Carlos Reusser Monsálvez
creusser@uchile.cl

LA PROTECCION DE LOS DATOS PERSONALES COMO DERECHO FUNDAMENTAL

1.- Sentido y alcance del Derecho Fundamental a la Protección de Datos en los albores del s. XXI

a) Evolución del Derecho a la Protección de Datos Personales

El derecho a la protección de datos personales ha recorrido un largo camino hasta adquirir la forma que hoy conocemos. Sus orígenes se remontan a la formulación de la *privacidad* realizada por Louis Dembitz BRANDEIS y Samuel Dennis WARREN, elaborada a partir de precedentes jurisprudenciales y publicada en la obra "The Right of Privacy",[1] este derecho, concebido como "the right to be let alone", el "derecho a ser dejado solo", a no ser molestado, trae aparejadas las consecuentes posibilidades de controlar la información que pertenece a la persona por emanar o referirse a ella. Su tesis[2] obedece a una construcción *ius privatista* de las garantías personales, que desarrolló su argumentación a partir del derecho de propiedad (*property*); de ahí se desprende que la doctrina haya entendido que vulneraba este derecho las violaciones a la confianza (*breach of confidence*), las violaciones al derecho de autor (*copyright*) o, finalmente la difamación (*defamation*), y que a su turno se haya concebido la reparación pecuniaria como mecanismo de indemnización.

---

[1] Esta obra fue publicada originalmente en la *Harvard Law Review*, vol. IV, núm. 5, 1890, y traducido al castellano por Benigno Pendás y Pilar Baselga como "El Derecho a la Intimidad", publicándose por editorial Civitas en Madrid, el año 1995. La traducción del título al castellano es errónea, lo que ha dado lugar a una de las confusiones más lamentables del mundo jurídico, pues en realidad debió llamarse "El Derecho a la Privacidad" o "El Derecho a la Vida Privada", ya que la intimidad y la privacidad son instituciones jurídicas diferentes y, más aún, la *privacy* es un concepto jurídico indeterminado propio del ámbito anglosajón.

[2] Destacan asimismo en esta línea argumental el ensayo titulado *Privacy*, de William PROSER (1960), publicado en *California Law Review*, agosto de 1960; de PARKER, en *A Definition of Privacy* (1974) y de FRIED, su trabajo *An Anatomi of Values* (1979).

De su parte, en el Derecho continental europeo se construye la protección de datos originalmente a partir del reconocimiento del derecho a la intimidad, del derecho al honor[3] y a la propia imagen, tema que fue cobrando progresiva relevancia, atendido el avance del desarrollo tecnológico.

Al respecto, el prof. SUÑÉ LLINÁS nos evidencia que ya en ese entonces fue manifiesta la tensión entre "la preocupación por proteger la intimidad de las personas y la capacidad invasiva de la tecnología"[4].

Mas, no podemos centrar nuestro análisis de la configuración de este derecho sólo en la intimidad, pues habremos de reconocer que desde mucho antes se hace manifiesta la tensión entre la libertad de información y la libertad personal en general. Así, ya en 1858 John STUART MILL[5] reconocía que la libertad es un bien muy preciado para la persona, que le garantizaba la posibilidad de conducir sus pensamientos y acciones en la forma que mejor estimare, sujeto eso sí a los efectos jurídicos de sus actos y que, por cierto, le garantizaba el derecho a asociarse libremente, siempre y cuando su acción no fuera contra el derecho de terceros. Pues bien, como derivación de la libertad, se desarrolló la libertad de información, derecho público subjetivo entre cuyos alcances y limitaciones está íntimamente ligado a la institución que nos ocupa, puesto que de una parte comprende el derecho a informar, o sea, a difundir noticias, expresar ideas o percepciones de la realidad y el derecho a ser informado, esto es, a exigir que se nos den a conocer los hechos que suceden o las ideas que se van desarrollando (y ciertamente las informaciones o ideas podrán referirse a personas determinadas o determinables); de otra parte está también la libertad de acción de la persona sin la intervención

---

[3] Véase por ejemplo, Rafael VELÁZQUEZ BAUTISTA, *Protección Jurídica de Datos Personales Automatizados*. Editorial Colex, Madrid, 1993.

[4] Emilio SUÑÉ LLINÁS, *Tratado de Derecho Informático*, 2ª Edición, Servicio de publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid, Madrid, 2002, pág. 43.

[5] John STUART MILL, *Ensayo sobre la Libertad*, Alianza editorial, Madrid, 1997, pág. 32.

ilegítima de terceros, en cuya concreción puede influir ciertamente la necesidad de ocultamiento de información personal.

En cuanto a las manifestaciones normativas de la protección de datos, ya en 1981, a través del Convenio 108 del Consejo de Europa, de 28 de enero de ese año, "para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal", firmado en Estrasburgo, se reconoce expresamente la necesidad de garantizar la intimidad de las personas "teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos personales que son objeto de tratamientos automatizados" y en el plano doctrinal, en 1982 Frosini nos evidenciaba como problemas asociados a la propia imagen el avance de las tecnologías: "la reproducción de la imagen, interferencias telefónicas, transmisión y recepción de programas televisivos, control sobre las opiniones religiosas o políticas de los súbditos, etc."[6].

Contra lo que pueda sostenerse respecto de esta época, estimamos que ya el Convenio 108 sienta las bases que permiten zanjar la cuestión de que las garantías fundamentales que se buscan proteger van más allá de la intimidad, al indicar en su exposición de motivos respecto de la protección de datos, que:

> "El presente Convenio tiene por objeto reforzar la protección de datos, es decir, **la protección jurídica de los individuos** con relación al tratamiento automatizado de los datos de carácter personal que les conciernen". [7]

Siguiendo nuestro análisis de la construcción del derecho fundamental a la protección de datos, creemos obligado referirnos a la sentencia del Tribunal Constitucional alemán, de 15 de diciembre de 1983[8], que declara inconstitucionales algunos artículos de la Ley del Censo de la RFA. Esta sentencia reconoce que:

---

[6] Vittorio FROSINI, *Cibernética, Derecho y Sociedad*. Editorial Tecnos, Madrid, 1982.

[7] Lo destacado es nuestro.

[8] Sentencia traducida por Manuel Daranas y publicada en el Boletín de Jurisprudencia Constitucional Nº 33 de las Cortes Generales. Madrid, 1984, págs.126 a 170.

> En las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitada de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1 [derecho general a la personalidad propia], en relación con el artículo 1º del párrafo 1 [protección de la dignidad humana] de la ley fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y utilización de los datos referentes a su persona.

Siendo así, independiza la protección de datos personales respecto de la intimidad, el honor y la propia imagen como garantías protegidas y recalca la función instrumental a la protección de la dignidad, la libertad y la igualdad que asisten a la persona humana en general, de las que derivan la generalidad de las garantías consagradas en los distintos catálogos de derechos.

Conforme a ello realiza una construcción a través de la cual reconoce la existencia del derecho a la *autodeterminación informativa*, que hace emanar directamente de la dignidad de la persona, que actúa con autodeterminación como miembro de una sociedad libre. Considera los peligros que entrañan para estos bienes jurídicos las condiciones imperantes en esa época y las que visualiza a futuro respecto de la elaboración automática de datos. Conforme a ello, sostiene que las necesidades de garantizar la autodeterminación demanda un nivel especial de protección, por cuanto:

> Los procesos de decisión ya no se pueden retrotraer como antiguamente a registros y documentos compilados manualmente; antes bien, hoy en día, gracias a la ayuda de la elaboración automática de datos, la información individual sobre las circunstancias personales u objetivas de una persona determinada o, en su caso determinable (…) son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquiera que sea la distancia. Es más, esa información puede -especialmente con el montaje de sistemas integrados de información- refundirse con otras colecciones de datos en un perfil de personalidad parcial o ampliamente definido, sin que el interesado pueda controlar suficientemente su exactitud y su utilización. De este modo se han ensanchado en una medida hasta ahora desconocida las posibilidades de indagación e influencia susceptibles de incidir sobre la conducta del individuo, siquiera sea por la presión psicológica que supone el interés del público en aquella.

Este derecho le faculta para decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida, de lo que se deduce "la libre eclosión de la personalidad del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona". Como cualquier otro, reconoce que este derecho no es absoluto, sin embargo las limitaciones que a su respecto se impongan:

> Sólo son admisibles en el marco de un interés general y necesitan un fundamento legal basado en la Constitución, que debe corresponder al imperativo de claridad normativa, inherente al Estado de Derecho. En su regulación debe el legislador observar, además, el principio de la proporcionalidad y tiene que adoptar asimismo precauciones de índole organizativa y de derecho a la salvaguardia de la personalidad.

Tal es evidente la vinculación de este derecho a la libertad y autodeterminación del individuo que la sentencia entiende que la conducta de la persona podrá verse afectada severamente a través de su vulneración. Así sostiene que:

> "El que [la persona] no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación (…) Quien se siente inseguro de si en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales (…) esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de los ciudadanos.

Continua diciendo que "De este modo, un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo la elaboración automática de datos, ninguno 'sin interés'"… a través de ellos, sostiene, puede elaborarse "una imagen total y

pormenorizada de la persona respectiva –un perfil de personalidad- incluso en el ámbito de su intimidad, convirtiéndose el ciudadano en un 'hombre de cristal'".

Por supuesto debemos reconocer que en esta época también hay una abundante normativa que acompaña el proceso de consolidación de este derecho y que va reflejando los giros legislativos y las experiencias de los países. Dentro de este contexto y a nivel internacional son referentes obligados las "Directrices para la Regulación de los archivos personales informatizados", adoptadas por las Naciones Unidas mediante Resolución 45/95, de la Asamblea General, de 14 de diciembre de 1990, y a nivel europeo, la Directiva europea 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995 *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, que sienta los principios bases en esta materia para el entorno comunitario, sin perjuicio que ha fijado las pautas para enfrentar esta materia a nivel mundial, por su grado de influencia y desarrollo.

