando un perfil genético es introducido en la base de datos es codificado asignándole alguno de los siguientes roles:

- **Sospechoso** - Muestra indubitable de un detenido o investigado.

- **Víctima** - Perfil indubitable de una víctima, testigo o perjudicado.

- **Muestra forense de origen desconocido** - Perfiles dubitados procedentes de la escena del crimen o muestras atribuidas.

- **Personal** - Corresponde a perfiles genéticos de personas que trabajan en el ámbito de policía científica. Su función es la de detectar posible contaminación de las muestras por manipulación defectuosa.

- **Familiar** – Corresponde a perfiles genéticos de familiares de personas desaparecidas utilizados en investigaciones humanitarias.

En los LDIS se lleva a cabo un primer cotejo de las muestras dependiendo de los roles asignados. De esta manera se descartan muestras forenses de origen desconocido que contengan perfil genético de agentes de la policía científica que han trabajado en el caso o de personal de laboratorio. También se desecharán los perfiles genéticos que coincidan

con los perfiles de víctimas, analizando cada *match* o coincidencia individualmente.

Aunque se trate de una muestra biológica facilitada como víctima, es relativamente sencillo que sea comparada con los perfiles dubitados existentes en la base de datos y que se pueda llegar a obtener una coincidencia en otro caso distinto como presunto autor. Estamos en un mundo computerizado y los análisis comparativos son llevados a cabo por máquinas, así que, si una persona que está involucrada en un proceso penal como víctima o testigo da su consentimiento para que su perfil genético sea comparado con los perfiles genéticos obtenidos de la escena de un crimen concreto, es muy fácil comparar ese perfil genético de víctima con todos los obrantes en la LDIS de ese cuerpo policial. Dependerá de la política del laboratorio o del cuerpo policial, el que esa información llegue a manos de los investigadores. De ser así, los investigadores no podrán utilizar dicha coincidencia como prueba y deberán empezar la investigación al revés: sabiendo quien es el autor, deberán encarar la investigación de manera que puedan obtener su perfil genético legalmente y sea comparado con los hallados en esa escena del crimen.

Los LDIS están conectados por la red SARA con el servidor estatal, conocido también por SDIS, base de datos de ADN a

nivel estatal, donde también se realiza una búsqueda sistemática de coincidencias. Cualquier coincidencia que se produzca, el SDIS informará a los LDIS involucrados para que se pongan en contacto.

En el fichero de interés criminal INT-SAIP del sistema SDIS se incluirán los siguientes perfiles genéticos:

- **Perfil genético procedente de muestras forenses de origen desconocido** que no hayan sido identificadas en la LDIS.

Si en un mismo caso se han detectado varias veces un mismo perfil, se remitirá a la SDIS una única vez. En cambio, si un mismo perfil se han detectado en diversos casos, será remitido una vez para cada caso, dejando constancia de todos los casos en los que ha sido detectado - perfil reincidente -.

- **Sospechoso** - Muestra indubitada de un detenido o investigado.

- **Víctima** - Perfil indubitado de víctimas, testigos o perjudicados que han dado su consentimiento para que sean introducidas en la base de datos y se crea conveniente su introducción.

En el SDIS los perfiles están asociados a un código identificador anónimo y a una referencia de laboratorio; nunca se comparten datos personales. A él no se envían los perfiles genéticos del personal del cuerpo de policía ni las de las persona que han facilitado su perfil genético como víctimas, testigos o perjudicados, a no ser que exista su consentimiento.

En virtud del Tratado de Prüm, los perfiles de ADN contenidos en el SDIS son cotejados periódicamente con otras bases de datos de ADN de los otros países que han suscrito el tratado.

En el fichero de interés social INT-FENIX - bases de datos de ADN de personas desaparecidas y restos cadavéricos - del sistema SDIS se incluirán:

- Perfil genético de muestras de cadáveres y restos humanos no identificados así como las de los cadáveres incompletos estén o no identificados, por si aparecieran restos de estos cadáveres incompletos.
- Perfil genético procedente de muestras antemortem de un desaparecido. Por ejemplo procedentes de cepillo de dientes, maquinilla de afeitar,...

- De familiares de las personas desaparecidas.
- Personas vivas no identificadas. Por ejemplo personas en coma o amnésicas.

Los datos procedentes de personas de interés criminal y los de personas desaparecidas y restos cadavéricos se integran en una única base de datos, hecho criticable, más si se tiene en cuenta que dicha base de datos no depende de un órgano independiente a la estructura policial.

6.4.- Sistema CODIS - (Combined DNA Index System) -

Se trata de un software que ha sido desarrollado por el FBI para la gestión de las bases de datos LDIS y SDIS. El sistema actualmente trabaja con:

- 23 marcadores STRs autosómicos para la base de datos nacional SDIS. Entre ellos se encuentran los 12 marcadores incluidos en el estándar europeo ESS y sobre los que los laboratorios acreditados han de realizar obligatoriamente los análisis.
- 27 Marcadores STRs del cromosoma Y (Y-STRs). Son los marcadores aceptados en la base de datos YHRD (Y chromosome haplotype reference database)

considerada internacionalmente como base de datos de referencia.

- Polimorfismos de ADN mitocondrial (mtDNA). Como mínimo se analizarán dos regiones del ADN mitocondrial.

La calidad de la muestra biológica y el tipo de kit comercial con el que se analice dicha muestra determina los marcadores concretos que serán introducidos en el CODIS. Así, para los STRs autosómicos se introducirán un mínimo de 13 marcadores en el caso de muestras indubitadas o de 9 marcadores para las muestras dubitadas, incluyendo las que exige el ESS. Para el análisis del cromosoma Y, se requerirán 15 y 9 marcadores respectivamente, y para el ADN mitocondrial será necesario el análisis de las dos regiones.

En cuanto a las muestras en las que se detectan mezclas de perfiles genéticos, el CODIS solo permite introducir perfiles de dos contribuyentes, es decir, con cuatro alelos por marcador. Para el análisis del cromosoma Y y del ADN mitocondrial, no se pueden introducir mezclas de perfiles.

Cuando el perfil sea introducido al CODIS:

1.- Se le asignará un código, de manera que solamente la institución que gestiona dicho perfil será la conocedora de toda la información de procedencia de dicho perfil. Este código estará formado de tres partes, una de las cuales hace referencia al tipo de asunto, o motivo por el que se tramita el perfil. En el caso de perfiles que se introducen en el INT-FENIX el código es IS - interés social -; en el INT-SAIP hace referencia al tipo de delito. - HO - Homicidio, AS - agresión sexual,...

2.- Se introducirá de quien procede la muestra: Si procede de un sospechoso, víctima, investigado, detenido, de un indicio, de un resto cadavérico...

La procedencia del perfil genético es un dato básico para hacer búsquedas. Según de donde procedan, se lanzaran contra unos u otros. Así, los perfiles genéticos que provienen de restos cadavéricos se lanzaran contra los de familiares de personas desaparecidas, por ejemplo.

Aunque se trate de dos bases de datos independientes - INT-SAIP o criminal y INT-FENIX de interés social - ambas están en el mismo servidor, siendo la única diferencia el dato que hace referencia al tipo de asunto. Ello significa que técnicamente es sencillo lanzar un perfil contra todos los

datos de la base, independientemente de la procedencia del dato. Así los datos facilitados por los familiares de personas desaparecidas pueden lanzarse contra los perfiles obtenidos a partir de muestras localizadas en la escena del crimen o los perfiles de personas detenidas pueden ser lanzados contra la base datos de personas desaparecidas.

Si como resultado de una búsqueda se obtiene una coincidencia, serán informados los laboratorios implicados y ellos decidirán si esa coincidencia corresponde a un *match*. El positivo será revisado por dos analistas, uno de cada laboratorio al que pertenecen las muestras, que deberán validar la coincidencia. De ser así, los laboratorios se intercambiarán la información asociada al perfil genético⁴²⁴.

Si se confirma, los dos cuerpos policiales se ponen en contacto y se intercambian la información relativa a la identidad de la persona que ha facilitado su perfil genético. Se puede dar el caso de *match* de muestras forenses de origen desconocido, cosa que puede significar un mismo autor para dos hechos distintos. En este caso se

⁴²⁴ Muestra a partir de la cual se obtuvo el perfil genético y circunstancias de la misma, hecho delictivo de que se trata y circunstancias, unidad policial interviniente, unidad judicial que entiende del caso, informe pericial que se emitió, información alélica del perfil, se facilitarán todos los datos de filiación conocidos y cualquier otra información que se considere de interés.

intercambiarán información sobre los casos de los que proceden las muestras.

En el año 2020 se introdujeron en el CODIS 14689 muestras indubitadas en España y, a 31/12/2020 el sistema contenía 400.004 muestras⁴²⁵.

6.5.- Intercambio de perfiles genéticos a nivel internacional.

A mi entender, el principal escollo en el intercambio de perfiles genéticos a nivel internacional son las distintas legislaciones existentes en lo referente a la protección de datos. Si en el seno de la UE ya existen diferencias entre los distintos países en el modo de como se han obtenido e introducido los perfiles genéticos en las bases de datos de cada país o la ética involucrada en el modo de obtención, cuando ello se traslada a nivel mundial, las diferencias se agudizan. Así por ejemplo, en el marco del Tratado de Prüm, España no intercambia perfiles de juveniles (menores de edad detenidos entre 14 y 18 años), ni los correspondientes a víctimas conocidas, las personas desaparecidas y perfiles relativos a familiares. Pero no todos los países actúan del mismo modo.

⁴²⁵ Memoria Enero – Diciembre 2020 de la base de datos policial de identificadores obtenidos a partir de ADN, p. 15.

Para análisis involucrados en casos humanitarios no debería suponer un problema, ya que a mayor número de personas en las bases de datos, mayor probabilidad de identificar el perfil genético dubitado. Pero de tratarse una investigación criminal las cosas podrían ser distintas, ya que el uso de las bases de datos no es humanitario.

Además, distintos países significa distintos estándares de datos. No existe una armonización internacional de procedimientos de análisis de ADN. Cada país sigue su propia metodología, por lo que cada país tiene sus propios marcadores para determinar un perfil genético. Así, el Consejo de la Unión Europea estableció el ESS como estándar europeo, en el que serán un mínimo de 12 marcadores⁴²⁶ los que deben ser analizados en el ADN nuclear para obtener un perfil genético. En cambio, el sistema CODIS trabaja con 23 marcadores – entre los que están incluidos los de ESS -. Para aumentar la efectividad en el intercambio de perfiles genéticos a nivel internacional deberían armonizarse los distintos procedimientos de análisis forense de ADN y así evitar falsos positivos o coincidencias accidentales, ya que a mayor número de marcadores comparados, menor es la probabilidad de error en la identificación.

⁴²⁶ Resolución del Consejo de 30 de noviembre de 2009 relativa al intercambio de resultados de análisis de ADN (2009/C 296/01).

El intercambio de información a nivel internacional relativa a perfiles genéticos, puede llevarse a cabo a través de tres métodos⁴²⁷. Uno de ellos es a través de los acuerdos bilaterales existentes entre países que permitan dicho intercambio de información. Así, un país puede solicitar información de carácter genético a otro país enviando la solicitud de información. Por los cauces establecidos en los acuerdos bilaterales dicha información será traspasada de un estado a otro.

Los otros dos métodos son a través de bases de datos internacionales de perfiles genéticos o a través de bases de datos nacionales que están vinculadas entre sí o en red.

6.5.1.- Bases de datos internacionales de perfiles genéticos.

En estas bases de datos los distintos países van introduciendo datos genéticos sobre personas de su interés y de sus asuntos nacionales con la finalidad de obtener coincidencias con los datos aportados por otros países en esa misma base de datos.

Un ejemplo de estas bases de datos son las que disponen INTERPOL y EUROPOL.

⁴²⁷ MACHADO y GRANJA (2019).

- Interpol.

El intercambio de perfiles genéticos a nivel mundial entre varios países se realiza a través de Interpol, cuya función es desarrollar una asistencia recíproca entre las autoridades de policía criminal, que debe llevarse a cabo en el marco del respeto a la Declaración Universal de Derechos Humanos⁴²⁸.

Esta organización dispone de una base de datos de perfiles de ADN – **Interpol DNA database (IDD)** - creada en 2002 y que actualmente cuenta con unos 180.000 perfiles procedentes de 84 países. La IDD depende de un órgano independiente⁴²⁹, en la que los países miembros envían perfiles genéticos de delincuentes, de personas desaparecidas, de restos humanos no identificados y de perfiles localizados en lugares donde se ha producido un delito⁴³⁰. Los datos pertenecen al país que los ha enviado y, por tanto, decidirá sobre su envío, rectificación o cancelación, en función de su ordenamiento jurídico y solo podrán usarse con una finalidad determinada, explícita y conforme con los objetivos y actividades de la Organización, entre las que

428 Art. 2 del Estatuto de la Organización Internacional de Policía Criminal - INTERPOL.

429 Depende de la *Comisión de Control de los Ficheros*, art. 1 del Reglamento sobre el Control de la Información y Acceso a los Ficheros de Interpol.

430 Creada en 2002, la base de datos de INTERPOL sobre ADN contiene más de 180000 perfiles aportados por 84 países miembros.

<https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/ADN> (última consulta 14/3/2022).

están la búsqueda de personas con miras a su detención, la localización de personas u objetos de interés para la policía y la identificación de personas o cadáveres⁴³¹. La Oficina Central Nacional será la que velará para que los datos que se introduzcan en la base de perfiles genéticos sean de interés para la cooperación policial internacional⁴³² - al tratarse de datos especialmente delicados, deben presentar un valor criminalístico de especial importancia⁴³³ - y si hay autorización para introducir-los.

Los perfiles genéticos se guardan en la base de datos asociados a un código. En caso de coincidencia se pone en conocimiento de los dos países afectados, a los cuales se les invita a establecer una cooperación bilateral. De esta manera se asegura que solo participan de la identidad de la persona afectada los países involucrados⁴³⁴.

Como en el caso de coincidencias de perfiles genéticos en el entorno Prüm, los datos personales asociados a dicho perfil no viajan con él, sino que quedan en poder del país al que pertenecen, bajo sus normas de protección de datos personales.

431 Art. 10 del Reglamento de INTERPOL sobre el Tratamiento de Datos.

432 Art. 35 del Reglamento de INTERPOL sobre el Tratamiento de Datos.

433 Art. 42 del Reglamento de INTERPOL sobre el Tratamiento de Datos.

434 ALLEYNE L. (2009).

Todos los estados miembros de la UE pertenecen también a INTERPOL. Cuando se transmitan datos desde uno de estos países a INTERPOL, será de aplicación la Directiva (UE) 2016/680 en relación a lo dispuesto en materia de transmisiones internacionales de datos.

- Europol.

En 2005 Europol creó el **Sistema de Información de Europol (EIS)**, que se trata de una base de datos con información e inteligencia policial referentes a las materias en las que tiene competencia⁴³⁵ y dispone información referente a delitos internacionales graves, personas sospechosas y condenadas. Se utiliza para comprobar si existe información a nivel europeo de personas, hechos u objetos que estén relacionados con un caso. Se trata de información relativa a personas, armas, vehículos, números de teléfonos o pasaportes, por citar algunos ejemplos.

En el sistema se almacenan los perfiles genéticos que corresponden, por un lado, a personas que sean condenadas

⁴³⁵ Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo.

EUROPOL tiene como objetivo esencial las formas graves de delincuencia: delincuencia organizada, tráfico de drogas, trata de seres humanos o delitos informáticos y terrorismo.

o sospechosas de haber participado en un delito que es competencia de Europol, por otro, personas sobre las que existan indicios concretos o motivos razonables para pensar que cometerán estos delitos.

Aunque el sistema puede almacenar perfiles genéticos de personas pertenecientes al segundo grupo, no se permite que sean cruzados con otros datos⁴³⁶. La finalidad es la de llevar a cabo análisis estratégicos o temáticos, de análisis operativos o de facilitación del intercambio de información entre Estados miembros, Europol, países terceros y otras organizaciones.

En este caso también nos encontramos con que la legislación disponible no permite profundizar más en el término sospechoso o asociado a un sospechoso, ni que autoridad o agente puede darle este rol a una persona. Son términos que pueden quedar ambiguos y la decisión de incluirlos en una u otra categoría dependerá de la autoridad policial encargada de la investigación. Si a esta ambigüedad se le añade que Europol recibirá una gran cantidad de datos, no podrá discernir si su tratamiento se adecúa al ordenamiento jurídico hasta que los haya tratado, lo que puede implicar el procesamiento de datos personales que no se adecúen al anexo II del reglamento.

⁴³⁶ Anexo II del Reglamento (UE) 216/794.

Los datos pertenecen al país que los ha introducido y no pueden ser alterados por ningún otro miembro o la propia Europol, de manera que dicho país se hace responsable de los datos que ha introducido en el EIS.

6.5.2.- Bases de datos nacionales que están vinculadas o en red. El Tratado de Prüm.

En base a la Decisión JAI/615/2008, que integró la mayor parte del Tratado de Prüm, se pueden realizar comprobaciones automáticas entre perfiles genéticos procedentes de bases de datos de distintos países de la UE. La base de datos SDIS constituye el núcleo de intercambio de información con los organismos internacionales y países extranjeros.

La finalidad del Tratado de Prüm es identificar perfiles genéticos procedentes de muestras forenses de origen desconocido, denominado *STAIN* y que hacen referencia, principalmente, a muestras procedentes de personas no identificadas y de vestigios o indicios recogidos durante una investigación y que pertenecen a personas de las que se desconoce la identidad. Por otro lado, a los perfiles genéticos indubitados se denominan *PERSONAS* e incluyen los perfiles procedentes de: Detenidos, sospechosos, condenados,

cadáveres identificados, indistintamente se trate de muestras atribuidas o indubitadas.

La comparación genética a través de la Decisión Prüm, se lleva a cabo en dos pasos:

Primer paso:

Hay dos formas de realizar el cotejo de las bases de datos entre los diferentes países:

1.- Artículo 4³⁷: Se comparan los STAIN de un país, con los STAIN y PERSONAS que estén introducidas en el SDIS del segundo país.

Se aplica país a país: primero un país lanza todos sus datos contra todos los datos que contiene la base de otro país; luego se realiza la operación a la inversa. Se suele aplicar la

437 Art. 4 de la Decisión 2008/615/JAI, de 23 de junio: *"Las Partes Contratantes llevarán a cabo, de mutuo acuerdo y a través de sus puntos de contacto nacionales, una comparación de los perfiles de ADN de sus huellas abiertas con todos los perfiles de ADN contenidos en los índices de referencia de los demás ficheros nacionales de análisis del ADN, para los fines de la persecución de delitos. La transmisión y la comparación se efectuarán de forma automatizada. La transmisión para los fines de la comparación de los perfiles de ADN de las huellas abiertas únicamente tendrá lugar en los casos en que se prevea dicha transmisión en el derecho interno de la Parte Contratante requirente."*

primera vez que un país entra en producción; luego se hace de forma periódica⁴³⁸.

2.- Artículo 3⁴³⁹: Consiste en comparar perfiles - STAINS y de PERSONAS - de un país, contra los perfiles genéticos que están en producción en las bases de datos de todos los países de la UE. Se consultan los perfiles genéticos que un país va añadiendo en sus bases de datos, con los del resto de países.

Las coincidencias generadas en SDIS por una consulta PRÜM son enviadas a los laboratorios LDIS involucrados los cuales confirmarán la coincidencia. Una respuesta positiva indica la coincidencia de al menos seis locus completamente determinados de ambos perfiles genéticos⁴⁴⁰. Para confirmar la coincidencia de un perfil genético de un país con el perfil genético de otro país los laboratorios traspasan únicamente los perfiles genéticos – código alfanumérico – y un código asociado al perfil.

438 Por ejemplo, entre las bases de datos de Francia y España se realiza cada tres meses aproximadamente.

439 Art. 3 de la Decisión 2008/615/JAI, de 23 de junio: "*Las Partes Contratantes permitirán que los puntos de contacto nacionales de las demás Partes Contratantes a que se refiere el artículo 6 tengan acceso, para los fines de la persecución de delitos, a los índices de referencia de sus ficheros de análisis del ADN, lo que incluirá el derecho a consultarlos de manera automatizada mediante una comparación de perfiles de ADN. La consulta deberá formularse únicamente para casos concretos y con arreglo al derecho de la Parte Contratante que realice la consulta.*"

440 Art. 1.2 del anexo de la Decisión 2008/615/JAI, de 23 de junio.

Dado que el sistema puede informatizar hasta 23 locus más la Amelogenina, el laboratorio descarta numerosos falsos positivos.

Segundo paso:

Una vez comprobada la coincidencia, para conocer la identidad de la persona a la que corresponde el código cuyo perfil genético ha dado el *match*, el intercambio de la información se realiza de acuerdo con el derecho interno del país que posee los datos de la identidad del sujeto⁴⁴¹. Se lleva a cabo a través de la oficina SIRENE: una de las partes facilitará la información del hecho por el cual se obtuvo el perfil dubitado y la otra facilitará los datos de la persona del perfil indubitado.

El Tratado de Prüm y la Decisión que lo integró en el ordenamiento jurídico de la UE solo regula el intercambio de datos relativos a los perfiles genéticos en sí y su comparativa. El intercambio de la información de la identidad del sujeto y de la inteligencia policial que ello puede conllevar, técnicamente, queda fuera de los acuerdos del Tratado.

441 Art. 5 de la Decisión 2008/615/JAI, de 23 de junio.

Pero son varios los países que no pueden llevar a la práctica la Decisión Prüm, por varias razones: dificultad de concentrar mayorías parlamentarias que permitan los cambios de legislación requeridos, conflictos internos sobre quien recae la responsabilidad de llevarlo a la práctica, falta de recursos económicos y/o humanos para llevarlos a cabo⁴⁴².

Actualmente 25 países tienen implementada la Decisión Prüm en lo referente al intercambio de información relativa a ADN. Pero cada país tiene sus propios niveles de conexión con el resto de los países. En 2020, España está conectada con 23 países. Según el Ministerio del Interior⁴⁴³, las coincidencias generadas durante el año 2020 en los intercambios realizados por España en el marco del Tratado de Prüm han sido:

Stain España – Persona Prüm – 831 coincidencias.

Stain España – Stain Prüm – 402 coincidencias.

Stain Prüm – Persona España – 1076 coincidencias.

Persona España – Persona Prüm - 3223 coincidencias.

442 MACHADO H. y GRANJA R. (2020).

443 Memoria Enero – Diciembre 2020 de la base de datos policial de identificadores obtenidos a partir de ADN, p. 33 y 34.

7.- Introducción de perfiles genéticos en las bases de datos.

En el estado español se introducen los perfiles genéticos relacionados con casos de delitos graves, como ya se ha dicho anteriormente. Si se cumple la primera premisa, la introducción de los perfiles genéticos indubitados de las personas relacionadas vendrá determinada por la situación procesal del individuo respecto al hecho.

7.1.- Según el tipo de delito investigado.

Todos los países de la Unión Europea han creado bases de datos en los que almacenan perfiles de ADN para los fines de la persecución de delitos⁴⁴⁴ y cuyos datos intercambiaran entre sí. Pero no todos ellos alimentan dichas bases bajo las mismas premisas. El elemento común en todos ellos es que la persona de la cual se le introduce el perfil genético está involucrada de algún modo en un ilícito penal. A partir de aquí, los matices dependen de los distintos modelos que aplican los Estados: puede ser que la implicación sea como autor o víctima de un delito, que el delito sea grave o leve, que haya una sentencia condenatoria o de inocencia, que se

⁴⁴⁴ Art. 2.1 de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

requiera el consentimiento de la persona en cuestión o no para introducir dicho perfil en la base de datos.

La introducción de perfiles genéticos en las bases de datos para facilitar la investigación criminal ha ido variando a lo largo del tiempo.

1.- Inicialmente los países introducían en sus bases de datos los perfiles genéticos de personas condenadas por infracciones graves. Principalmente eran personas que habían cometido delitos de naturaleza sexual y debía evitarse que reincidieran; en caso de hacerlo, debían ser identificados y localizados con prontitud.

Por este motivo, las personas condenadas por este tipo de delitos deberían esperar una expectativa disminuida de su derecho a la protección de datos personales en favor de la sociedad en general, para que esta se sintiera más segura, dado que de este modo se podría aumentar la eficacia policial en la resolución de delitos de esta índole.

2.- Con el paso del tiempo el catálogo de delitos se fue ampliando.

Un ejemplo de ello es el *Code de procédure pénale* francés, que fue modificado con la Ley n°98-468 de 17 junio de 1998,

para crear el *fichero nacional automatizado de huellas genéticas*, con la finalidad de identificar y localizar los autores de *infracciones sexuales*. Posteriormente, se volvió a modificar en 2001 para ampliar el catálogo, donde incluyeron otro tipo de delitos, además de los sexuales⁴⁴⁵.

3.- Finalmente, el Estado pugna por tener el máximo número de perfiles genéticos en las bases de datos, bajo la tesis de que a mayor número de perfiles genéticos en la base de datos, mayor es la probabilidad de identificar y localizar el autor de un delito.

La rapidez que necesita la sociedad para resolver delitos graves - identificando a los autores, a los que considera que son personas peligrosas dado que cometen ilícitos graves - la prevención de la reincidencia de este tipo de hechos penales, prevalecen sobre el derecho a la privacidad de los ciudadanos.

Seguridad versus privacidad.

La sociedad actual utiliza ampliamente las nuevas tecnologías, las cuales dejan una huella digital que puede ser rastreada por los gobiernos. El uso de los teléfonos móviles puede seguirse a través de los datos recopilados por las

⁴⁴⁵ Ley n° 2001-1062 de 15 noviembre de 2001.

compañías telefónicas o aplicaciones móviles como Facebook o Google; también puede seguirse la actividad de una persona a través de las tarjetas de crédito, cámaras de tráfico, las de vigilancia de espacios públicos o privados, por citar algunos; es muy larga la lista del rastro digital que puede dejar un individuo por el solo hecho de vivir en la sociedad actual. El problema no radica en el rastreo en sí, sino en que las nuevas tecnologías trabajan ininterrumpidamente rastreando todo y a todas las personas. Una fuga de información en el campo de la protección de datos puede provocar consecuencias irreparables en la privacidad del individuo.

Desde que en 1984, Sir Alec John Jeffreys empezó a desarrollar las técnicas de la huella genética y los perfiles de ADN hasta la actualidad, la investigación en la ciencia forense - y una vez alcanzado un grado de fiabilidad infalible - ha avanzado en la dirección de disminuir el coste económico que supone tanto el recoger muestras biológicas en el lugar de los hechos como el análisis de dichas muestra en el laboratorio, de manera que su uso se ha hecho universal e indispensable en la investigación penal de delitos graves.

Algunos autores⁴⁴⁶ se muestran a favor de la creación de una base de datos de perfiles genéticos de todos los ciudadanos de un país para ser utilizada en la investigación criminal dado que actualmente se podría asumir el coste que supone el análisis de millones de muestras genéticas de ciudadanos. De esta manera se podría evitar la discriminación de subgrupos poblaciones marginales en los cuales hay una alta población delincuencia. Al haber más proporción de perfiles genéticos introducidos en las bases de datos policiales, hay mayor probabilidad de identificar autores pertenecientes a este grupo.

Para conseguir este objetivo, toda la sociedad en su conjunto debería renunciar al derecho a la protección de datos personales, en este caso datos genéticos, en orden de (1) aumentar la eficacia policial para resolver delitos violentos e identificar a los autores y (2) evitar la estigmatización de subgrupos poblaciones marginales en los cuales hay una alta tasa de población delincuencia.

Una base de datos genéticos con toda la población, equivaldría a la creación de un gran hermano genético, que además de ser útil en la investigación criminal, podría ser útil también para realizar otros tipos de estudios, médicos por

⁴⁴⁶ Por ejemplo VALERIO JAMINIAN, M.E. en "Nuevas técnicas de control social: Análisis jurídico de las bases de datos de ADN", Tesis doctoral UPF, 2015.

ejemplo, con los cuales el estado podría ajustar el presupuesto sanitario. De esta manera, por ejemplo, se podría llegar a saber el número de personas que padecerían una determinada enfermedad.

Pero un mal uso de estos datos podría causar un daño irreparable en la sociedad. No se debe olvidar la sentencia *S. y Marper c. Reino Unido* en la que el TEDH considera que la mera conservación de muestras celulares supone una violación del art. 8.1 del CEDH. Aunque se trate de una sucesión de números, estos contienen una cantidad significativa de los datos personales que, procesados automáticamente con los sistemas informáticos actuales, permiten ir más allá de la simple identificación, como se verá en el siguiente capítulo.

A mi entender, es suficiente con que sean los condenados y las personas sospechosas, detenidas o imputadas, las que deben reducir su expectativa de privacidad en aras de aumentar la eficacia policial a través de las bases de datos genéticas. Aplicando *Lopez Ribalda versus España*⁴⁴⁷ debe ponderarse, por un lado, el derecho a la vida privada de los individuos y por el otro el interés de la sociedad en proteger a todos sus miembros y su buen funcionamiento.

447 STEDH de 7 de octubre de 2019. Caso Lopez Ribalda II c. España.

A los individuos con antecedentes de delitos graves se les asciende a la categoría de sospechosos de cometer delitos de esta índole, no vulnerando así el art. 8 de la CEDH⁴⁴⁸. De esta manera, no es necesario que para aumentar la capacidad de perseguir crímenes y proteger a los ciudadanos de delitos violentos deba menoscabarse el derecho a la protección de datos personales del conjunto de una sociedad. Por lo tanto, la medida de introducir en las bases de datos los perfiles genéticos de personas con antecedentes de delitos graves, parece una medida apropiada y proporcionada para lograr el fin legítimo de identificar y detener autores de estos delitos.

Cuando una persona sospechosa, detenida o imputada resulta condenada, una consecuencia accesoria del delito tiene que ser que su perfil genético sea introducido en una base de datos. En cambio, si una persona detenida o imputada no resulta condenada, es decir, se dictara contra ella sobreseimiento libre o sentencia absolutoria, su perfil genético debería ser borrado de las bases de datos policiales. Pero ni los jueces lo ordenan, ni los interesados ni sus abogados lo suelen exigir.

448STEDH de 5 de octubre de 2010. Caso Köpke c. Alemania;
STEDH de 28 de noviembre de 2017. Caso Antovic y Mirković c.
Montenegro.

Si el perfil genético de una persona que no debería estar en la base de datos diera una coincidencia con un perfil indubitado, debería provocar la nulidad de la prueba obtenida⁴⁴⁹. Pero la información ya estaría en poder de las autoridades policiales y, con obtener nuevamente el perfil indubitado del investigado - ya sea con consentimiento o a través de una orden judicial - quedaría subsanada la prueba.

7.2.- Situación procesal del donante de la muestra

Cuando una persona accede a ceder muestras biológicas para que se le extraiga su perfil genético lo hará firmando un acta de consentimiento. En dicha acta debería quedar constancia de la autorización expresa a ceder su perfil genético y con qué muestras será comparado su perfil genético.

Los Cuerpos y Fuerzas de Seguridad del Estado español disponen de dos tipos de actas en los que recogen el consentimiento de la persona que cede el perfil genético, que dependerá de **su situación procesal**. El contenido mínimo de las actas fue aprobado por la Comisión Nacional para el uso forense del ADN el 2010.

⁴⁴⁹ En aplicación del art. 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

a.- Persona investigada o detenida.

Si la fuerza policial solicita el consentimiento a una persona que está siendo **investigada/detenida** por la presunta comisión de un delito, para que su perfil genético sea comparado con las muestras biológicas recogidas en la escena del crimen, el consentimiento debe ser dado en presencia de su letrado⁴⁵⁰. Una vez recogida la muestra biológica con los hisopos, se obtendrá el perfil genético que será introducido en las bases de datos policiales y se comparará con todos los perfiles genéticos dubitados que existen en ellas.

Esta acta de consentimiento tiene la siguiente estructura⁴⁵¹:

Encabezado:

En él constan los datos de la actuación que da lugar a la toma de muestras, los datos de filiación del donante de la

450 STS núm. 296/2011 de 18 abril, FJ 1: "*Es decir, el consentimiento ha de estar exento de todo elemento susceptible de provocar o constituir error, violencia, intimidación o engaño (artículo 1265 del Código Civil), pues si tales rigurosas exigencias son requeridas para las relaciones contractuales, mucha más severidad habrá de aplicarse cuando se trata de renunciar a un derecho fundamental del individuo...*".