Asimismo, y también en el plano jurisprudencial, habremos de mencionar en los años 90 la concepción elaborada en España por su Tribunal Constitucional en la STC 254/1993 que menciona por primera vez en ese entorno el derecho a la "libertad informática" como un derecho fundamental en sí mismo, que junto al artículo 18.4 de la Carta Fundamental de 1978 constituyen las bases de la construcción española.

En nuestros días asistimos ya a la consagración en la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en diciembre del 2000, en su artículo 8 que dispone:

> 1. Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Concluimos en este punto entonces que no obstante su origen primigenio, la problemática del tratamiento de datos personales progresivamente fue abstrayéndose de la sola protección de las garantías de intimidad, honor y propia imagen, fruto de la evidencia que mostró que la recogida, desvelación y sistematización de información personal podía asociarse directamente con la dignidad humana frente a la evidencia que las intromisiones vulneraba o podía vulnerar un cúmulo de derechos fundamentales, tales como la vida, como dejó en evidencia la historia reciente de muchos países afectados por la llaga de la dictadura, en que los órganos de terrorismo de Estado recopilaban furtivamente información de los tipos de lecturas que escogían los estudiantes, las personas con que interactuaban, etc., a fin de determinar si eran afines o no al régimen *de facto* para, sobre esa base, decidir (arbitrariamente por cierto) sobre su vida, libertad y/o seguridad personal.

Siendo así, las concepciones jurídicas más avanzadas entienden hoy que el derecho a la protección de datos integra la categoría de derecho fundamental, y así lo consagran expresamente en su Constitución Política, directamente en el caso de Portugal, o a través de construcciones jurisprudenciales como los caso de Alemania y España, país en que su Tribunal Constitucional fue cambiando sus tesis al respecto, pasando de presentarlo como:

> Un mero derecho de carácter instrumental, a modo de garantía y presupuesto de la protección de otros derechos, a resoluciones posteriores en que se configura como un nuevo derecho o libertad fundamental de carácter autónomo e independiente respecto del derecho a la intimidad personal y familiar[9].

Consistente con esta nueva concepción, el Tribunal Constitucional español, en sentencia 292/2000 de 30 de noviembre, precisó expresamente que son datos sujetos al derecho fundamental a la protección de datos:

> Todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquiera otra

[9] ABELLÁN y SÁNCHEZ-CARO, Op. Cit., pág. 8.

índole, **o que sirvan para cualquiera otra utilidad que en determinadas circunstancias constituyan una amenaza para el individuo**[10].

Conforme este nuevo avance, progresivamente se le ha considerado como un derecho autónomo cuyo objetivo jurídico es proteger todos los demás derechos, fundamentales o no, reconocidos en un ordenamiento normativo.

Es decir, el proceso evolutivo lleva a distinguir claramente que uno es el derecho fundamental a la intimidad y una cuestión distinta es el derecho fundamental a la protección de datos, estando el primero destinado proteger a las personas de invasiones a su vida personal y familiar y el segundo a dar un poder de disposición sobre los datos que le conciernen, tanto en su uso como destino. Por tanto, a través de este derecho no sólo se protegen los datos íntimos, sino a cualquier tipo de dato personal, como los genéticos o los de perfiles de ADN, pues su conocimiento por terceros pueden vulnerar toda la escala de derechos de las personas, sean fundamentales o no.

Debemos asimismo traer a colación en este punto que en su momento se generó una polémica por considerarse el término "Protección de Datos", poco feliz, ya que da a entender que el objeto de la protección son los datos en sí y no la persona que es titular de los mismos[11].

b) La Protección de Datos Personales en el Estado Democrático

Hoy en día las necesidades de información acerca de las personas recorre prácticamente todos los sectores de la sociedad. La Sociedad de la Información según ROCANGLIOLO[12] enraíza más bien en la tradición cultural europea y tiene implicancias y significaciones conceptuales más

[10] Lo destacado es nuestro.

[11] La menciona Miguel Ángel DAVARA RODRÍGUEZ en su *Manual de Derecho Informático*, 3ª edición. Editorial Aranzadi, Navarra, 2001, págs. 48 y 49.

[12] Rafael RONCAGLIOLO. "¿Se Construye Ciudadanía en la Sociedad de la Información?" en *Ciudadanos en la Sociedad de la Información*. Pontificia Universidad Católica del Perú y The British Council Perú. Lima, 1999.

ricas que las *information highways* ("autopistas de la información") norteamericana. En efecto, Europa ha realizado esfuerzos notables por entrar en la nueva era previendo un marco que garantice un pleno respeto a las garantías fundamentales. Hoy en día se reconoce que la libre circulación de los datos personales es un imperativo no sólo para el desarrollo de la nueva economía, sino además para el funcionamiento del sistema democrático, como nos evidencia SAARENPÄÄ:

> No, no podemos manejarnos sin disponer de datos personales. Estamos acostumbrarnos a usar diferentes formas de identificación, desde nuestro nombre o una imagen hasta diversos identificadores biométricos. Usamos estas formas de identificación para comprobar nuestra identidad y permitirnos ser identificados en diferentes situaciones.[13]

Conforme este autor el problema de la identificación es complejo, por cuanto la persona puede disponer de muchas identidades, tantas como sus datos personales le permitan. Siendo así, podríamos distinguir entre la identidad física, que podríamos calificar como única, y la identidad jurídica que en parte importante dependerá de las esferas en las cuales la persona se desenvuelve. Por ejemplo, frente a los datos personales de identificación, en el tema que nos ocupa, podemos decir que la persona ante la justicia criminal podrá tener al menos tres tipos de identidades, como legitimado activo (la víctima), legitimado pasivo (el denunciado o querellado) o tercero ligado al proceso (el juez que resuelve, el testigo que declara, etc.).

Siendo así, y siguiendo la línea argumental de SAARENPÄÄ, en la Sociedad de la Información uno de los temas radicales ha sido la implementación de sistemas de identificación, tal es el caso de los controvertidos números únicos de identificación personal y otro, más controvertido aún e incluso repudiado en el mundo nórdico, es el de los sistemas biométricos de identificación, no obstante constituir técnicamente un "sistema infalible de identificación".

---

[13] Ahti SAARENPÄÄ. "Europa y la Protección de Datos Personales" en *Revista Chilena de Derecho Informático* n° 3, editada por el Centro de Estudios en Derecho Informático de la Universidad de Chile. Santiago de Chile, 2003, pág. 15.

Como podemos apreciar, el tema es complejo, puesto que la llamada eficiencia del sistema y las exigencias del Estado Democrático de Derecho nos llaman a perfeccionar los sistemas de identificación, pero aunque se conciba al aparato público como un entramado de recursos materiales y humanos al servicio de la persona humana, no es legítimo que se llegue a establecer un sistema que en definitiva comprometa en su esencia al derecho a la autodeterminación. Siguiendo esta línea argumental este autor sostiene que:

> Concedemos a la sociedad, a los medios de comunicación y al mercado autorización en la medida necesaria para supervisar y monitorearnos y usar nuestros datos personales. Formalmente en la democracia burocrática, los ciudadanos existen para la máquina, los medios y la organización; aquí se nos conceden ciertas libertades, donde hay razones para ello. La diferencia entre estas dos formas de democracia es substancial. El estándar de protección de datos (…) constituye un indicador de la democracia: mientras más efectivamente protegemos nuestros datos personales, más cerca nos encontramos de la idea de democracia. Y por otro lado, podemos preguntarnos si un Estado sin legislación sobre protección de datos personales es una democracia realmente.[14]

Esta afirmación es consecuente con lo que dispone la Declaración Universal de Derechos Humanos, en sus artículos 29 y 30:

> Artículo 29
>
> 1.- Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad.
>
> 2.- En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones **establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás**, **y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática**.[15]
>
> 3.- Estos derechos y libertades no podrán en ningún caso ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas.
>
> Artículo 30

[14] Ahti SAARENPÄÄ. Op. Cit., pág. 18

[15] Evidentemente, lo destacado es nuestro.

> Nada en la presente Declaración podrá interpretarse en el sentido de que confiere derecho alguno al Estado, a un grupo o a una persona, para emprender y desarrollar actividades o realizar actos tendientes a la supresión de cualquiera de los derechos y libertades proclamados en esta Declaración.

Así, la premisa que tendremos presente en el desarrollo de nuestro trabajo es que en nuestros días el derecho a la protección de los datos personales se presenta como un elemento esencial para el libre desarrollo de la personalidad en las sociedades democráticas.

2. El Estatuto Jurídico de los Datos Personales

a) Concepto de Datos Personales

Para comprender a cabalidad que ha de entenderse por datos personales, habremos remitimos en primer lugar a qué se entiende por "dato" y luego cuales son las condiciones particulares que lo califican como "personal". En efecto, ayuda a la comprensión de esta categoría que tengamos presente que se entiende generalmente por "dato" aquel antecedente o noticia primera que permite investigar acerca de la verdad de un hecho y por ende es "personal" aquel dato, esto es, cualquier antecedente o noticia que proporcione información acerca de las circunstancias de una persona. Así lo ha recogido el legislador comunitario, cuando la Directiva 95/46/CE, del Parlamento Europeo, dispone que es tal: **"Toda información sobre una persona física identificada o identificable"**[16]**.**

Como podemos apreciar, el concepto considera dato personal a ***"toda información";*** por tanto se trata de un concepto amplio, que no discrimina los datos por su naturaleza ni por el soporte en el cual consta. Abarca tanto imagen, sonido, o conjuntos de caracteres grafológicos y/o

[16] Artículo 2 a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, publicada en el Diario Oficial de la Comunidad Europea de 23 de Noviembre de 1995.

numéricos, debiendo tenerse presente que pueden manifestarse por distintos medios y adoptar diversas formas de representación. Esto será importante al momento de analizar los datos de perfiles de ADN, por cuanto en primer lugar podemos sostener *a priori* que son datos personales, y en segundo lugar, por que pueden constar en distintos soportes.

El concepto supone que estos datos "***conciernan a una persona física***". Pues bien, este requisito determina el ámbito de aplicación de la protección de datos, en cuanto excluye aquellos datos que se refieran a personas jurídicas. Podemos entender que, emanando la protección de datos personales directamente de la dignidad humana, sólo la persona física puede ser titular de la protección, aunque si atendemos a la literalidad del artículo 3º del Convenio 108 leeríamos que:

> "Se aplicará asimismo el presente Convenio a informaciones relativas a grupos de personas, asociaciones, fundaciones, sociedades, corporaciones o cualquier otro organismo formado directa o indirectamente por personas físicas, tuvieren o no personalidad jurídica".

Creemos que para salvar esta aparente contradicción debemos entender este precepto en un sentido garantístico y con ello sostener que el precepto busca amparar dentro de su marco a las personas que integran la organización de que se trata. La norma no se refiere a los datos concernientes a la persona jurídica o entidad de hecho en sí, sino en la medida que estén formados directa o indirectamente por personas físicas. Se cierra así el círculo de protección de datos personales a fin de dar una efectiva protección a los titulares de dichos datos.

En todo caso, cualquiera sea la postura que en definitiva se acepte, en cuanto a si la protección alcanza a los datos de personas físicas o jurídicas, queda claro que el objeto de protección jurídica es la persona titular de los datos y que el término "dato personal", ha sido generalmente aceptado por adecuarse a la terminología informática y por considerarlo apto al momento de determinar el sentido y alcance de la protección brindada a los sujetos.

Además de lo anterior, el concepto requiere para que el dato sea personal que la persona concernida sea ***identificada o identificable****,* a cuyos efectos la misma Directiva 95/46/CE nos entrega el criterio para los efectos de determinar cuando se cumple esta condición, al disponer en el artículo 2 letra a) que será tal:

> Toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Ayuda a la interpretación de esta norma, lo indicado en la motivación 26 de la Directiva, en cuanto señala que para ello habrá que considerar el conjunto de los medios que puedan ser razonablemente utilizados, tanto por el responsable del tratamiento como por cualquier otra persona, para identificar a un sujeto.

El criterio de la Directiva 95/46/CE es más amplio que el previamente establecido en el Convenio 108, conforme al cual se cumple con el requisito sólo si la persona "puede ser fácilmente identificada; no se incluye al respecto la identificación de personas por métodos complejos", concepto que excluía, de suyo, todo método de carácter científico o técnico de identificación, tal como el análisis de huellas digitales, el procesamiento de imágenes o sonidos, o el tema principal que nos ocupa, que son las huellas genéticas, todos métodos perfectamente posibles hoy, atendido el avance tecnológico.

El criterio de la Directiva tuvo el mérito de ser más adecuado a la realidad tecnológica y social, pues hoy en día existen técnicas y procedimientos hábiles para la identificación del sujeto a partir de diversas circunstancias, sin imponer esfuerzos exorbitantes al responsable del tratamiento o encargado del tratamiento de datos personales.

En efecto, por ejemplo el tipo de datos que nos ocupan, tienen la habilidad de, mediante procedimientos técnicos determinados, identificar a una persona. Siendo así habremos de tener especial cuidado al analizarlos en cuanto a su calificación y regulación de los bancos de datos en los que se registre.

Si bien constituye una máxima generalmente aceptada que los datos de carácter personal deben ser objeto de un régimen de garantías, en tanto son necesarios para la protección de la persona, no todo dato goza del mismo nivel de protección. En efecto, conforme la normativa, estos son susceptibles de una **clasificación** a partir de sus condiciones de las mayores o menores posibilidades de afectación de las garantías fundamentales comprometidas.

Es así como dentro de los datos de carácter personal se ha establecido un orden de prelación, que va desde datos públicos o irrelevantes, hasta datos especialmente protegidos, previéndose para cada uno de estos tipos un régimen de protección especial.

De esta manera, cada uno de ellos ocupará un lugar en el orden de prelación atendiendo principalmente a su naturaleza y aptitud para vulnerar, mediante su difusión, los derechos fundamentales objeto de la protección. Dicho de otra forma, para determinar la ubicación que corresponde a cada tipo de dato de carácter personal dentro de dicha escala deberemos atender al grado de riesgo de vulneración de derechos fundamentales que el tratamiento de esos datos lleva implícito.

De esta manera, y siguiendo el criterio antes enunciado, se reconocen las siguientes categorías de datos de carácter personal, a saber:

En primer lugar los **datos públicos**, que son aquellos que "de acuerdo con el valor que les atribuye la conciencia social, son conocidos por cualquiera"[17]. Se caracterizan porque son comúnmente conocidos por la generalidad de las personas o, al menos son fácilmente accesibles por encontrarse en registros públicos de libre acceso, tales como guías telefónicas. Originalmente también se les denominó "datos irrelevantes", pero actualmente se tiene plena conciencia de que no hay datos personales irrelevantes, pues por escasa importancia que parezca tener un dato individualmente considerado, al relacionarlos con otros suelen adquirir un valor trascendental.

[17] Miguel Ángel DAVARA RODRÍGUEZ, op. cit., pág. 55.

En contraposición a los anteriores, los **datos sensibles** son aquellos que conforme al valor que les asigna la conciencia social, "solamente serán conocidos o por voluntad del titular o en circunstancias especiales y tasadas por las leyes"[18]. Estos datos se refieren a cuestiones especialmente delicadas, directamente vinculadas al núcleo de la personalidad y dignidad humana, que incluso pueden inducir a decisiones discriminatorias a su respecto o cuya revelación constituirá una lesión a su intimidad, propia imagen, honor, libertad sindical, etc. Es por esto que se les denomina "especialmente protegidos", en cuanto el legislador es extremadamente cuidadoso al momento de señalar los procedimientos y limitaciones en su tratamiento. Siendo así la Directiva en principio prohíbe su tratamiento, salvo las circunstancias específicas que analizaremos a continuación a propósito del **consentimiento del interesado** como condición legitimante del tratamiento de datos personales.

Como ya señalamos, no es pertinente agrupar aquí los perfiles de ADN, pues se deducen a partir del ADN no codificante, pero si sería parte de estas categorías especiales los datos las secuencias de ADN codificante, esto es, que contienen información genética.

b) El Tratamiento de Datos Personales.

Como hemos venido sosteniendo, los datos *per sé* no tienden a proporcionar información, en pos de general conocimiento. Para que esto suceda es necesario someterlos a distintos procedimientos que podrán ser simples, como el registro de datos de ubicuidad de una persona en una agenda manual, o más complejos, como su sistematización e interrelación con otros datos, integración en sistemas compartidos, etc.; siendo así el problema de los datos personales se suscrita al momento que son "tratados", es decir, cuando son sometidos a dichos procedimientos. En esta materia el legislador comunitario ha sido especialmente cuidadoso, en

[18] Idem.

el sentido de procurar que por vía de una mala calificación de las operaciones que comprende el tratamiento, en definitiva la persona quede en indefensión frente a terceros que han recopilado y/o trafican datos que le conciernen.

Esta preocupación la vemos en la definición de tratamiento de datos que adopta la Directiva, cuando dispone:

> Se entiende por "tratamiento" cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.[19]

Conforme a este concepto, el tratamiento de datos comprende **cualquier operación o conjunto de operaciones**, con lo cual se trata de un concepto amplio, que reconoce el carácter complejo del procedimiento de tratamiento de datos personales. Comprende por tanto desde la fase de recogida de los datos hasta su difusión, que pasa por la revelación de información a una persona (o a varias personas) como la consulta de la información por esas personas[20]. Asimismo, de este elemento se desprende el carácter meramente enunciativo de las operaciones que posteriormente enumera, por lo que estamos frente a un concepto amplio y flexible, susceptible de ir adecuándose a los cambios tecnológicos en la materia.

También nos dice la definición que las operaciones del tratamiento de datos podrán ser efectuadas o no mediante procedimientos automatizados. En este aspecto es más garantista que la contenida en el Convenio 108, que en términos generales sólo consideraba que las fases automatizadas estaban bajo su esfera de protección al señalar en su artículo 2 que:

---

[19] Artículo 2 a), capítulo I, Directiva 95/46/CE.

[20] "Notas Explicativas del Convenio 108 del Consejo de Europa." Número 31.

"Comprenderá las operaciones siguientes, efectuadas en todo o parte con ayuda de medios automatizados: almacenamiento de datos, aplicaciones a tales datos de operaciones lógicas o aritméticas, o de ambas, su modificación, borrado, recuperación o difusión".

Las falencias de este concepto dicen relación por una parte con la inconveniencia de establecer una enumeración taxativa, cuando la técnica avanza a pasos y por caminos insospechados, y que por lo demás no considera la fase de recogida de los datos, a pesar de la importancia que reviste, por cuanto en ese momento se deben satisfacer todos y cada uno de los imperativos que inspiran el tratamiento de datos. Además, como somos conscientes hoy, en esta etapa se pueden producir afectaciones a los derechos de los titulares de datos, por ejemplo, mediante sistemas de escucha tecnológica. De otra parte, también es defectuosa en tanto exige que el conjunto de operaciones que comprende el tratamiento sean realizadas a lo menos "con ayuda de medios automatizados", quedando así abierta una brecha a través de la cual los titulares de bancos de datos, a fin de eludir la normativa, podrían substraer ciertas etapas "riesgosas" para la dignidad de la persona, del tratamiento automatizado.