451 "*Acta de recollida de mostres biològiques i consentiment informat per a l'anàlisi d'ADN de persones detingudes o investigades en una investigació criminal*" - Documento I61.b del Cos de Mossos d'Esquadra.
"*Formulario de toma de muestras y consentimiento informado para obtención de muestras de ADN en asunto criminal*" de la Guardia Civil.

muestra y, finalmente, los datos del letrado que presta la asistencia.

Datos de la toma de muestra:

1.- En primer lugar, se hace constar el consentimiento expreso que da el interesado, seguido de una pequeña explicación relativa a en que consiste la extracción de la muestra (introducción en la boca de dos torundas) y que las muestras son para el estudio de ADN *"que proporcione exclusivamente información genética reveladora de la identificación de la persona y de su sexo"*.

2.- Se avisa que los *"datos y los resultados obtenidos a partir de la realización de este análisis podrán ser utilizados para la identificación genética sobre ADN meramente identificador, en una **investigación criminal en curso o en otros, anteriores o bien futuras**, en relación con la comisión de cualquier delito por el cual la legalidad vigente autoriza el tratamiento de los perfiles de ADN"*.

3.- *Cesión de los datos "contenidos en la mencionada base de datos a las autoridades judiciales, fiscales o policiales de terceros países, de acuerdo con aquello previsto en los convenios internacionales vigentes que hayan sido ratificados por España"*.

El perfil genético del investigado correrá la misma suerte que el de la persona detenida: inicialmente será introducido en la **LDIS** – bases de datos local - para, posteriormente, pasar a la **SDIS** – base de datos estatal -. Finalmente, en virtud del Tratado de Prüm, será comparado con perfiles anónimos de bases de datos de perfiles de ADN de terceros países. No se distingue diferencia de trato entre perfil genético procedente de persona detenida o persona investigada; pero a nivel de instrucción policial sí que la hay.

4.- El análisis de las muestras lo llevarán a cabo laboratorios acreditados y *"corresponde a la autoridad judicial la decisión sobre su ulterior conservación"* de las muestras o vestigios.

Como se ha dicho anteriormente, raras veces la autoridad judicial se pronuncia sobre el destino de este tipo de muestras biológicas. Por lo tanto, será el laboratorio el que decidirá sobre la conservación de las muestras.

5.- Se informa del periodo de conservación y de cancelación de los perfiles genéticos obtenidos en las bases de datos.

6.- Derechos que tiene el interesado: Acceso, cancelación, rectificación y oposición, establecidos en la Ley Orgánica 15/1999, de 13 de diciembre. Actualmente esta ley no está

en vigor y debería figurar la Ley Orgánica 7/2021, de 26 de mayo.

El "*Acta de recollida de mostres biològiques per a l'anàlisi d'ADN*" del Cos de Mossos d'Esquadra, cierra este apartado informando al sujeto que es necesaria la presencia letrada para dar el consentimiento.

Cierre del acta:

El interesado firma y marca su huella digital. También firma el letrado.

b.- Persona víctima o testigo.

Las actas de consentimiento de cesión voluntaria de perfil genético deberían estar formadas por dos apartados: (1) consentimiento para que el perfil genético del interesado sea comparado con los perfiles genéticos hallados en una investigación concreta. (2) Consentimiento que el perfil genético del donante sea introducido en la **LDIS** i en el sistema **CODIS**.

Desgraciadamente, el "*Acta de recollida de mostres biològiques per a l'anàlisi d'ADN*" del *Cos de Mossos d'Esquadra* que firma una víctima o testigo de un hecho

delictivo cuando cede una muestra biológica para que se obtenga su perfil genético y sea comparado con otros perfiles relacionados con su causa, es exactamente igual a la que firma una persona detenida o investigada. No hay ninguna variación en la redacción. Los puntos anteriores son exactamente válidos para cuando se trata de víctimas. Con la firma del contenido de las actas I61 de dicho cuerpo policial, una víctima accede a que su perfil genético sea introducido en el **CODIS**, lo cual es completamente desproporcionado. Una vez que su perfil genético ha sido utilizado para la finalidad para la que fue solicitado - descartar muestras biológicas de la víctima en la escena del crimen - el perfil genético debería ser borrado.

En cambio, en el *"Formulario de toma de muestras y consentimiento informado para obtención de muestras de ADN en asunto criminal"* de la Guardia Civil la diferencia es evidente. Así el perfil genético de la víctima o testigo será *"cotejado para su descarte con otros procedentes de muestras relacionadas con la investigación policial de referencia al objeto de esclarecer el exclusivamente el hecho que se investiga"*. En cambio, el perfil genético constará inscrito en la base de datos mientras *"se mantenga su relación con el mencionado laboratorio"*, bajo la excusa de *"detectar y controlar posibles contaminaciones"*.

En el caso de la Guardia Civil, queda claro que el perfil genético solo se utilizará para la investigación por la cual fue recabado. Pero su conservación en la base de datos tampoco tiene un periodo claro de borrado, ya que ¿cuando finaliza la relación de una muestra con el laboratorio? la respuesta puede ser nunca.

Otro aspecto a tener en cuenta es la situación procesal de la persona de la que se obtiene la muestra. Como se ha dicho anteriormente, la Ley Orgánica 10/2007 regula la inclusión del perfil genético en las bases de datos de perfiles genéticos de las personas sospechosas, detenidas o imputadas y de las que han prestado expresado su consentimiento.

A mi juicio, el hecho de expresar consentimiento no debería ser motivo suficiente para grabar los datos en la base de datos. En el caso de una investigación criminal, debería estar prohibido introducir los datos de víctimas y testigos en la SDIS, más allá de la inscripción en la LDIS y para compararlas con las del caso concreto. Tal como está redactada el acta de cesión de datos genéticos de los Mossos d'Esquadra, todas las personas que la firmen podrán tener introducido su perfil genético en las base SDIS y luego ser comparada con otras bases de datos Europeas, teniendo

el mismo trato que el de los detenidos o investigados⁴⁵². Y el tiempo de conservación del perfil genético en la base de datos vendrá dado por el delito del cual ha sido víctima: cuanto más grave, mayor tiempo de conservación, ya que se conservará el mismo periodo de tiempo que el del detenido o investigado.

En la mayoría de los casos, las muestras obtenidas con el consentimiento del sujeto activo no detenido, corresponden a testigos o víctimas de los que se necesitan las muestras para descartar. En el marco de una investigación, las fuerzas del orden pueden tener una serie de candidatos como presuntos autores y, teniendo el perfil genético del autor, se solicita a esos candidatos que faciliten voluntariamente muestras biológicas para que el perfil genético que se obtenga sea comparado con el de dicho autor. Para demostrar su inocencia y no quedar estigmatizados ante la negativa, muchas serán las personas que cederán muestras biológicas para la investigación policial, con la condición que solo se van a utilizar para esa investigación concreta.

En el caso de víctimas de un robo violento, pongamos por caso, en el cual se han obtenido vestigios biológicos durante la inspección ocular, los investigadores les requerirán la

⁴⁵² Nos consta que no es el caso y que, los perfiles genéticos facilitados por víctimas y testigos solo son introducidos en el LDIS.

cesión de una muestra biológica para poder descartar su perfil genético del autor. Dicha víctima tiene dos opciones:

1.- Ceder una muestra biológica para que el laboratorio descarte su perfil genético. Tiene el inconveniente que su perfil permanecerá en la LDIS del cuerpo policial hasta que prescriba el delito o alguien decida borrarlo antes.

2.- No ceder la muestra biológica. En ese caso, los perfiles genéticos obtenidos serán tratados como indubitados, lo que implica que se introducirán en el CODIS i serán comparados con perfiles genéticos de toda Europa. No serán borrados hasta que sean identificados o prescriba el delito.

Como víctima, ninguna de las dos opciones es buena. Ya que todas las víctimas, y terceros implicados de buena fe, se ven "*obligados*" a ceder muestras biológicas, los cuerpos policiales deberían actuar con sumo tacto y esmero para que este tipo de muestras permanezcan en las bases de datos el tiempo mínimo imprescindible. Además, es necesario descartar el perfil de la víctima para poder identificar el del autor y tratarlo como tal. Por tanto, los perfiles de víctimas y testigos, una vez comparados, deberían ser borrados de la bases de datos policiales y nunca podrán ser transferidos a otras bases de datos o cuerpos policiales. Si una vez borrado

el perfil genético de una víctima o testigo fuera necesario de nuevo, se le podría volver a solicitar.

Cabe hacer notar también que en el siglo XXI ya no existen las comparaciones manuales por lo que, para llevar a cabo el proceso, los perfiles serán introducidos en las bases de datos del cuerpo policial, la LDIS, y será un programa informático el que comparará los perfiles genéticos de los testigos/presuntos autores con los perfiles genéticos obtenidos del autor en la investigación en cuestión. Pero también hará la comparación con todos los perfiles genéticos anónimos que todavía no han sido identificados y que proceden de investigaciones anteriores. De manera que, si hubiera alguna coincidencia con un perfil genético anónimo que nada tiene que ver con el caso para el cual se le ha pedido el consentimiento, podría provocar un *match*.

Entonces, el laboratorio podría informar a la unidad que está llevando dicha investigación de la coincidencia de perfiles. Así, los agentes de esa unidad, sabedores de la identidad del autor, solo tendrían que obtener legalmente el perfil genético del sujeto en cuestión, por ejemplo a través de una muestra atribuida. La persona que cedió su perfil genético para la investigación concreta nunca llegaría a saber que esa

muestra cedida le habría provocado la imputación en un hecho delictivo completamente distinto.

c.- Trabajadores públicos de emergencias .

En las bases de datos policiales hay introducidos perfiles genéticos que corresponden al personal que trabaja en el laboratorio o personal operativo que recoge muestras genéticas en una investigación para poder detectar cualquier contaminación que haya ocurrido en el mismo laboratorio.

A mi juicio, debería introducirse también el perfil genético de todos los agentes de policía del territorio de donde tiene el ámbito competencial el laboratorio de referencia y debería valorarse también el de introducir el de los trabajadores del sector de emergencias, como son los bomberos, protección civil y emergencias médicas.

De esta manera se conseguirían al menos dos objetivos:

- **Eliminación de líneas de investigación falsas.** Los que siempre acuden al lugar de los hechos son los agentes de policía y, en menor medida, trabajadores del sector de las emergencias. Cabe la posibilidad que, por accidente o por una mala manipulación, estos empleados públicos dejen muestras biológicas en el lugar de los hechos y que

posteriormente los agentes de la policía científica lo recojan como un indicio. El perfil genético obtenido de tales muestras nunca será identificado y, de serlo, no tendrá ninguna relación con el autor de los hechos. Si el laboratorio dispone de los perfiles genéticos de todos los trabajadores de emergencias, podrán descartar desde el inicio la línea de investigación que podría generar dicho perfil evitando un gasto de recursos innecesario.

- Incremento de número de personas en la base de datos.

La introducción de los perfiles genéticos de estos empleados públicos en la base de datos incrementaría el número de personas introducidas.

Tal como ocurrió en la investigación que se llevó a cabo en los EEUU referente al Golden State Killer o, más recientemente el asunto de los agentes de la Guardia Urbana de Barcelona, los casos en los que hay involucrados agentes de la ley como autores de delitos graves pueden ser difíciles de resolver ya que son conocedores de las técnicas que se usan en la investigación de delitos. Si saben que sus perfiles genéticos están introducidos en la base de datos puede hacer que reprima la comisión del delito. En caso de cometerlo, su perfil genético ya estará en el sistema y podrá ser utilizado durante la investigación.

Dado que son profesiones de riesgo, también servirá en caso de accidente con difícil identificación del cuerpo, ya que si el perfil genético está en la base de datos se produciría una rápida identificación.

7.3.- Cancelación de los datos.

Los perfiles genéticos inscritos en las bases de datos tienen presunción de legalidad en cuanto a su utilización para otras causas, por lo que debe ser el interesado el que demuestre la ilicitud de obtención de la muestra a partir de la cual se ha codificado su perfil genético⁴⁵³ o que, si se ajusta a derecho la obtención de la muestra, debe cuestionar la legalidad de la introducción⁴⁵⁴. Por lo tanto, cuando haya una coincidencia entre una muestra dubitada y una indubitada, debe ser el sujeto el que demuestre que su perfil genético no debería estar introducido en la base de datos. Pero el *match* ya habrá saltado y bastará con que se obtenga legalmente una muestra genética para subsanar el procedimiento. Ello obliga a que los responsables de las bases de datos genéticas actúen con suma pulcritud en el momento de decidir la inscripción de dichos perfiles, las cuales deben ajustarse escrupulosamente a la legalidad.

453 STS 286/ 2016 de 7 abril.

454 Acuerdo del Pleno No Jurisdiccional de la Sala Segunda del Tribunal Supremo de 24-09-2014, sobre toma biológica de muestras para la práctica de la prueba de ADN.

Los perfiles genéticos permanecerán en la base de datos hasta que prescriba el delito o hasta que se cancelen los antecedentes policiales. Dado que la base de datos es policial, no existe correlación entre antecedentes policiales y judiciales.

Si durante el proceso judicial hubiera un sobreseimiento libre o una sentencia absolutoria, los datos deberían borrarse. Pero la legislación obliga al ciudadano a solicitar el borrado de sus datos, por que de lo contrario, no serán eliminados hasta que no haya transcurrido el tiempo que señala la ley para la prescripción del delito⁴⁵⁵ en cuestión.

Esta situación no diferencia entre las personas que han sido condenadas por un delito de las que han sido eximidas de responsabilidad penal, contradiciendo el dictamen del TEDH en el caso S. y Marper contra Reino Unido⁴⁵⁶ y vulnerando el principio de presunción de inocencia. El TEDH entiende que *“se menosprecia la presunción de inocencia si una decisión judicial que afecta a un procesado refleja la sensación de que éste es culpable, cuando en realidad su culpabilidad no*

⁴⁵⁵ Art. 9 de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

⁴⁵⁶ STEDH S y Marper c. Reino Unido de 4 de diciembre 2008, párrafo 122: *“Particularmente preocupante en este caso es el riesgo de estigmatización, que deriva del hecho de que las personas en la situación de los demandantes, que no fueron declarados culpables de ningún delito y tienen derecho a la presunción de inocencia, sean tratados de la misma manera que los condenados.”.*

*ha sido previamente establecida legalmente*⁴⁵⁷. Manteniendo el perfil genético en las bases de datos policiales de individuos que han sido detenidos policialmente, pero no se ha demostrado su culpabilidad, se estaría violando el art. 6.2 del Convenio. Una de las finalidades de dicho artículo “es evitar que los funcionarios y las autoridades públicas traten como si fueran de hecho culpables de la acusación formulada en su contra a las personas que han sido absueltas de cargos penales, o respecto a las cuales sus procesos penales han sido sobreseídos”⁴⁵⁸. No hay diferencia de trato en este aspecto entre la persona que ha sido condenada judicialmente y la que ha sido absuelta.

Si se ha sobreseído la causa en la que una persona sospechosa estaba siendo investigada - y no tenga ninguna otra causa pendiente -, sus datos deberían ser borrados de oficio en cuanto la resolución fuera firme, sin que sea necesario que el individuo ejerza el derecho de cancelación de datos y solicite que estos sean borrados de la bases de datos.

Dada la falta de comunicación de los Tribunales con las autoridades policiales en cuanto al dictamen de las sentencias, si el interesado o el juez no solicita la

457 STEDH de 16 de febrero de 2016. Caso Vlieeland Boddy y Marcelo Lanni c. España, párrafo 38.

458 STEDH de 12 de Julio de 2013. Caso Allen c. Reino Unido, párrafo 94.

cancelación de los datos de las bases de datos policiales, estos no serán borrados hasta que lleguen el momento de su cancelación. A mi entender, bastaría con que los datos de personas investigadas, sean o no detenidas, pudieran guardarse un tiempo limitado en la base de datos a efectos de hacer las pesquisas de investigación necesarias y, transcurrido ese periodo, si dicho almacenamiento no está avalado por una autoridad judicial, deberían ser eliminados. No nos referimos exclusivamente al almacenamiento de perfiles genéticos, sino que debería aplicarse también a los antecedentes policiales, haciéndolo extensible a huellas dactilares y fotografías.

Cuando un laboratorio borra los datos de un perfil genético, lo eliminará de todas las LDIS. Si les constan coincidencias, se solicitará a los laboratorios implicados y al SDIS que cancelen los datos. Las perfiles genéticos procedentes de muestras dubitadas permanecerán inscritas en la base de datos mientras se mantenga dicho anonimato. Es decir, hasta que no se identifique la persona de la que procede dicha muestra o que el delito vinculado a la muestra haya prescrito.

Otro motivo en que la ley prevé la cancelación de datos es cuando se tenga conocimiento de la defunción del interesado, siempre que no sean necesarios para finalizar

procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas⁴⁵⁹. También se eliminarán los datos de los familiares asociados.

Durante el año 2020 se han borrado un total de 2.404 perfiles genéticos de las bases de datos nacionales – Cuerpo Nacional de Policía, Guardia Civil, Mossos d’Esquadra, Erzaintza, Policía Foral, Instituto Nacional de Toxicología - y desde que se mantienen registros de ello, un total de 37.369 perfiles⁴⁶⁰.

Conclusiones.

En el SXIX, los investigadores criminales iban a la escena del crimen con diversos reactivos que servían para revelar huellas dactilares de distintos tipos de superficies. En el SXX a este kit se le sumó primero la fotografía y después el video. Actualmente, además de todos estos enseres, llevan una torunda que en uno de los extremos tiene un fino algodón y que sirve para recoger muestras biológicas. Esa torunda es

⁴⁵⁹ Sería el caso de localización de algunos restos cadavéricos de una persona. Podría darse el caso que a lo largo del tiempo aparecieran más restos que, en caso de borrar su perfil genético de las bases de datos, nunca podrían identificarse.

⁴⁶⁰ Datos procedentes de la Memoria Enero – Diciembre 2020 de la base de datos policial de identificadores obtenidos a partir de ADN, p. 37.

fruto de la gran revolución criminalística de las últimas décadas.

El uso de los datos genéticos en la investigación policial ha permitido la identificación de numerosos autores de delitos graves y de una manera muy efectiva, dado que los resultados obtenidos tienen el valor de prueba pericial y sirven para condenar o exonerar a una persona. Si la principal herramienta policial del siglo pasado era el estudio de las huellas dactilares, en este siglo lo es el análisis genético de muestras biológicas. La individualización que permite un perfil genético hace que se pueda convertir en una prueba irrefutable en el momento del juicio. Además, si no se produce una coincidencia entre la muestra dubitada y el perfil genético de una persona que esta introducido en la base de datos, esta persona queda eliminado de la lista de sospechosos.

El perfil genético es un código alfanumérico único para cada individuo formado por el número de repeticiones de bases genéticas que se dan en determinados puntos de la cadena de ADN. En la muestra biológica a partir de la cual se obtiene el ADN se halla toda la información genética de la persona. Por lo tanto, el tratamiento tanto de la muestra biológica

como del perfil genético, debe hacerse de forma restrictiva y con todas las medidas de seguridad disponibles.

La legislación española desarrollada hasta el momento determina la obtención de la muestra biológica a analizar en función de la situación procesal del sujeto. Pero dicha situación viene dada a partir de las diligencias policiales y no las judiciales, de manera que es el instructor policial el que decide el rol que tiene el sujeto durante la investigación policial. Dicha investigación es incipiente y en numerosas ocasiones el rol procesal del sujeto variará dependiendo del avance de la investigación judicial, llevada a cabo con todas garantías procesales, y que finalizará con un juicio que establecerá la culpabilidad o la inocencia del sujeto. Sería más razonable inscribir el perfil genético del investigado en la base de perfiles genéticos policial provisionalmente y, si al finalizar el procedimiento judicial resultara condenado, el perfil genético se mantendría inscrito en la base. Por contra, si resultara absuelto o sobreseído el caso, el perfil sería eliminado tal como establece la Recomendación del Consejo de Europa R (92).

Otro aspecto mejorable, a mi juicio, es la ambigüedad en cuanto a ordenar la destrucción de la muestra biológica una vez obtenido el perfil genético. Como recoge el TEDH, la

información contenida en una muestra biológica es información sensible del individuo, entre la que hay la relativa a su salud⁴⁶¹. Pero no solo hay información referente a él mismo, sino la de sus familiares biológicos también. Podría entenderse la conservación de muestras biológicas dubitadas obtenidas en la escena del crimen durante largos periodos de tiempo: dado que se pretende identificar el autor, puede aducirse que en un futuro no muy lejano dicha muestra se podrá volver a analizar y obtener otro tipo de información que ayudaría a la identificación del culpable.

Pero cuando se trata de muestras indubitadas, no es aceptable. Las muestras, una vez analizadas y obtenido el perfil genético, deben ser destruidas. En caso de que sea necesario llevar a cabo nuevos análisis de la muestra indubitada – por ejemplo, porque ha habido una evolución en los marcadores genéticos estudiados -, se debería volver a solicitar dicho consentimiento. El consentimiento dado por un individuo para que se le extraiga una muestra biológica indubitada, debe ceñirse a la época en la que se le extrae. No se puede guardar dicha muestra *sine die* para analizarla al cabo de unos años y llevar a cabo un tipo de análisis completamente distinto al que se debería de haber realizado en el tiempo de la solicitud. Se trata de una vulneración del

461 STEDH de 4 de Diciembre de 2008. Caso Marper c. Reino Unido, párrafo 72.

art. 8 del CEDH, ya que el solo hecho de producirse la retención sistemática de material celular una vez obtenido el perfil genético del individuo, se considera una intromisión en el ámbito de este artículo⁴⁶². Por tanto, se debería establecer un borrado de los datos introducidos en las bases de datos de oficio, con un sistema de caducidad, de manera que cuando éstos sean introducidos, ya se establezca la fecha en la que serán borrados automáticamente. Los datos genéticos de un individuo son demasiado sensibles para que permanezcan en una base datos sin una finalidad concreta cuando finaliza el tiempo de almacenamiento permitido.

En el intercambio de datos genéticos a nivel Europeo, a mi juicio, la UE ha establecido reglas claras y prima salvaguardar el derecho a la protección de datos que tienen los ciudadanos antes que intercambiar la información entre países sin que haya una causa justificada. Lo ha conseguido haciendo que cada país gestione su propia base de datos y, para establecer coincidencias, solo se transfieren los perfiles genéticos asociados a un código, de manera que solo los funcionarios del país de donde procede el perfil genético conocen la identidad de la persona a quien corresponde.

⁴⁶² En *Kinnunen c. Finlandia* (no. 24950/94, Commission decision de 15 Mayo 1996) el TEDH afirma que la retención sistemática de muestras celulares constituye una injerencia al art. 8.1 del CEDH atendiendo a los usos futuros de la información contenida en dichas muestras.

Antes de ceder dicha identidad, la coincidencia pasará por una serie de filtros humanos que serán los encargados de establecer la idoneidad o no del traspaso de la información. De esta manera se implican funcionarios de ambos países que deben adaptarse a sus respectivas legislaciones.

En el intercambio de datos genéticos entre distintos países no ocurre lo mismo que con el intercambio de otro tipo de información. La creación de vínculos entre los oficiales de las distintas fuerzas policiales, conlleva también el intercambio de información a nivel de persona a persona, de manera que se eluden los controles formales de comunicación establecidos. Así, una buena relación personal entre los agentes favorece el intercambio de cualquier tipo de información contenida en sus respectivas bases de datos.

CAPÍTULO IV

ADN FORENSE EN LA INVESTIGACIÓN CRIMINAL A LA LUZ DE LA EVOLUCIÓN JURISPRUDENCIAL EN EUROPA: PROPUESTA DE FUTURO.

1.- Introducción.

El uso del ADN ha producido un gran avance en la investigación criminal. Las nuevas técnicas permiten identificar⁴⁶³ la persona a la cual pertenece un indicio biológico localizado en una escena del crimen de manera que, las autoridades policiales, pueden averiguar quién es el autor, detenerlo y enjuiciarlo en los tribunales. Permiten, además, establecer relaciones entre crímenes que han tenido lugar en diferentes lugares o en espacios temporales distintos, todo ello sin ser necesario que se identifique el autor. La simple coincidencia de muestras permite establecer una relación entre diversos crímenes.

Pero no solo pueden identificar al culpable, sino que las pruebas de ADN tienen la capacidad de exonerar de culpa a

⁴⁶³ En realidad se trata de probabilidades: la probabilidad de que dos personas tengan el mismo perfil genético es de una entre un billón o incluso un trillón.

una persona inocente, incluso contra el criterio del propio denunciante o de testigos. Así, aunque una víctima reconozca en una rueda de reconocimiento a su presunto autor, si las pruebas genéticas lo contradicen, a dicho reconocimiento podría no dársele la veracidad suficiente para condenar a una persona. Pongamos el caso de una agresión sexual en la que el autor haya dejado restos de semen; aunque la víctima reconozca a través de una fotografía al presunto autor, si el perfil genético de dicho autor no coincide con el de los restos de semen, difícilmente una acusación podría seguir adelante.

Como hemos explicado en el capítulo anterior, la actual legislación permite comparar el perfil genético de una muestra procedente de una escena del crimen, con los perfiles genéticos que están almacenados en las bases de datos policiales, los cuales proceden de personas que cumplen determinados criterios penales. Pero, ¿qué ocurre cuando la muestra dubitada procedente de la escena del crimen no coincide con ninguno de los perfiles que hay en las bases de datos? Debemos recordar que en las bases de datos policiales españolas de perfiles genéticos están registrados **23 marcadores STRs autosómicos**, cuyo conjunto forman lo que se denomina perfil genético de un individuo. Si una muestra dubitada no coincide con los marcadores

procedentes de la muestra indubitada no se produce un *match*, lo que significa que la persona buscada, la que dejó dicha muestra, no se encuentra en la base de datos.

La genética forense ha desarrollado diversas técnicas para identificar la persona que abandonó una muestra biológica en el lugar de los hechos, de manera que cuando no se ha obtenido una coincidencia con los perfiles genéticos contenidos en las bases de datos, es capaz de proporcionar una lista de candidatos con perfiles genéticos similares a partir de los familiares biológicos del donante de la muestra.

Otras técnicas consisten en realizar un retrato robot de este individuo a partir de la muestra biológica dubitada, esbozando sus características físicas visibles⁴⁶⁴, de manera que se puede averiguar si se trata de una persona rubia o morena, de ojos azules o marrones, de piel clara u oscura.

Pero la ciencia sigue su curso y las aplicaciones del análisis del ADN forense van evolucionando, mejorando las ya existentes y desarrollando nuevas. La aplicación de herramientas que actualmente están siendo utilizadas en el campo de la investigación médica abre unas expectativas que todavía no somos capaces de evaluar ni predecir⁴⁶⁵.

464 **Externally Visible Characteristics** de sus siglas en inglés **EVC**.

465 HEPPLER B. et. al. (2007)

En este capítulo vamos a estudiar diversos tipos de análisis que pueden realizarse sobre la muestra biológica para identificar la persona que la dejó en el lugar de los hechos y la afectación que pueden tener sobre los derechos humanos - principalmente el de la privacidad y la protección de datos – de los individuos con un perfil genético similar al de la muestra dubitada.

Las nuevas técnicas que vamos a analizar en este capítulo son las siguientes:

Coincidencia parcial:

Cuando se compara el perfil genético de la muestra dubitada con los que contienen las **bases de datos policiales** y no se establece una coincidencia o *match*, hay ocasiones en las que se obtienen coincidencias en determinados marcadores. Es decir, alguno de los 23 alelos que forman parte del perfil genético dubitado coincide con la muestra indubitada. Cuanto mayor sea el número de marcadores coincidentes, mayor sería la probabilidad que se trate de muestras relacionadas biológicamente entre sí, de manera que esta coincidencia parcial podría indicar algún tipo de parentesco entre los propietarios de ambas muestras.

"familial searching" o búsqueda familiar:

Las coincidencias parciales obtenidas en el punto anterior podrían ser fruto de la coincidencia y del azar. Utilizando la técnica de *familial searching*, los perfiles coincidentes parcialmente se combinan con algoritmos matemáticos que son utilizados como motores de búsqueda, para así identificar posibles relaciones de parentesco entre ambos donantes⁴⁶⁶. Es decir, se buscan probabilidades de parentesco entre las dos muestras.

Si no se puede establecer ninguna relación familiar entre la muestra dubitada y los perfiles genéticos contenidos en las **bases de datos policiales**, algunas autoridades policiales pueden recurrir a otras bases de datos - que pertenecen a empresas privadas - en las que se guardan perfiles genéticos de personas que los han cedido a cambio de recibir ciertos servicios⁴⁶⁷. Estas bases de datos pertenecen a las llamadas compañías **DTC - (Direct-to-Consumer Genetic Testing)**, que ofrecen servicios individualizados asociados a las características genéticas de cada individuo. Los perfiles

⁴⁶⁶ La primera búsqueda genética de familiares se llevó a cabo de la Gran Bretaña el año 2002, en la que se llegó a identificar el hijo de un violador en serie de los años 70.

PATTOCK (2011) p. 860.

⁴⁶⁷ En 2019 la compañía **Family Tree DNA** anunció que estaba colaborando con el FBI en investigaciones criminales. <https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy>

genéticos que utilizan están formados por miles de marcadores, distintos a los que usan las bases de datos genéticos policiales.

El método de “*familial searching*” sirve para obtener inteligencia policial para resolver crímenes en los que se han agotado las líneas de investigación. El uso policial de estos datos abre un apasionante debate en el que se cuestiona la legalidad, la equidad y la eficacia de como las autoridades públicas deberían utilizar esta metodología. Por este motivo, y antes de que sea un método de investigación ampliamente utilizado, deberían introducirse pautas claras sobre su uso con la finalidad de evitar una intrusión en la privacidad familiar. Es un método de investigación en el que los beneficios que puede aportar en la resolución de delitos graves deben equilibrarse con la posible lesión de derechos fundamentales de personas inocentes, básicamente familiares potenciales del autor y los propios candidatos a autor.

No debemos olvidar que estas técnicas no son exactas y dan “probables” candidatos a familiar del autor o al autor mismo.

Características físicas visibles – EVC -.

El realizar un retrato robot a partir del indicio biológico localizado en la escena del crimen todavía no es posible, pero quizás no tardemos mucho en verlo. De momento, las nuevas técnicas permiten averiguar ciertas características físicas de la persona que ha dejado la muestra biológica en la escena del crimen, como son el color del pelo o de los ojos y la procedencia geográfica de sus ancestros. Actualmente, durante la investigación policial, esta técnica se usa para reducir el número de personas sospechosas o contrastar declaraciones de testigos.

Si con el uso de estas técnicas se consiguiera identificar la persona que abandonó la muestra localizada en el lugar de los hechos, seguiría siendo necesario corroborarlo con el análisis del perfil genético indubitado del autor.

Estos avances tecnológicos deben ser "*objeto de un debate público apropiado, a la luz, en particular, de las implicaciones médicas, sociales, económicas, éticas y jurídicas pertinentes*"⁴⁶⁸ para así identificar los problemas que pueden conllevar y buscar soluciones sociales, jurídicas y éticas haciendo que la sociedad establezca los límites que crea

⁴⁶⁸ Art. 28 del "*Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina*" de 4 de abril de 1997.

necesarios. Es esencial identificar los riesgos que conlleva el uso de la tecnología genética para prevenir el posible menoscabo que supone a los derechos civiles de los ciudadanos, entre los que se encuentran la defensa de la presunción de inocencia, la privacidad genética y la integridad moral y física de los sospechosos o personas investigadas⁴⁶⁹.

En este capítulo vamos a ver, como hemos dicho, en qué consisten estas técnicas genéticas y que problemática supone desde el punto de vista de vulneración de los derechos humanos.

2.- Búsqueda familiar – familial search - utilizando las bases de datos genéticas policiales.

Como se ha visto en el anterior capítulo, los perfiles genéticos indubitados que hay en las bases de datos policiales españolas están formados por **23 marcadores STRs autosómicos**. Su finalidad es la de identificar perfiles genéticos dubitados comparándolos con los perfiles genéticos de personas identificadas que han sido introducidos en la base de datos. La coincidencia de dos

469 MACHADO y GRANJA (2020)

perfiles indica que ambas muestras provienen de la misma persona.