Es impropia además desde el punto de vista de los derechos humanos, por cuanto el bien jurídico protegido, como hemos dicho, es la autodeterminación de la persona, su dignidad y la libertad que debe gozar en la toma de decisiones sobre si misma y el objeto regulado son los datos personales cuando son sometidos a tratamiento. Siendo así, y reconociendo que el riesgo de afectación es mayor cuando los datos se incluyen en sistemas automatizados, no es menos cierto que la sola tenencia de datos personales debe tener un marco de regulación que propenda a la protección integral de sus titulares. Así lo reconoció el concepto de la Directiva, que corrige estas deficiencias, ampliando la protección a cualquiera de las etapas del tratamiento, sean éstas efectuadas por medios automatizados o manuales. Incluso de su tenor puede desprenderse que la protección opera incluso si todas las fases del tratamiento se llevan a cabo por medios manuales, y tampoco se discrimina en cuanto a los artilugios técnicos que se empleen en cada una de las etapas que comprende (lógicos o físicos).

c) El Fichero de Datos Personales

Teniendo claros los sujetos del tratamiento de datos, creemos importante analizar el objeto de la normativa de datos personales, esto es el *fichero*, definido desde el campo normativo por el Convenio 108, que entiende por fichero automatizado **"todo conjunto de informaciones que fuere objeto de un tratamiento automatizado"**, concepto un tanto impreciso, ya que confunde el contenido del fichero, esto es, el conjunto de informaciones incorporadas a él, con el fichero en sí.

Sin embargo, la Directiva resulta clarificadora en la definición que incluye en su artículo 2 d), al decir que entiende por "fichero":

> Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido en forma funcional o geográfica.

No cualquier colección de datos es un fichero como podemos apreciar. En efecto, habremos de estar ante un **conjunto estructurado** de datos y para ser tal es necesario que se haya dispuesto su organización, de manera tal que sea susceptible de ser recuperada la información conforme a un criterio preestablecido. En este sentido, cobra importancia la interacción entre los conceptos "dato", "información" y "conocimiento". Un conjunto estructurado de datos es el que proporciona información, a fin de lograr el conocimiento.

La Directiva 95/46/CE se diferenció de la regulación anterior en la materia en cuanto no establece como requisito que se trate de un fichero automatizado, tendencia que tradicionalmente había seguido hasta entonces la legislación. Se reconoce de esta manera que los ficheros manuales también tienen la aptitud para lesionar estos derechos.

En cuanto a los fundamentos de la ampliación de la protección, en la motivación número 27 de la Directiva se señala al respecto que “El alcance de la protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión...”

Además de estructurados, los datos habrán de ser **accesibles con arreglo a criterios determinados**. La definición sigue acogiendo el concepto general de base de datos, en cuanto continente de información estructurada en vistas a su recuperación. Sólo de esta forma es susceptible de proporcionar conocimiento a quien la consulta.

Esta exigencia cobra importancia tratándose de ficheros manuales, ya que la Directiva en la motivación 27 precisa que para que un fichero manual quede comprendido dentro de su ámbito de aplicación, es necesario que se estructure conforme a criterios específicos relativos a la persona, que permitan acceder a los datos personales. De esta manera, los papeles y documentos, por muy relevante que sea la información personal que contengan, si no están estructuradas de esta forma quedan excluidas de la normativa de la Directiva.

En tercer lugar, el fichero **podrá ser centralizado, descentralizado o repartido en forma funcional o geográfica**. A nuestro entender, con este elemento sólo se pretende dar un carácter acabado a la protección, pues permite delimitar responsabilidades respecto del fichero e impedir la transgresión de los principios que inspiran su normativa.

Debe tenerse presente aquí que dentro de este contexto se ubican las bases de datos de perfiles de ADN, pues por medidas de seguridad básicas generalmente estarán divididas en forma funcional entre una base de identidades y otra de perfiles de ADN, o también pueden estar descentralizadas o repartidas geográficamente, lo que no les quita el carácter de ficheros de datos personales automatizados.

d) Sujetos Intervinientes en el Tratamiento de Datos Personales

En el tratamiento de datos personales se encuentran involucrados distintos sujetos, a los cuales tocará una actuación concreta dentro del proceso a que éste da lugar. Estos sujetos son conceptualizados y regulados por la normativa de protección de datos personales, conforme pasamos a analizar:

El primer sujeto del tratamiento de datos, sin lugar a dudas es el **titular de datos** personales o datos de carácter personal. Se trata de la persona física identificada o identificable a quien los datos se refieren y es por tanto el "afectado por el tratamiento de datos". En cuanto a quien puede ser el titular de datos, baste lo ya dicho al momento de analizar el contenido y alcance del concepto de datos de carácter personal. En este punto lo que nos interesa es hacer presente que si bien, el titular no interviene directamente en las operaciones de tratamiento, es un sujeto esencial del mismo, ya que en el ejercicio de sus derechos podrá gatillar que se realicen determinadas operaciones que pueden incluso representar la eliminación definitiva de los datos personales que le conciernen.

Otro sujeto interviniente es el **responsable del tratamiento**, quien conforme al art. 2 letra d) de la Directiva 95/46/CE, es la:

> Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho Nacional o Comunitario.

Conforme a ello podrá ser responsable del tratamiento toda persona natural o jurídica, a diferencia del *interesado* que sólo puede ser una persona física. Podrá el responsable ser un ente público o privado, pues lo relevante en este caso no es el tipo de persona de que se trate, sino que el énfasis esta puesto en las atribuciones que tiene respecto del fichero de datos personales, en tanto que es este el elemento nuclear del concepto. En efecto, el responsable es **quien determina**, solo o conjuntamente con otros, los **fines y medios del tratamiento de**

datos personales. Siendo así, para ser considerado responsable es necesario que se tengan atribuciones soberanas sobre el fichero de que se trate. Claro está que esto es a menos que dichos fines y medios queden fijados por la normativa interna o internacional, caso en el cual los Estados parte podrán fijar los criterios al efecto de determinar la persona del responsable.

De lo anterior queda claro que para la identificación del responsable habrá que estarse al principio de realidad jurídica. Esto significa que independiente de la identificación que se dé al órgano que ejerza estas facultades, para los efectos de la normativa sobre protección de datos estaremos ante el responsable del tratamiento cuando nos encontremos con quien cumpla con las características señaladas por el art. 2° del Convenio 108:

> "Responsable del fichero" significará la persona física o jurídica, autoridad pública, servicio u otro organismo que según la ley fuere competente para decidir sobre que clase de datos de carácter personal deben ser almacenados y que operaciones deberán serles aplicadas.

Respecto de la Directiva 95/46/CE, basta señalar que esta simplemente acoge y desarrolla los criterios que ya establece el Convenio.

En cuanto a los **derechos y obligaciones del responsable del tratamiento**, la legislación comunitaria le reconoce atribuciones soberanas sobre el fichero. Ello implica el derecho a decidir acerca del contenido del mismo y los procedimientos que habrá de aplicarse, pero también la obligación de cumplir y hacer cumplir la normativa y, sobre todo, guardar los principios informadores en resguardo de las garantías personales reconocidas por el ordenamiento jurídico.

Al respecto, deberá tenerse presente ciertos criterios del artículo 16 de la Directiva 95/46/CE, en cuanto establece la **confidencialidad del tratamiento,** que se impone a las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último. Asimismo, como consecuencia de este principio se deriva la limitación referida a que los sujetos que intervienen en el tratamiento sólo podrán tratar datos personales a los que tengan acceso cuando se lo encargue el responsable del tratamiento, salvo imperativos legales.

Finalmente, en el responsable radicará la responsabilidad civil o penal por los daños y perjuicios causados al titular de los datos por el tratamiento que no cumpla tales principios.

De esta manera, y a vía de conclusión, podemos señalar que el responsable de un tratamiento, particularmente si este abarca perfiles de huellas de ADN, tiene entre sus obligaciones:

- Cumplir con el deber de notificación del fichero.
- Recibir y dar cumplimiento a todo tipo de comunicaciones de parte de la Autoridad de Control.
- Dar cumplimiento al principio de información al titular de los datos.
- Procurar que se recabe el consentimiento del afectado al momento de la recogida de datos, en aquellos casos en que éste sea necesario para la legitimación del tratamiento.
- Dar cumplimiento al derecho de acceso, rectificación y cancelación.
- Salvaguardar que el tratamiento se lleve a cabo en forma leal y lícita.
- Prever las medidas de seguridad necesarias para el tratamiento de datos, y
- Guardar el deber de secreto.

También respecto del fichero, la Directiva identifica a otro sujeto: el **encargado del tratamiento**, quien conforme a su art. 2 letra e) es:

> La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

La principal diferencia con el responsable del tratamiento es que el encargado actúa como mandatario del primero y por tanto habrá de ceñirse en su actuación acorde a las finalidades del tratamiento de datos y dentro de las pautas que fije el responsable del tratamiento.

Finalmente, de cara al fichero, cobra importancia la persona del **destinatario**, que de acuerdo al art. 2 letra g) de la Directiva, es:

> La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que

> puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios.

En la comprensión de este concepto, deberemos tener presente cuáles son los sujetos que normalmente solicitan información acerca de los datos personales. Cobrará importancia, en este punto, atender a la importancia que adquieren las Administraciones Públicas como entes que requieren información sobre datos personales para los efectos de realizar sus objetivos.