También se ha explicado que las partes de ADN que se usan en la investigación forense forma parte del ADN no codificante dado que - por lo que se sabe actualmente - no revelarían ningún tipo de información sobre la genética del individuo o de su familia. Así, no transmiten información relativa a las características físicas de la persona o su tendencia a tener o transmitir, el individuo o sus familiares, enfermedades hereditarias.

De él se extrae una serie de fragmentos - los **marcadores** o **locus** - ubicados en distintos cromosomas, que están formados por pequeñas regiones de unos 100 - 500 nucleótidos compuestos por una unidad de 4 - 5 nucleótidos que se va repitiendo en tándem a lo largo de dicha región durante un determinado número de veces (**Short Tandem Repeats - STRs**). El número de repeticiones que se produce en cada marcador forma el perfil genético, que se representa en forma de código alfanumérico o numérico. El perfil genético es, simplemente, un código asociado a la identidad de una persona. Una vez obtenido el perfil genético, se almacena en las bases de datos policiales y son utilizados para la investigación de determinados delitos.

En ausencia de una coincidencia entre una muestra dubitada y las que contienen la base de datos policiales de perfiles genéticos, surge la pregunta de qué puede hacerse para identificar dicha muestra. Si los familiares biológicos tienen material genético común, dado que comparten ancestros, ¿puede identificarse algún familiar del donante de la muestra dubitada y que tenga introducido su perfil genético en la base de datos policial?

El ADN que se encuentra en las células de una persona proviene un 50% del ADN del padre y el otro 50% de la madre. El hermano de esta persona también tendrá la mitad del ADN de la misma madre y la mitad del mismo padre, pero no compartirán los mismos fragmentos de la cadena, ya que la recombinación es aleatoria. Los familiares biológicos comparten material genético que proviene de sus ancestros y, cuanto más próximo es el grado de parentesco, mayor es la probabilidad de compartir carga genética común.

Veamos por ejemplo los perfiles genéticos de la última familia imperial rusa, formada por el Zar Nicolás II, su esposa la Zarina Alexandra y sus cinco hijos Olga, Tatiana, Maria, Anastasia y Alexei⁴⁷⁰.

470 <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0004838>
(última consulta 14/03/2022).

	Tsar Nicholas II	Tsarina Alexandra	Olga	Tatiana	Maria or Anastasia	Anastasia or Maria	Alexei
Amelog	X, Y	X, X	X, X	X, X	X, X	X, X	X, Y
D3S1358	14, 17	16, 18	17, 18	17, 18	16, 17	17, 18	14, 18
TH01	7, 9.3	8, 8	8, 9.3	7, 8	8, 9.3	7, 8	8, 9.3
D21S11	32.2, 33.2	30, 32.2	30, 33.2	32.2, 33.2	30, 33.2	30, 33.2	32.2, 33.2
D18S51	12, 17	12, 13	12, 12	12, 12	13, 17	12, 17	12, 17
D5S818	12, 12	12, 12	12, 12	12, 12	12, 12	12, 12	12, 12
D13S317	11, 12	11, 11	11, 11	11, 11	11, 11	11, 11	11, 12
D7S820	12, 12	10, 12	12, 12	10, 12	12, 12	10, 12	12, 12
D16S539	11, 14	9, 11	11, 11	11, 11	11, 14	9, 11	11, 14
CSF1PO	10, 12	11, 12	11, 12	11, 12	10, 11	10, 12	10, 12
D2S1338	17, 25	19, 23	17, 19	23, 25	17, 19	17, 23	23, 25
vWA	15, 16	15, 16	15, 16	15, 16	15, 16	15, 16	15, 16
D8S1179	13, 15	16, 16	13, 16	15, 16	13, 16	15, 16	15, 16
TPOX	8, 8	8, 8	8, 8	8, 8	8, 8	8, 8	8, 8
FGA	20, 22	20, 20	20, 22	20, 20	20, 22	20, 22	20, 22
D19S433	13, 13.2	13, 16.2	13.2, 16.2	13.2, 16.2	13, 16.2	13, 13	13, 13.2

Como hemos dicho, los hijos comparten aleatoriamente los alelos de los padres. Los cuatro alelos de los padres que hay en cada locus se van combinando en cada hijo. De este modo se puede comprobar que el Zar Nicolas II era el padre de los cinco niños porque uno de sus alelos está en todos los locus de las criaturas, al igual que ocurre con la Zarina Alexandra. Así por ejemplo, en el locus D2S1338, los niños tienen un número de alelos 17 o 25 por el lado paterno y 19 o 23 por el materno. El hecho de que tengan uno u otro de cada progenitor es completamente aleatorio.

Con los marcadores STR, aunque someramente, pueden establecerse relaciones de familiaridad biológica, por lo que cabría replantearse el concepto de ADN “basura” ya que no servirá para averiguar datos genéticos sobre la persona, pero

sí que sirve para establecer relaciones de parentesco. Además, quizás con el análisis de 23 alelos no puedan determinarse rasgos genéticos de un individuo, pero si el perfil genético estuviera compuesto por 1000 alelos, se podría averiguar alguna característica genética, todo y que esos alelos no formen parte de ningún gen; y si fueran 10.000 los alelos estudiados, el resultado sería más preciso. Así, si se estudiaran 10.000 alelos es fácil intuir que todas las personas de ojos azules compartirán alguna coincidencia, aunque sea de ADN no codificante.

Por tanto, la aplicación de la *familial searching* en los análisis genéticos conlleva un cambio de paradigma en el uso de ADN utilizado hasta la fecha en las bases de datos genéticos policiales, ya que amplían la información que éste puede facilitar. Hasta ahora era utilizado para obtener coincidencias entre perfiles genéticos, pero con estas nuevas aplicaciones se pueden establecer relaciones de parentesco. Con los 23 alelos que actualmente componen un perfil genético en las bases de datos policiales, una *familial searching* tiene poca precisión, pero a mayor número de alelos estudiados, más preciso sería el resultado obtenido.

2.1.- Búsqueda familiar - familial search - usando las bases de datos policiales.

La Comisión Nacional para el uso forense del ADN en su informe de actividades de 2012⁴⁷¹, ya prevé el uso de *familial searching* en la investigación criminal. Señala que pueden realizarse dos tipos de búsqueda familiar:

2.1.1.- Búsqueda familiar indirecta.

Esta forma es la utilizada para identificar cadáveres de personas desaparecidas, víctimas de catástrofes, restos humanos, restos cadavéricos, cadáveres localizados en grandes catástrofes y cualquier otro tipo de cadáveres que no puedan ser identificados a través de huellas dactilares o se encuentren en muy mal estado. El protocolo de las Fuerzas y Cuerpos de Seguridad sobre personas desaparecidas⁴⁷² establece que deben recogerse enseres de

471 La Comisión Nacional para el uso forense del ADN es un órgano adscrito al Ministerio de Justicia que tiene encomendadas, entre otras funciones la elaboración y aprobación de los protocolos técnicos oficiales sobre la obtención, conservación y análisis de las muestras, incluida la determinación de los marcadores homogéneos sobre los que los laboratorios acreditados han de realizar los análisis además de formular propuestas para mejorar la eficacia del uso de ADN en la investigación, persecución de delitos y la identificación de cadáveres.

Real Decreto 1977/2008, de 28 de noviembre, por el que se regula la composición y funciones de la Comisión Nacional para el uso forense del ADN.

472 http://www.interior.gob.es/documents/642317/1203227/Protocolo_de_actuacion_de_FFCCSS_ante_personas+desaparecidas_126190173.pdf/906a7721-4274-43c1-8772-a27d58d69bef (última consulta

las víctimas, tales como cepillos de dientes, máquinas de afeitar, peines,... y obtener de ellos el perfil genético a partir de las células residuales que quedan en dichos objetos. A la vez, contactan con familiares para que, en caso que del análisis de los objetos personales no se obtenga un resultado concluyente⁴⁷³, se lleve a cabo el análisis del ADN de los familiares, obtener su perfil genético y pueda ser comparado con el que se obtenga de la víctima. A este efecto se extraerán muestras genéticas de los familiares biológicos de estas personas, principalmente padre, madre e hijo/a.

Una vez se obtienen los perfiles genéticos, éstos se comparan: si el 50 % de los alelos provienen del padre y el otro 50 % de la madre, la mitad del número de alelos del hijo debe coincidir con la mitad de cada uno de sus progenitores, como hemos visto con los hijos del antiguo Zar de Rusia.

Con este método se comparan dos muestras biológicas entre sí directamente, prescindiendo de bases de datos genéticas, ya que se busca la relación familiar entre dos muestras.

14/03/2022).

473 Puede ocurrir que en los objetos recogidos haya una mezcla de perfiles o se tengan dudas que el único usuario hubiera sido la víctima.

2.1.2.- Búsqueda familiar directa.

Cuando se lleva a cabo la comparación entre perfiles genéticos en el sistema CODIS, el operador puede solicitar que se realice con una exigencia **alta, media o baja**. La alta exigencia significa que coincidan los alelos en todos los locus analizados de ambas muestras. El operador también puede especificar un número determinado de alelos coincidentes entre dos muestras, produciéndose entonces una exigencia moderada o media. Finalmente, una exigencia baja supone que al menos coincidan en un alelo. Los resultados obtenidos de aplicar una media o baja exigencia se les denomina *coincidencia parcial*.

El resultado obtenido con una alta exigencia da lugar a un *match* y supone que las dos muestras comparadas pertenecen a una misma persona. Es el método tratado en el capítulo anterior y significa que el donante de la muestra indubitada es la persona a la que pertenece la muestra dubitada.

En cambio, un resultado obtenido de una exigencia moderada o baja supone una coincidencia parcial. Estas se pueden dar porque el perfil genético proviene de una muestra degradada y el perfil genético era incompleto o porque

realmente algunos de los alelos de las dos muestras coincidan⁴⁷⁴. Ello significa que las dos muestras no proceden de la misma persona, pero los donantes de ambas muestras pueden estar emparentados biológicamente. Cuanto mayor sea el número de locus en los que coincidan, mayor probabilidad hay que las muestras procedan de personas emparentadas.

2.1.2.1.- Coincidencia parcial inadvertida.

Mientras el laboratorio está llevando a cabo la comparación de perfiles genéticos dubitados con los existentes en la base de datos buscando una coincidencia, el operador puede estar utilizando una exigencia media para encontrar coincidencias en muestras incompletas⁴⁷⁵, por ejemplo. Ello puede dar origen a coincidencias parciales en las cuales no todos los locus coincidan. Entonces el analista tiene la opción de comunicar el hallazgo al investigador policial o puede comunicar que no ha habido coincidencia y, por tanto, la muestra dubitada no ha sido identificada. Dicha decisión dependerá de si la legislación autoriza o no dicha comunicación y, de no existir dicha legislación, se atenderá a la costumbre que haya en el cuerpo policial a tal efecto. A

474 PATTOCK (2011)

475 Perfiles genéticos incompletos se dan cuando las muestras se encuentran degradadas, por ejemplo en avanzado estado de descomposición y al realizar el análisis no es posible obtener todos los locus.

mayor número de alelos coincidentes, mayor será la probabilidad que las dos muestras estén emparentadas biológicamente y el parentesco sea de menor grado.

Pero se debe tener en cuenta que el CODIS no está diseñado para buscar relaciones de parentesco biológico entre dos muestras, sino que su función es localizar coincidencias exactas entre perfiles. El analista puede localizar coincidencias entre alelos de determinados perfiles, pero que por sí mismos no significa que estén relacionados biológicamente. Esa coincidencia parcial, sin embargo, puede ser un punto de partida para iniciar una investigación policial.

2.1.2.2.- Coincidencia parcial intencionada.

Con los datos obrantes en las bases de datos policiales de perfiles genéticos el operador lleva a cabo la búsqueda de coincidencias con una exigencia media o baja. De esta manera, se realiza una búsqueda de coincidencia entre el perfil dubitado y los obrantes en la base de datos; de no obtenerse, se estudian las coincidencias parciales que podrían indicar la posible relación de parentesco.

Los perfiles genéticos que contienen las bases de datos policiales están formados por los datos de 23 locus, lo que

significa que los parientes deberían compartir exactamente los mismos alelos, cosa que no siempre sucede. Cuanto mayor fuera el número de locus a analizar de una muestra, mayor sería la probabilidad de localizar material genético igual entre dos familiares. Por otro lado, cuantos más perfiles genéticos sean introducidos en las bases de datos, mayor será la probabilidad que dos personas que no estén emparentadas compartan al menos algún alelo de los analizados.

Para aumentar su efectividad, los motores de búsqueda utilizan algoritmos matemáticos con los que localizan perfiles genéticos que cumplan determinados parámetros de los que tiene el perfil dubitado. A la vez, se pueden tener en cuenta otros factores no genéticos como pueden ser la edad, el sexo o el origen geográfico, el domicilio,... por citar algunos ejemplos. Estos algoritmos calculan un índice de parentesco entre dos perfiles genéticos que se materializa en una terna de personas entre las que se pueden hallar familiares de la persona que dejó la muestra dubitada localizada en el lugar de los hechos.

Los motores de búsqueda pueden tener en cuenta:

a.- Coincidencia de un número elevado de alelos en el perfil genético.

Compartir un número superior a la media de alelos. Así familiares de primer grado – padres e hijos – comparten el 50% de material genético. Por tanto, se realizaría una búsqueda de perfiles genéticos que coincidan en al menos un 50% de los alelos. Familiares de segundo grado – abuelos, nietos, sobrinos - comparten una cuarta parte de su material genético entre sí. Pero no se analiza toda la cadena de ADN, sino solamente una serie de fragmentos. Es decir, la cuarta parte del material genético de los abuelos está repartido de forma aleatoria por toda la cadena de ADN de los nietos. Dado que un perfil genético se obtiene a partir del análisis de 23 zonas muy concretas de los cromosomas, el perfil genético de un nieto podrá tener mayor número de coincidencias con un abuelo que con otro, pero en la composición genética de todo el ADN celular solo habrá una cuarta parte del material genético del abuelo.

En la tabla anterior de la familia Imperial Rusa Romanov, podemos ver que el Zar y la Zarina tenían hasta 14 alelos iguales en los 15 locus analizados – casi un 50 % de coincidencia -, lo cual indica cierto grado de parentesco. Esto

es fruto de ser primos segundos por una línea genealógica y primos terceros por otra línea⁴⁷⁶.

b.- *Compartir una frecuencia alélica en un mismo locus.*

Para una determinada población genética hay repeticiones en ciertos locus que son menos frecuentes que otras de más comunes.

Según ciertos estudios⁴⁷⁷, una persona originaria de la zona noreste de Italia tiene una probabilidad de un 0,2 % de tener 19 repeticiones en el locus **D10S1248**. En cambio la probabilidad de tener 13 repeticiones en ese locus es de un 31,6 %. Por lo tanto de cada 1.000.000 de personas solo habrá unas 2.000 personas con 19 repeticiones y unas 316.000 personas con 13 repeticiones en dicho locus.

Cuanto menor es la incidencia en la población de referencia, menor será el número de personas que comparten dicha frecuencia alélica. Por lo tanto, si el perfil dubitado procede de una muestra biológica de esa zona y tiene 19 repeticiones en ese locus, se podría empezar por investigar los familiares de las personas que tengan esa frecuencia alélica.

476 Compartían bisabuela común – la princesa Guillermina de Baden – a la vez que tenían como antecesor común al rey Federico Guillermo II de Prusia.

477 TURRINA, FILIPPINI y DE LEO (2011)

c.- Cromosoma Y.

Comparar el perfil del cromosoma Y de la muestra dubitada con los obrantes en las bases de datos relativos al cromosoma Y. La coincidencia indicaría que pertenecen a un mismo linaje genético masculino, con lo cual se pueden construir árboles genealógicos o excluir otras ramas familiares.

Hay estudios que afirman que a través de marcadores del cromosoma Y de una muestra biológica dubitada, entrecruzándolos con bases de datos genealógicas - algunas de ellas públicas y gratuitas - y con metadatos como pueden ser la edad o el lugar de residencia, se puede inferir el apellido del donante de dicha muestra anónima. Se estima que cuanto menos común es el apellido, mayor es la probabilidad de inferir el apellido⁴⁷⁸.

d.- ADN mitocondrial.

Realizar análisis del ADN mitocondrial de la muestra dubitada y compararla con los perfiles genéticos de la base de datos relativos al ADN mitocondrial. De esta manera se puede establecer la línea genética materna.

478 GYMREK et al. (2013)

e.- Algoritmos matemáticos.

Estos permiten calcular el índice de parentesco – *Kinship Likelihood Ratio (LR)* - en las muestras que presentan elevadas coincidencias en el número de alelos o de alelos raros. Los candidatos que presentan un elevado índice *LR* pueden ser sometidos a otros análisis, como el del cromosoma Y o el ADN mitocondrial, determinar el grado de parentesco y establecer si puede tratarse de una línea de investigación viable. El *Scientific Working Group on DNA Analysis Methods*, en sus recomendaciones de 2014 sobre las búsquedas familiares, aboga por utilizar el índice de parentesco como método de comparación más eficiente que el de comprar el número de alelos compartidos o la rareza de estos⁴⁷⁹.

Las bases de datos policiales de perfiles genéticos españolas solo permiten la inscripción de información genética reveladora de la identidad de la persona y de su sexo⁴⁸⁰. El análisis del ADN del cromosoma Y y del ADN mitocondrial, proporcionan elementos de identificación del linaje del individuo, pero no del individuo en sí. Por tanto, son datos

479 El informe se puede consultar en:

http://media.wix.com/ugd/4344b0_46b5263cab994f16aeedb01419f964f6.pdf (última consulta 14/03/2022).

480 Art. 4 de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

que pueden ser obtenidos del análisis de las muestras, pero no pueden ser introducidos en bases de datos policiales para ser almacenados. Ello significa, que tanto el análisis del cromosoma Y como el del ADN mitocondrial no podrán utilizarse en los algoritmos de búsqueda familiar en las bases de datos policiales de perfiles genéticos españolas.

En España, las bases de datos policiales, así como su legislación, están orientadas hacia la coincidencia de perfiles genéticos, comparan perfiles genéticos dubitados con perfiles genéticos indubitados, o perfiles genéticos dubitados entre sí, para determinar si proceden del mismo donante. Todo y que técnicamente se habla de probabilidades, cuando se habla de identificación su certeza es absoluta.

En cambio, cuando se trata de *familial searching* no es así. El resultado que se obtiene es una lista de personas candidatas a ser familiares del donante del perfil genético dubitado. Los agentes de la policía investigaran las personas incluidas en esta lista para averiguar si alguna de ellas es realmente un familiar. Es decir, se investigaran personas que son inocentes respecto al hecho delictivo para localizar a sus familiares biológicos, con la esperanza que alguno de estos familiares sea el autor. Así, los familiares investigados serán tratados como presuntos culpables, al menos inicialmente. Estas

personas pueden ver mermados su derecho a la privacidad, intimidad y al de la protección de datos.

Una vez localizado un candidato a autor, la merma de sus derechos se verá agudizada, ya que éste será considerado un presunto autor y deberá demostrar su inocencia. Para ello deberá ceder una muestra biológica que será comparada con la muestra biológica localizada en el lugar de los hechos. Hasta que no se obtenga el resultado, esa persona será vista como presunto culpable. Y no digamos si se negara a ceder una muestra biológica para hacer las comprobaciones necesarias.

El principio de la presunción de inocencia exige que no se parta de la idea preconcebida de culpabilidad del investigado. *“El peso de la prueba recae sobre el Ministerio Fiscal, y cualquier duda debe beneficiar al acusado”*⁴⁸¹. Pero, al menos socialmente, la carga de la prueba está invertida ya que debe ser el investigado quien demuestre su inocencia y lo tiene que hacer cediendo su material genético, por lo que se estará violando su presunción de inocencia. Esta persona está obligada a ceder su material genético para demostrar su inocencia. La negativa a la cesión de una muestra biológica en estas condiciones podría suponer un indicio de

481 STEDH de 20 de marzo de 2001. Caso Telfner c. Austria, párrafo 15.

culpabilidad que podría ser utilizado como motivación para obtener de forma coercitiva dicho material genético.

Los comentarios que reciban los investigados relativos a la responsabilidad del delito, entraran dentro de la protección contra la difamación y al derecho a reclamar derechos civiles en los tribunales, afectando los art. 8 y 6 del CEDH⁴⁸², aunque expresar dudas sobre la inocencia de la persona investigada en el marco de la investigación es lícito siempre que en el transcurso del proceso penal se haya tomado una decisión al respecto⁴⁸³.

2.2.- ¿Pueden usarse bases de datos genéticas policiales para llevar a cabo este tipo de *familial search*?

Actualmente estamos en la fase que la identificación a partir de ADN forense está plenamente consolidada. Existe poca o nula discusión jurídica en cuanto al uso de técnicas genéticas para identificar la persona que dejó una muestra biológica en una escena del crimen. La localización, recogida y análisis de muestras biológicas en la escena del crimen y su posterior análisis y comparación con los perfiles genéticos ya no se pone en duda jurídicamente. Ahora es el momento de avanzar en el uso del ADN forense y utilizar el perfil genético

482 STEDH de 27 de noviembre de 2003. Caso Zollmann c. Reino Unido;
STEDH de 24 de abril de 2008. Caso Ismoilov y otros c. Rusia, párrafo 160.

483 STEDH de 25 de agosto de 1993. Caso Sekanina c. Austria, párrafo 30.

dubitado localizado en la escena del crimen como elemento de investigación.

Así, las bases de datos policiales de perfiles genéticos que se utilizan para identificar ADN dubitativo procedente de la escena del crimen, deberían usarse para llevar a cabo *familial search* e identificar el presunto autor de los hechos. Las personas que tienen introducido su perfil genético en ellas – a consecuencia de una infracciones penales cometidas – han perdido parte de su derecho a la privacidad y, al igual que existe una base de datos de fotografías o de huellas dactilares de personas que han sido detenidas y que son utilizadas para resolver ilícitos penales, los datos procedentes del material genético de estas personas debe ser utilizado en investigaciones criminales para identificar a otros criminales.

En el estado español, las bases de datos policiales de carácter genético solo permiten el almacenamiento de "*los identificadores obtenidos a partir del ADN, en el marco de una investigación criminal, que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo*". Los 23 locus que actualmente se almacenan en el sistema CODIS español hace que la capacidad de búsqueda genética de familiares

esté muy limitada ya que dicha búsqueda se llevaría a cabo estableciendo comparaciones entre estos alelos. Cuanto mayor sea el número de alelos a comparar, mayor será la probabilidad de localizar relaciones de parentesco, obteniendo resultados más eficientes para la investigación policial⁴⁸⁴. Con los datos que actualmente se almacenan en el CODIS, solo podrían identificarse parientes muy próximos, los más alejados no pueden ser identificados.

Las bases de datos genéticas policiales deben servir a las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado para la "*averiguación de los delitos y el descubrimiento y aseguramiento de los delincuentes*"⁴⁸⁵ de manera que, a mi entender e interpretando de manera amplia el enunciado, permiten llevar a cabo la *familial search* en el transcurso de una investigación criminal por lo que su aplicación generalizada solo es cuestión de tiempo. Hay laboratorios policiales que cuando comparan distintos perfiles de ADN, lo hacen con una exigencia media, de manera que si se diera el caso de una elevada coincidencia en el número de alelos entre dos perfiles, ésta sería detectada y la información podría ser traspasada a la unidad de policía judicial que investiga el caso para que valorara su posible utilidad en la investigación.

484 WICKENHEISER (2019)

485 Artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

El legislador debería ser el primero en mostrar el camino a seguir para utilizar esta técnica tan incipiente e invasiva en cuanto a la afectación de derechos fundamentales. Recordemos que las coincidencias en los alelos solo hace que tengan probabilidades de que ambas muestras procedan de dos personas emparentadas genéticamente. La investigación policial que se iniciaría a consecuencia de esta coincidencia va encaminada hacia la confirmación o no de este parentesco.

Por este motivo, a mi juicio, el legislador debería regular bajo que condiciones deberían utilizarse los datos contenidos de las bases de datos policiales en técnicas de *familial search*. A modo de propuesta, los aspectos a tratar deberían ser los siguientes:

- Definición de los delitos en los que podría aplicarse esta técnica. Deberían ser delitos graves, los mismos para los cuales se autoriza el uso del ADN forense para su investigación.
- Aplicación en casos en los que las líneas de investigación están agotadas. Si no se usara esta técnica, el caso quedaría definitivamente archivado sin autor conocido.

- Aspectos técnicos y algoritmos matemáticos a utilizar, como pueden ser el tipo de marcadores que deben ser utilizados, establecer a partir de qué número de coincidencias puede considerarse a una persona como candidata o los registros en los que debe dejarse constancia de las acciones llevadas a cabo con los resultados obtenidos.

- La intervención de un comité que valorará si el resultado técnico obtenido es de suficiente entidad como para que se dé traslado del resultado al equipo investigador.

- En cuanto a la persona candidata a presunto autor, debería regularse la clase de medidas limitadoras de derechos fundamentales a las que podrían verse sometidas estando bajo investigación; una investigación que serviría para confirmar si esta persona puede ser el autor buscado. Parece claro que han de estar tuteladas por un juez o fiscal, el cual debe valorar la proporcionalidad de dichas medidas. Deben evitarse problemas de discriminación dada la alta concentración de perfiles genéticos de minorías en las bases de datos policiales ya que se verán sometidos a más

investigaciones de esta índole. Más adelante profundizaremos en este punto.

En mi opinión, es acertada la guía de uso emitida por el *Departamento de Justicia de los EEUU* en 2019 dirigida a las agencias del mismo departamento para utilizar las técnicas de *familial search* en casos de crímenes sin resolver. Así, cuando una muestra biológica localizada en el escenario del crimen no coincide con ninguna de las que están en las bases de datos, puede ser sometida a un proceso de *familial search*. Para ello, la muestra será trasladada a un laboratorio externo donde se llevaran a cabo nuevos análisis genéticos, cuyo resultado será introducido en uno o más servicios de genealogía genética – DTC's - que explícitamente permitan su uso a las fuerzas del orden y será comparada automáticamente con las muestras existentes en sus bases de datos. Un algoritmo informático evaluará las posibles relaciones de parentesco localizadas. El resultado se comunicará al fiscal, al laboratorio oficial y a la agencia investigadora que valoraran si se trata de una nueva línea de investigación y actuaran en consecuencia. Al finalizar, todas las muestras trasladadas al laboratorio externo y los datos que estas hayan podido generar serán destruidos⁴⁸⁶.

486 Se puede consultar en <https://www.justice.gov/olp/page/file/1204386/download> (última consulta 14/03/2022).

En diversos estados de los EEUU se ha autorizado el uso de estas técnicas. Así por ejemplo en 2008, el Departamento de Justicia de California⁴⁸⁷ adoptó una política en la que también permite aplicar técnicas de *family search* en casos en los que las líneas de investigación se han agotado. De esta manera, si durante la búsqueda rutinaria en el CODIS, se da una *coincidencia genética parcial* en la que al menos 15 alelos de los 20⁴⁸⁸ posibles y además existe concordancia en el cromosoma Y, el nombre de dicha coincidencia es facilitado al equipo investigador. Si lo que se quiere es reactivar una investigación y llevar a cabo una *family search* con una muestra dubitada, es necesario que las líneas de investigación se hayan agotado y se requiere una solicitud previa al *Bureau of Forensic Services*. El resultado obtenido será analizado por un comité que valorará si se deben revelar los nombres de los familiares potenciales del presunto autor al equipo investigador para que se inicie una investigación con ellos.

Además de California, son 11 los Estados de los EEUU en los que se permite la *family search* usando las bases de

487 Puede consultarse en <http://www.dnaresource.com/documents/CAfamilialpolicy.pdf> (última consulta 14/03/2022).

488 En 2017 la base de datos genéticos del FBI incrementó el número de locus de 13 a 20. <https://www.fbi.gov/services/laboratory/biometric-analysis/codis> (última consulta 14/03/2022).

datos policiales: Colorado (2007), Texas (2010), Florida y Wyoming (2012), Michigan, Wisconsin, Utah y Virginia (2014), Ohio (2016), Arizona y Nueva York (2018). Haciendo el promedio entre todos ellos, la tasa de éxito es del 33%⁴⁸⁹. Por otra parte, también hay estados como el de Maryland⁴⁹⁰ en donde, de momento, no se permite utilizar técnicas de *family search* durante la investigación policial.

Esta técnica puede ser muy útil en la resolución de delitos y lo que realmente es necesario es regular su utilización con la finalidad de evitar malas prácticas, más que prohibir su uso. Se tienen que adecuar las técnicas de investigación para que se respeten los derechos fundamentales de los ciudadanos.

3.- Búsqueda familiar utilizando las bases de datos genéticas no policiales.

Vista la limitación que conlleva el uso de bases de datos policiales para llevar a cabo la búsqueda de familiares genéticos del donante de una muestra - básicamente debido a que los perfiles genéticos almacenados en ellas contienen información referente a pocos locus -, las autoridades policiales miran a otras bases de datos, en las que se

489 WICKENHEISER (2019).

490 <https://law.justia.com/codes/maryland/2010/public-safety/title-2/subtitle-5/2-506/> (última consulta 14/03/2022).

almacenan perfiles genéticos de miles de personas, pero que están compuestos por miles de marcadores. Esta información, además de estar guardada en un formato que no es compatible con las bases de datos policiales, está almacenada en bases de datos genéticas que ni pertenecen ni son gestionadas por autoridades del ámbito de la seguridad pública. Son bases de datos de propiedad privada, pública o semipública cuya finalidad no es la de ser utilizadas para identificar delincuentes.

3.1.- Tipos de Bases de datos genéticas no policiales.

Las bases de datos de perfiles genéticos que utilizan las fuerzas policiales, y que se han tratado ampliamente en el capítulo anterior, son las *bases de datos forenses*. Su función es generar coincidencias entre un perfil dubitado hallado en la escena del crimen y los perfiles que hay introducidos en ellas, dado que se conoce la identidad de sus donantes. Permiten además identificar dos perfiles anónimos sin que sea necesario tener identificado al donante de la muestra. Para ello utilizan marcadores STR para definir el perfil genético.

Fuera del ámbito policial existen *bases de datos genéticos* que contienen datos de personas que los han cedido a

empresas comerciales con la finalidad de obtener una prestación de servicios. Así, hay productos en el mercado que realizan pruebas citogenéticas en las que se evalúan todos los cromosomas para detectar posibles enfermedades hereditarias⁴⁹¹ o localizar familiares biológicos⁴⁹². A este grupo pertenecen las compañías DTC, donde cada compañía utiliza sus propios marcadores genéticos SPN.

También son de interés policial las *bases de datos genéticos de secuencias concretas del genoma humano*, las cuales contienen fragmentos del cromosoma Y o del ADN mitocondrial, que permiten llevar a cabo estudios de ancestralidad⁴⁹³. Son utilizadas en genética forense para establecer linajes de procedencia de las muestras. El linaje paterno vendrá establecido por el cromosoma Y y el materno por el ADN mitocondrial.

Obviamente, hay otros tipos de bases de datos genéticas pero que no serían de interés para este trabajo.

491 <https://www.agenciasinc.es/Noticias/Un-nuevo-test-genetico-es-capaz-de-detectar-552-enfermedades-hereditarias> (última consulta 14/03/2022).

492 **MyHeritage** (<https://www.myheritage.es/>) En 2019 afirmaba que tienen unos 80 millones de usuarios en todo el mundo y 2,5 millones de perfiles de ADN. En España serían unos 1,5 millones de usuarios, pero no precisan cuántos perfiles. El análisis de ADN en esta empresa costaba entre 59 y 79 euros. La noticia completa en https://elpais.com/sociedad/2019/05/16/actualidad/1558035084_458086.html (última consulta 14/03/2022).

493 <https://www.23andme.com/en-int/> (última consulta 14/03/2022).

La investigación sobre la aplicación del ADN forense en la investigación criminal está en la línea de implementar el uso de bases de datos genéticas que no son del ámbito policial. Así, la primera búsqueda para identificar quién dejó un perfil de ADN dubitativo localizado en un lugar determinado se realiza en las bases de datos policiales de perfiles genéticos; una coincidencia significa la identificación de la persona que dejó el perfil en la escena del crimen. En caso de no existir la coincidencia, las nuevas técnicas forenses permiten utilizar el propio ADN como elemento de investigación, es decir, utilizar el ADN como se puede utilizar una fotografía o un dato telefónico.

Actualmente en España, la *familial searching* se está llevando a cabo en los procesos de identificación de personas desaparecidas y restos humanos de los que se desconoce la identidad. Con los datos obrantes en el sistema CODIS, y a través de algoritmos matemáticos, se realiza una búsqueda del perfil genético procedente de un cadáver de identidad desconocida y se compara con los datos de personas que están introducidas en la base de datos de Personas Desaparecidas y Restos Humanos (PDYRH). En algunos casos se puede llegar a obtener un cierto grado de compatibilidad familiar. Los analistas estudian dicha compatibilidad manualmente; de haberla, lo comunican a la

unidad policial que lleva la investigación para que se pongan en contacto con el familiar candidato y hagan las comprobaciones pertinentes.

Compañías DTC - (Direct-to-Consumer Genetic Testing)

Se trata de compañías que ofrecen servicios de análisis genéticos directamente a personas físicas, con la finalidad de realizar informes de estilos de vida que mejoren su salud y bienestar⁴⁹⁴, detectar desordenes genéticos⁴⁹⁵, la posibilidad de transmitir enfermedades hereditarias a sus descendientes⁴⁹⁶ o secuenciar el genoma completo del cliente⁴⁹⁷. Otras ofrecen incluso la posibilidad de descargarse el resultado del análisis en "*bruto*" para que puedan ser analizadas por otras compañías del sector o por profesionales de la salud⁴⁹⁸.

Uno de los servicios que ofrecen estas compañías es el de la localización de ancestros familiares⁴⁹⁹, es decir, busca los

494 <https://www.23andme.com/compare-dna-tests/> (última consulta 14/03/2022).

495 <https://www.invitae.com/en/physician/panelsgenes/> (última consulta 14/03/2022).

En su catálogo ofrecen análisis genéticos para detectar desordenes metabólicos, nefrológicos, cáncer hereditario, cardiopatías y otros tipos de enfermedades genéticas.

496 <https://myriadwomenshealth.com/provider/foresight-carrier-screen/> (última consulta 14/03/2022).

497 <https://www.veritasgenetics.com/myGenome> (última consulta 14/03/2022).

498 <https://customercare.23andme.com/hc/en-us/articles/212196868-Accessing-Your-Raw-Genetic-Data> (última consulta 14/03/2022).

499 Por ejemplo en <https://www.myheritage.es/> (última consulta 14/03/2022).

parientes biológicos de una persona entre los usuarios de dicho servicio⁵⁰⁰. Ésta aplicación de la genética es la que ha llamado la atención de las autoridades policiales.

Su uso adquirió relevancia pública en 2018, a partir de la detención del conocido como el *Golden State Killer* en los EEUU⁵⁰¹. Los intentos de identificar genéticamente a este *serial killer* se remontan al año 2014 cuando, utilizando bases de datos abiertas del cromosoma Y se identificaron a diversas personas, pero nada tenían que ver con el asesino. En 2018 los investigadores crearon un perfil falso en la compañía *GEDmatch* e introdujeron muestras genéticas del asesino que habían sido recogidas de los distintos sucesos. Así localizaron a primos terceros y cuartos, lo que permitió reconstruir el árbol genealógico del asesino desde el siglo XIX⁵⁰². De este modo dieron con él.

Al finalizar el primer trimestre de 2020, las cuatro principales compañías que actualmente ofrecen análisis genéticos directos al consumidor - DTC - disponen de los datos de más

⁵⁰⁰ La primera compañía que lanzó al mercado este servicio fue 23andme en 2009. <https://blog.23andme.com/news/introducing-relative-finder-the-newest-feature-from-23andme/> (última consulta 14/03/2022).

⁵⁰¹ El año 2018, el FBI detuvo a Joseph James DeAngelo acusado de ser el Golden State Killer, un asesino en serie que cometió al menos 13 asesinatos, 50 violaciones y más de 100 robos en California entre los años 1974 y 1986. <https://theweek.com/articles/761206/michelle-mcnamaras-tantalizing-roadmap-finding-long-lost-serial-killer> (última consulta 14/03/2022).

⁵⁰² <https://abcnews.go.com/US/inside-terrifying-golden-state-killer-crime-spreek-key/story?id=54849196> (última consulta 14/03/2022).

de treinta millones de personas, cuando en 2017 eran unos siete millones⁵⁰³. Entre los servicios que ofrecen está el de localizar los parientes biológicos a través de la identificación de fragmentos del ADN que comparten las personas con un antecesor común⁵⁰⁴.

Marcadores STR versus SNP.

Las compañías DTC han cambiado el paradigma de los análisis de ADN, ya que no utilizan marcadores STR para encontrar familiares.

Hasta la fecha las autoridades policiales han utilizado el ADN para identificar el donante de una muestra biológica. Es decir, compara dos muestras y determina si ambas proceden de la misma persona. Para ello, como hemos dicho, se usa fragmentos del ADN no codificante y no contiene información sobre los genes del individuo. Para obtener los marcadores STR de las cadenas de ADN se extrae una serie de fragmentos - marcadores - ubicados en distintos cromosomas, que están formados por pequeñas regiones de unos 100 - 500 nucleótidos compuestos por una unidad de 4 - 5 nucleótidos que se van repitiendo en tándem a lo largo de dicha región durante un determinado número de veces (*Short*

503 <https://thednageek.com/dna-tests/> (última consulta 14/03/2022).

504 En 2018 las cuatro compañías utilizaban versiones personalizadas de *Illumina* en los que se analizaban hasta 650,000 locus. PHILLIPS (2018).

Tandem Repeats - STRs) y que presentan una alta variabilidad entre los individuos. Cuanto mayor es el número de marcadores que se estudian, menor es la probabilidad que dos individuos tengan el mismo número de repeticiones en todos los fragmentos estudiados. Así, el perfil genético de un individuo en las bases de datos genéticas policiales está formado por el número de repeticiones que hay en cada uno de los 23 puntos de la cadena que se comparan, que son los que almacenan las bases de datos policiales españolas, por ejemplo. A cada lugar concreto de la cadena se le denomina locus y corresponde a uno de los números que componen un perfil genético.

Por contra, la genealogía genética usa los llamados ***nucleotide polymorphisms - (SNPs)*** – que son variaciones en la secuencia del ADN que afectan a una base. Es decir, a lo largo de la cadena de ADN se produce la modificación de una base nucleótida. De promedio, cada 1300 bases se suele dar una de estas mutaciones genéticas lo que significa que una de las bases de nucleótidos varía. Éste método permite determinar relaciones de parentesco de hasta la décima generación (de primos segundos a primos novenos).

El grado de parentesco entre dos personas vendrá dado por la cantidad esperada de ADN compartido. Durante el proceso

de división celular, las cadenas de ADN de cada progenitor se dividen de manera que solo pasa a su descendencia la mitad de la información contenida en el ADN de cada uno de ellos, pero el trozo de cadena transferida es aleatoria. Los nucleótidos que están más próximos, tienen mayor probabilidad de ser heredados conjuntamente. Por tanto, a medida que los fragmentos de ADN se vayan recombinando se irán fragmentando, así las personas que estén más cercanas familiarmente, compartirán fragmentos más largos de ADN y cuanto mayor haya sido la recombinación, más cortos serán dichos segmentos. Las pruebas genéticas realizadas por estas compañías muestrean cientos de miles de estos marcadores SNP, que oscilan entre los 500.000 y los 900.000⁵⁰⁵.

Sería necesario un 2% de los datos de una población determinada para tener al menos un primo tercero de todos los individuos de dicha población en la base de datos. Así, en el caso de la población de los EEUU que son descendientes de europeos, con una base de datos de 3 millones de estos individuos, un 99% de la población de descendientes de europeos tendría un primo tercero en dicha base de datos y un 65 % un primo segundo⁵⁰⁶.

505 KENNETT (2019)

506 ERLICH et al. (2018)

Son varios los factores que intervienen en la transmisión del ADN a los descendientes, ya que al tratarse de recombinación, puede darse el caso que primos cercanos no compartan ningún fragmento de los que comparten otros descendientes. También influye el tamaño del grupo poblacional: cuanto más endogámico es el grupo menos efectivos son los análisis ya que tienen mayor número de fragmentos de ADN comunes dado que comparten varios antecesores.

3.2.- Uso de bases de datos genéticos no policiales para la investigación de delitos graves.

El uso de bases de datos genéticas no policiales supone vencer, además de los problemas jurídicos, los problemas técnicos que aparecen. Las bases de datos policiales utilizan marcadores STR y las de las compañías DTC utilizan marcadores SNP; ello significa que deben realizarse nuevos análisis genéticos con el fin de homogeneizar los marcadores.

Así, para que las autoridades policiales puedan llegar a la identificación de un perfil genético dubitado a través de bases de datos genéticas de compañías DTC debería seguirse el siguiente proceso:

1.- En primer lugar, la muestra biológica de interés debería ser analizada para obtener el perfil genético que estaría compuesto por 23 alelos. Dicho perfil sería introducido en las bases de datos policiales donde se almacenan los perfiles genéticos de personas con antecedentes policiales de delitos graves.

De no producirse un match con las muestras que contiene la base de datos, se debería llevar a cabo una *familial searching* con los perfiles genéticos de la base de datos. Dado el reducido número de marcadores genéticos disponibles, su uso en búsqueda familiar da lugar a resultados deficientes.

2.- Uso de las bases de datos no policiales, esto es de **Compañías DTC.**

De no obtener un uso satisfactorio en el primer punto, la muestra biológica dubitada debería ser enviada a una compañía DTC donde se debería llevar a cabo un nuevo análisis con el que se obtendrían los marcadores que la compañía utiliza.

Hay compañías que explícitamente no permiten que los *“funcionarios encargados de hacer cumplir la ley presenten muestras en nombre de un preso o alguien bajo custodia*

*estatal que haya sido acusado de un delito*⁵⁰⁷. En cambio, a raíz de lo acontecido en la investigación del Golden State Serial Killer, otras compañías han actualizado sus normas de confidencialidad para permitir que la información genética que contienen sus bases de datos sean utilizadas por las autoridades policiales⁵⁰⁸.

Para ello se requiere que el Estado cree una obligación en el responsable del tratamiento de los datos para que le obligue a cederlos. En caso de no existir una legislación que ampare el uso de estos datos por las autoridades policiales, su uso debería ser autorizado por los tribunales cuando *actúen en ejercicio de su función judicial*⁵⁰⁹. Por lo tanto, el único modo que las autoridades policiales pudieran utilizar datos genéticos almacenados por las compañías DTC sería bajo autorización judicial, en el ejercicio de sus funciones de investigación de delitos. Así, un juez debería emitir una orden dirigida a una determinada compañía para que fueran introducidos los datos del perfil dubitado en su base de

507 La compañía **23andme** lo considera una violación de sus condiciones contractuales. No así la cesión de datos bajo un requerimiento judicial. <https://www.23andme.com/en-int/law-enforcement-guide/> (última consulta 14/03/2022).

508 La compañía **GEDmatch** autoriza que se introduzca “*ADN obtenido y autorizado por la policía para identificar a un autor de un delito violento contra otra persona, donde 'delito violento' se define como asesinato, homicidio no negligente, violación agravada, robo o agresión agravada*”. <https://www.gedmatch.com/terms-of-service-privacy-policy> (última consulta 14/03/2022).

509 Art. 9 del Reglamento (UE) 2016/679.

datos. En mi opinión, el fundamento en el que podría basarse dicha orden, sería en el deber de colaboración que tienen cualquier persona física o jurídica con las autoridades judiciales, el Ministerio Fiscal o la Policía Judicial según la cual deben facilitar los datos que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales⁵¹⁰. Dichas compañías están obligadas a facilitar los datos que estas autoridades les soliciten.

Así, no es aceptable que se utilicen datos de personas inexistentes para encontrar familiares biológicos de perfiles dubitados que están involucrados en una investigación criminal. Pero si alguna unidad policial - con poca ética profesional - hiciera uso de este tipo de bases de datos, sería difícil detectarlo, dado que el resultado obtenido solo sería un mero indicio, carente de cualquier valor probatorio y requeriría de una posterior investigación.

El perfil social de las personas que utilizan los servicios de las Compañías DTC difieren en gran medida del perfil de las personas que tienen introducidos sus datos en las bases de datos policiales, ya que mayoritariamente pertenecen a personas que forman parte de estratos sociales distintos. Dado que los servicios que suelen dar las compañías que disponen de este tipo de bases de datos son de pago, las

510 Art. 7.1 de la ley Orgánica 7/2021, de 26 de mayo.

personas que los demandan suelen tener cierto poder adquisitivo. Por tanto, el uso de este tipo de bases de datos significaría ampliar el número de personas sobre el cual buscar parentesco con personas que, en principio, no suelen constar en las bases de datos policiales.

La búsqueda de familiares del presunto autor no se realizaría solamente entre los familiares de las personas detenidas y condenadas que tienen sus datos en las bases de datos policiales. De esta manera, se ampliaría el número de personas sobre las que se realiza la búsqueda a la vez que disminuiría la presión sobre colectivos vulnerables⁵¹¹. Más adelante volveremos sobre este tema.

3.3.- Análisis genéticos en masa.

Los análisis genéticos en masa o *dragnet* en inglés, consisten en *análisis genéticos de un grupo poblacional, más o menos amplio, en el que pueda encontrarse el responsable de un hecho criminal, con el fin de realizar la comparativa con las muestras genéticas obtenidas de la víctima o en el lugar del delito*⁵¹². Actualmente deberíamos precisar que no

⁵¹¹ Hay ciertos autores que defienden la creación de una base de datos genética universal, de manera que los colectivos socialmente más desfavorables no padecerían la presión de ser los que aportan mayor número relativo de candidatos. (BIEBER, BRENNER y LAZER 2006).

⁵¹² Definición dada por la Comisión Nacional Para El Uso Forense del ADN en 2012 en el resumen de actividades de 2012.

es necesario que se encuentre el responsable del hecho criminal en el grupo que facilita la muestra genética. Bastaría con que se encontrara un familiar próximo en ese grupo para poder llegar hasta él.

Ésta es una manera de “ampliar” el número de perfiles genéticos para que sean comparados en un caso concreto. Si la muestra localizada en el lugar de los hechos no coincide con los perfiles genéticos que hay en las bases de datos policiales, puede llevarse a cabo la *familial search* en la misma base de datos y, en caso de no encontrar ningún candidato a familiar del autor, se podrían utilizar bases de datos no policiales, como las de las compañías DTC que hemos explicado anteriormente.

Si no se obtuviera candidato alguno, podría llevarse a cabo un análisis genético en masa a un grupo concreto de población entre el que podría hallarse el presunto autor. Normalmente suelen involucrar cientos o miles de personas de la zona donde residiría el presunto autor y que compartirían una serie de características genéticas con él. Para ello los ciudadanos deberían ceder voluntariamente una muestra de saliva para extraer su información genética y ser comparada con la obtenida en la escena del crimen.

Cuantos más datos se disponga del autor, más acotado será el grupo poblacional sobre el que se solicitará que se realicen las pruebas genéticas y más fácil será detectar si una persona no se ha sometido a dichas pruebas. El sexo, el color de la piel, la franja de edad o el lugar de residencia, puede ayudar a reducir el número de personas a las que se realizarán las pruebas de ADN y hacer viable éste método de investigación.

La **Comisión Nacional Para El Uso Forense del ADN** establece una serie de requisitos para llevar a cabo esta ingente recolección de material genético:

- Se tienen que haber agotado todas las líneas de investigación en relación con ese caso concreto. La dificultad que puede suponer estos análisis genéticos masivos, a nivel económico, logístico y de movilización de personal, obligaría a ser llevado a cabo de manera excepcional, en casos graves y sin líneas de investigación viables. Por ello sería necesario también disponer de un nicho poblacional definido al cual se le va a solicitar el material genético.
- Dada la intromisión al derecho a la privacidad y al de la protección de datos que supone una medida de estas

características, se requeriría una autorización judicial para llevarla a cabo.

- Las personas que cedan su material genético lo deben hacer de forma voluntaria, sin ningún tipo de coacción. Dicho material genético solo podrá usarse en la investigación para la que ha sido recabado y una vez ya no sea útil, deberá ser destruido, sin ser comparado con los datos obrantes en las bases de datos policiales.

Respecto al último punto, parece que las personas que se ofrecen a participar en un evento de este tipo no pueden hacerlo con total libertad de decisión, sino que lo hacen bajo la coacción de su entorno. La presión puede consistir en que si no ceden su material genético voluntariamente, podrían verse señaladas por sus propios vecinos como presunto autor ya que si se es inocente, no tiene por qué negarse a ayudar a las autoridades a prender un autor de un delito grave. Y cuanto mayor es el número de personas que acceden a ceder sus datos genéticos, mayor será la presión que se ejerce sobre los individuos para que accedan a participar.

Por otro lado, la policía puede utilizar dicha negativa para iniciar una investigación contra esa persona, lo cual podría

suponerle la vulneración de otros derechos. Al final, para salir indemne de la investigación, un individuo debería ceder su material genético para que pueda ser comparado, sino la sombra de la sospecha sobre él podría ser permanente.

4.- Problemática jurídica en el uso de la *familial search*.

Una vez vistas las posibilidades que ofrece el análisis de ADN en la investigación criminal y hacia dónde va la ciencia en este campo, vamos a analizar detalladamente la problemática jurídica que conlleva estas nuevas técnicas en el campo de la vulneración de derechos fundamentales. Esta técnica no solo afecta al implicado, sino también a los numerosos familiares biológicos de éste que se verán afectados por los medios utilizados por las autoridades policiales en la resolución del crimen.

En un plato de la balanza debe colocarse el derecho a la libertad y a la seguridad que tienen los ciudadanos. El estado tiene la obligación de disponer de los medios legalmente necesarios para identificar, detener y poner a disposición judicial a los responsables de haber cometido delitos, sobre todo si son graves. Por eso dispone de un cierto margen de maniobra para elegir los medios necesarios para conseguir

dicha finalidad; pero ello no supone que no esté sujeto a la supervisión, tanto en lo que respecta a la legislación como a las decisiones que la aplican⁵¹³. La amplitud de dicho margen dependerá de la naturaleza del derecho amenazado, la importancia de dicho derecho para el individuo, la naturaleza de la interferencia así como la finalidad perseguida. El margen será más estrecho cuando se trate de derechos más íntimos o cruciales. Cuando no haya consenso entre los distintos estados del Consejo de Europa, ya sea sobre la importancia del derecho en juego o sobre la mejor manera de protegerlo, el margen de apreciación será más amplio⁵¹⁴.

Cada vez son más los países del Consejo de Europa que utilizan este método para identificar a delincuentes a partir del ADN dubitado localizado en la escena de un crimen. A pesar de la escasa legislación existente sobre su utilización, parece que su aplicación se va extendiendo. Esta técnica se empezó a utilizar en el Reino Unido y los Países Bajos; en otros países como España, Portugal e Italia, su aplicación es escasa a causa del poco desarrollo de sus bases de datos genéticas. En Francia, en cambio, falta desarrollar la legislación específica⁵¹⁵.

513 STEDH de 4 de diciembre de 2015. Caso Roman Zakharov c. Rusia.

514 STEDH de 30 de enero de 2020. Caso Breyer c. Alemania, párrafo 80.

515 GARCÍA O., CRESPILO M. y YURREBASO I. (2017).

A continuación vamos a ver una serie de aspectos críticos en lo que se refiere a protección de derechos fundamentales y a los que las nuevas técnicas de investigación criminal basadas en el ADN deberán hacer frente en un futuro no muy lejano.

4.1.- Datos genéticos.

En 2008 el TEDH dictó la sentencia Marper en la que concluía que la mera retención de los datos genéticos supone una injerencia al derecho a la vida privada de las personas involucradas dada la capacidad que tienen este tipo de datos personales de proporcionar relaciones entre personas. El Tribunal hacía referencia a la relación ADN y origen étnico/geográfico de los individuos, pero actualmente hemos visto que la relación que puede establecer va más allá que la del origen geográfico⁵¹⁶.

Los datos genéticos, todo y que son utilizados para obtener la coincidencia entre dos muestras, no pueden ser considerados al mismo nivel de vulneración de la intimidad que las huellas dactilares. Aún con los pocos marcadores que utilizan los laboratorios policiales para obtener un perfil genético, de ellos pueden inferirse relaciones de parentesco biológico. No se podrán obtener datos relacionados con

⁵¹⁶ STEDH de 4 de enero de 2008, Caso S. y Marper c. Reino Unido, párrafo 75.

características genéticas, como por ejemplo enfermedades hereditarias, pero sí se pueden intuir relaciones familiares, como hemos visto en el caso de la familia imperial rusa. En cambio, a partir de las huellas dactilares, no puede inferirse nada más que la coincidencia entre dos huellas.

Lo que hace especialmente sensible al uso de perfiles genéticos en las investigaciones policiales es su capacidad de establecer relaciones entre individuos. No es el hecho de permitir identificar la persona a la que pertenece una muestra genética localizada en un lugar determinado, que de igual modo se puede conseguir con la comparación de las huellas dactilares; sino que es la información potencial que existe en el perfil genético del individuo. Esto es lo que convierte en sensibles los datos que componen un perfil genético: su uso potencial en *familial searching*. Y con las nuevas técnicas genéticas, la información que puede obtenerse a partir de una muestra biológica es cada vez mayor. Las investigaciones policiales se llevan a cabo, entre otras cosas, con información y lo que puede ofrecer el *familial search* es mucha información procedente de esa muestra biológica.

Además, todos los candidatos que proporciona el sistema después de aplicar una *familial search* son potencialmente familiares del autor y deberían ser investigados de igual

manera. De entrada todos ellos serán presuntos familiares del autor, en mayor o menor medida, lo que implica que cuanto mayor sea el número de potenciales parientes, menor será la probabilidad de hallar el presunto autor ya que se dificulta enormemente el recabar información sobre los familiares de todos ellos. Si de la aplicación de las técnicas de *familial searching* a las muestras biológicas dubitadas resulta que se debe investigar a tres o cuatro personas, es relativamente sencillo recoger ADN de estos individuos, incluso sin que se den cuenta, y analizarlo para contrastarlo con la muestra dubitada. Estas personas sufrirán una vulneración de su derecho a la privacidad de la que, en muchos casos, no serán conscientes. Pero, si la técnica de *familial searching* proporciona 50 o 100 candidatos, nada impide a las fuerzas del orden actuar del mismo modo. Que se lleve a cabo o no dependerá de una decisión político-policial. Se tendrán en cuenta factores logísticos, económicos, así como de la gravedad de los hechos de que se trata. Las fuerzas policiales tendrán más en cuenta estos ítems que no la vulneración de derechos a la que se podrán ver sometidas las personas investigadas.

Desde la sentencia Marper, la investigación genética en las ciencias forenses ha evolucionado y la *familial search* en el ámbito policial se ha convertido en una realidad. Además,

todo indica que el uso de los datos genéticos en las investigaciones policiales de delitos graves irá adquiriendo cada vez más importancia y su uso se hará más generalizado. Por ello, en 2020, en el caso Gaughran el Tribunal volvió a recordar que la *“capacidad de los perfiles de ADN para proporcionar un medio de identificar las relaciones genéticas entre individuos es en sí misma suficiente para concluir que su retención interfiere con el derecho a la vida privada de los individuos en cuestión”*. Por tanto, el uso de la familiar searching en las investigaciones policiales *“es de naturaleza altamente sensible y existe la necesidad de controles muy estrictos a este respecto”*⁵¹⁷, necesidad con la que no podemos estar más de acuerdo. Antes de que se empiece a generalizar el uso de la genética forense como medio de investigación y evitar vulneraciones de derechos fundamentales, sería necesaria una regulación, a ser posible, consensuada entre todos los sujetos activos que participan en ella.

El tratamiento de los datos genéticos con el objetivo de investigar infracciones penales entra dentro del campo de aplicación de la Directiva 2016/680. Ésta considera los datos genéticos como una categoría especial de datos personales por lo que solo se permitirá su tratamiento *“cuando sea*

⁵¹⁷ STEDH de 13 de febrero de 2020. Caso Gaughran c. Reino Unido, párrafo 81.

estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado” y bajo unas premisas muy concretas. Por ello, cuando se delegue su tratamiento, el encargado de dicho tratamiento deberá ofrecer *"garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente Directiva y garantice la protección de los derechos del interesado"*⁵¹⁸. Por tanto, la Directiva autoriza a que las autoridades policiales puedan ceder datos genéticos a empresas para que se lleve a cabo una *familial searching* con un perfil dubitado localizado en la escena del crimen. Dicha cesión debería ir vinculada a un acto jurídico que obligue a ambas partes, de manera que no sería aceptable que las autoridades policiales introdujeran un perfil genético en una base de datos de una DTC de forma subrepticia, sin informar a la compañía del objetivo que se persigue al utilizar sus servicios.

A mi entender, urge una legislación en la que se acoten las técnicas que puedan utilizarse, una legislación lo suficientemente amplia que permita su uso salvaguardando el derecho a la intimidad de las personas que se puedan ver implicadas. Este tipo de técnicas deberían supeditarse al

518 Art. 22 de la Directiva (UE) 2016/680.

control judicial para que pondere la necesidad social de atrapar al delincuente frente a la vulneración de derechos que se producirá llevando a cabo la investigación con estas técnicas.

4.2.- Implicación de distintos laboratorios.

Los laboratorios forenses que usan las FCSE utilizan técnicas de análisis de microsátélites STRs - Short Tandem Repeats -. En cambio, los laboratorios de las Compañías DTC utilizan métodos de análisis de polimorfismos puntuales SNPs - *Single Nucleotide Polymorphisms* -. Pero cada compañía DTC utiliza sus propios SNP, dependiendo de cuál sea el objetivo comercial de la compañía. De manera que en función del tipo de resultado que se busque, serán necesarios distintos análisis y, posiblemente, se llevarán a cabo en laboratorios privados que necesitarían de una homologación.

Las técnicas de laboratorio que utilizan las compañías del sector están adaptadas a sus necesidades - como no puede ser de otra manera -, por lo que los marcadores SNP que analizan depende de cada empresa. Además, estos marcadores han ido evolucionando a lo largo del tiempo, a la

vez que mejorando sus *outputs*. Así, no hay un estándar de análisis ni de algoritmos a aplicar.

4.3.- Investigación policial que afecta a personas sin relación con el hecho delictivo.

La búsqueda de familiares genéticos del donante de la muestra dubitada se llevará a cabo cuando no se produzca ninguna coincidencia con los perfiles que hay introducidos en la base de datos policial. Por tanto, los candidatos que se obtengan lo serán porque compartirán algunas características genéticas con el presunto autor. Pero, para poder llegar hasta él, será necesario investigar a estos candidatos, con los que no existe sospecha alguna sobre su vinculación con el hecho delictivo al no coincidir su perfil genético con el de la muestra dubitada. Dicha investigación podrá afectar a su derecho a la privacidad, al de intimidad y al de protección de datos por el simple hecho de ser presunto familiar de una persona a la que se quiere identificar. La *familial search* genera posibilidades de coincidencia, lo cual da lugar a falsos positivos.

Cuando en la base policial de datos genéticos se da una coincidencia entre un perfil dubitado y uno indubitado, dicha coincidencia es única. Los alelos analizados de ambas

muestras coinciden. Cuando se aplican técnicas de *familial search* solo coinciden algunos alelos, de manera que un mismo sujeto puede verse afectado por la investigación relativa a la identificación de familiares biológicos de diversas muestras dubitativas. Tener un alelo poco frecuente, por ejemplo, puede provocar ser candidato a investigado en diversas ocasiones.

La persona que tiene introducido su perfil genético en la base de datos sale beneficiada respecto de las personas que no las tienen. Así, al no producirse un match con los perfiles de dicha base, resulta que el autor no está en ella y se debe buscar entre los parientes de dichas personas. Las personas de la bases de datos serán escudriñadas con la finalidad de identificar sus familiares y, al final, los investigadores compondrán su árbol genealógico, con las implicaciones familiares que ello conlleva. Son muchas las personas sobre las que los investigadores pondrán la lupa. La investigación sobre ellas finalizará cuando las mismas personas que son investigadas cedan – voluntaria o involuntariamente - su perfil genético para que sea comparado con el perfil dubitado. Si el perfil de esta persona estuviera introducido en la base de datos policial, ya habría sido descartada anteriormente y su privacidad, quizás, no se habría visto afectada.

Así, se da la paradoja que las personas que tienen introducidos los datos genéticos en bases de datos policiales - que son personas con antecedentes penales o policiales - se libran de la investigación, pero no así sus familiares, que al no tener antecedentes no estarán en las bases de datos policiales y, por tanto, son posibles candidatos a averiguar si su perfil genético coincide con el perfil dubitado.

En el caso del asesino del Golden State, se llegó a investigar el antecesor común que compartían el asesino y un familiar biológico que tenía su perfil genético introducido en las bases de datos de una compañía DTC. Este familiar común, fue el padre de sus respectivos tatarabuelos y vivió sobre el 1800. Así, la investigación requirió averiguar todos los antepasados de dicho familiar actual y, una vez identificado el padre de su tatarabuelo, se investigaron los descendientes de ese antepasado común. De esta manera se llegó a dos individuos que vivían en la costa Oeste y que tenían características coincidentes con el asesino. El ADN de una de estas personas fue comparado con el del autor pero el resultado fue negativo. Siguiendo la otra línea genealógica, se fue a dar con un ex-oficial de policía al que se le recogió ADN sin su consentimiento. En este caso, su perfil genético coincidió con el del asesino, por lo que fue detenido⁵¹⁹.

519 LA Times, at <https://www.latimes.com/local/lanow/la-me-golden-state-dna-match-20180427-story.html>. (última consulta 14/03/2022).

Una investigación de este tipo requiere un gran esfuerzo de medios técnicos y humanos todo y que tiene un final incierto. Si alguna de las ramas de la familia emigró a otro país, por ejemplo, sería muy difícil seguir el rastro genealógico. Por no hablar de proles muy numerosas o de pérdida de registros escritos, que podría llevar a investigar ramas familiares que nada aportarían a la investigación, como de hecho sucede.

Estas investigaciones son muy costosas en dos sentidos: en primer lugar la afectación de derechos fundamentales que supone investigar a un grupo tan numeroso de terceras personas de las que no existe, ni en muchos casos puede existir sospecha, pudiendo incluso estar muertas muchas de ellas. La segunda, es la inversión económica, de tiempo y de dinero que supone una investigación de estas características que, de ningún modo, con la tecnología actual supone una garantía de éxito.

Una vez pasado el filtro de la investigación de los familiares, llega el turno a los candidatos a autor de los hechos. Como hemos dicho anteriormente, una investigación de este tipo no tiene por qué dar un único candidato a culpable; de hecho suelen ser varios. Por lo tanto, el último paso es obtener la muestra de ADN del presunto autor para cotejarla con la hallada en la escena criminal. Al llegar a ese punto, debe

estudiarse el perfil genético de esa persona, por lo que el individuo se halla ya bajo sospecha y que puede ser culpable de un delito grave. La mera sospecha de ser autor de un delito de esta índole puede significar el final de una trayectoria laboral, un divorcio o una simple mirada de desprecio en un supermercado. Y no solo afecta al individuo en cuestión, sino también a su entorno familiar.

En 1973 tres adolescentes fueron asesinadas y de la escena del crimen se localizaron muestras biológicas que serían del autor. 28 años después sin obtener resultados, se realizó *familial searching* con dichas muestras utilizando la base de datos de ADN Británica (NDNAD) y se identificó a una persona que compartía el 50% de su ADN con el del autor: era el hijo del autor. Pero resulta que el padre, Joseph KAPPEN, había muerto hacia 10 años. Llegados a ese punto, los investigadores convencieron a la familia para que diera muestras de ADN y confirmaron su culpabilidad. Entonces exhumaron el cuerpo del difunto, obtuvieron muestras genéticas y confirmaron que, efectivamente, se trataba del asesino⁵²⁰. El caso se cerró.