Además de los anteriores, la Directiva se encarga de definir a los terceros en los siguientes términos:

> f)"tercero": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

Nótese que de acuerdo a esta normativa, un organismo que recibe y gestiona perfiles de ADN, sería destinatario; en cambio, los organismos policiales a los que se comunique la información en el marco de una investigación, no tendrán tal carácter, sino que serán un tercero.

Por la entidad de los tipos de datos de que se trata, esto es, huellas de ADN, entendemos que la Directiva por sí sola resulta demasiado amplia, y pueden presentarse riesgos innecesarios de vulneración de derechos fundamentales.

En este punto nos detendremos en el **estatuto especial del Estado como responsable del tratamiento de datos personales**, pues constituye una base esencial para el trabajo que realizaremos en la tercera parte de esta tesis, cual es definir el conjunto de principios y normas "modelo" que debieran inspirar el diseño e implantación de una base de datos de perfiles de ADN con fines de investigación criminal.

Como bien sostenía FROSINI[21], la Administración en la sociedad post industrial puede ser concebida como un "sistema complejo de información". Dicho de otra forma, la realización de

[21] Vittorio FROSINI, *Informática y Derecho.* Editorial Temis, Bogotá, 1988, págs. 89 y siguientes.

los fines para los cuales se ha establecido el entramado público requiere contar con información acerca no sólo de los administrados, sino también de quienes ejercen los cargos de administración. La detección de necesidades sociales y la definición de políticas públicas tendentes a darles solución, la prestación de servicios públicos y las labores que realiza en pos de la ordenación de los mercados y en fin, el solo hecho de constituirse más que en ejecutor de servicios en supervisor de los mismos, le impone recabar información de los agentes sociales, la que por cierto pasa a engrosar los sistemas de tratamiento de información publificados.

En esta tarea el Estado habrá de tener presente los principios de legalidad de la acción pública y del pleno respeto a las garantías fundamentales de los administrados como condiciones de legitimidad del acopio de datos personales.

> Tradicionalmente se ha entendido el tratamiento administrativo de la información como una actividad material, técnica, soporte o instrumental al procedimiento administrativo; y en consecuencia, sin relevancia jurídica, sino relegada al campo de la ciencia de la Administración. Sin embargo hoy en día se impone un definitivo cambio de perspectiva. El gran volumen de información que trata la Administración tiene una incidencia decisiva en el orden de las garantías de los derechos de los ciudadanos en este sentido, como nueva técnica de control social, amenaza con desequilibrar el delicado entramado de garantías ciudadanas y prerrogativas administrativas que constituyen la base del Derecho Administrativo.[22]

Nuevamente se levanta la sospecha en orden a que la tenencia de información sin límites por parte de la Administración puede llevar a que se vulneren garantías esenciales, en desmedro de la democracia en su conjunto y en sus bases. Esta es la razón por la cual desde los albores de la legislación sobre tratamiento de datos personales se ha puesto especial énfasis en la regulación del Estado como tenedor de datos, y más cuidado aún habremos de tener tratándose de datos que puedan propender a la creación de sistemas cerrados de identificación en base a

[22] Celeste GAY FUENTES, *Intimidad y Tratamiento de Datos en las Administraciones Públicas*. Editorial Complutense, Madrid, 1995, pág. 18.

parámetros biométricos, como el que nos ocupa, aun cuando la finalidad esgrimida es la prevención general o especial de la criminalidad.

Para iniciar nuestro análisis, pensemos en las fuentes a través de las cuales la Administración entra en contacto con datos personales y cuáles son, en términos generales, las funciones del Estado en que se inserta el tratamiento de datos personales, pues ello nos ayudará a construir los principios básicos del tratamiento de datos al interior de los órganos públicos.

En primer lugar existe información "**propia**" de la Administración… decimos *propia* entre comillas porque los datos personales nunca cambian de propiedad, puesto que conforme lo que hemos visto con anterioridad, siempre serán de titularidad de la persona a quienes conciernen. Pero pensemos que el conjunto de datos constituyen "información", en el sentido técnico de las Ciencias de la Información, y esa información es elaborada por el Estado, que en el marco de sus atribuciones realiza **recogidas de datos** desde la ciudadanía y las incorpora a sus sistemas de gestión. Luego, el mismo organismo que recoge estos datos puede realizar estudios y elaborar conclusiones en base a los mismos.

En segundo lugar, una Administración Pública puede entrar en contacto con datos personales a través de información de otros organismos públicos. En este caso, los datos le son **comunicados** por el organismo que los detenta. En esta hipótesis, la información recibida podrá acrecentar sus sistemas de información o simplemente mantenerse segregada. Ello no quita que el organismo público receptor elabore asimismo informes a partir de la información recibida.

En tercer lugar la Administración es **fuente de datos**, es decir, sus registros son consultados por la ciudadanía y la Administración en este caso les comunica datos personales.

Esta relación de la Administración con los datos nos lleva a sostener que el Estado participa en una cadena compleja de tratamiento de datos que reviste especial relevancia desde el punto de vista de la *autodeterminación informativa*, en primer lugar por el alcance geográfico de su actuar

y de otra por su alcance funcional, que alcanza prácticamente a todas las esferas de la vida cotidiana.

Esto sin perjuicio que habremos de reconocer que prácticamente todos los ordenamientos jurídicos consideran la posibilidad que el Estado cuente con registros llamados generales y registros especiales, entendiéndose a los primeros como "Instrumentos de control de los documentos cuando entran, circulan o salen de las oficinas públicas",[23] mientras que los registros especiales serán aquellos que el administrador genera en función de satisfacer necesidades específicas de información, suyas o de la ciudadanía. Ejemplos de registros especiales son el Registro Civil (o registro civil de identificación) y el Registro de la Propiedad Raíz o el Registro de Comercio, todos los cuales en principio buscan dar certeza al ciudadano en el tráfico jurídico. Sin embargo, esta categoría de registros progresivamente va adquiriendo un carácter mixto, lo que resulta especialmente evidente tratándose del Registro Civil, que actualmente es empleado también con fines de investigación criminal para elaborar, por ejemplo, listas de personas relacionadas por razón de parentesco.

Existen también otros registros, originariamente establecidos con finalidades de control asociadas a las necesidades de información, que están supeditados a una determinada norma pública en que se asigna como función al Estado la gestión de un determinado recurso escaso. Es el caso del registro de aguas, del registro del espectro radioeléctrico.

Finalmente hay registros que tienen por objeto controlar a la ciudadanía y los efectos de sus actuaciones de cara a la Administración, si bien en algunos casos pueden ser asequibles a terceros en razón de sus necesidades de información específica. Este es el caso de los registros de reos y rebeldes, también llamados "prontuarios".

Hoy en día la pretensión general de los Estados es aprovechar las bondades de los sistemas de tratamiento automatizado de la información y de los sistemas telemáticos de transmisión de la

[23] José Manuel Castells Arteche, "El derecho al acceso a la documentación de la Administración Pública, en Revista Vasca de Administración Pública, 10, 1984, págs. 135-153

misma y por esta vía generar sistemas integrados de datos, cobrando entonces especial relevancia el análisis de la problemática que nos ocupa.

Si seguimos las opiniones de autores, como por ejemplo SÁNCHEZ BLANCO[24], estos sistemas integrados encontrarían su fundamento en las necesidades de agilizar el procedimiento administrativo y por esta vía contribuir a la concreción de los derechos ciudadanos; sin embargo de nuestra parte sostenemos que cualquier intento de concretar este sistema habrá de realizarse con pleno respeto a las garantías fundamentales y por ende a la *libertad informática*.

e) Condiciones de legitimidad del tratamiento de datos personales.

El legislador comunitario europeo reconoce que todo tratamiento de datos personales debe ser objeto de protección. Es por esto que en términos generales se establecen principios informadores del tratamiento en cada una de sus fases, a fin de garantizar la realización de los mismos. No obstante lo anterior, como ya señalamos, la normativa distingue particularmente los llamados datos sensibles, para efectos de su tratamiento y especial protección.

Esto se ve reflejado en el artículo 6 del Convenio 108, que prohíbe que sean objeto de tratamiento automatizado, salvo que el Derecho interno previere las oportunas garantías. De su parte, la motivación 33 de la Directiva 95/46/CE señala que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo que el interesado consienta expresamente en ello. Más adelante justifica que se hagan tratamiento de datos sensibles, por razones de interés público importante, en sectores tales como la salud pública y la protección social, siempre que se establezcan las

[24] Ángel SÁNCHEZ BLANCO. "Los derechos ciudadanos en la ley de administraciones públicas" en *Revista de Administración Pública* N° 132. Editada por el Centro de Estudios Políticos y Constitucionales, Madrid, 1993, págs. 41 a 97.

garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas (motivación 34 de la Directiva).

Por ende, aun cuando las bases de datos de perfiles de ADN no pertenecen a categorías especialmente protegidas, si lo fueran, podrían ser objeto de tratamiento pues los derechos fundamentales no son absolutos y existe el interés de la sociedad y de las víctimas en la investigación, persecución y castigo de los infractores de la ley penal, con lo que el tratamiento se justificaría en un interés público legítimo, con las correspondientes salvaguardias para los afectados.

- EL CONSENTIMIENTO DEL AFECTADO COMO CONDICIÓN LEGITIMANTE DEL TRATAMIENTO DE DATOS PERSONALES

Como ya hemos explicado, se ha considerado que la protección de datos personas constituye una garantía individual, derivada de la condición de persona humana. En este sentido, sería inalienable e imprescriptible, estando fuera del comercio humano. Pues bien, esto no varía por el hecho que el sujeto renuncie voluntariamente a que ciertos hechos o antecedentes que, en principio, quedan amparados bajo la esfera de la protección de datos personales, salgan de la esfera de protección y, por tanto, sean dados a conocer a terceros. Esta renuncia, que representa el ejercicio de la **autonomía de la voluntad**, es la que se ha concebido como condición legitimante del tratamiento de datos personales que conciernen a un sujeto determinado. De los requisitos y condiciones del ejercicio de este derecho es que trataremos en el presente apartado.