Ahora bien, qué habría pasado si los investigadores hubieran llevado a cabo todos los pasos y al final, después de analizar

⁵²⁰ Se puede consultar la noticia en <http://aboutforensics.co.uk/joseph-kappen/> (última consulta 14/03/2022).

las muestras exhumadas, resultara que no es el asesino. Todo y coincidiendo los perfiles genéticos, el Sr KAPPEN no puede defenderse y quizás tuviera una respuesta de porqué su ADN estaba en la escena del crimen, sin ser el autor. Aquí podrían darse otras víctimas, que son la familia del presunto autor. Tanto derecho tienen los familiares inocentes del autor a verse libres de esta victimización, como el derecho de los familiares de la víctima o la propia víctima a que se identifique y se castigue al autor. El Estado debe mediar para que haya un equilibrio entre los derechos de ambas partes.

En 2015 el Sr Ursy fue acusado de la muerte de una mujer ocurrida en 1996, ya que se obtuvo una coincidencia parcial que se daba entre el cromosoma Y del Sr Ursy – que había subido su perfil genético a una base de ADN pública - y el del semen localizado en el cadáver de la víctima. Cuando se hizo la comparación de perfiles, se comprobó que el Sr Ursy no era el asesino. Las pruebas tardaron un mes que Ursy vivió en suspenso por temor a ser detenido, independientemente del resultado de las pruebas⁵²¹.

Las personas investigadas, sobre las que la sociedad tiende a tratar como presuntos culpables, no pueden permanecer demasiado tiempo bajo el impacto de una acusación y debe

⁵²¹ https://www.nola.com/article_d58a3d17-c89b-543f-8365-a2619719f6f0.html.
(última consulta 14/03/2022).

dirimirse sobre la legitimidad de la fundamentación de la acusación⁵²². Este tipo de análisis debería llevarse a cabo con celeridad, sobre todo si el interesado es consciente que está siendo investigado. No debemos olvidar que esta técnica se basa en la probabilidad que dos personas sean familiares biológicos y hasta que no se compare el perfil genético del presunto autor con el obtenido de la muestra dubitada, no se habrá acabado el proceso.

Por lo tanto, estas investigaciones deben ser llevadas a cabo con tacto, evitando inmiscuirse innecesariamente en la vida de las personas investigadas y preservando al máximo su derecho a la intimidad. Es importante que las autoridades policiales actúen con discreción, no facilitando información referente a las personas que están siendo investigadas y así evitar una victimización como consecuencia de la propia investigación. En una sociedad democrática, son inevitables los comentarios severos de la prensa en asuntos que interesan al público⁵²³, dado que el coste personal de aparecer públicamente conectado, de cualquier modo a algún delito, es innegable, máxime si la información permite identificar a la persona, en el contexto actual de rápida y efectiva profusión de las noticias tanto mediante los medios de comunicación, como mediante las redes sociales.

522 STEDH de 27 de junio de 1968. Caso Wemhoff c. Alemania, párrafo 18.

523 STEDH de 30 de junio de 2009. Caso Viorel Burzo c. Rumanía, párrafo 160.

4.4.- El consentimiento informado, ¿es suficiente?.

Como se ha visto en el capítulo anterior, una de las formas de obtener el perfil genético indubitado de una persona es a partir del análisis de una muestra biológica que ha sido facilitada voluntariamente, con un *consentimiento informado*. El interesado tiene derecho a tener la información completa referente a los cargos que podrían pesar contra él en caso de que su perfil genético sea coincidente con el de la muestra dubitada, es decir, la calificación jurídica que un tribunal pudiera adoptar en su contra⁵²⁴.

Desde el punto de vista jurídico, y a mi juicio, la obtención del perfil genético de una persona que da el *consentimiento informado* para la cesión voluntaria de la muestra biológica no genera ningún problema, si la finalidad es hacer una comparación de perfiles genéticos para obtener una coincidencia. Es decir, se comprará el perfil genético cedido por el individuo con el de la muestra dubitada hallada en el lugar de los hechos.

Actualmente, las autoridades policiales utilizan los 23 marcadores extraídos del ADN no codificante de una muestra genética, que constituye el perfil genético, y que supone un

⁵²⁴ STEDH de 25 de marzo de 1999. Caso Pélissier y Sassi c. Francia, párrafo 52; STEDH de 1 de marzo de 2006 Caso Sejdovic c. Italia, párrafo 90.

código numérico que identifica sin ningún género de dudas el donante de la muestra. Pero, a partir de un perfil genético, es posible también conocer características del perfil genético de sus progenitores o de sus descendientes, en definitiva, de sus familiares biológicos. ¿Se le informa de este aspecto al donante de la muestra?; ¿es consciente el donante que a través de su muestra puede establecerse una relación entre un familiar suyo y la muestra dubitada?

En el ADN celular no hay información exclusiva del donante, sino que también contiene información genética relativa a sus parientes biológicos próximos y a sus ancestros. Las técnicas más modernas de análisis de parentesco permiten obtener datos del donante de la muestra, como pueden ser color de los ojos, de la piel o enfermedades de genéticas. Esta información no solo pertenece a la persona donante de la muestra, sino que es compartida también por sus familiares biológicos, un conjunto de personas que no han intervenido en su toma de decisión cuando accedió a dar su muestra biológica. Si esa persona tiene una enfermedad que se transfiere genéticamente, por ejemplo, dicha información puede estar compartida también con sus ascendentes, descendentes y hermanos. Este tipo de información no solo es de la persona que da el consentimiento, sino que también pertenece a sus familiares biológicos. La cesión de los datos

genéticos de un individuo implica también ceder los datos genéticos de otras personas.

En los formularios policiales de consentimiento informado que firman los donantes de una muestra biológica deberían estar preparados para recoger este tipo de eventualidades si se quieren utilizar las nuevas técnicas genéticas de *familial search* en la investigación criminal.

De todas formas, el resultado de este tipo de análisis nunca será definitivo ya que a nadie se le va poder imputar un delito por el hecho de tener los ojos azules o el pelo rizado. Siempre deberá realizarse una prueba de ADN a una muestra biológica de la persona sospechosa que es la que determinará su culpabilidad.

En el ámbito no policial, las compañías que ofrecen análisis genéticos directos al consumidor - DTC - subsanan este punto previendo en sus formularios de *consentimiento informado* hasta donde debe llegar la obligación de la empresa. Hay autores que han llevado a cabo un listado con la información que estas compañías deberían facilitar a sus clientes para obtener tal consentimiento. Los campos que incluyen son los siguientes: el ámbito del test, la descripción del proceso a realizar, los posibles beneficios y riesgos,

disponibilidad de pruebas alternativas, posibilidad de rechazar las pruebas, el uso futuro de los datos y las muestras, confidencialidad de los resultados y la gestión de los resultados casuales⁵²⁵.

La responsabilidad de informar a familiares de los hallazgos realizados que les puede afectar debería recaer sobre el interesado, el donante de la muestra genética, que no tiene por qué ser el mismo que solicita el análisis. Todo individuo es propietario de su información y tiene el derecho de revelarla a quien crea conveniente.

De esta manera, el donante de la muestra podría informar a los familiares que se han visto afectados por los hallazgos genéticos que ha realizado la compañía en cuestión. A mayor gravedad de la afectación a terceras personas, mayor sería la responsabilidad ética o moral, que no jurídica, de comunicarlo al familiar afectado. Por su parte, el TEDH no se opone a que existan obligaciones a los Estados que les exija proporcionar información esencial a las personas afectadas sobre los riesgos para su salud⁵²⁶.

525 Niemiec et al. (2016).

526 STEDH de 19 de febrero de 1998. Caso Guerra y otros c. Italia, párrafos 58 y 60.

4.5.- Derecho a no conocer.

Los usuarios de los servicios de compañías DTC tienen la necesidad de obtener información sobre sí mismos. Así, a partir del estudio de su ADN obtendrán información acerca de su genealogía, como mejorar su alimentación, forma física, salud y otras muchas aplicaciones que tiene la genética recreativa.

Pero nuestra sociedad está fundamentada en relaciones sociales, que no tienen por qué coincidir con las biológicas. Utilizar técnicas de *familial search* con el material genético de una persona hace que se pueda revelar información acerca de ellos mismos y de sus familiares, pero que ni estos ni el interesado tienen por qué desear conocer. Pueden revelarse vínculos de parentesco y, por ende, de no parentesco. Así, pueden salir a la luz relaciones familiares “ocultas” o privadas como pueden ser adopciones, infidelidades, casos de incesto,... que ninguna de las personas involucradas en el análisis genético puede desear conocer. Si las personas que ceden sus datos genéticos a las compañías DTC lo hacen para obtener información acerca de su salud, la información que reciba este sujeto debería ser relativa a este campo. No debería recibir información sobre otros aspectos, como

pueden ser su genealogía o posibles relaciones familiares que desconozca.

Del mismo modo, los familiares biológicos del autor nunca deberían llegar a conocer que cierto familiar está siendo buscado por las autoridades policiales por haber cometido un delito grave. Ninguno de los dos debería llegar a conocer que a través de uno de ellos se ha llegado a la identidad del otro.

El derecho a no conocer sería el que, quizás, más fácilmente podría salvaguardarse, ya que con la discreción y la reserva que requieren este tipo de investigaciones policiales, bastaría con la no comunicación de la información obtenida.

De este modo, la policía cedería la muestra biológica a analizar a la compañía DTC en cuestión. Ésta llevaría a cabo el análisis y cotejaría el resultado con sus bases de datos, obteniendo una serie de candidatos con cierto grado de parentesco familiar de la persona buscada. La muestra biológica debería retornar a las autoridades policiales con el resultado para iniciar la investigación. A partir de aquí, los datos obrantes en la base de datos de la compañía DTC deberían ser eliminados y la compañía tampoco debería hacer ninguna comunicación a ninguno de sus clientes: todo el proceso debería quedar en la reserva de la investigación y

ser la autoridad judicial quien decidiera las comunicaciones que se deben llevar a cabo en base de los resultados obtenidos.

Pero, las personas involucradas en el resultado obtenido, ¿tienen derecho a conocer que están siendo investigadas? En mi opinión, si no se han vulnerado los derechos fundamentales de estas personas, no sería necesaria esta comunicación. Así, la aplicación de técnicas de *familial search* hará que se produzca una terna de personas que nada tienen que ver con el delito, pero que pueden estar emparentados con el autor. La investigación policial se cernirá sobre estos familiares del autor y, si no se les vulneran derechos fundamentales, no creemos que sea necesario que deban de tener conocimiento de que han sido investigados. De hecho, durante una investigación convencional, la policía sigue una serie de pistas que al final le permiten identificar y detener el autor de los hechos. En numerosas ocasiones, esas pistas consisten en placas de matrícula de vehículos, direcciones o números de teléfonos, todo lo cual lleva asociados datos de personas. Sería absurdo tener que comunicar a todas las personas que han aparecido a lo largo de una investigación el hecho de haberse visto involucradas en la misma de uno u otro modo.

Así, bajo mi criterio, el factor determinante que debe pesar sobre una persona para que se le comunique su implicación en una investigación, viene dada por la vulneración de derechos fundamentales. Si a esa persona se le han vulnerado derechos fundamentales durante la investigación, se le debería poner en conocimiento dicha vulneración; de no ser así, no sería necesario.

De todos modos, la comunicación debería realizarse una vez finalizada la investigación o agotada la línea en la que se ha visto involucrada esta persona.

4.6.- Uso de bases de datos genéticas policiales.

Como se ha dicho anteriormente, el tratamiento de los datos genéticos entra dentro de la protección del art. 8 del CEDH. Las excepciones al derecho a la protección de datos que se enumeran en el punto 8.2 del artículo deben interpretarse de manera restrictiva; la norma debe ceñirse a una de las finalidades que menciona dicho apartado⁵²⁷.

Aplicado a nuestro caso, el objetivo de llevar a cabo *familial search* en las bases de datos policiales no es otro que el de prevenir el crimen y, para ello, se utilizará datos identificativos obtenidos a partir de los análisis de ADN procedentes de una

⁵²⁷ STEDH de 8 de abril de 2010. Caso de Aliyev c. Azerbaijan, párrafo 182.

investigación criminal y que sean reveladores, exclusivamente, de la identidad del sujeto y del sexo. No se utilizarán los de naturaleza codificante que puedan revelar cualquier otro dato o característica genética⁵²⁸.

Entonces debemos examinar si actualmente el uso de las bases de datos policiales para llevar a cabo *family search* - como forma de tratamiento de datos personales - cumple los requisitos que establece el segundo párrafo del mencionado art. 8. Así, el tratamiento se debe llevar a cabo en **concordancia con la ley**, que sea **necesaria en una sociedad democrática** para conseguir uno de los objetivos que menciona el articulado - el de la prevención de infracciones penales - y que la medida sea **proporcional a los fines perseguidos**.

La **concordancia con la ley** exige que la medida tenga la base en el derecho interno, ser lo suficientemente accesible, el interesado debe prever las consecuencias de la aplicación de dicha ley y, finalmente, el derecho interno debe ser compatible con el estado de derecho⁵²⁹. La norma marco para llevar a cabo el tratamiento de datos personales por parte de las autoridades encargadas de la investigación de infracciones penales, entre otras finalidades, es la Directiva

528 Considerando II de la Ley Orgánica 10/2007.

529 STEDH de 1 de Julio de 2008. Caso Liberty y otros c. Reino Unido, párrafo 59.

2016/680⁵³⁰. A nivel nacional existe la Ley Orgánica 10/2007 que crea la base de datos policial sobre identificadores obtenidos a partir del ADN con la finalidad de ser utilizada por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado en la investigación de los delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada⁵³¹.

Parece que este caso no plantearía ningún problema respecto a la accesibilidad de la ley, la cual es previsible, suficientemente precisa y el ordenamiento jurídico español proporciona garantías adecuadas y efectivas contra el abuso de la misma⁵³². Esta norma, como hemos visto en el capítulo anterior, acota los casos en los que se puede utilizar la información genética incluida en la base de datos. Por lo tanto, la calidad de la ley cumpliría los estándares solicitados por el TEDH⁵³³.

530 Art. 1 Directiva (UE) 2016/680.

531 Art. 3.1.a y art. 7.1 de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

532 STEDH de 24 de abril de 20158. Caso Benedik c. Eslovenia, párrafo 125.

533 STEDH de 16 de febrero de 2000. Caso Amann c. Suiza, párrafo 52.

En cuanto a determinar si la *injerencia es necesaria en una sociedad democrática*, el propio Tribunal ha reconocido que para equilibrar el interés del Estado en la lucha contra el crimen frente la gravedad de la injerencia en el derecho de que se trate, las autoridades nacionales disponen de cierto *margen de apreciación*, el cual estará sujeto a la supervisión europea. La frontera entre las obligaciones positivas y negativas del Estado según el art. 8 no se prestan a una definición precisa⁵³⁴. La evaluación dependerá de todas las circunstancias del caso, tales como la naturaleza, el alcance o la duración de las medidas, el motivo por el que se ordenan, las autoridades competentes que las llevan a cabo, la supervisión y el tipo de recurso que facilita la legislación nacional⁵³⁵. La expresión *necesario para una sociedad democrática* ya lleva inherente un amplio concepto de proporcionalidad, que requiere de una conexión racional entre las medidas adoptadas y el objetivo que se persigue, o sea, que deben ser medidas idóneas para producir el efecto deseado⁵³⁶.

Utilizando la *familial search* con las bases de datos policiales de perfiles genéticos, se lleva a cabo un uso ligeramente

534 STEDH de 5 de octubre de 2010. Caso Köpke c. Alemania.

535 STEDH de 25 de mayo de 2021. Caso big brother watch y otros c. Reino Unido, párrafo 308.

536 STEDH de 15 de octubre de 2015. Caso Perinçek c. Suiza, párrafo 246. STEDH de 24 de abril de 2015. Caso Benedik c. Eslovenia.

distinto para el que inicialmente están previstas. No se buscaran coincidencias totales entre dos perfiles genéticos sino que se tendrán en cuenta también las coincidencias parciales. A mi entender, se trata de una aplicación compatible para conseguir – al menos teóricamente - la finalidad perseguida.

Si, por lo que parece, bajo el punto de vista legal no hay problema en usar los datos obrantes en las bases de datos policiales para llevar a cabo la *familial search*, no estaríamos tan de acuerdo en la idoneidad del proceso desde el punto de vista técnico. Se debe tener en cuenta que los perfiles genéticos que hay en estas bases de datos están formados por 23 alelos. Como se ha dicho, la búsqueda de familiares con este tipo de datos es poco precisa.

Cambiar los marcadores y utilizar marcadores SNP para hacer más efectiva la búsqueda, significaría utilizar otro tipo de datos genéticos, algunos de los cuales se asientan en partes de la cadena de ADN que proporcionan información genética del individuo, extremo que la actual ley no lo permite. También significaría tener que volver a analizar todas las muestras, tanto de personas detenidas como las de muestras biológicas localizadas en la escena del crimen lo que supondría un desembolso económico importante.

Por dar algunas cifras, estamos hablando que en 2018 en España había más de 370.000 perfiles genéticos indubitados - un 0,8% de la población - y casi 110.000 de dubitados⁵³⁷. Pero en la National DNA Database - NDNAD - del Reino Unido en septiembre de 2020 había más de 5.600.000 perfiles genéticos indubitados⁵³⁸. La National DNA Index (NDIS) de los EEUU, en las mismas fechas contenía más de 18.400.000 de perfiles indubitados⁵³⁹. Ello supone casi un 8,5% de la población de la gran Bretaña y un 5,6% de la población de los EEUU.

Si los datos introducidos fueran marcadores SNP, sería más fácil encontrar familiares de cualquier perfil dubitado con el que se compara. Según *ERLICH et al. (2018)*, solo es necesario un 2% de los datos genéticos de una población determinada para tener al menos un primo tercero de todos los individuos de dicha población en la base de datos.

537 Según la memoria de la Base De Datos Policial De Identificadores Obtenidos A Partir De ADN que publica el Ministerio del Interior. Se puede consultar en:

http://www.interior.gob.es/documents/642317/1203227/Base_de_datos_policial_identificadores_ADN_126190539_web.pdf/dc70bfcf-1c18-4720-a9df-b773e185359d (última consulta 14/03/2022).

538 La estadística se puede consultar en <https://www.gov.uk/government/statistics/national-dna-database-statistics> (última consulta 14/03/2022).

539 Se puede consultar en <https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics> (última consulta 14/03/2022).

Algunos autores⁵⁴⁰ afirman que la realización de familiar search utilizando bases de datos oficiales puede frenar la comisión de delitos por parte de personas que no tienen informatizados sus perfiles genéticos. Así, si el autor de un delito grave abandona una muestra genética en la escena del crimen, puede temer que a través del ADN de un familiar que sí está introducido en la base de datos policial, llegue a ser identificado y detenido. Sí un delincuente sin perfil genético informatizado es conocedor que puede ser identificado a través de la coincidencia de su ADN con la de un familiar que está en la base de datos, quizás no delinquirá.

Este razonamiento no hace más que ampliar el llamado *efecto disuasión* según el cual los delincuentes evitarán llevar a cabo un delito, si la probabilidad de ser identificados y detenidos es elevada⁵⁴¹. Si una persona tiene antecedentes policiales sabe que sus huellas dactilares y su perfil genéticos están introducidos en el sistema, por lo que a la hora de cometer un delito tomará precauciones para evitar dejar este tipo de vestigios o, sencillamente, no delinquirá. Con la familiar searching, las personas que no tienen antecedentes policiales pero sí los pueden tener sus familiares, podrían plantearse la comisión de cierto tipo de delitos.

540 PATTOCK (2011) p. 867.

541 TOOM, et al. (2019).

Algunos autores afirman que los delincuentes de delitos graves responden racionalmente a los incentivos de no cometer el delito, de manera que la existencia de bases de datos policiales con perfiles genéticos de delincuentes tienen un efecto de disuasión sobre los delincuentes condenados, provocando una disminución de delitos, sobre todo en los delitos contra el patrimonio y los de carácter violento⁵⁴².

En la terna de personas producto de la aplicación de la *familial searching* a partir de la cual se iniciaría una investigación policial, las primeras personas en ser investigadas serán las que tienen familiares en las bases de datos genéticas policiales. Por tanto, una persona puede ser un presunto culpable por asociación biológica, una especie de determinismo biológico, que por el hecho de tener unos determinados parámetros genéticos se convierte en un posible autor.

Ello significa que no todos los ciudadanos tienen las mismas opciones a ser candidatos a autor o, lo que es lo mismo, a ser investigados. Dado que el contenido de las bases de datos policiales varían según la raza, la etnia, el origen geográfico o la clase social, las personas de un determinado origen biológico tienen mayor probabilidad a ser investigadas que las de otros orígenes, ya que las personas ligadas

⁵⁴² DOLEAC et al. (2017).

genéticamente a las que están inscritas en las bases de datos tienen más probabilidad de ser investigadas. Así, se podría estar hablando de “*personas inocentes de primer nivel*”, que nunca van a ser investigadas utilizando este método dado que no están ligadas biológicamente a personas convictas, y “*personas inocentes de segundo nivel*”, que entran en la terna de posibles candidatos por el hecho de compartir material genético con personas convictas que no tienen ninguna relación con el hecho delictivo.

Utilizar bases de datos policiales para llevar a cabo búsqueda genética lleva aparejado un aumento de discriminación de ciertos grupos poblacionales, que son los que están mayoritariamente representados en las bases de datos. El hecho de que los marcadores STR no favorezcan la eficiencia técnica, incrementa dicha discriminación.

Debe entenderse que el legislador, cuando autoriza al Estado a guardar los datos genéticos de una persona convicta en una base de datos, dicho individuo pierde su privacidad en ese aspecto. Por el hecho de tener antecedentes policiales o penales, se adquiere la condición de *sospechoso habitual* por lo que sus datos genéticos pueden ser utilizados para comprobar si ha participado en otros hechos delictivos, al igual que son utilizadas sus huellas dactilares o su fotografía.

Digamos que es una pena accesoria que se adquiere por el hecho de ser delincuente.

Pero las personas que tienen relación genética con las que están introducidas en la base de datos, también resultan perjudicadas ya que han perdido parte de su derecho a la privacidad sin haber cometido ningún delito. Porque al introducir los datos genéticos de un sujeto en la base de datos y aplicar la técnica de *familial searching*, resulta que no solo se está comparando con el perfil genético del sujeto, sino que se compara también con el de sus familiares. Esta es una circunstancia que no se da con las bases de datos de huellas dactilares o de fotografías; estas solo afectan al individuo en cuestión, no a su entorno familiar.

Con la aplicación de la técnica de *familial search* se consigue ampliar la base de datos de perfiles genéticos, con el agravante que, como no se dispone de todo el perfil genético de los familiares, nos estamos moviendo en el campo de la probabilidad. Así, cuando en las bases de datos genéticas se introducen datos genéticos de una persona porque el legislador lo ampara, resulta que estamos introduciendo datos de familiares de estos individuos que bajo ningún concepto deberían estar en dichas bases de datos. Al aplicar el *familial search* se está esgrimiendo un motivo para

investigar a dichos familiares, los cuales se convierten en posibles culpables si se obtiene algún pariente que puede ser candidato a autor y que necesitará de acciones para establecer su inocencia.

Serán revelados una serie de datos genéticos – que quizás desconozca hasta ese momento – que lo van a convertir de forma arbitraria en sospechoso de un delito y será investigado como tal. Una persona no debe ser más *presunta culpable* que otra por el mero hecho de ser familiar de un convicto. Por tanto debería tener el mismo derecho a ser investigada que otra persona que no tiene ningún familiar convicto.

¿Dónde es más probable identificar el autor de un hecho delictivo: entre los familiares de convictos, pero que nunca han cometido delitos graves, o entre personas que no son familiares de convictos?. Estadísticamente cabe esperar que la probabilidad sea la misma en ambos grupos poblacionales. Los dos grupos tienen la misma probabilidad de contener el autor de un hecho delictivo grave, por lo que ambos grupos deberían tener la misma probabilidad a ser investigados. Si solo se utilizan las bases de datos policiales para llevar acabo la *familial searching*, resultará que solo se estará investigando a los familiares de personas con antecedentes y

no se investigará al resto de la población. Por lo tanto, solo se van a resolver por este método los delitos que hayan cometido los familiares biológicos de personas que tienen introducido su perfil genético en las bases de datos policiales y no los delitos que hayan cometido las personas que no son familiares de delincuentes. Ello significará hacer hincapié siempre en el mismo nicho poblacional que es el de las personas con antecedentes policiales, con el agravante que a quién se va a investigar esta vez será a sus familiares biológicos que no estén incluidos en la base de datos y, por tanto, que no han delinquido, ya que los que están incluidos en ella han sido descartados al no producirse un *match*. A los familiares de delincuentes, pero que nunca han delinquido, se les supone una presunción de criminalidad, mientras que el resto de la población disfruta de la presunción de inocencia.

En los EEUU, en 2018 las personas de origen afroamericano y de color tienen una tasa de encarcelamiento de 592 individuos por cada 100,000 personas, las de origen indio americano y de Alaska es de 401 individuos y para las personas de origen hispano y blanco europeo es de 182 y 187 respectivamente⁵⁴³. Para hacernos una idea, el año 2000

⁵⁴³ La estadística completa se puede consultar en el boletín «Jail inmates 2018» del Bureau of Justice Statistics del US Department of Justice. <https://www.bjs.gov/content/pub/pdf/ji18.pdf> (última consulta 14/03/2022).

los EEUU, el 12,3 % de la población era de origen afroamericano, el 0,9 % era de origen indio americano y de Alaska, un 12 % era hispano/latino y un 75,1 % era de origen blanco europeo⁵⁴⁴. La población afroamericana triplica la tasa de encarcelamiento de la población blanca europea, cuando hay casi siete veces más de blancos europeos que de afroamericanos en los EEUU.

Dados estos índices de encarcelamiento para determinados orígenes raciales, parece que es más equitativo usar las bases de datos policiales y las no policiales para llevar a cabo la *familial searching*. Las bases de datos policiales tienen un sesgo poblacional por orígenes geográficos de manera que en ellas no hay el mismo porcentaje poblacional que el que existe en todo el país. Ello significa que las búsquedas genéticas que se llevaran a acabo con estos parámetros de sobre representación provocará que se identifiquen más personas que pertenecen a estos grupos poblacionales desfavorecidos y que hayan cometido delitos, pero no se van a identificar las personas de otros grupos poblacionales que hayan cometido los mismos delitos, porque las bases de datos no dispondrán su información familiar. Esto provoca que las bases de datos policiales se

⁵⁴⁴ La estadística completa se puede consultar en el boletín «Overview of Race and Hispanic Origin - Census 2000 Brief» que está en <https://www2.census.gov/library/publications/decennial/2000/briefs/c2kbr01-01.pdf> (última consulta 14/03/2022).

llenen con datos de personas de grupos poblacionales más desfavorecidos, haciendo que cada vez mayor la brecha, dando lugar a pensar que los familiares de delincuentes de estos orígenes también son delincuentes, cuando en realidad, lo que sucedería es que, por ejemplo en los EEUU, todos los delitos cometidos por personas de origen negro o afroamericano y indio nativo americano o de Alaska se resolvería, esto es, se identificaría su autor, pero los delitos cometidos por personas de otros orígenes raciales no se resolverían. Esto provocaría que los grupos poblacionales mas desfavorecidos se vieran más culpables a los ojos del resto de la población.

Por este motivo, en los casos en los que no se dispone de ninguna información sobre el autor, es más justo centrar la búsqueda en todo el espectro poblacional del país que no solo en los familiares de los sospechosos habituales.

4.7.- Uso de bases de datos genéticas NO policiales.

En Febrero de 2019 las compañías DTC disponían de los datos genéticos de 25 millones de personas⁵⁴⁵. Estas

⁵⁴⁵ AncestryDNA con los datos de unos 15 millones de individuos, 23andMe unos 9 millones, MyHeritage y FamilyTreeDNA (FTDNA) unos 3,5 millones entre los dos.

<https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/> (última consulta 14/03/2022).

personas les han proporcionado sus datos genéticos con una finalidad concreta, determinada por el contrato que han suscrito. Es cierto que muchas de estas empresas tienen entre sus cláusulas contractuales la de colaboración con las fuerzas del orden⁵⁴⁶, pero ello no significa que estas bases de datos comerciales deban convertirse en una ampliación de las bases de datos policiales.

Los usuarios de estos servicios tienen una expectativa razonable de privacidad en lo que respecta a los datos cedidos a estas compañías, la cual vendrá determinada, en parte, por el marco legal y normativo aplicable⁵⁴⁷. El consentimiento del interesado destruye dicha expectativa. Así, si el interesado accedió a que la compañía DTC tratara sus datos genéticos y, a la vez, accedía también a que esta compañía colaborara con las fuerzas del orden cediendo sus datos genéticos, dicha cesión se ajustaría a la legalidad.

En el caso que una compañía DTC en cuestión no tenga entre sus cláusulas la de la colaboración con las autoridades policiales, se debe equilibrar el interés que tiene la sociedad en localizar y detener los autores de delitos graves con el derecho a la protección de datos de los individuos que se

⁵⁴⁶ Por ejemplo las condiciones de la compañía ANCESTRY - <https://www.ancestry.ca/c/legal/privacystatement> (última consulta 14/03/2022).

⁵⁴⁷ STEDH de 24 de abril de 20158. Caso Benedik c. Eslovenia, párrafo 118.

realizan pruebas genéticas, más aún cuando esta información será cedida sin el consentimiento ni conocimiento del interesado. Dado que se trata de datos genéticos, nos encontramos bajo la protección del artículo 8 del CEDH, por lo que el uso de bases de datos comerciales por parte de las autoridades policiales deberá llevarse a cabo *en base a una ley* que constituya una medida necesaria en una sociedad democrática para perseguir el delito y defender el orden.

En el estado español cualquier persona física o jurídica, *“proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas”*, así como para *“el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública.”* El interesado no será informado de la transmisión de los datos a las autoridades policiales⁵⁴⁸.

548 Art. 7 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El uso policial de los datos que disponen estas Compañías, puede ir en detrimento de los beneficios de la propia compañía y provocar una disminución de ingresos, dado que los clientes deben ser conocedores que sus datos genéticos podrán ser utilizados por la policía durante una investigación. Aunque debe tenerse en cuenta que las personas que usan dichos servicios suelen tener cierto poder adquisitivo y entre sus intenciones, seguramente, no está el de cometer un delito grave y por tanto, quizás no les preocupe que las autoridades policiales puedan utilizar su perfil genético para identificar al autor de un delito grave.

En una encuesta llevada a cabo entre unas 1500 personas en los EEUU, la mayoría se mostraron de acuerdo con que la policía utilizara datos genéticos procedentes de compañías DTC para identificar autores de delitos violentos (80%), contra niños (78%) o en personas desaparecidas (77%). Un 39% estaba a favor de utilizar este tipo de datos para identificar autores de delitos no violentos⁵⁴⁹.

Los usuarios de estos servicios es muy probable que se vean más como víctima que como autor y, por lo tanto, estarían en disposición de cooperar. La población en general sabe que las autoridades policiales utilizan los datos de la telefonía móvil en investigaciones policiales con la finalidad de

⁵⁴⁹ La encuesta se puede consultar en GUERRINI et al. (2018).

identificar autores de delitos y no por ello, los ciudadanos que no tienen en su *modus vivendi* la comisión de delitos, dejan de utilizar los servicios de la telefonía móvil. En cambio, los delincuentes siguen usando la telefonía pero aplicando medidas de seguridad⁵⁵⁰.

Con el uso de bases de datos genéticas no policiales para llevar a cabo la *familial search* se atenúa la discriminación hacia los grupos poblacionales más desfavorables de la sociedad. Como hemos visto antes, el utilizar solo las bases de datos policiales acentúa la brecha existente entre distintos grupos, pero si se utilizan las bases de datos no policiales es mayor el número de personas que se ven afectadas por la investigación y no solo están bajo sospecha los familiares biológicos de las personas que contienen las bases de datos policiales.

Las DTC son empresas del sector privado que se dedican a un nicho concreto de mercado y ofrecen sus servicios para unos propósitos establecidos. Así, hay compañías que analizan el perfil genético para obtener información relativa a la salud del cliente. Otras compañías, en cambio, buscan

⁵⁵⁰ Los delincuentes suelen utilizar palabras clave para hablar por teléfono, aplicaciones que no se pueden intervenir o simplemente no hablan por teléfono. El último grito de medida de seguridad telefónica es la encriptación de la información contenida en el teléfono, lo que suele llamarse vulgarmente “encrochado”.

información acerca de los ancestros y genealogía o relaciones de parentesco entre sus clientes. También las hay que analizan los datos obtenidos a partir del ADN de sus clientes para mejorar sus estilos de vida, como pueden ser la nutrición, la forma física, la piel,.... Ello significa que cada compañía usa sus propios marcadores genéticos y algoritmos matemáticos para obtener la información, por lo que serían necesarios distintos análisis de la misma muestra para cada tipo de resultado que se desee.

Uno de los problemas que plantea el uso de estas bases de datos es de tipo económico: cuantos más análisis distintos deban llevarse a cabo, más se encarecerá la investigación. Por otro lado, no siempre hay suficiente cantidad de muestra dubitada para realizar este tipo de análisis, o puede estar degradada, y siempre debería quedar muestra suficiente para realizar un contra análisis.

Otro problema que tiene el uso de bases de datos genéticas no policiales es, precisamente, que son no policiales. Por tanto, se trata de empresas externas las que llevaran a cabo el análisis y no deberían quedarse con la información obtenida. Las autoridades policiales que recurran a estas compañías deben tener estrictos acuerdos, de manera que el perfil genético introducido por las autoridades policiales no

debe quedarse en las bases de datos de dichas compañías para obtener futuros resultados. Los familiares de la muestra dubitada no deben saber que un pariente suyo está involucrado en una investigación policial. Ni, por supuesto, el donante de la muestra dubitada – del que inicialmente se desconoce su identidad – debe conocer la identidad de familiares biológicos que tengan los datos en esas bases de datos. Por lo tanto, bajo ningún concepto las autoridades policiales deberían utilizar estos análisis de manera subrepticia, sin el conocimiento de las compañías ya que la DTC, sin saberlo, podría vulnerar el derecho a la privacidad del donante de la muestra dubitada al comunicarle dicha coincidencia a su cliente de buena fe. A ello se añade que las autoridades policiales pierden el control de la información externalizando este tipo de análisis, ya que es transferida al sector privado, por lo que son necesarios establecer estrictos controles de seguridad.

Finalmente, debe tenerse en cuenta que los datos genéticos que contienen estas bases de datos comerciales están formados por polimorfismos puntuales - SNP -. Cada compañía utiliza sus propios SNP, dependiendo del objetivo comercial de la compañía, por lo tanto, el perfil genético de un individuo estará formado por miles o cientos de miles de SNPs procedentes del ADN celular, tanto ADN basura como

ADN codificante. La actual legislación no permite la inscripción en bases de datos policiales de datos genéticos que revelen información de naturaleza codificante o característica genética, a excepción de la identidad y el sexo⁵⁵¹.

4.8.- Destino final de las muestras genéticas.

El *familial searching* debe ser un método de investigación, un procedimiento para identificar la persona que dejó la muestra biológica en la escena del crimen. La investigación finalizará con el análisis de una muestra biológica del presunto autor para que sea comparada con la localizada en el lugar de los hechos. La coincidencia de estas dos muestras indicará la identidad de la persona que ha dejado la muestra, momento en que finalizará esa línea de investigación.

Hasta llegar a este punto, en numerosos casos será necesario el análisis de muestras biológicas de diversas personas, que nunca habrán tenido ninguna relación con los hechos. Para evitar un mal uso de estas muestras y los distintos resultados obtenidos, deberían destruirse tanto las muestras biológicas de estas personas como la información obtenida a partir de ellas. Dichos resultados no deberían ser

⁵⁵¹ Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

utilizados en contra de estas personas, ni deberían ser almacenadas en las bases de datos para la investigación de delitos posteriores. No pueden utilizarse en otras investigaciones distintas para las que ese material genético fue recogido.

Así, si las muestras o algún tipo de información sobre cualquier persona involucrada en la búsqueda han abandonado el circuito de laboratorios oficiales, tanto la muestra como la información deben ser destruidas una vez realizado su propósito. El resultado de la muestra no debe entrar en el circuito de las muestras de las compañías DTC, como si fuera un cliente más.

5.- La regulación de la *familial search*: propuesta de mejora.

El TJUE reconoce que la eficacia de la lucha contra delitos graves, en particular el terrorismo y el crimen organizado, puede depender del uso de modernas técnicas de investigación, pero no por ello, los ciudadanos deben dejar de tener suficientes garantías de protección de sus derechos⁵⁵².

⁵⁵² STJUE de 21 de diciembre de 2016, *Tele2 Sverige y Watson y otros*, C-203/15 y C-698/15, EU:C:2016:970.

Por su parte, el TEDH recuerda que el examen de la adecuación de las leyes al derecho a la privacidad de los ciudadanos debe hacerse "*cuando los poderes conferidos al estado son oscuros, creando un riesgo de arbitrariedad, especialmente cuando la tecnología disponible se está volviendo cada vez más sofisticada*"⁵⁵³. La limitación de derechos fundamentales que supone la aplicación de técnicas genéticas de *familial search* debería estar prevista en la legislación y evitar llegar a extremos de uso arbitrario de esta metodología que es muy invasiva en el derecho a la privacidad de las personas. No olvidemos que estamos tratando datos altamente sensibles de personas que, en principio, no tienen relación con el hecho delictivo.

La última reforma de la Ley de Enjuiciamiento Criminal en España reguló el uso del ADN por parte de los Cuerpos y Fuerzas de Seguridad del Estado en la investigación de delitos, una técnica que ya era ampliamente utilizada en el campo de la identificación de personas. El siguiente paso debería ser la regulación del uso de la *family search* en la investigación policial. A mi juicio, el Legislador debería establecer los casos en que podrían aplicarse estas nuevas técnicas de investigación sobre las muestras dubitadas; así, debería concretar en qué tipo de delitos podría aplicarse,

⁵⁵³ STEDH de 24 de gener de 2019. Caso Catt c. Reino Unido, párrafo 114.

quién debería dar autorización para que se llevara a cabo o si se debería esperar a agotar todas las líneas de investigación para utilizarlas, por citar algunos aspectos a regular.

La *Comisión Nacional para el uso Forense del ADN* - CNUFADN - en sus actividades de 2012⁵⁵⁴, expone una serie de puntos a considerar durante el redactado de una norma que regulara la *familial search* y que comparto plenamente. Estos son:

a.- Se debe tener en cuenta que es una *herramienta de investigación, no debe utilizarse como elemento de culpabilidad*. La aplicación de los algoritmos de la búsqueda familiar darán como resultado un conjunto de personas que, potencialmente, son familiares del presunto autor. Ello significa que cuando se obtenga la identidad del presunto autor, su perfil genético debe ser comparado con el perfil dubitado que proceda de la muestra biológica localizada en el lugar de los hechos. Solo la coincidencia del ambos perfiles genéticos - autor y muestra dubitada - podría significar un elemento de culpabilidad.

554 Puede consultarse en:

https://www.mjusticia.gob.es/es/ElMinisterio/OrganismosMinisterio/Documents/1292428320905-Memoria_de_la_Comision_Nacional_para_el_Uso_Forense_del_ADN_Actividades_2012.PDF (última consulta 14/03/2022).

De por sí, esto nos lleva a dos aspectos a tener en cuenta sobre la muestra dubitada:

- Se debe disponer de la suficiente cantidad de muestra biológica que permita la realización de análisis contradictorios.

- El perfil de ADN extraído de la muestra biológica debería estar completo, de manera que el análisis obtenido permita un resultado sin paliativos a la hora de ser comparado con el perfil genético del donante de la muestra indubitada. Las muestras biológicas degradadas no deberían ser utilizadas para iniciar un proceso de *familial search*.

Debemos recordar que las personas que están introducidas en las bases de datos no serán investigadas. A quien se va a investigar será a sus familiares, personas que no tienen ninguna relación respecto al hecho investigado y sobre los que no hay una brizna de culpabilidad más que un cierto parentesco con personas que constan en las bases de datos. Pero su ADN ya ha sido introducido indirectamente en las bases de datos, ya que en el ADN de cada individuo, hay ADN de sus familiares biológicos. Así las personas que son realmente culpables de otros delitos y a los cuales se les ha extraído ADN para obtener su perfil genético que ha sido

introducido en la base de datos, han introducido involuntariamente fragmentos del ADN de sus familiares biológicos.

Por tanto, el uso de la *familial search* conlleva, de una parte, utilizar el ADN que hay en las bases de datos de personas que han cometido algún delito de una manera distinta para la que fue solicitado. En las actas de consentimiento de los Cuerpos policiales y que ha sido tratado ampliamente en el capítulo anterior, las muestras que se obtienen son para el estudio de ADN "*que proporcione exclusivamente información genética reveladora de la identificación de la persona y de su sexo*"⁵⁵⁵. En ningún momento se habla que esa muestra será utilizada para identificar a familiares. Por lo tanto se trata de utilizar unos datos personales que fueron recogidos con una finalidad determinada y usarlos para otra finalidad. Es decir, de manera estricta, no se dispone del consentimiento informado de la persona que cedió sus datos genéticos para que sean utilizados con otra finalidad o, en su defecto, actualmente tampoco se dispone un amparo legal que lo permita.

⁵⁵⁵ "Acta de recollida de mostres biològiques i consentiment informat per a l'anàlisi d'ADN de persones detingudes o investigades en una investigació criminal" - Documento I61.b del Cos de Mossos d'Esquadra.

"Formulario de toma de muestras y consentimiento informado para obtención de muestras de ADN en asunto criminal" de la Guardia Civil.

Y ese consentimiento es importante, por que según la Ley de Enjuiciamiento Criminal no están obligados a declarar “*los parientes del procesado en líneas directa ascendente y descendente, su cónyuge o persona unida por relación de hecho análoga a la matrimonial, sus hermanos consanguíneos o uterinos y los colaterales consanguíneos hasta el segundo grado civil*”⁵⁵⁶. El interesado que cede su material genético debe conocer que puede ser utilizado en contra de sus familiares biológicos y debería tener el derecho a negarse,

Por otro lado, tampoco existe el consentimiento de los familiares autorizando a almacenar fragmentos de su ADN en la base de datos. De todas maneras, sería absurdo preguntar a todos los familiares de las personas que tienen introducidos los datos en las bases de datos genéticas y que dieran su consentimiento. Con toda probabilidad desconocen por completo que tienen parte de sus datos genéticos en las bases de datos.

De llevarse a cabo la *familial search* es preciso que sea con las máximas garantías. Se deben aplicar algoritmos fiables y con perfiles genéticos con un suficiente número de alelos para que el resultado obtenido sea eficiente. Los resultados que se obtengan deben ser lo más precisos posibles, dentro
556 Art. 416.1 de la Ley de Enjuiciamiento Criminal.

del campo de la estadística en el que se mueven este tipo de análisis. Pero si se parte de un perfil genético con escasos alelos, por ejemplo, los 23 alelos actuales que contienen el sistema CODIS, el resultado no puede ser muy prometedor. Cuanto más preciso sea el resultado, menos candidatos a investigar y menos vulneración de derechos fundamentales de personas completamente ajenas al autor.

b.- Ésta técnica debería utilizarse para investigar delitos, al menos, tan graves como en los que se autoriza el uso del ADN en su investigación. Esto es delitos *graves contra la vida, la integridad de las personas, la libertad, la indemnidad sexual, de terrorismo o cualquier otro delito grave que conlleve un riesgo grave para la vida, la salud o la integridad física de las personas*⁵⁵⁷.

Además, no debería usarse en todos los casos sino en los que han visto agotadas todas las líneas de investigación. El método de la *familial search* debe ser la *última ratio*. *En algunos estados de los EEUU estas técnicas se aplican para investigar delitos graves contra las personas cuando las líneas de investigación se han agotado, la línea de investigación requiere un gran esfuerzo o en casos de causa mayor como puede ser el terrorismo*⁵⁵⁸.

⁵⁵⁷ Art. 129.bis de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

⁵⁵⁸ WICKENHEISER (2019).

En los inicios de su aplicación, con esta técnica se identificó y arrestó a un individuo que dejó un rastro de sangre al romper una ventanilla de un vehículo para robar 1,40 \$⁵⁵⁹. Hoy en día no debe investigarse un caso de estas características utilizando esta técnica.

Esto puede llevar implícito el problema que supone el paso del tiempo. La fe ciega en las pruebas genéticas llevan a confiar excesivamente en las muestras que fueron recogidas del lugar de los hechos y que presumiblemente pertenecen al autor. La identificación de una muestra biológica dubitada décadas después de ser recogida o identificar como sospechosas a personas que no tengan una coartada muy sólida, pueden ver mermado su derecho a la presunción de inocencia y de defensa. Esto va ligado a la dificultad que tendrán las autoridades policiales en obtener pruebas concluyentes al investigar un caso que ha ocurrido varios años antes, o incluso décadas. La investigación se basará en acciones que fueron llevadas a cabo muchos años antes, donde las personas que participaron en la recogida quizás ya no estén. Todo ello provocaría que no pudiera realizarse la contradicción de la prueba con todas las garantías.

⁵⁵⁹ La noticia se puede consultar en [https://www.eastbaytimes.com/2010/02/09/familial-dna-searches-draw-heat/amp/](https://www.eastbaytimes.com/2010/02/09/familial-dna-searches-draw-heat/) o en <https://www.denverpost.com/2009/11/16/familial-dna-software-may-catch-on-in-catching-criminals/> (última consulta 14/03/2022).

c.- Dado que es previsible que se limiten derechos fundamentales de las personas que se investigan como medio para llegar a la identidad del presunto autor, el uso de esta técnica debería estar tutelada por una autoridad judicial.

De esta forma se subsanaría utilizar datos personales que fueron recogidos para un fin y van a ser utilizados para otro de distinto. Como hemos dicho, no existe el consentimiento expreso de la persona que cede su perfil genético ni el de sus familiares, ni existe tampoco el amparo legal que permita llevar a cabo este cambio de finalidad. Con la autorización judicial se subsanarían dichos requisitos a la vez que se podría llevar a cabo una revisión de la investigación antes de iniciar las pesquisas sobre personas inocentes.

Cabría añadir que es necesaria la formación de los agentes que aplicaran estas técnicas genéticas en las investigaciones. Este método proporcionará el nombre de un candidato a familiar del presunto autor y debería ser tratado como tal, tanto desde el punto de vista ético, salvaguardando la privacidad genética a la que tiene derecho, como desde el punto de vista de la investigación, de manera que se puedan seguir los pasos más eficientes y menos lesivos jurídicamente para identificar al presunto autor. Cabe

recordar que son investigaciones complejas que requieren manejar mucha información genealógica.

Antes de que en la UE se generalice el uso de estas técnicas, se debería regular su uso, ya que se ha demostrado que puede ser vulneradora de derechos fundamentales y afecta exclusivamente a personas que, hasta que se demuestre lo contrario, son inocentes. De todos los candidatos que se obtienen al aplicar la *familial search*, a lo sumo, uno de ellos será el culpable, el resto de personas que se habrán visto implicados en la investigación serán inocentes.

6.- Obtención de las EVC⁵⁶⁰ del donante de la muestra: una técnica de investigación genética complementaria y prometedora.

Al mismo tiempo que se lleva a cabo la búsqueda de un familiar del donante de la muestra dubitada o independientemente a ésta, se pueden realizar otros tipos de análisis. Uno de ellos es el que permite obtener las características visibles de una muestra de ADN dubitada: el género del individuo, etnia, pigmentación de la piel, color del iris de los ojos, color natural y textura del pelo, características

⁵⁶⁰ *Externally Visible Characteristics* de sus siglas en ingles EVC.

de la nariz, hoyuelos en la barba y mejilla, características de los lóbulos de las orejas, altura, tipo de calvicie, edad, mano dominante, anchura de los labios, pecas y, en algunos casos, incluso el apellido⁵⁶¹.

El análisis de las EVC de una muestra biológica localizada en la escena del crimen, podría resultar muy útil en el inicio de la investigación policial ya que permitiría reducir el número de personas a investigar. Esta técnica podría dar una descripción detallada de ciertas características de la persona que abandonó la muestra biológica en dicho lugar, al igual que lo haría un testigo presencial - o quizás mejor -, de manera que la investigación policial se centraría en personas que tuvieran esas características físicas, descartando las que no las tuvieran. Además, es una técnica que no afecta a la información genética de terceras personas, ya que se utilizan bases de datos que contienen información genética anonimizada. Esta técnica, por si misma, nunca podrá dar el nombre del autor, como sí lo puede llegar a hacer la *familial searching*.

La primera vez que se utilizó este tipo de análisis fue durante la investigación de una serie de asesinatos que tuvieron lugar en Louisiana del Sur (EEUU) en 2002. Inicialmente, la policía estuvo buscando a un hombre de raza blanca que conducía

561 MACLEAN (2014).

un vehículo blanco, por lo que se hicieron numerosos análisis de ADN a personas que cumplieran esas características. Pero después de obtener las EVC a las muestras genéticas recogidas en el lugar de los hechos resultó que el asesino era un hombre de origen afroamericano, por lo que se abrieron nuevas líneas de investigación que finalmente culminaron con la localización del asesino⁵⁶².

Ello no significa que debe despreciarse cualquier trabajo de campo realizado por la policía y basar toda la investigación en el ADN hallado en la escena del crimen. Las declaraciones de testigos, las imágenes de cámaras de vigilancia, las confesiones o cualquier otro método de investigación tradicional debe tenerse en cuenta y ser estudiada conjuntamente con las muestras biológicas halladas en el lugar de los hechos. Los análisis del ADN localizado en la escena del crimen no se van a equivocar y los resultados deben ser del todo fiables; pero el error puede estar en la muestra: desde una contaminación o una transferencia secundaria hasta la recogida de una muestra que se encontraba en el lugar pero que no pertenecía al autor.

562 Más información en <https://www.wafb.com/2019/11/20/dna-testing-played-major-role-derrick-todd-lee-case-ubr-district-attorneys-office-says/> y en <https://forensiccoe.org/js2-cs9/> (última consulta 14/03/2022).

Debe tenerse en cuenta que tanto los resultados biológicos como las otras pruebas localizadas a partir de las gestiones de investigación deben hablar de la misma persona, o sea, del autor de los hechos. En caso de que haya discrepancias entre ellas, debe analizarse si quien se equivoca es el testigo, las imágenes no muestran el verdadero culpable o la muestra biológica recogida no correspondía al autor sino a otra persona.

La información genética que contienen las células de una persona – **genotipo** -, sería el principal factor que determina las características externas del individuo; un ejemplo de ello son los gemelos monozigóticos que se parecen como dos gotas de agua. Pero en el aspecto exterior de una persona también influyen las características del ambiente en el que se ha desenvuelto este individuo – **fenotipo** -. Así, una persona que esté bien alimentada, hace deporte y no fuma, tendrá unas características físicas distintas a si esa misma persona es bebedora, fumadora y sedentaria. Pero el punto de partida para el aspecto físico final será el mismo, la genética; el individuo, con el comportamiento podrá ir variando - de forma voluntaria o no - sus características físicas externas. La activación de un gen determinado viene dado por el ambiente donde se encuentra, es decir, por los otros genes que forman parte del organismo. Las nuevas técnicas genéticas unidas

con los avances informáticos permiten monitorizar miles de genes y sus productos para, de esta manera, determinar como esos genes se reflejan finalmente en el individuo.

Los análisis a los que se ha hecho referencia en los puntos anteriores, no implicaban el estudio de los genes del ADN. Pero para obtener las características físicas del donante de la muestra genética es necesario analizar las porciones de la cadena de ADN que contribuyen a exteriorizar un rasgo determinado de la persona física. A diferencia de la *familial searching*, no es necesario disponer de una base de datos de perfiles genéticos de personas para llevar a cabo los análisis, ni se investigarán familiares de personas que constan en bases de datos genéticas. Los marcadores que se analizan están estandarizados y son comunes a todas las personas.

No es sino desde hace unos años que se ha visto un avance significativo en la genética forense en este campo, principalmente en la detección de pigmentos y de la altura del individuo, ya que es una técnica cara y que precisa de personal cualificado y, hasta el momento, la investigación de la expresión genética del individuo ha ido encarada hacia determinar los genes que se ven implicados en el desarrollo de enfermedades hereditarias⁵⁶³. Son investigaciones complejas ya que no es un único gen el que determina las

563 WALSH et al. (2013).

características exteriores del individuo, sino que son varios los que se ven involucrados⁵⁶⁴. Estudiando los denominados *Single Nucleotide Polymorphism* (SNP) se puede determinar una región del genoma que estaría asociada a un fenotipo determinado. Técnicamente, no se trata de analizar un gen o genes concretos, sino los marcadores que se asocian a una expresión genética determinada. Por tanto, lo que se busca es localizar fragmentos de la cadena de ADN que acompañan a una determinada expresión genética concreta del individuo, fragmentos que no suelen estar en las zonas codificantes del genoma⁵⁶⁵.

Con este tipo de análisis, se pretende obtener la información que proporciona un testigo ocular del autor de los hechos. En cualquier investigación policial, una de las primeras gestiones que se realizan es la de buscar testigos que hayan visto el autor, los cuales serán interrogados con la finalidad de, entre otras cosas, aportar información de las características físicas del autor. Ese testigo deberá recurrir a sus recuerdos para dar su descripción, que a veces se ayudará de retratos robot, reconocimientos fotográficos, etc. La precisión de la descripción que facilitará el testigo dependerá de muchos factores, como son del estrés del momento, su memoria, de

⁵⁶⁴ En un estudio reciente se ha visto que serían 5 los genes que se verían implicados en la forma de la cara de los europeos. KAYSER, (2013).

⁵⁶⁵ MANFRED et al. (2009a).

lo que ha visto o el tiempo transcurrido. En cambio, estudiando las características externas del sujeto que dejó la muestra biológica en el lugar del crimen a partir del ADN de dichas muestras, la información puede ser más precisa y ya no dependerá de la persona que facilita la información, sino que es la ciencia la que la facilita y es inequívoca. Al fin y al cabo, la información sobre el autor de los hechos que se obtiene con esta técnica es la misma que puede facilitar un testigo ocular, pudiendo ser mucho más objetiva que la proporcionada por éste.

Algunos autores lo llaman *DNA intelligence*⁵⁶⁶ ya que se trata de herramientas que las autoridades policiales las pueden utilizar en una fase temprana de la investigación para, por ejemplo, corroborar la versión de un testigo ocular o descartar posibles candidatos. Puede reducir el número de sospechosos de la misma manera que lo puede hacer la declaración de un testigo ya que así se puede acotar un determinado grupo poblacional en el que centrar la búsqueda del autor de una forma más fiable. De lo que hay que estar seguro es que la muestra biológica sea del autor ya que, de no ser así, supondría tener que iniciar de nuevo la investigación.

566 WALSH et al. (2013).

No se trataría tampoco de elementos para llevar a juicio como carga de prueba. La finalidad de estas pruebas genéticas es obtener datos del autor para poder identificarlo. Una vez se conozca su identidad, por los distintos métodos existentes se le extraerá una muestra genética que deberá ser comparada con la localizada en el lugar de los hechos y que pertenece al autor. Solo si hay una coincidencia se podrá afirmar que se trata del autor. Por lo tanto, el resultado obtenido de las EVC únicamente sirve a efectos de investigación policial, para acotar el número de personas a investigar.

El uso de esta técnica es poco invasiva en cuanto a afectación de los derechos fundamentales de los ciudadanos se refiere. Por un lado, no se requieren bases con datos genéticos de otras personas; la información obtenida de la muestra dubitada simplemente debe ser comparada con los datos procedentes de muestras anónimas de estudios anteriores. Por otro lado, la información que aportan es la misma que facilitaría un testigo de los hechos o la grabación de una cámara de seguridad; es una descripción física del presunto autor.

A continuación se exponen algunas de aplicaciones que, desde mi punto de vista, pueden ser más relevantes en la

investigación de delitos y sin ánimo de ser exhaustivos, dado que existen diversos estudios que asocian estos marcadores a otras muchas características físicas del individuo, tales como modelos de calvicie masculina⁵⁶⁷, del cabello de la cabeza⁵⁶⁸, la edad⁵⁶⁹, la altura⁵⁷⁰ o el plegamiento del lóbulo de la oreja⁵⁷¹, por citar algunos.

6.1.- Identificación de la zona geográfica de procedencia (*BioGeographical Ancestry -BGA-*)⁵⁷².

Podemos definir *ancestrabilidad* como *la herencia genética que cada individuo porta de sus antepasados o ancestros, los cuales – en un pasado más o menos remoto – han ocupado un determinado lugar geográfico a lo largo del tiempo*. Pero en un mundo globalizado como el nuestro, acotar un lugar determinado puede ser tanto o más complicado como describir las características de las personas que lo habitan. Cuantos menos movimientos poblacionales, migraciones, mezclas de ADN procedentes de otros orígenes geográficos haya entre los ancestros del

567 HAGENAARS S.P. et al. (2017).

568 POSPIECH E. et al. (2018).

569 ZBIEC-PIEKARSKA R. et al. (2015).

570 LELLO L. et al. (2018).

571 SHAFFER J.R. et al. (2017).

572 **Ancestralidad biogeográfica (BGA)** es el término que propone el *Race, Ethnicity, and Genetics Working Group* del *National Human Genome Research Institute* para substituir las etiquetas raza, étnico o ancestral. HALDER et al. (2008).

donante de ADN dubitado, más concluyentes podrán ser los resultados.

Este método puede ser relevante para la investigación criminal cuando el donante de la muestra procede de una población estructurada donde conviven subpoblaciones de diferente tipo étnico y genético que todavía no se han mezclado, siempre que el perfil genético analizado pertenezca a uno de los grupos minoritarios. Cuanto mayor sea la mezcla poblacional, menos efectivo será aplicar este análisis.

Así, la capacidad de obtener resultados concluyentes para la investigación policial va a depender de diversos factores: los orígenes geográficos de los antepasados del donante, de los marcadores que se analicen o de la lejanía de la población originaria del donante respecto de la población del lugar donde se ha localizado. Estos son indicadores que, a priori, se desconocen del autor y hasta que se lleve a cabo el análisis no se sabrá si es necesario o concluyente dicho análisis.

Los test de ancestrabilidad ofrecen información relativa a los antepasados, de varias generaciones atrás; en cambio la *familial search* ofrece información relativa a los familiares

más cercanos, de pocas generaciones anteriores. Habitualmente para estudios de identificación de ancestros o línea genealógica, se analiza la variabilidad del ADN mitocondrial, para establecer la línea materna, y el análisis de STR del cromosoma Y para la paterna. Pero ello hace muy difícil aplicarlo a un único individuo ya que son millones las persona que comparten ese linaje en la actualidad. Estos resultados se combinan con el análisis de Marcadores Informativos de Ancestralidad – AIM -, formados por miles de marcadores de la cadena de ADN de la muestra dubitada.

Cada método de análisis utiliza distintos patrones variacionales de población como referencia que se comparan con la muestra dubitada y, aplicando herramientas estadísticas⁵⁷³ se puede averiguar, con una alta probabilidad, la procedencia geográfica del donante de la muestra biológica dubitada. Las muestras que se utilizan para comparar proceden de muestras anónimas de estudios anteriores, por lo tanto no afectan a la intimidad de terceras personas.

Inicialmente, las zonas geográficas que se podían acotar eran el África Subsahariana, Europeo/Caucásico, Asia Oriental, Indígenas Americanos i Oceanía. Posteriormente se

573 A modo de ejemplo, dos páginas web utilizadas para este propósito por los investigadores forenses: <http://frog.med.yale.edu/FrogKB/index.jsp> y <http://mathgene.usc.es/snipper/>. (última consulta 14/03/2022).

han diferenciado tres grupos: Europa, Asia Central/Sud y Oriente Medio. El análisis de estos marcadores son más fiables que los que se obtienen del análisis de los cromosomas sexuales o del ADN mitocondrial ya que estos solo permiten identificar linajes y aquellos diferencian entre grupos poblaciones.

Actualmente se utilizan una nueva serie de marcadores denominados Next Generation Sequencing - NGS - que realizan miles o millones de operaciones de secuenciación genéticas paralelas reduciendo los costes de los análisis y en los que se combinan el análisis de marcadores de linaje con Marcadores Informativos de Ancestralidad - AIM -.

6.2.- Genero.

Como es sabido, todos los seres humanos disponen de un cromosoma que determina el sexo. Las mujeres tienen dos cromosomas X y los hombres tienen un cromosoma X y un cromosoma Y. La determinación del género del donante de una muestra se lleva a cabo a través de la detección del gen de la **Amelogenina** que se encuentra ubicado en los cromosomas X e Y, pero su longitud varía dependiendo de si se encuentra en uno u otro cromosoma.

Este tipo de análisis es sencillo, rápido y económico, además de requerir poca cantidad de muestra⁵⁷⁴. La fiabilidad es bastante elevada, aunque hay individuos que presentan un borrado del gen de la amelogenina en su cromosoma Y, de manera que en aplicación de este método daría un resultado erróneo. Así y todo, en la población europea el error se estima en un 0,02 %, aunque en la población del sudeste asiático sería de un 1,8 %⁵⁷⁵.

6.3.- Color de los ojos.

Al igual que el género, la determinación del color los ojos del donante de la muestra biológica suele ser bastante precisa y útil para las investigaciones policiales. Hay herramientas que determinan con precisión el color azul y marrón del iris de los ojos basándose en el estudio de diversos SNP's que están asociados a ocho genes involucrados en la síntesis de la melatonina, que es la proteína que determina el color de los ojos. El tipo, la distribución y la cantidad de pigmentos que hay presentes en el iris determina el color de los ojos de las personas, el cual no se hereda de forma mendeliana estricta, aunque sí se ha visto que el iris de color azul sigue un patrón de gen recesivo⁵⁷⁶.

574 SALVADOR VELARDE-FÉLIX (2008).

575 MACLEAN (2014).

576 <https://journals.plos.org/plosgenetics/article?id=10.1371/journal.pgen.1000934> (última consulta 14/03/2022).

En estudios realizados se ha visto que este sistema tiene una precisión del 83 al 95 %, dependiendo de la población europea a la que pertenece el donante de la muestra⁵⁷⁷.

6.4.- Color del pelo.

Un único gen localizado en el cromosoma 16 implicado en la producción de melanina, determina el color de la piel y del pelo en los mamíferos.

Pero dicho color también se ve influenciado por otros factores como pueden ser el sexo y la edad. Las mujeres tienden a ser más pálidas que los hombres. A medida que nos vamos haciendo mayores el pelo tiende a caer y a volverse blanco, perdiendo su coloración. Además, hay personas que a medida que van creciendo, se activan ciertos genes que hacen que el color del pelo vaya variando.

Existe un sistema de análisis que puede predecir simultáneamente el color del pelo y del iris de los ojos a partir del análisis de 24 variantes en la cadena de ADN⁵⁷⁸.

⁵⁷⁷ WALSH et al. (2011).

⁵⁷⁸ WALSH et al. (2013).

6.5.- Inconvenientes de la obtención de EVC.

La determinación de las EVC, al igual que el uso de técnicas de *familial searching*, no están exentas de ciertos problemas de orden jurídico.

a.- Uso de datos genéticos.

En la determinación de las EVC se estudian miles de polimorfismos de un solo nucleótido (SNP). Pero estos marcadores, a diferencia de los STR, provienen de partes de la cadena de ADN que, sin ser técnicamente codificantes, proporcionan información relativa a las áreas del cromosoma que forman los genes. La línea que separa el ADN codificante y el no codificante está muy clara sobre el papel, pero no en la práctica. El Reglamento (UE) 2016/679 prohíbe el "*tratamiento de datos genéticos*", y tratamiento significa también el mero hecho de obtener los datos⁵⁷⁹.

Los genes no son cadenas continuas y compactas de nucleótidos, son más bien paquetes que se suelen heredar intactos⁵⁸⁰, por lo que no está tan clara la diferencia. Siendo estrictos, no se realiza un análisis de los genes que intervienen en las características EVC, sino que son

⁵⁷⁹ Art. 4 del Reglamento (UE) 2016/679.

⁵⁸⁰ MANFRED et al. (2009a).

fragmentos genéticos de ADN no codificante que están asociadas a dichas características y que revelan las mismas características que las genéticas. Así se infiere información genética a partir de fragmentos de cadena no codificantes. Pero esta lectura tan formal de la norma podría llevar a una "*slippery slope*" en la cual sería peligroso entrar⁵⁸¹. Deberíamos preguntarnos si resulta ético analizar fragmentos de ADN no codificante que por su "proximidad" al ADN codificante puede revelar la misma información que la que proporciona el codificante.