Evidentemente, la regla general es que el consentimiento del interesado legitime el tratamiento de datos, salvo en aquellos casos en que la legislación de los Estados parte lo prohíban en determinados casos.

El consentimiento en general puede conceptualizarse como la manifestación de voluntad hábil para producir derechos y obligaciones. En materia de tratamiento de datos personales, la Directiva 95/46/CE, en su artículo 2, letra h), lo conceptualiza en los siguientes términos:

> Toda manifestación de voluntad libre, específica e informada, mediante el que el interesado consienta el tratamiento de datos personales que le conciernan.

Como podemos apreciar, entiende por consentimiento **toda manifestación de voluntad**. Al respecto cabe preguntarse si podrá ser tácita, presunta o requiere ser expresa. En principio, deberemos sostener que el legislador no distingue, por lo que, conforme a los principios interpretativos, no nos será lícito distinguir. Por tanto, el consentimiento podría otorgarse por cualquiera de las formas admisibles en Derecho, salvo para aquellos casos en que se exija expresamente el consentimiento expreso.

En segundo lugar, habremos de tener presente que no basta con la simple manifestación de voluntad para sostener que existe consentimiento. En efecto, la Directiva califica esta manifestación al decir de debe ser prestada en forma **libre, específica e informada.**

Libre, lo que implica que debe haber sido prestado exento de vicios del consentimiento (error, fuerza o dolo). En segundo lugar y ligado a lo anterior habrá de ser **informado**, lo cual incide en la condición anterior, por cuanto un consentimiento "desinformado" no podrá ser libre por estar afectado por ejemplo por el error. **Específico,** en tanto la manifestación de voluntad debe referirse a un proceso de tratamiento específico, y no podrá ser dado en términos generales "para todo tratamiento de datos sobre mi persona". Esto no obstante el concepto continúe en términos más amplios "Mediante la que el interesado consiente en el tratamiento de datos personales que le conciernen".

En este punto habrá de hacerse mención a la *teoría del control*, patente al analizar la historia del nacimiento del concepto de *privacy* en WARREN y BRANDEIS. En efecto, para estos autores la *privacy* tiene como característica el control del afectado sobre los datos que le conciernen. Asimismo, ello se encuentra patente en la tesis planteada por el Tribunal Constitucional alemán

en cuanto estima indispensable para la autodeterminación el que la persona pueda controlar la información que a ella se refiere. *Ergo*, al exigir el consentimiento del interesado, el legislador comunitario está haciendo suyo este criterio.

En todo caso, tenemos que tener presente que la Directiva exige, como condición del consentimiento, que éste sea prestado en términos inequívocos.

Esto es válido tanto para los datos públicos como para los datos sensibles. En efecto, en términos generales, el artículo 7 a) dispone que "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca" y en términos específicos, tratándose de datos sensibles, conforme al artículo 8 número 2, letra a) de la Directiva, ésta nos dice que no tendrá aplicación la prohibición de tratar datos sensibles en los casos que "a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado".

Siendo así, la diferencia entre una y otra categoría está dada porque tratándose de datos públicos el consentimiento podrá ser tácito (aunque inequívoco), aún cuando estimamos que no basta la mera tolerancia de la tenencia del dato para estimar que hay consentimiento; en cambio, tratándose de datos sensibles, sólo se entenderá que hay consentimiento tácito en aquellos casos que el afectado haya hecho manifiestamente públicos los datos, sin perjuicio de la prerrogativa de los Estados de prohibir que incluso con el consentimiento del afectado sea legítimo el tratamiento.

En todo caso, la Directiva prevé algunos casos en que podrán tratarse estos datos aún **sin el consentimiento del interesado**, que son los que pasamos a analizar en este punto:

En primer lugar, en términos generales y tratándose de todo tipo de tratamiento de datos, la Directiva prevé que estos podrán ser tratados, aún sin el consentimiento del afectado, en las siguientes circunstancias:

> b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado

En este caso, la legitimidad del tratamiento está dada por el **interés del afectado**. Estimamos en todo caso que por razones de buena fe, el contrato del cual se desprenda el tratamiento debe al menos satisfacer las exigencias derivadas del deber de información.

> c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.

En este caso en cambio lo que se viene a satisfacer es el **interés del responsable del tratamiento**. Cuando nos señala que es el cumplimiento de una obligación jurídica, entendemos que se trata de una obligación legalmente contraída y no necesariamente emanada de la ley, sino que perfectamente podrá ser contractual.

> d) es necesario para proteger el interés vital del interesado

Evidentemente, en este caso estamos en presencia de una colisión de derechos, en que debe primar el interés vital del interesado. La problemática estará dada por la calificación de un interés como vital, cuestión que estimamos habrá de ser resuelta caso a caso por los tribunales competentes.

> e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

En este caso, la legitimación viene dada por el bien común, que debe ser perseguido por los órganos públicos. Creemos en todo caso que la calificación del interés público no puede quedar a la calificación de la autoridad administrativa de turno, sino que tratándose de órganos públicos, habrá de buscársela en la ley que defina las competencias del responsable y del

tercero al que se comuniquen los datos. Lo contrario abriría una brecha inconmensurable, a través de la cual podrían producirse atroces violaciones a los derechos que se busca proteger.

> f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

En este caso, la novedad está en la posibilidad de realizar el tratamiento de datos con prescindencia del consentimiento del afectado, ya no sólo para satisfacer un interés legítimo del responsable, sino que también se reconoce esta posibilidad a el o los terceros, a quienes se comunican los datos. En todo caso, esta hipótesis supone la calificación previa en cuanto si no se afecta con ello un derecho o libertad fundamental del afectado. Estimamos que ante la oposición del afectado, serán los tribunales de justicia o los órganos administrativos competentes quienes tendrán la última palabra. Es decir, habrá que resolver caso a caso.

Tratándose de **datos sensibles**, la Directiva es más estricta a la hora de establecer las condiciones en las cuales podrá realizarse el tratamiento sin el consentimiento del afectado y que son las que analizaremos a continuación:

> b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

Siendo así, no es el cumplimiento de cualquier obligación del responsable la que legitima, sino que sólo las emanadas del Derecho Laboral. Además no basta la mera consagración del deber en esta legislación, sino que deben preverse las garantías adecuadas.

> c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

Nuevamente aquí supone una condición especial para legitimar el tratamiento de datos, como es que el interesado esté afectado por alguna condición física o jurídica que le impida prestar su consentimiento. En este sentido, debe tenerse presente que la consideración 31 de las motivaciones de la Directiva señala que debe estimarse lícito el tratamiento de datos personales cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado.

Estamos ante una colisión de derechos fundamentales, en la que se opta por aquel que se estima de una mayor entidad, cual es un interés vital de una persona, indiferentemente de si se trata del titular de los datos o de un tercero. Tal será el caso de la revelación de las relaciones de parentesco entre dos personas, al momento que deciden contraer matrimonio, a fin de impedir una relación incestuosa.

> d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados.

En este caso la legitimante está dada por las necesidades de funcionamiento y comunicación con los asociados o relacionado a las entidades a que se refiere. Más no es cualquier comunicación la que justifica el tratamiento sin consentimiento, sino aquella referida a la finalidad de la organización y siempre que los datos no se comuniquen a terceros.

> e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos, o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Habiéndonos ya referido a la necesidad de que el consentimiento tácito, nos queda señalar que además legitima el tratamiento la necesidad derivada del interés del afectado en materia de ejercicio de sus derechos en juicio.

> 3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

En este caso, son las necesidades derivadas de las políticas sanitarias las que justifican este tratamiento de datos. Se trataría de una calificación especial de los intereses vitales del interesado y de terceros.

> 4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

Aquí nos deja claro la Directiva que no basta la actuación de la autoridad pública, por si y ante si, para considerar legítimo el tratamiento por razones de interés público, sino que habrá ser el legislador o la autoridad de control la que califique estas circunstancias. Creemos que las referencias a la legislación nacional impiden que normas de rango inferior establezcan estas excepciones, salvo que emanen de la autoridad de control. Asimismo, para garantizar los derechos de los titulares, se prevé que las excepciones que se establezcan sean comunicadas a la Comisión.

El problema, en este caso, viene dado por la necesidad de dotar de contenido la expresión "interés público importante", concepto jurídicamente indeterminado, esencialmente mutable, y que en todo caso estará condicionado por la concepción del Estado que impere en un momento y lugar determinado.

Lo anterior se ve morigerado por la exigencia que impone la Directiva en el número 6 de este artículo 8, en el sentido que las excepciones fundadas en este número deberán ser notificadas a la Comisión.

En todo caso resulta clarificador, a los efectos de interpretar la norma, lo señalado en el considerando 34 de las motivaciones de la Directiva, en cuanto dispone que se deberá autorizar el tratamiento de datos sensibles cuando esté justificado por razones de un interés de esta naturaleza, en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas.

> 5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.
>
> Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

En este caso se trata de salvaguardar que este tipo de registros no sea llevado por privados, a fin de resguardar los derechos de los justiciables o ajusticiados y nuevamente se prevé que en los casos que se establezcan excepciones en esta materia habrá que comunicarlo a la Comisión.