De todas maneras, el Reglamento (UE) 2016/679 contempla excepciones que permiten el tratamiento de estos datos, la primera de las cuales es el consentimiento del donante de la muestra. Pero al tratarse de muestras dubitadas, se desconoce la identidad de dicho donante.

Otra de las excepciones es la del poder realizar el análisis cuando el tratamiento es necesario para que "*los tribunales actúen en ejercicio de su función judicial*"⁵⁸². Por tanto las autoridades policiales podrían solicitar a un juez autorización para determinar las **características visibles externas** del donante de la muestra dubitada.

581 MANFRED et al. (2009b).

582 Art. 9.2.f. del Reglamento (UE) 2016/679.

El tratamiento de datos personales es un derecho fundamental del individuo, aunque no un derecho absoluto. Así, el Convenio Europeo de Derechos Humanos (CEDH) permite la injerencia de los poderes públicos en la esfera de protección de derechos siempre que esté prevista por la ley. Por lo tanto, en lo que al estado español se refiere, un juez no podría autorizar este tipo de análisis durante una investigación criminal dado que se trataría de una vulneración de derechos no amparada por la ley.

En 2003 se realizó una modificación legal en Holanda que permite el uso de marcadores genéticos para predecir EVC, incluyendo la identificación de la zona geográfica de origen, siendo el primer país europeo en el que se permite este tipo de análisis⁵⁸³.

La información obtenida en estos análisis genéticos es relativa a algunas características físicas del individuo que todas las personas pueden ver. No se trataría de información que infringiera el derecho a la privacidad ya que es visible a todas las personas, más allá que la persona tenga canas y no quiera que se sepa que se tiñe el pelo o que se esconde las pecas con maquillaje. Por otro lado también, la información no es absoluta y se mueve por parámetros de probabilidad.

583 MANFRED et al. (2009b).

El resultado que se obtiene con estas técnicas es una herramienta de investigación, una ayuda para identificar el donante de la muestra; no será aportada durante el acto del juicio oral ya que carece de valor identificativo por sí misma. Las autoridades policiales pueden utilizar estas técnicas para llegar al donante de la muestra y presunto autor que, una vez identificado, deberá compararse su perfil genético con el de la muestra y, en caso de coincidencia, se trataría de una prueba de cargo definitiva.

b.- Poca precisión en los resultados.

Actualmente, los resultados obtenidos aplicando esta técnica son poco precisos ya que se mueve en el campo de las probabilidades.

Por ejemplo, al hablar de zona de procedencia de los ancestros del donante de la muestra, puede que no se trate de una única zona. Las personas nos hemos ido cruzando genéticamente desde tiempos inmemoriales; por ese motivo es difícil precisar características de personas los ancestros de las cuales son originarias de zonas de transición que existen entre las distintas zonas geográficas - como puede ser Oriente Medio -, personas originarias de distintas zonas geográficas pero que mantienen semejanzas aparentes -

como ocurre con la zona Subsahariana y Oceanía⁵⁸⁴ - o simplemente personas los antepasados de los cuales proceden de diversas áreas geográficas.

Además, si nos remontamos a 20 generaciones anteriores, en nuestro material genético están los genes de más de un millón de personas de aquella época, que ha sido combinado aleatoriamente a lo largo de los siglos hasta llegar a nosotros. Debemos tener en cuenta que la genética proporciona cierta información que no tiene porqué estar en el ámbito público de una persona; es más, seguramente no conoce ciertos rasgos genéticos de sus ancestros.

Pero no debemos olvidar que en cualquier investigación policial, una de las primeras gestiones que se realizan es la de buscar testigos que hayan visto el autor de los hechos, los cuales serán interrogados con la finalidad de, entre otras cosas, aportar información de las características físicas del autor. Ese testigo deberá recurrir a sus recuerdos para dar una descripción del autor, pudiendo incurrir en errores de apreciación que dependerán del propio testigo, de lo que ha visto, el tiempo transcurrido,.... Es decir, las declaraciones testificales también llevan asociadas imprecisiones.

584 KAYSER (2013).

c.- Confusión de zona geográfica de procedencia de los ancestros con la raza.

Los especialistas no se ponen de acuerdo de si existen razas de seres humanos. El material genético que contiene las células humanas no distingue entre razas, no hay unos alelos típicos de una raza que no se encuentran en otra y que permitan distinguir una raza de otra. Hay combinaciones genéticas que permiten distinguir rasgos visibles de los individuos, infiriendo sus características externas, pero no la raza en sí. La *raza* se asimila a la zona de procedencia de los ancestros que principalmente se acotarían en África Subsahariana, Europeo/Caucásico, Asia Oriental, Indígenas Americanos y Oceanía.

Tradicionalmente hay determinados sectores de la población que tienen prejuicios contra determinados grupos poblacionales, que a menudo comparten ciertos rasgos fisionómicos característicos y suelen ser minorías respecto de la población principal. La realización de este tipo de pruebas genéticas a muestras procedentes de la escena del crimen de manera sistemática haría dirigir la atención hacia el segmento poblacional en el que se encuentra el verdadero culpable. Así, si sobre una determinada población minoritaria recae el peso de la sociedad en el sentido que siempre son

personas de esas características físicas las que llevan a cabo determinados ilícitos penales, la realización de este tipo de pruebas genéticas a todas las muestras biológicas procedentes de estos delitos, podría ayudar a rebajar la tensión social. Al menos, se aportarían elementos objetivos para evitar la discriminación en la administración de justicia. En realidad, hay más probabilidad que los autores de estos hechos pertenezcan a la población dominante que a las poblaciones minoritarias.

Pero, una vez realizados los análisis y comprobado que el autor pertenece a la población mayoritaria, puede ser más costoso a las fuerzas policiales intentar localizar a este autor, que no al autor que pertenezca a una población minoritaria. Ello puede llevar a dejar impunes los delitos graves cometidos por la población mayoritaria y a investigar más a fondo los delitos graves cometidos por autores pertenecientes a poblaciones minoritarias, ya que hay un menor número de candidatos. Incluso, con los grupos raciales no dominantes podría plantearse llevar a cabo análisis genéticos en masa o *dragnet*, que podrían resultar inviables para los grupos raciales mayoritarios⁵⁸⁵.

No deja de ser muy peligroso unir en una misma frase los conceptos raza, genética y delincuencia, ya que activan

585 OSSORIO (2016).

estereotipos que pueden afectar a la vida de las poblaciones minoritarias. El concepto raza asociado a la delincuencia vendría reforzado por el término genético, herencia, determinismo, activando estereotipos y afectando a todas las personas que compartirían los mismos rasgos externos.

6.6.- Ventajas del uso de EVC.

A medida que la ciencia y la técnica vayan avanzando, se podrá ir mejorando la descripción de la persona que abandonó su material genético en el lugar de los hechos. Como hemos dicho, el resultado que se obtiene con esta técnica es información acerca de las características que suelen ser visibles a simple vista del individuo, la misma información que puede facilitar una fotografía o un testigo ocular de los hechos sobre la descripción del sospechoso. La información obtenida es visible a todos los ciudadanos y, por lo tanto, no tendría porqué producirse ninguna violación del derecho a la privacidad de las personas, ya que no es una información que el individuo pueda mantener oculta al resto de las personas. Tampoco se ven afectadas terceras personas; no se requiere realizar comparaciones entre distintos individuos para ir avanzando en la investigación y obtener un candidato. Solo haría falta un pequeño cambio que permitiera analizar fragmentos de la cadena de ADN asociados a manifestaciones genéticas.

La información que es útil para la investigación es el resultado final, la descripción de las características, pudiéndose prescindir de cualquier otro dato genético procedente de la muestra dubitada. Así, los datos relativos al perfil genético obtenidos en el laboratorio podrían quedarse en él, ya que no es necesario que sean transmitidos a ningún cuerpo policial o judicial. Como herramienta de investigación, con el resultado sería suficiente para acotar el número de candidatos durante la búsqueda del autor. Una vez éste sea localizado, se le deberá someter a análisis genéticos que confirmen que se trata del autor.

Imaginemos que, con el perfeccionamiento de esta técnica puede obtenerse una representación muy precisa del rostro de este individuo. Dicha fotografía podría compararse con las fotografías de personas con antecedentes policiales inscritas en las bases de datos policiales de manera que el individuo pudiera ser identificado a través de reconocimiento facial. Ello significaría que ya no sería necesario llevar a cabo muchas de las gestiones policiales que se utilizan actualmente y que pueden vulnerar derechos fundamentales. Además, podría utilizarse esa fotografía para localizarlo a través de las cámaras de reconocimiento facial que existen en lugares públicos.

Esta técnica de investigación que podría utilizar la policía para identificar un autor es mucho menos lesiva que el estudio de ADN de la muestra. Consistiría en realizar los análisis de parámetros de EVC y obtener una imagen del sospechoso, la cual sería la herramienta utilizada por la policía para investigar. De una imagen no puede inferirse ningún aspecto relativo a la privacidad del individuo: vínculos familiares, enfermedades hereditarias o ancestros.

La finalización de la investigación se produciría al comparar una muestra biológica procedente del sospechoso con la hallada en el lugar de los hechos y comprobar que ambas proceden del mismo individuo. La ventaja con este sistema es que no sería necesario que los cuerpos policiales dispusieran de bases de datos de ADN de personas detenidas para ser utilizadas en investigaciones policiales, ya que no haría falta compararla con todos los perfiles genéticos.

Las EVC del individuo se obtiene comparando la información procedente del ADN con bases de datos estandarizadas y anónimas. Por lo tanto, a las autoridades policiales se les facilitarían las características físicas del individuo, su imagen, dejando de lado cualquier dato genético.

Estas herramientas podrían reducir el número potencial de sospechosos hasta niveles que permitieran abrir nuevas líneas de investigación, acotando la búsqueda policial y optimizando recursos, sin interferir en el derecho a la privacidad de terceras personas. A la vez, pueden reducir la presión policial sobre determinados colectivos, evitando episodios de discriminación, ya que las autoridades trabajaran con certezas científicas cuando deban investigar a personas que comparten características externas semejantes a las del autor.

Conclusiones

Durante muchos años, la ciencia forense ha utilizado el ADN para identificar si una muestra biológica recogida en una escena del crimen correspondía con una u otra persona, del mismo modo que se ha utilizado la dactiloscopia. Las huellas dactilares no tienen ningún otro uso más allá de la identificación, ya que la disposición de las crestas dactilares no contiene ninguna información relativa a la persona; en cambio, las cadenas de ADN nuclear que están en las células disponen de toda la información del individuo. Era cuestión de tiempo que se explotara esta información más

allá de los efectos identificativos y que pudiera ser utilizada como línea de investigación, es decir, utilizar la información contenida en los cromosomas como líneas de investigación para llegar a identificar el autor de un hecho delictivo. Han sido las empresas privadas del campo de la genómica las que han abierto la puerta a dar un uso policial al análisis de ADN, cuando las agencias policiales se han servido de ellas para localizar familiares de personas – *familial searching* - que dejaron restos biológicos en una escena criminal.

Con esta técnica se produce un cambio de paradigma en el análisis genético policial, ya que se deberán utilizar otros marcadores genéticos y la finalidad del análisis será la obtención de información de las características físicas y genéticas del presunto autor.

Pero el uso de estas técnicas genéticas en la investigación de delitos puede afectar severamente a derechos fundamentales de numerosas personas, las cuales no tendrán ninguna relación con el delito en sí. Ser un candidato a autor o a familiar de autor, conlleva que sobre esta persona se vaya a centrar una investigación policial, sin saber si tiene alguna implicación con el hecho en sí o con el mismo autor. La sospecha se va a basar en cálculos de probabilidad. A la vulneración del derecho a la protección de datos que supone

la obtención del perfil genético de una persona, hay que añadirle el menoscabo de la intimidad que se produce al ser el centro de una investigación policial ya que, en muchos casos, significa estudiar su pasado, sus relaciones personales, su entorno y los movimientos que hizo un determinado momento. Además, para utilizar la *familial searching*, es necesario comparar el perfil genético investigado con perfiles genéticos de otras personas. Cuanto mayor sea la base de datos con la que comparar, más precisos pueden ser los resultados obtenidos, pero mayor será el número de personas afectadas. Su uso implica investigar personas que se sabe que son inocentes, con la vulneración de derechos fundamentales que ello conlleva.

A mi juicio, se trata de una herramienta necesaria y útil en la investigación de delitos y que se irá implantando en un futuro no muy lejano, ya que las ventajas pueden ser enormes en lo que se trata de identificar delincuentes.

Para evitar la vulneración de derechos que se produce cuando se aplica esta técnica, hace falta que se regule su uso. Es necesaria una reforma legislativa que aborde un cambio de paradigma dado que se utilizan fragmentos de ADN codificante. Ya no tiene sentido la distinción entre ADN codificante y el no codificante, porque fragmentos

pertenecientes al ADN no codificante van asociados a otros de codificante o activan determinados genes. Además, hay rasgos genéticos que no afectan al derecho a la intimidad, como son el color de los ojos o del pelo, por ejemplo. Estas son características del individuo que el resto de personas pueden ver y que viene determinado por la genética. El legislador debería concretar en qué tipología penal debería aplicarse esta técnica, en qué punto debería encontrarse la investigación en la que se va a utilizar o quién puede autorizar su uso, como parámetros que deberían clarificarse antes de usar la técnica de manera genérica. En mi opinión, debería utilizarse solo en casos de delitos graves, sin línea de investigación y estar supervisada por un juez o un fiscal. Al finalizar la investigación, todos los datos obtenidos deberían ser destruidos.

También es necesario saber qué bases de datos podrán utilizarse al aplicar esta técnica. El uso policial de bases de datos genealógicas privadas genera muchos problemas, entre los que destaca la falta de consentimiento de las personas que tienen los datos en ellas para que su información genética sea utilizada con una finalidad distinta a la que inicialmente habían previsto. Por contra, significa ampliar enormemente el número de candidatos con los que comparar el perfil genético dubitado, disminuyendo la presión

sobre las personas que tienen introducido su perfil genético en las bases de datos policiales.

Otro de los avances científicos en el campo del ADN forense ha sido el análisis de material biológico para obtener las EVC – características externas visibles - de un individuo. Esta técnica no tiene implicación para terceras personas ya que el perfil genético dubitado se compara con bases de datos genéticas anónimas. Actualmente se trata de una técnica mucho menos desarrollada que la anterior y la información que actualmente puede facilitar a un equipo investigador es más bien escasa. El objetivo ideal que debería obtenerse sería hallar una imagen del presunto autor a partir de su información genética, con la suficiente calidad como para llevar a cabo una búsqueda en las bases de datos policiales o fuentes abiertas de información que reportara posibles candidatos. Así, la afectación a terceras personas sería mínima y la información con la que trabajarían las autoridades policiales no iría más allá de las características físicas visibles del individuo, es decir, lo que el resto de ciudadanos ve de esa persona. Estamos hablando de obtener una fotografía del presunto autor a partir de una muestra de ADN localizada en el lugar de los hechos.

Los parámetros que el legislador debería considerar para utilizar esta técnica deberían ser los mismos que en el uso de la familiar search – tipo de delito, estado de la investigación, supervisión judicial -. Debería determinarse también qué rasgos físicos podrían ser utilizados, para así evitar conductas de discriminación u odio.

Dado que el uso del ADN en la ciencia forense continuará evolucionando, es preciso que el legislador tome conciencia de ello. Las genéticas son técnicas muy útiles en la investigación de delitos, pero muy peligrosas desde el punto de vista de los derechos fundamentales. La ciencia genética está evolucionando a pasos agigantados y la ciencia forense lo está aprovechando para desarrollar su función, que no es otra que la de identificar autores de hechos criminales. El legislador debería llevar la iniciativa y establecer un marco legal para evitar el abuso en la utilización de datos genéticos como mero elemento de investigación, sobre todo si las personas afectadas son ciudadanos que nada tienen que ver con el delito que se investiga.

CONCLUSIONES GENERALES

El establecimiento en la Unión Europea de un espacio sin fronteras ha facilitado la circulación de personas y mercancías entre los estados miembros, pero también ha favorecido la delincuencia transfronteriza y el crimen organizado. En los últimos tiempos el crimen organizado ha cambiado, volviéndose más diverso en cuanto a sus métodos, grupos, estructuras y en el impacto que causa en la sociedad; es más móvil, con grupos más flexibles que operan en múltiples jurisdicciones y sectores criminales, mejorando la capacidad de identificar y explotar nuevos mercados ilícitos.

Además, se están observando elevados índices de cooperación entre distintos grupos criminales que van más allá de las nacionalidades o las diferencias étnicas, de manera que los estados lo tienen cada vez más complicado para luchar contra él, ya que sus integrantes se adaptan mejor a las condiciones y a los medios en los que se desarrolla que las fuerzas del orden.

Por este motivo, la eliminación de fronteras debe ir unida a la necesidad de reforzar la cooperación policial entre estados. Los diferentes cuerpos de policía de los distintos estados deben trabajar coordinadamente, compartiendo recursos, con rapidez y efectividad. El principal elemento con el que las fuerzas policiales trabajan es con la información, la cual está almacenada en distintas bases de datos. Cuando se produce la cooperación policial, estas bases de datos interaccionan para llevar a cabo dicha cooperación y que se verá reflejada en el resultado de una investigación policial.

Pero dicha investigación debe estar en equilibrio con los derechos fundamentales de las personas porque la protección de los derechos individuales fortalece a la persona como individuo frente al estado. Uno de los derechos que se ven mermados en el transcurso de una investigación policial es el derecho a la protección de datos personales. Este derecho nació a finales del SXIX como parte del derecho a la intimidad y a lo largo del SXX y principios del SXXI ha ido evolucionando hasta considerarse un derecho autónomo, principalmente a causa del desarrollo de la informática y su aplicación al tratamiento de datos. La protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitadas de sus datos personales queda englobada en el derecho general de protección de la persona y debe

determinar por sí mismo la divulgación y la utilización de los datos.

Las nuevas tecnologías permiten un tratamiento de los datos de forma masiva de manera que es posible conocer aspectos de la vida de un individuo a partir de datos aparentemente inocuos. En la investigación policial es muy reveladora la teoría del mosaico formulada por MADRID CONESA, según la cual, los datos de una persona aisladamente no tienen ningún valor pero considerados en un conjunto adquieren su significado, al igual que ocurre con las teselas de un mosaico. Durante una investigación policial se va reuniendo información relativa a una o varias personas, información que va desde números de teléfono hasta direcciones de personas, pasando por lugares que estas frecuentan o personas con las que diariamente se encuentra. Inicialmente estos datos pueden parecer que aportan poca información, pero analizándolos en su conjunto pueden facilitar información relevante para la investigación, a la vez que la aportan sobre la vida privada de un individuo. Las autoridades son conscientes de este aspecto y tratan de proteger a los ciudadanos del abuso que puede ejercer el sector privado o la propia administración pública utilizando esta información; pero, por otro lado, deben proteger también el principal recurso de que disponen las autoridades

policiales para luchar contra el crimen: la información, gran parte de ella formada por datos personales.

El TEDH considera que la protección de los datos personales juega un papel fundamental en el ejercicio del derecho al respeto de la vida privada y familiar garantizado en el art. 8 de la Convención. El almacenamiento de este tipo de datos entra dentro de su ámbito de protección ya que el término vida privada tiene una noción amplia y no es susceptible de una definición exhaustiva. Pero no todos los datos de carácter personal deben ser considerados como relativos a la vida privada de una persona, aunque el tratamiento de dichos datos sí constituirá una injerencia a la vida privada del individuo. Los datos personales forman parte de la esfera de la vida privada del individuo y éste debe poder decidir libremente sobre ellos.

El cuerpo legislativo relativo a la protección de datos ha ido adaptándose a los avances científicos que se han producido en este campo por un lado y a las necesidades que ha ido experimentando la sociedad al ver que dicho avance ha supuesto una merma del derecho a la privacidad de los individuos por el otro. Dicha adaptación debe seguir produciéndose ya que la sociedad no se puede permitir prescindir de ciertos avances - como los que se han visto en

el campo de la genética - por el hecho que afecten a la privacidad de las personas. Cuando un individuo está siendo investigado por las autoridades policiales su expectativa de privacidad disminuye; la policía utilizará sus datos, entre ellos los personales, para investigarlo. En una sociedad como la actual, donde muchos aspectos de la vida cotidiana están informatizados y los medios técnicos para tratar datos son muy potentes, no se puede pedir a las autoridades policiales que no los use en sus investigaciones; debe regularse su uso para evitar la vulneración de derechos a los ciudadanos, pero no prohibir su uso. Estas técnicas deben ser usadas respetando los derechos de los ciudadanos, de manera que sean lo menos lesivas posible, pero tienen que ser utilizadas para luchar contra el crimen, especialmente en la investigación de delitos graves.

La facultad que tienen los estados de establecer excepciones a los derechos y obligaciones no puede justificar que la excepción a la obligación de garantizar el derecho a la privacidad y a la protección de datos se convierta en la regla. La restricción de los derechos, en este caso el derecho a la privacidad, debe hacerse de forma excepcional y cuando se cumplan los requisitos establecidos en la legislación y las medidas restrictivas no deben ir más allá de lo estrictamente

necesario para dar cumplimiento al objetivo de luchar contra la delincuencia grave.

Los cuerpos policiales trabajan con distintas bases de datos para llevar a cabo una investigación criminal y el uso en sí de dichas bases de datos ya supone un riesgo añadido al derecho a la intimidad y al de la protección de datos. Para prevenir vulneración de derechos, el legislador europeo ha regulado el tratamiento de los datos que las autoridades policiales disponen acerca de los ciudadanos y de cómo deben usarse durante las investigaciones policiales.

Aún así, hay aspectos que, en mi opinión, no han quedado bien resueltos como es el derecho al olvido que tienen los ciudadanos. Con las nuevas tecnologías, y especialmente en Internet, con los tratamientos automatizados de datos o el big-data no se implementa lo suficiente el borrado de datos antiguos, hecho que provoca que las personas se conviertan en prisioneras de su propio pasado. Al igual que los antecedentes penales o las sanciones disciplinarias en el ámbito administrativo caducan, los datos que se disponga de un individuo en un archivo policial han de poder caducar y ser borrados del sistema. La Directiva (UE) 2016/680 contempla el derecho a la supresión de datos, pero permite que las autoridades policiales conserven los datos si se dan

ciertas circunstancias, tales como proteger la seguridad pública o proteger la seguridad nacional, conceptos demasiado amplios, en mi opinión, y que permiten prescindir fácilmente de la aplicación de este derecho.

Para que la libertad de circulación de personas y bienes en la Unión Europea no sea un campo abonado donde prolifere la criminalidad internacional, es necesario disponer de mecanismos que hagan posible que la lucha policial y judicial contra el crimen organizado, terrorismo y la comisión de delitos graves sea eficiente. Entre las personas que se desplazan, hay individuos que aprovechan el cambio de país para delinquir, convencidos de que cuando lo abandonen, su historial delictivo no les seguirá. Otros residen en un país y se desplazan a otro durante un período de tiempo relativamente corto para delinquir y regresar de nuevo a su país para disfrutar el botín. Por este motivo, la UE ha creado una serie de estructuras legislativas que permiten que el intercambio de información entre las distintas autoridades policiales sea eficiente y rápido.

En aras de la coordinación policial se llevan a cabo encuentros de autoridades policiales de distintos países, estableciéndose relaciones personales que son aprovechadas para el intercambio de información peer-to-

peer en ámbitos específicos. Es una de las ventajas que tienen los encuentros en foros policiales internacionales. Pero no es aceptable que cuerpos policiales de distintos países compartan información relativa a delitos leves como hurtos o estafas, cuando no hay indicios suficientes de la existencia de una organización criminal, por ejemplo. No deberían utilizarse los instrumentos creados en estos foros para llevar a cabo la difusión europea de este tipo de información. En sus investigaciones, las autoridades policiales trabajan, básicamente, con información que obtienen de distintos canales, uno de los cuales es la cooperación que se produce entre distintas unidades policiales, cuerpos policiales de un mismo país o cuerpos policiales de países distintos. Por lo que el intercambio de información procedente de distintas autoridades policiales siempre va existir. Pero la información que manejan es sensible y puede afectar seriamente al derecho a la intimidad y a la protección de datos de un individuo, por lo que deberían establecerse ciertos controles tanto de buena praxis como normativos.

Cuando las autoridades policiales de un país soliciten información a las de otro país, éste debe facilitar exclusivamente la información solicitada. Dicha información podrá ser utilizada durante una investigación, pero no deberá

ser utilizada en un procedimiento judicial si no ha sido contrastada y con el consentimiento explícito del estado que la ha facilitado, que significará que ha sido obtenida respetando los derechos fundamentales de las personas implicadas.

El Acervo de Schengen ha sido un gran avance en la cooperación policial en el marco de la UE, permitiendo una cooperación muy estrecha entre autoridades policiales. Los cruces de fronteras entre policías de distintos países, los Centros de Coordinación Policial y aduanero, el SIS o los Equipos Conjuntos de Investigación se han revelado muy útiles en la cooperación policial europea. Además permite que los cuerpos policiales puedan consultar las bases de datos de policías de otros países cuando lo necesiten en aplicación del principio de disponibilidad o, incluso, llevar a cabo operaciones en el territorio de un país de la Unión Europea.

Y en aspectos donde los estados no han llegado a un acuerdo sobre la forma de como cooperar, se han utilizado mecanismos que el mismo tratado preveía, como es la cooperación reforzada. Este ha sido el origen del Tratado de Prüm que, vista su utilidad, ha sido incorporado a la legislación europea posteriormente.

Pero, a veces, estos canales de intercambio de información no son utilizados exclusivamente para investigar delitos graves, crimen organizado o terrorismo. Se aprovechan para transmitir cualquier tipo de información. En este trabajo se han mencionado dos casos concretos en los que la cooperación policial a nivel internacional se utiliza en temática que, a mi juicio, no sería la adecuada y que, a la vez, pueden vulnerar derechos fundamentales: uno de ellos es el de los condenados por delitos sexuales y el otro el de los boletines mensuales que publica EUROPOL sobre pickpockets. En ambos casos el intercambio de información entre autoridades policiales de distintos países, a mi entender, es abusiva y discriminatoria.

En el caso de condenados por delitos sexuales, la disparidad legislativa existente entre los diferentes estados en materia policial y penal provoca un tratamiento policial distinto entre individuos que han cometido un mismo hecho. En ciertos países se hace un seguimiento exhaustivo del comportamiento de personas condenadas por este tipo de delitos. Cuando uno de esos condenados viaja a otro país, dicho seguimiento se traslada también a ese nuevo país. Así, cuando estas personas se trasladan a un país donde no se hace dicho seguimiento a este tipo de condenados, sí se les llevará a cabo el seguimiento si el estado donde reside

habitualmente lo solicita. Se trata de una medida, a mi entender, discriminatoria ya que se aplica solo a los nacionales de una serie de países y no a otros. Están más controlados los condenados por delitos sexuales de esos países que los condenados del propio país.

En el caso de los boletines de pickpockets, la información que las autoridades policiales transmiten entre sí, realmente hace referencia a información de personas con rasgos físicos diferentes a los residentes de esa ciudad o país, de manera que las autoridades que transmiten la información presuponen que la persona que lleva a cabo pequeños hurtos y tiene aspecto distinto al de los nacionales de ese país, es de interés para todas las policías europeas y deben tener su fotografía ya que, antes o después, realizará el mismo tipo de delito en otro país. Es decir, se hace difusión de los pickpockets que aparentan ser extranjeros y no se hace de los que aparentan ser nacionales del país en cuestión. Por lo visto, los que aparentan ser extranjeros pertenecerían a una organización criminal y los que aparentan ser nacionales de ese país no pertenecen a ninguna, valoración que se hace exclusivamente a través del aspecto de ese individuo.

En ambos casos nos encontramos, a mi entender, con un uso inadecuado de la transmisión de información policial a nivel europeo. No estamos en una policía europea globalizada por lo que no todas las policías europeas deben tener toda la información que disponen las otras policías. Por lo tanto el intercambio de información debe realizarse atendiendo a determinados criterios, como puede ser el de investigación de delitos graves o crimen organizado. No es aceptable que cuerpos policiales de distintos países compartan información relativa a delitos leves como hurtos o estafas, cuando no hay indicios suficientes de la existencia de una organización criminal, por citar un ejemplo.

La información que se maneja en una investigación criminal es muy sensible y puede afectar seriamente al derecho a la intimidad y a la protección de datos de un individuo, por lo que es necesario que se establezcan ciertos controles. Cuando se produzca intercambio de información policial entre países de la UE, ésta debe ser rigurosa, contrastada y no debe suponer una violación de derechos fundamentales de las personas implicadas.

La UE ha creado instrumentos legales muy útiles para luchar contra la delincuencia transnacional, pero no debería olvidar que ha de instar a los estados a armonizar su legislación

penal para que, de esta forma, evitar un tratamiento policial distinto entre individuos que han cometido un mismo tipo de ilícito penal.

Por mi parte, valoro muy positivamente el cuerpo normativo creado en la UE para la lucha contra el crimen en el ámbito de la UE, todo y las pequeñas disyunciones que se han detectado. Este es el camino que debe seguirse en la cooperación policial europea, mientras no se dote a Europol de más competencias y se convierta en una fuerza policial real en todo el ámbito de la Unión.

La segunda parte de la tesis ha consistido en estudiar el uso de la genética forense en la investigación policial y como se intercambia dicha información en el ámbito de la UE. Dado que se trata de datos muy sensibles desde el punto de vista de derechos fundamentales, se ha analizado el menoscabo de derechos que supone estudiar el perfil genético de un individuo con una finalidad policial, el almacenamiento de dicha información y su posterior intercambio entre distintos cuerpos policiales. Dado que se trata de una ciencia que está evolucionando rápidamente, creo que el mayor peligro, en cuanto a vulneración de derechos, está por venir si no se actúa con celeridad.

En el SXIX, los investigadores criminales iban a la escena del crimen con diversos reactivos que servían para revelar huellas dactilares en distintos tipos de superficies. En el SXX a este kit se le sumó primero la fotografía y después el video. Actualmente, además de todos estos enseres, llevan una torunda que en uno de los extremos tiene un fino algodón y que sirve para recoger muestras biológicas. Esa torunda es fruto de la gran revolución criminalística de las últimas décadas.

El uso de los datos genéticos en la investigación policial ha permitido la identificación de numerosos autores de delitos graves y de una manera muy efectiva, dado que los resultados obtenidos tienen el valor de prueba pericial y sirven para condenar o exonerar a una persona. Si la principal herramienta policial del siglo pasado era el estudio de las huellas dactilares, en este siglo lo es el análisis genético de muestras biológicas. La individualización que permite un perfil genético hace que se pueda convertir en una prueba irrefutable en el momento del juicio oral, dependiendo de la investigación. Además, si no se produce una coincidencia entre la muestra dubitada y el perfil genético de una persona que está introducido en la base de datos, esta persona queda eliminado de la lista de sospechosos.

El perfil genético es un código alfanumérico único para cada individuo formado por el número de repeticiones de bases genéticas que se dan en determinados puntos de la cadena de ADN. Pero no podemos quedarnos con que el perfil genético de un individuo es una lista de números y letras, como si se tratara del número de la seguridad social, por ejemplo. En la muestra biológica a partir de la cual se obtiene el ADN se halla toda la información genética de la persona. Por lo tanto, el tratamiento tanto de la muestra biológica como del perfil genético, debe hacerse de forma restrictiva y con medidas de seguridad.

La legislación española determina la obtención de la muestra biológica de un individuo y su posterior inscripción en la base de datos en función de la situación procesal del sujeto. Pero su situación viene dada a partir de las diligencias policiales y no las judiciales, de manera que es el instructor policial el que decide el rol que tiene el sujeto durante la investigación policial. Dicha investigación es incipiente y en numerosas ocasiones el rol procesal del sujeto variará dependiendo del avance de la investigación judicial, llevada a cabo con todas garantías procesales, y que finalizará con un juicio que establecerá la culpabilidad o la inocencia del sujeto. Sería más razonable inscribir el perfil genético del investigado en la base policial de perfiles genéticos provisionalmente y

compararlo exclusivamente con la investigación en curso en la que se está viendo involucrado el individuo. Si al finalizar el procedimiento judicial resultara condenado, el perfil genético se mantendría inscrito en la base y podría usarse en otras investigaciones. Por contra, si resultara absuelto o sobreseído el caso, el perfil debería ser eliminado, tal como establece la Recomendación del Consejo de Europa R (92).