No obstante haberse regulado esta materia a propósito de los datos sensibles, estimamos que en este caso la circunstancia que califica al dato es que este se refiera a condenas penales o medidas de seguridad, con independencia de si el dato en si se considera público o sensible. Esto es importante por cuanto las bases de datos de huellas genéticas contendrán usualmente información proveniente de personas sospechosas[25], imputadas o condenadas por delitos, pero

[25] El profesor Carlos María ROMEO CASABONA, en su conferencia sobre "Derechos Fundamentales y Bases de Datos de ADN en poder de la Administración", impartida en el *X Congreso Iberoamericano de Derecho e Informática*

ello no cambia ontológicamente la naturaleza de los datos, sobre todo si consideramos que en estos bancos de datos existirán básicamente secuencias alfanuméricas.

> 7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Como podemos apreciar esta norma es directamente atingente a la materia que abordamos en nuestra tesis. En efecto, siendo los perfiles de ADN métodos de identificación, y no obstante que no es posible calificarlos como "datos sensibles", no basta el silencio legislativo para implementar su tratamiento, sino que es necesario que se regule en cuanto a sus finalidades, funcionalidades y demás condiciones de operación.

Debe tenerse claro que la normativa supranacional constituye un mínimo exigible a los Estados. De esta manera, si los Estados parte deciden establecer un sistema de protección más riguroso que el que ella dispone, podrán hacerlo. Lo que no está permitido es que la normativa interna no garantice a la persona, al menos, que se dará satisfacción a este mínimo.

- SUJECIÓN A LOS PRINCIPIOS INFORMADORES DEL TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES

Este es quizás el aspecto más importante de la evolución doctrinaria y legislativa de la protección de datos, o sea, el establecimiento de una serie de principios con pretensión de universalidad, esto es, válidos para cual país o lugar. Estos principios se deducen fundamentalmente en la Directiva 95/46/CE y, en menor medida, se apoyan en el Convenio 108, teniendo como base que el espíritu del legislador de la *Sociedad de la Información* es la

---

(Santiago de Chile, 6 al 9 de septiembre de 2004), expresaba su preocupación por el uso de este término, que no es propiamente jurídico y que, por lo mismo, tanto gusta a los organismos policiales por sus peligrosas posibilidades de expansión. Compartimos con este académico su preocupación, sobre todo si consideramos que una categoría, cuando no se delimita a nada, es susceptible ampliarse al todo.

promoción de la autorregulación como modelo eficiente para normar las actuaciones de los sujetos en este nuevo estadio social.

De esta manera, y para los efectos de regir el tratamiento de datos personales, se han establecido una serie de principios informadores a los que deberán atender los responsables de ficheros al momento de desempeñar sus labores, pero lo que reviste mayor novedad es el impulso e importancia que se da a los códigos de conducta como principios informadores del tratamiento de datos personales.

Se trata de normas deontológicas, prescritas por la Directiva, para contribuir en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la norma comunitaria.

En este sentido, la Directiva en su art. 27 entrega a los Estados miembros y a la Comisión la función de promocionar la elaboración de estos códigos. A este efecto señala que los Estados establecerán que las asociaciones profesionales y las demás organizaciones representantes de otras categorías de responsables de tratamientos que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar los ya existentes, puedan someterlos a examen de las autoridades nacionales.

Asimismo, la Directiva exige a los Estados que establezcan que la autoridad nacional a que corresponda este examen vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones internas adoptadas en aplicación de la Directiva. Para estos efectos, si lo considera conveniente, dicha autoridad recogerá las observaciones de los interesados o de sus representantes.

Para el caso de códigos comunitarios, así como la modificación o prórroga de alguno existente, se establece que podrán ser sometidos a examen del Grupo de Protección de Datos, quien informará acerca de la conformidad de las propuestas con la legislación nacional adoptada en conformidad con la Directiva.

Sobre esta base, analizaremos a continuación los principios del tratamiento de datos personales:

i. Principios relativos a la Lealtad y Licitud en el Tratamiento de Datos

Con fines de sistematización, diremos que en general el tratamiento de datos personales debe llevarse a cabo dentro de un marco de **lealtad y licitud**. Entendemos que esta manifestación del Legislador comunitario entraña la inserción del tratamiento de datos dentro de los principios generales del Derecho, conforme a los cuales el tratamiento debe ser llevado a efecto de **buena fe**, *con la conciencia de realizar el tratamiento de datos y las operaciones a que da lugar exento de fraude y de todo otro vicio*. No basta con la autorización legal para realizar el tratamiento de datos, sino que además debe realizarse dentro de este marco de buena fe que podríamos llamar "calificada". Es por esto que, a renglón seguido, el legislador comunitario fija ciertas pautas de conducta que dan cuerpo a esta buena fe en el tratamiento de datos. Creemos que las mismas tienen asimismo mucho que ver con lo que se ha dado en llamar el orden público tecnológico.

Siendo así, en primer lugar analizaremos las pautas generales de este marco de lealtad y licitud para luego analizar aquellos principios que estimamos más específicos. Esto porque la lealtad y licitud en el tratamiento de datos subsume tanto aquellas pautas referidas a la calidad y legitimación, así como las referidas a cada una de las fases del proceso de tratamiento de datos personales. Todos ellos son manifestaciones de este marco general de referencia, que informará al tratamiento como supranorma a la que deberá subordinarse toda la legislación de tratamiento de datos personales en cuanto a su interpretación como aplicación.

Así, será leal y lícito el tratamiento de datos que obedezca al principio de **publicidad del tratamiento de datos**, que exige la adopción de las medidas necesarias para garantizar el

conocimiento de la ciudadanía general sobre la existencia de actividades de tratamiento, cuáles son sus finalidades, quiénes actúan como responsables del mismo y todos aquellos otros elementos que permitan su correcta identificación y la vigencia de las garantías establecidas en favor de los interesados.

La publicidad del tratamiento obedece a que siendo el bien jurídico protegido la *autodeterminación informativa*, resulta evidente que para que los sujetos puedan ejercer el respectivo **control** sobre los datos que le conciernen y se establezcan los mecanismos para comprobar que la actividad del responsable del fichero o del encargado del tratamiento de datos personales se lleva a cabo acorde a los principios generales que rigen el tratamiento de datos personales, siendo la primera de estas medidas la de publicidad.

Como manifestaciones de este principio, debemos mencionar el deber de notificación y de registro en una autoridad de control, esto es, en agencias independientes orgánica y funcionalmente, cuyo principal objetivo es velar por el cumplimiento de la normativa de protección de datos personales. La formulación de este principio la encontramos en los albores de la definición de la *privacy*, a través del proyecto BAKER. Sin embargo, debe destacarse que es el proyecto HUCKFIELD (1971), titulado “Control of Personal Information” el que establece claramente entre sus motivaciones la creación de un Tribunal y una inspección de bancos de datos que contengan información de carácter personal, a fin de tomar todo tipo de medidas para prevenir el abuso de las informaciones memorizadas en los bancos de datos, sean éstos manuales o informáticos.

El legislador de la Directiva comprende dos aristas de control, una es la que corresponde a la autoridad pública y la otra está referida al propio interesado, que da lugar al principio de información y a los derechos de acceso, rectificación y cancelación respecto de los propios datos. Analizamos en las líneas siguientes esta segunda faceta.

La **información al interesado** está íntimamente ligado al consentimiento como condición legitimante del tratamiento de datos, puesto que la satisfacción del principio de información

condicionará la formación del consentimiento del interesado ya que, como vimos, para que el consentimiento del interesado sea válido es necesario que se preste libre e informadamente. En este contexto el principio de información exige la puesta en conocimiento del titular de los datos acerca de las circunstancias y antecedentes del tratamiento de los mismos, del para qué se le solicitan los suyos, de su derecho a prestar o no el consentimiento y, en caso de no prestarlo, cuales serán las consecuencias jurídicas de su negativa.

De acuerdo a SÁNCHEZ-CARO y ABELLÁN, apoyándose en el art. 10 de la Directiva, esto implica que es obligatorio "informar a los interesados, sobre el objetivo del tratamiento, sobre la identidad del responsable del mismo y, en su caso, de su representante, y sobre cualquier otro elemento preciso para garantizar un trato leal"[26]. Por ende, este principio implica necesariamente la existencia de los derechos de acceso, rectificación y oposición, esto último con las restricciones señaladas genéricamente al abordar el principio de finalidad.

Otro aspecto de la lealtad y licitud en el tratamiento de datos personales está dado por el **principio de seguridad en el tratamiento de datos personales,** conforme al cual el responsable del tratamiento de datos debe disponer las medidas necesarias para el debido resguardo de datos personales que mantiene y somete a tratamiento.

En esta materia, el artículo 7 del Convenio, dispone que:

> Se adoptarán las medidas de seguridad oportunas para proteger los datos de carácter personal registrados en archivos automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, modificación o difusión no autorizados.

Como podemos apreciar, esta norma hace alusión a la oportunidad y adecuación de las medidas. Estimamos en todo caso que la oportunidad está condicionada por la periodicidad del tratamiento de datos y no sólo por la salida y entrada concreta de un dato al fichero. En efecto,

---

[26] SÁNCHEZ-CARO y ABELLÁN, op.cit., pág. 4, aun cuando estos autores estiman que estas características están integradas al principio de transparencia.

durante toda la época que dure el tratamiento de datos habrán de satisfacerse los estándares de seguridad que garanticen la no destrucción, alteración o fugas indebidas de datos personales del sistema de tratamiento de datos.

Asimismo, habremos de tener presente que la norma incluso hace responsable a los tenedores de datos personales de las pérdidas o daños accidentales que sufran los datos por fallas de seguridad en el sistema de tratamiento de datos. Esta responsabilidad agravada, que estimamos adecuada, dice directa relación con las necesidades de garantizar los derechos del afectado.