Para ello es necesario implementar una mejor comunicación entre los órganos judiciales y los policiales, de manera que la inscripción de los datos genéticos en las bases de datos policiales, no dependa exclusivamente de datos policiales. Actualmente, si una persona sale absuelta de un juicio, debe solicitar expresamente el borrado de sus datos de las bases de datos policiales.

Otro aspecto mejorable, a mi juicio, es la ambigüedad en cuanto a ordenar la destrucción de la muestra biológica una vez obtenido el perfil genético. Como recoge el TEDH, la información contenida en una muestra biológica es información sensible del individuo, entre la que hay la relativa a su salud. Pero no solo hay información referente a él mismo, sino que incluye la de sus familiares biológicos. Podría entenderse la conservación durante largos periodos de tiempo de muestras biológicas dubitadas procedentes de

investigaciones obtenidas en la escena del crimen: dado que se pretende identificar el autor, puede aducirse que en un futuro no muy lejano dicha muestra se podrá volver a analizar y obtener otro tipo de información que ayudaría a identificar al culpable. Lo que actualmente sería un análisis para cuerpos policiales con elevados presupuestos, en pocos años pueden resultar económicamente asequibles para una investigación en cuerpos policiales con presupuestos más modestos. Además, el resultado del análisis de una muestra biológica no será el mismo si se hubiera llevado a cabo hace 30 años que si se realiza actualmente. En aquella época los análisis eran más rudimentarios, al igual que los resultados, y solo se obtenía un perfil genético que consistía en un código alfanumérico que permitía una identificación neutra del individuo. En los próximos años, es de esperar que las técnicas de análisis de ADN vayan más allá de la mera identificación y permitan extraer otras características. Por este motivo tiene sentido, a mi juicio, conservar las muestras dubitadas el máximo tiempo posible, que sería el de prescripción de la responsabilidad penal del delito cometido. Además, como se desconoce de quién procede esta muestra, no se le pueden aplicar los derechos ARCO - Acceso, Rectificación, Cancelación y Oposición -.

Pero cuando se trata de muestras indubitadas, el almacenamiento durante largos periodos de tiempo no es aceptable. Las muestras, una vez analizadas y obtenido el perfil genético, deben ser destruidas. En caso de que sea necesario llevar a acabo nuevos análisis de la muestra indubitada – por ejemplo, porqué ha habido una evolución en los marcadores genéticos estudiados -, se debería volver a solicitar dicho consentimiento. El consentimiento dado por un individuo para que se le extraiga una muestra biológica indubitada, debe ceñirse a la época en la que se le extrae. No se puede guardar dicha muestra *sine die* para analizarla al cabo de unos años y llevar a cabo un tipo de análisis completamente distinto al que se debería de haber hecho en el tiempo de la solicitud. Se trata de una vulneración del art. 8 del CEDH, ya que el solo hecho de producirse la retención sistemática de material celular una vez obtenido el perfil genético del individuo, se consideraría una intromisión en el ámbito de este artículo.

Por tanto, se debe establecer un borrado de oficio de los datos introducidos en las bases de datos, con un sistema de caducidad, de manera que cuando éstos sean introducidos, ya se establezca la fecha en la que serán borrados automáticamente. Actualmente no hay ninguna autoridad independiente que vele por el tiempo de almacenamiento de

estas muestras ni que compruebe su destrucción. Los datos genéticos de un individuo son demasiado sensibles para que permanezcan en una base datos sin una finalidad concreta cuando finaliza el tiempo de almacenamiento permitido.

Una huella dactilar o una fotografía aporta la misma información hoy en día que la que aportaba antaño. El estudio de las crestas dactilares no podrá servir para ir más allá de la mera identificación, a pesar del tiempo transcurrido. No se debe caer en el error de comparar el perfil genético de una persona con sus huellas dactilares o su fotografía. Cuanto más evolucione la ciencia forense, mayor será la cantidad de información que se podrá obtener de una muestra biológica, tanto del donante como de sus familiares biológicos; no podemos decir lo mismo de las huellas dactilares y de las imágenes. Por lo tanto, el grado de protección jurídica a la que se deben someterse las muestras biológicas y los datos genéticos debe ser superior al que tienen las huellas dactilares o de las fotografías.

En el intercambio de datos genéticos a nivel Europeo, a mi juicio, la UE ha establecido reglas claras y prima salvaguardar el derecho a la protección de datos que tienen los ciudadanos antes que intercambiar la información entre países sin que haya una causa justificada. Lo ha conseguido

haciendo que cada país gestione su propia base de datos y, para establecer coincidencias, solo se transfieren los perfiles genéticos asociados a un código, de manera que solo los funcionarios del país de donde procede el perfil genético conocen la identidad de la persona a quien corresponde. Antes de ceder dicha identidad, la coincidencia pasará por una serie de filtros humanos que serán los encargados de establecer la idoneidad o no del traspaso de la información. De esta manera se implican funcionarios de ambos países que deben adaptarse a sus respectivas legislaciones.

Pero, ¿qué ocurre cuando la muestra dubitada procedente de la escena del crimen no coincide con los perfiles que hay en las bases de datos?, pues que no se produce un *match*, lo que significa que la identidad de persona a la que pertenece la muestra dubitada no se encuentra en la base de datos. Durante muchos años, la ciencia forense ha utilizado el ADN para identificar si una muestra biológica recogida en una escena del crimen se correspondía con una u otra persona, del mismo modo que se ha utilizado la dactiloscopia. Era cuestión de tiempo que se explotara esta información más allá de los efectos identificativos y que el ADN en sí pudiera ser utilizado como línea de investigación, es decir, utilizar la información contenida en los cromosomas con la finalidad de identificar el autor de un hecho delictivo a partir de una

muestra biológica localizada en el lugar de los hechos. Han sido las empresas privadas del campo de la genómica las que han abierto la puerta a dar un uso policial al análisis de ADN, y las agencias policiales se han servido de ellas para localizar familiares de personas - llevando a cabo la familiar searching - que dejaron restos biológicos en una escena criminal.

Con esta técnica se produce un cambio de paradigma en el uso de los datos genéticos en la investigación criminal, ya que se deberán utilizar otros marcadores genéticos y la finalidad del análisis será la de identificar a familiares del autor para poder llegar hasta él.

Pero el uso de estas técnicas genéticas en la investigación de delitos puede afectar severamente a derechos fundamentales de numerosas personas, las cuales no tendrán ninguna relación con el delito en sí. Ser un candidato a autor o a familiar de autor, conlleva que sobre esta persona se vaya a centrar una investigación policial, sin saber si tiene alguna implicación con el hecho en sí o con el mismo autor. La sospecha se va a basar en cálculos de probabilidad. A la vulneración del derecho a la protección de datos que supone la obtención del perfil genético de una persona, hay que añadirle el menoscabo de la intimidad que se produce al ser

el centro de una investigación policial ya que, en muchos casos, significa estudiar su pasado, sus relaciones personales, su entorno y los movimientos que hizo un determinado momento. Debemos tener en cuenta que las personas que están introducidas en las bases de datos no serán investigadas. A quien se va a investigar será a sus familiares, personas que son inocentes respecto al hecho investigado y sobre los que no hay una brizna de culpabilidad más que un cierto parentesco con personas que constan en las bases de datos. Pero su ADN ya ha sido introducido indirectamente en las bases de datos, ya que en el ADN de cada individuo hay ADN de sus familiares biológicos.

Además, para utilizar la *familial searching*, es necesario comparar el perfil genético investigado con perfiles genéticos de otras personas. Cuanto mayor sea la base de datos con la que comparar, más precisos pueden ser los resultados obtenidos, pero mayor será el número de personas afectadas. Su uso implica investigar personas que se sabe que son inocentes, con la vulneración de derechos fundamentales que ello conlleva.

A mi juicio, se trata de una herramienta necesaria y útil en la investigación criminal y que se irá implementando en un

futuro no muy lejano, ya que las ventajas pueden ser enormes en lo que se trata de identificar delincuentes.

Pero no debemos olvidar el factor tiempo en la investigación policial ya que puede llevar un problema implícito. La fe ciega en las pruebas genéticas puede hacer confiar excesivamente en las muestras que fueron recogidas del lugar de los hechos y que presumiblemente pertenecen al autor. La identificación de una muestra biológica dubitada décadas después de ser recogida o identificar como sospechosas a personas que no tengan una coartada muy sólida, pueden ver mermado su derecho a la presunción de inocencia y de defensa. Esto va ligado a la dificultad que tendrán las autoridades policiales en obtener pruebas concluyentes al investigar un caso que ha ocurrido varios años antes, o incluso décadas. Todo se basará en acciones que fueron llevadas a cabo tiempo atrás, donde las personas que participaron en la recogida quizás ya no estén, al igual que testigos, víctimas o el propio autor. Todo ello provocaría que no pudiera realizarse la contradicción de la prueba con todas las garantías. Pero éste es un dilema que deberán resolver los tribunales, caso a caso.

Antes de que se empiece a generalizar el uso de la genética forense como medio de investigación y evitar vulneraciones

de derechos fundamentales, sería necesaria una regulación, a ser posible, consensuada entre todos los sujetos activos que participan en ella. A mi juicio la STEDH S. y Marper c. Reino Unido ha quedado antigua y debe superarse. Por eso urge una legislación en la que se acoten las técnicas que puedan utilizarse, una legislación lo suficientemente amplia que permita su uso salvaguardando el derecho a la intimidad de las personas que se puedan ver afectadas. Este tipo de técnicas, como ya he dicho, deberían supeditarse al control judicial para que pondere la necesidad social de atrapar al delincuente frente a la vulneración de derechos que se producirá llevando a cabo la investigación con estas técnicas.

Así, cabe esperar una reforma legislativa que aborde un cambio de paradigma dado que en este proceso se utilizan fragmentos de ADN codificante. Ya no tiene sentido la distinción entre ADN codificante y el no codificante, porque se ha visto que hay fragmentos pertenecientes al ADN no codificante que van asociados a otros de codificantes o que activan determinados genes. De llevarse a cabo la *familial search* es preciso que sea con las máximas garantías. Se deben aplicar algoritmos fiables y con perfiles genéticos con un suficiente número de alelos para que el resultado obtenido sea eficiente. Los resultados que se obtengan deben ser lo más precisos posibles, dentro del campo de la estadística en

el que se mueven este tipo de análisis. Pero si se parte de un perfil genético con escasos alelos, por ejemplo, los 23 alelos actuales que contienen el sistema CODIS, el resultado no puede ser muy prometedor. Cuanto más preciso sea el resultado, menos candidatos a investigar y menos vulneración de derechos fundamentales de personas completamente ajenas al autor.

Estas investigaciones deben ser llevadas a cabo con tacto, evitando inmiscuirse innecesariamente en la vida de las personas investigadas y preservando al máximo su derecho a la intimidad. Es importante que las autoridades policiales actúen con discreción y así evitar una victimización como consecuencia de la propia investigación, ya que, en una sociedad democrática, son inevitables los comentarios severos de la prensa en asuntos que interesan al público pero, a su vez, el coste personal de aparecer públicamente conectado, de cualquier modo a algún delito, es innegable, máxime si la información permite identificar a la persona, en el contexto actual de rápida y efectiva profusión de las noticias tanto mediante los medios de comunicación, como mediante las redes sociales.

El legislador debe concretar en qué tipología penal podría aplicarse esta técnica, en qué punto debe encontrarse la

investigación en la que se va a utilizar o quién puede autorizar su uso, por citar algunos parámetros que deben clarificarse antes de usar la técnica de manera genérica. En mi opinión, debería utilizarse solo en casos de delitos graves, sin línea de investigación y estar supervisada por un juez o un fiscal. Al finalizar la investigación, todos los datos obtenidos que ya no sean necesarios deberían ser destruidos.

También es necesario saber qué bases de datos podrán utilizarse al aplicar esta técnica. El uso policial de bases de datos genealógicas privadas genera muchos problemas, entre los que destaca la falta de consentimiento de las personas que tienen los datos en ellas para que su información genética sea utilizada con una finalidad distinta a la que inicialmente habían previsto. Creo que su uso debería estar tutelado por un juez que tiene que valorar la proporcionalidad de las medidas que se acuerden. El uso de bases de datos genealógicas privadas ayudaría a evitar problemas de discriminación dada la alta concentración de perfiles genéticos de minorías que existe en las bases de datos policiales.

La limitación de derechos fundamentales que supone la aplicación de técnicas genéticas de *familial search* debe

estar prevista en la legislación para evitar el uso arbitrario de esta metodología muy invasiva en el derecho a la privacidad de las personas.

Otro de los avances científicos en el campo del ADN forense ha sido el análisis de material biológico para obtener las EVC – características externas visibles - de un individuo. Esta técnica no tiene implicación para terceras personas ya que el perfil genético dubitado se compara con bases de datos genéticas anónimas. Actualmente se trata de una técnica mucho menos desarrollada que la anterior y la información que puede facilitar a un equipo investigador policial es muy superficial. El objetivo ideal que debería obtenerse aplicando esta técnica sería la de hallar una imagen del presunto autor a partir de su información genética, con la suficiente calidad como para llevar a cabo una búsqueda en las bases de datos policiales o fuentes abiertas de información que reportara posibles candidatos. Así, la afectación a terceras personas sería mínima y la información con la que trabajarían las autoridades policiales no iría más allá de las características físicas visibles del individuo, es decir, lo que el resto de ciudadanos ve de esa persona. Estamos hablando de obtener una fotografía del presunto autor a partir de una muestra de ADN localizada en el lugar de los hechos.

Los parámetros que el legislador debería considerar para utilizar esta técnica tendrían que ser los mismos que en el uso de la *familial search* – tipo de delito, estado de la investigación, supervisión judicial -. Debería determinarse también que rasgos físicos podrían ser utilizados, para así evitar conductas de discriminación u odio.

Dado que el uso del ADN en la ciencia forense continuará evolucionando, es preciso que el legislador tome conciencia de ello. Las genéticas son técnicas muy útiles en la investigación de delitos, pero muy peligrosas desde el punto de vista de los derechos fundamentales. La ciencia genética está evolucionando a pasos agigantados y la ciencia forense lo está aprovechando para identificar criminales. El legislador debería llevar la iniciativa y establecer un marco legal para evitar el abuso en la utilización de datos genéticos como mero elemento de investigación, sobre todo si las personas afectadas son ciudadanos que nada tienen que ver con el delito que se investiga.

Bibliografía.

ALLEYNE, L. (2009). *Manual de Interpol Sobre ADN*. 2nd ed.
<https://www.slideshare.net/ATUX/manual-de-interpolsobreadn1>. (última consulta 04/04/2022).

ALMUZARA ALMAIDA C., COUDERT F., MARZO PORTERA A. y NAVALPOTRO NAVALPOTRO Y. (2005). Estudio práctico sobre la protección de datos de carácter personal (LEX NOVA SA (ed.); 2ª).

ALVAREZ RIGAUDIAS C. (2014). Sentencia Google Spain y el derecho al olvido. Actualidad Jurídica Uría Menéndez.
<http://www.uria.com/documentos/publicaciones/4370/documento/fe04.pdf?id=558> (última consulta 04/04/2022).

ARENAS RAMIRO M. (2006). *El Derecho fundamental a la protección de datos personales en Europa* (1a ed.). Tirant lo Blanch.

ARENAS RAMIRO M. (2008). La protección de datos personales en los países de la Unión Europea. *Revista Jurídica de Castilla y León*, 113–168.

<http://dialnet.unirioja.es/servlet/articulo?codigo=3057994&orden=362890&info=link> (última consulta 04/04/2022).

- BRADY, H. (2007). Europol y El Modelo Europeo de Inteligencia Criminal: Una Respuesta No Estatal a La Delincuencia Organizada. Análisis del Real Instituto Elcano (ARI) N° 126/2007.
- CALE C.M., EARLL M.E., LATHAM K.E., BUSH G.L. (2016). Could Secondary DNA Transfer Falsely Place Someone at the Scene of a Crime?. J Forensic Sci 2016; 61(1):196–203.
- CASADO, M. y GILLEN M. (2011). ADN Forense: Problemas Éticos y Jurídicos. Barcelona: Publicacions i Edicions de la Universitat de Barcelona.
- CATE F. H. (1997). Privacy in the information age. Brookings Institution Press.
- CORRERIA, F. (2007). DOCUMENTO DE TRABAJO sobre una Decisión del Consejo relativa a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. Comisión de Libertades Civiles, Justicia y Asuntos de Interior.

http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824es.pdf. (última consulta 04/04/2022).

DARANAS PELAEZ M. (1984). Jurisprudencia Constitucional extranjera. Tribunal Alemán. Ley del Censo. Boletín de Jurisprudencia Constitucional. Núm. 33. p 126 y ss.

DEL POZO PÉREZ M. (2006). El agente encubierto como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal española. Criterio Jurídico, 6, 267–310.

<https://dialnet.unirioja.es/servlet/articulo?codigo=2717795> (última consulta 04/04/2022).

DOLEAC J., BATTEN F., BERNHEIM D., BJERK D., EIL D., EVANS B., FRIEDBERG L., GALE B., GARRETT B., HOXBY C., KUZIEMKO I., MEER J. Y SANDERS N. (2017). The Effects of DNA Databases on Crime. American Economic Journal: Applied Economics. 9(1): 165–201. <https://doi.org/10.1257/app.20150043> (última consulta 04/04/2022).

EICHLER H. (1973). Codificación de Derecho Civil y Teoría de los Sistemas de Derecho. Revista Da Faculdade de Direito, Universidade de São Paulo, 68(2), 229–256.

<https://core.ac.uk/download/pdf/268355411.pdf> (última consulta 04/04/2022).

ENFSI, Review recommendations, DNA Working and Group April. (2017). Dna Database Management.

EXPÓSITO LÓPEZ L. (2015). El agente encubierto. REVISTA DE DERECHO UNED, 17, 251–286.

<http://revistas.uned.es/index.php/RDUNED/article/view/16277> (última consulta 04/04/2022).

ERLICH, YANIV, TAL SHOR, ITSIK PE'ER, and SHAI CARMI. (2018). Identity Inference of Genomic Data Using Long-Range Familial Searches. Science 362 (6415): 690–94.

<https://doi.org/10.1126/science.aau4832> (última consulta 04/04/2022).

European Union Committee. 29th Report of Session 2007–08. House of Lords (2008). Europol: coordinating the fight against serious and organised crime.

<https://publications.parliament.uk/pa/ld200708/ldselect/lddeucom/183/183.pdf> (última consulta 04/04/2022).

GARCÍA O., CRESPILO M. y YURREBASO I.,. (2017). Suspects Identification through 'Familial Searching' in DNA Databases of Criminal Interest. Social, Ethical and Scientific Implications. Spanish Journal of Legal Medicine 43 (1): 26–34.

<https://doi.org/10.1016/j.remle.2017.02.002> (última consulta 04/04/2022).

GARZON VALDES E. (2003). Lo íntimo, lo privado y lo público. Claves de Razón Práctica núm. 15, 14–24.

GUERRINI, CHRISTI J., JILL O. ROBINSON, DEVAN PETERSEN y AMY L. MCGUIRE. (2018). Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique. PLoS Biology 16 (10): e2006906.

<https://doi.org/10.1371/journal.pbio.2006906> (última consulta 04/04/2022).

GUTWIRTH S., POULLET Y., HERT P., NOUWT S. Y TERWANGNE C. (2009). Reinventing Data Protection?. Springer Science+Business Media.

GYMREK, M., AMY L. MCGUIRE, GOLAN G., HALPERIN E. y ERLICH Y. (2013). Identifying Personal Genomes by Surname Inference. Science 339 (6117): 321–24.

<https://doi.org/10.1126/science.1229566> (última consulta 04/04/2022).

HAGENAARS S.P., HILL W.D., HARRIS S.E., RITCHIE S.J., DAVIES G., LIEWALD D.C. et al. (2017) Genetic pre-

diction of male pattern baldness. PLoS Genet 13: e1006594.

<https://doi.org/10.1371/journal.pgen.1006594> (última consulta 04/04/2022).

HALDER I., SHRIVER M., THOMAS M., FERNANDEZ J.R. y FRUDAKIS T. (2008). A panel of ancestry informative markers for estimating individual biogeographical ancestry and admixture from four continents: Utility and applications. Human Mutation. Vol 29. num. 5. 648 – 658.

HEPPLE B., COOKE G., HOLM S., LAURIE G., PARRY B., READ A. y WILLIAMS R. (2007) The Forensic Use of Bioinformation: Ethical Issues. Nuffield Council on Bioethics.

<https://www.nuffieldbioethics.org/assets/pdfs/The-forensic-use-of-bioinformation-ethical-issues.pdf> (última consulta 04/04/2022).

IGNACIO J. y ECEIZABARRENA U. (2014). Breves apuntes sobre las sentencias básicas del tribunal de justicia de la unión europea. UNED - Teoría y Realidad Constitución, 33, 443–480.

<http://revistas.uned.es/index.php/TRC/article/viewFile/13022/12015>

(última consulta 04/04/2022).

JAEN VALLEJO M. (2004). “Una visión del problema desde una perspectiva constitucional: el estudio particular de la protección de la intimidad y los bancos genéticos”. Cuadernos de derecho judicial. Vol. VI : 93 – 134.

JEFFREYS A. J., BROOKFIELD J.F.Y and SEMEONOFF R. (1985). Positive Identification of an Immigration Test-Case Using Human DNA Fingerprints. Nature 317 (6040): 818–19.

<https://doi.org/10.1038/317818a0> (última consulta 04/04/2022).

JIMÉNEZ SÁNCHEZ, F. (2015). Europol: cooperación y coordinación policial en la Unión Europea. Tesis doctoral.

http://e-archivo.uc3m.es/bitstream/handle/10016/21378/tesis_fernando_jimenez_sanchez.pdf?sequence=1
(última consulta 04/04/2022).

JOUBERT C. Y BEVERS H. (1996). Schengen investigated. International, Kluwer Law.

KAPPLER S. (2011). El consentimiento en la toma de muestras de ADN. Especial referencia a los procesos de menores (Parte II). Revista de derecho y genoma humano. Vol. 34: 51 – 97.

KAYSER, M. (2013). Forensic DNA Phenotyping: DNA Testing for Externally Visible Characteristics. Encyclopedia of Forensic Sciences: Second Edition. 2nd ed. Elsevier Ltd.

<https://doi.org/10.1016/B978-0-12-382165-2.00067-2>

(última consulta 04/04/2022).

KAYSER, MANFRED y SCHNEIDER P.M. (2009). DNA-Based Prediction of Human Externally Visible Characteristics in Forensics: Motivations, Scientific Challenges, and Ethical Considerations. Forensic Science International: Genetics 3 (3): 154–61.

<https://doi.org/10.1016/j.fsigen.2009.01.012> (última

consulta 04/04/2022).

KENNETT D. (2019). Using Genetic Genealogy Databases in Missing Persons Cases and to Develop Suspect Leads in Violent Crimes. Forensic Science International 301 (August): 107–17.

<https://doi.org/10.1016/j.forsciint.2019.05.016> (última

consulta 04/04/2022).

KUPCHINSKY, R. (2004), Intelligence and police coordination in the EU, Radio Free Europe, Organized Crime and Terrorism Watch, 4/11, 21 de abril.

<https://www.rferl.org/a/1342339.html> (última consulta 04/04/2022).

LELLO L., AVERY S.G., TELLIER L., VAZQUEZ A.I., DE LOS CAMPOS G., HSU S.D.H. (2018). Accurate Genomic Prediction of Human Height. *Genetics* 210: 2477-2497

LLANO C. H. del. (2005). Los derechos fundamentales en la Unión Europea (A. Editorial (ed.)).

LUCENA CID I. V. (2014). Concepto intimidad en los nuevos contextos tecnologicos. In Tirant Lo Blanch (Ed.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación* (1st ed., pp. 15–53).

MACHADO H. y GRANJA R. (2019). Risks and Benefits of Transnational Exchange of Forensic DNA Data in the EU: The Views of Professionals Operating the Prüm System. *Journal of Forensic and Legal Medicine* 68 (November).
<https://doi.org/10.1016/j.jflm.2019.101872> (última consulta 04/04/2022).

MACHADO H. y GRANJA R. (2020). *Forensic Genetics in the Governance of Crime*. Palgrave Mcmillan.
<https://doi.org/10.1007/978-981-15-2429-5> (última consulta 04/04/2022).

MACLEAN C. E. (2014). Creating a Wanted Poster from a Drop of Blood: Using DNA Phenotyping to Generate an Artist's Rendering of an Offender Based Only on DNA Shed at the Crime Scene. Hamline L. Rev 36 (3): 1. <http://digitalcommons.hamline.edu/cgi/viewcontent.cgi?article=1022&context=hlr> (última consulta 04/04/2022).

MADRID CONESA F. (1984) Derecho a la intimidad, informática y estado de Derecho, Universidad de Valencia, Valencia.

MARICA, A. (2012) El sistema de tratamiento de la información en Europol. Universidad Carlos III de Madrid. <https://www.icps.cat/archivos/WorkingPapers/wp309.pdf?noga=1> (última consulta 04/04/2022).

MARTIN PATOR J. (2013). La obtención de muestras de ADN, dubitadas e indubitadas, por la Policía Judicial y el régimen de sometimiento del sospechoso a los actos de inspección, registro o intervenciones corporales. Las Bases de Datos Policiales de ADN (Dykinson S.L.) (Issue 2013): 197–219 <https://dialnet.unirioja.es/servlet/articulo?codigo=6973597> (última consulta 04/04/2022).

MARTÍNEZ PÉREZ, F. ; POZA CISNEROS, M. (2013). El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm. Consejo General del Poder Judicial.

Ministerio del Interior, Secretaría de Estado de Seguridad (2021). Base de Datos Policial de Identificadores Obtenidos a Partir de ADN. Memoria Enero – Diciembre 2020.

http://www.interior.gob.es/documents/642317/12463021/Base_de_datos_policial_identificadores_ADN_Memoria_2020_126200173_web.pdf/da283060-bc1e-464a-bb4c-df30fc61ef60 (última consulta 04/04/2022).

Ministerio del Interior. Manual técnico de procedimiento del sistema de gestión nacional de identificadores obtenidos a partir de ADN (SIGENI). Versión 7_1.

NIEMIEC E., BORRY P., PINXTEN W. y HOWARD H.C. (2016). Content Analysis of Informed Consent for Whole Genome Sequencing Offered by Direct-to-Consumer Genetic Testing Companies. *Human Mutation* 37 (12): 1248–56.

<https://doi.org/10.1002/humu.23122> (última consulta 04/04/2022).

Nuffield Council on Bioethics. The Forensic Use of Bioinformation: Ethical Issues. (2015). Jahrbuch Für Wissenschaft Und Ethik 13 (1).

<https://doi.org/10.1515/9783110196832.3.419> (última consulta 04/04/2022).

OSSORIO P. N. (2006). About Face: Forensic Genetic Testing for Race and Visible Traits. In Journal of Law, Medicine and Ethics, 34:277–92.

OUBIÑA BARBOLLA S. (2015). Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: Las nuevas propuestas normativas y la STJUE de 8 de abril de 2014. Aranzadi (Ed.), La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea (p. 851).

PATTOCK A. (2011). It's All Relative: Familial DNA Testing and the Fourth Amendment. Minnesota Journal of Law, Science & Technology 12 (2): 851–76.

POSPIECH E., CHEN Y., KUKLA-BARTOSZEK M., BRESLIN K., ALIFERI A., ANDERSEN J.D., et al. (2018). Towards broadening Forensic DNA Phenotyping beyond pigmentation: Improving the prediction of head hair shape from DNA. Forensic Sci Int Genet 37: 241-251.

REBOLLO DELGADO L., y SERRANO PEREZ M. M. (2006).
Introducción a la protección de datos.

REBOLLO DELGADO L. (1998). Derechos de la personalidad y datos personales. Revista de Derecho Político, 44, 143–206.
<http://e-spacio.uned.es/revistasuned/index.php/derechopolitico/article/download/8725/8319> (última consulta 04/04/2022).

SALVADOR VELARDE F.J., MOLINA-BENÍTEZ C. E., SOLÓRZANO-ROSALES R. et Al., (2008). Identificación del sexo mediante análisis molecular del gen de la amelogenina. Revista Mexicana de Patología Clínica y Medicina de Laboratorio. Vol 55 núm. 1: 17 – 20
<https://www.medigraphic.com/pdfs/patol/pt-2008/pt081b.pdf> (última consulta 04/04/2022).

Secretaría de la CNUFADN. Instituto Nacional de Toxicología y Ciencias Forenses (2012). Comisión Nacional Para El Uso Forense Del Adn.
https://www.mjusticia.gob.es/es/ElMinisterio/OrganismosMinisterio/Documents/1292428320905-Memoria_de_la_Comision_Nacional_para_el_Uso_Forense_del_ADN_Actividades_2012.PDF (última consulta 04/04/2022).

- SHAFFER J.R., LI J., LEE M.K., ROOSENBOOM J.,
ORLOVA E., ADHIKARI K., et al. Multiethnic GWAS
(2017). Reveals Polygenic Architecture of Earlobe
Attachment. *Am J Hum Genet* 101: 913-924.
- SOCIETY I., Web, W. W., & Ts, I. C. (2003). Agenda for
Action: February.
- SOLOVE D. J. (2008). Understanding privacy. Harvard
University Press.
- THOMPSON J. B. (2011). Los límites cambiantes de la vida
pública y la privada. *Comunicación y Sociedad*, 15, 11–
42.
<http://www.scielo.org.mx/pdf/comso/n15/n15a2.pdf>
(última consulta 04/04/2022).
- TOOM V., GRANJA R. Y LUDWIG A. (2019). The Prüm
Decisions as an Aspirational regime: Reviewing a
Decade of Cross-Border Exchange and Comparison of
Forensic DNA Data. *Forensic Science International:
Genetics*. Vol 41. 50 – 57.
- TURRINA S., FILIPPINI G. y DE LEO D. (2011).
Concordance Study and Allele Frequencies for 5 New
European Standard Set (ESS) Loci in the North-East
Italian Population. *Forensic Science International:
Genetics Supplement Series* 3 (1): e329–30.

<https://doi.org/10.1016/j.fsigss.2011.09.027> (última consulta 04/04/2022).

VILASAU M. (2006). La Directiva 2006/20/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad. *Revista d'Internet Dret i Política*, 2006, núm. 3, pp. 1-15.

WALSH S., FAN L., BALLANTYNE K.N., VAN OVEN M., LAO O. y KAYSER M. (2011). IrisPlex: A Sensitive DNA Tool for Accurate Prediction of Blue and Brown Eye Colour in the Absence of Ancestry Information. *Forensic Science International: Genetics* 5 (3): 170–80.
<https://doi.org/10.1016/j.fsigen.2010.02.004> (última consulta 04/04/2022).

WALSH S., FAN L., WOLLSTEIN A., KOVATSI L., RALF A., KOSINIAK-KAMYSZ A., BRANICKI W. y KAYSER M. (2013). The HIrisPlex System for Simultaneous Prediction of Hair and Eye Colour from DNA. *Forensic Science International: Genetics* 7 (1): 98–115.
<https://doi.org/10.1016/j.fsigen.2012.07.005> (última consulta 04/04/2022).

WARREN S. y BRANDEIS L. (1890). The Right to Privacy. *Harvard Law Review*, IV(5).

http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (última consulta 04/04/2022).

WICKENHEISER R. (2019). Familial Searching Internal Validation and Implementation. *Forensic Science International: Synergy* 1: S18–19. <https://doi.org/10.1016/j.fsisyn.2019.04.005> (última consulta 04/04/2022).

ZBIEC-PIEKARSKA R., SPOLNICKA M., KUPIEC T., PARYS-PROSZEK A., MAKOWSKA Z., PALECZKA A., et al. (2015). Development of a forensically useful age prediction method based on DNA methylation analysis. *Forensic Sci Int Genet* 17: 173-179.