De su parte, en la Directiva esta materia es tratada en el artículo 17, que exige a los Estados miembros:

> Que establezcan la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental o contra la alteración, la difusión o el acceso no autorizado, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.
>
> Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

La Directiva acusa el avance tecnológico eclosionado con posterioridad a la firma del Convenio. En efecto, ahora se extiende la responsabilidad por el tratamiento de datos que sean objeto de transmisiones electrónicas. En todo caso, se trata de niveles de seguridad que habrán de actualizarse permanentemente, en atención al avance científico y a la calificación de los datos personales que en definitiva se contengan en un fichero de datos personales. Al efecto, se ha discutido cuál sería el criterio para definir los niveles de seguridad en un fichero de datos personales que contenga datos públicos y sensibles o públicos y “categorías especiales de datos” como podrían ser los datos de identificación única; al respecto se ha llegado a la

conclusión que el nivel de seguridad integral del sistema ha de ser el que corresponda a los datos de mayor entidad registrados en el mismo.

A su turno, en caso de que el tratamiento sea llevado a cabo por un tercero al que el responsable del tratamiento le ha encargado esta tarea, la Directiva exige:

1. Que el responsable, al momento de elegir al encargado, escoja a aquel que reúna las garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

2. Que la realización del tratamiento por encargo esté regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, que se haga constar por escrito o en otra forma equivalente, a efectos probatorios y que disponga en particular:

> - que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;
>
> - que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

Otro aspecto de la lealtad y licitud en el tratamiento de datos está representada por la temporalidad del tratamiento de datos, que la Directiva ha conceptualizado dentro de la "conservación", en el sentido que los datos personales almacenados en un sistema de tratamiento de datos deben permitir la identificación de los interesados:

> Durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.
>
> Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

La clave de bóveda de la licitud y lealtad en el tratamiento de datos personales está condicionado por que se proporcione una **tutela efectiva al interesado**, conforme a lo cual

habrán de disponerse todas las medidas necesarias para que el interesado pueda ejercer sus derechos ya sea directamente ante el responsable del tratamiento, o en caso que éste no satisfaga sus derechos adecuadamente, pueda reclamar ante el organismo de control pertinente acerca de las decisiones del responsable del fichero que puedan afectarle o vulnerar sus derechos, e incluso accionar judicialmente en pos del reestablecimiento de los mismos.

A este respecto la Directiva señala, en su artículo 22, que sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial (SIC) en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

Esta norma resulta evidentemente equívoca, por cuanto no deja claro a qué autoridad judicial se refiere en uno u otro caso. ¿Es que acaso la norma prevé un acceso directo de los afectados a una instancia judicial internacional?. Es una interrogante abierta al debate.

ii.- Principios relativos a la Calidad de los Datos

Muy ligado a los anteriores, se ha estructurado una línea complementaria de principios que se engloban dentro de la conceptualización general “calidad de datos” y que son los que analizamos a continuación:

En primer lugar, esta línea de principios exige que el tratamiento de datos se lleve a efectos conforme al principio de finalidad, de acuerdo al cual los datos personales deben ser:

> recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento

> posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas.[27]

No obstante la formulación concreta de la Directiva, se estima en general que la *finalidad* inspira el tratamiento de datos personales en su conjunto. Así, no sólo habrá de ceñirse a él en la recogida de datos, sino que además en todas las fases del tratamiento de datos, al extremo de condicionar incluso su cancelación en caso que ya no sean necesarios acorde a la finalidad.

En segundo lugar, se dice que sólo serán de calidad los datos que obedezcan a un imperativo de **pertinencia**, reconocida en el Convenio en su art. 5 letra c) y en la Directiva en el art. 6, número 1, letra c). Para que se cumpla este imperativo es necesario que los datos que se sometan a tratamiento sean adecuados y no excesivos en función a la finalidad del tratamiento de datos.

Resulta evidente asimismo la relación de la pertinencia con la temporalidad del tratamiento. En efecto, el artículo 6 letra e) de la Directiva busca sentar como base de la pertinencia la temporalidad del tratamiento de datos personales y en razón de esto dispone que los datos serán conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos, o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período mas largo del mencionado, con fines históricos, estadísticos o científicos.

Como podemos apreciar, este principio afecta asimismo a todas las etapas del tratamiento de datos personales, pues incluso en la fase de creación del fichero exige que junto a la *predeterminación* de las finalidades del tratamiento se defina el tipo de datos personales que serán objeto del mismo. Entonces, ello implica que desde la recogida, sólo se recabarán aquellos datos que sean necesarios para la realización de los fines previamente determinados;

---

[27] Directiva 95/46/CE, art. 6 b)

consecuentemente la cancelación de los datos personales se efectuará por haberse satisfecho a su respecto las finalidades o haber perdido éstas la legitimación necesaria para su mantención.

En el proyecto BAKER ya se reconoce la pertinencia como uno de los principios que inspiran el tratamiento de datos, con la sola diferenciación que en el se habla de "relevancia de los datos" en razón de la finalidad. Creemos que no obstante ser expresiones que difieren, por cuanto pertinencia es menos restringido que relevancia (expresión que supone que sólo será legítimo incorporar el dato en el sistema de tratamiento cuando revista un grado de interés suficiente como para ser considerado "relevante"), la base fundante es la misma, sobre todo si analizamos el texto del proyecto.

> La recogida de datos debe guiarse por el principio según el cual se memorizan sólo los datos relevantes para la finalidad para la cual se ha creado el banco de datos y según la cual los datos sólo son accesibles para estos fines.[28]

Otra cara de la calidad de datos es la de la **exactitud o veracidad** de los datos personales contenidos en un sistema de tratamiento de datos personales, conforme a la cual los datos registrados deben reflejar en todo momento la situación real del titular. De esta manera, infringe el principio todo aquel tratamiento que de cualquier manera pueda inducir a un error de apreciación de la situación personal del interesado. Ello supone que los datos deben ser actualizados cuando sea necesario por haber cambiado la situación del afectado, corregidos cuando sean erróneos o incompletos, bloqueados si han sido puestos en tela de juicio, y cancelados cuando han devenido en falsos.

El Convenio ya reconocía este principio en su artículo 5 letra d), que exige que los datos registrados sean exactos y, si fuere necesario, puestos al día. Esta norma se relaciona asimismo con la de conservación, consagrado en la letra e) de ese mismo artículo, que

[28] Proyecto BAKER sobre *privacy* y ordenadores, pág. 1.

establece que habrá de conservarse los datos en forma que permita la identificación de los interesados durante un plazo que no exceda del necesario para los fines para los que fueron registrados.

De su parte la Directiva consagra el principio en su artículo 6 número 1, letra d), al disponer que los datos deben ser exactos y, cuando sea necesario, actualizados; debiendo tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

En cuanto a los tratamientos sectoriales, debe preverse especiales cuidados en cuanto a la exactitud de los datos contenidos en estos ficheros, atendidas las implicancias que pueden tener en la vida del interesado.

- PRINCIPIOS INFORMADORES DEL TRATAMIENTO DE DATOS APLICABLE AL ESTADO COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

Además de los principios que hemos enunciado, el Estado habrá de ceñirse a los principios generales que rigen la actuación de los órganos públicos en el tratamiento de datos que realice. En algunos casos, los principios informadores del tratamiento de datos se verán modificados o enfatizados cuando el sujeto tenedor de datos sea el Estado. Por esto, en este acápite intentaremos dar noticia de aquellos que nos parecieron más relevantes al objeto de nuestra tesis.

El primer principio que rige la actuación de los órganos públicos es el de **legalidad**. Conforme a ello cada órgano público sólo podrá realizar operaciones de tratamiento de datos dentro del ámbito de su competencia. Esto resulta especialmente simple tratándose de datos públicos, por cuanto siendo tales, basta que la ley que define las competencias del órgano suponga una interacción con la ciudadanía para que se entienda legitimado el tratamiento. La problemática

está dada con las **categorías especiales de datos**, respecto de las cuales estimamos que en primer lugar la asignación de competencia ha de ser ***a través de* ley** y en segundo lugar **específica.**

La problemática viene dada además por la forma como el Estado puede solicitar información al ciudadano. En efecto, según la doctrina, en aquellos casos en que no existe una vinculación jurídica del afectado con el órgano que solicita la información en virtud de su potestad administrativa genérica a la que se sujeta a todos los ciudadanos, estamos ante un caso de limitación al derecho a la autodeterminación y por tanto debe estar prevista en una norma con rango de ley, la que además de imponer la obligación debe prever las consecuencias jurídicas de la negativa a proporcionar la información o la entrega de información errónea o falsa[29]. Tal es el caso, por ejemplo, del deber de someterse a los exámenes de alcoholemia (entrega de información sobre ingesta de alcohol) o la mera información de la identidad de la persona cuando le es requerida en la vía pública por un funcionario facultado al efecto.

Distinto es el caso en que el administrador y administrado actúan en el marco de una relación jurídica ordenada administrativamente. En este caso, se ha dicho que el marco regulador de esta actividad es suficiente para facultar la solicitud de información.

En el caso de captación de información por parte de la administración, o dicho de otra forma, cuando la administración recoge información no desde el afectado sino de terceros o mediante actividades de investigación y policía, como podría ser la recogida de muestras de ADN del lugar del suceso, la doctrina es unánime en que la facultad le debe haber sido conferida por una norma con rango legal.

El segundo principio en juego es el de **proporcionalidad**, conforme al cual se califica el principio de finalidad en el tratamiento de datos personales en el sentido que no basta que los datos sean relevantes para la finalidad que se ha previsto en el tratamiento de datos, sino que

---

[29] Ramón PARADA VÁZQUEZ, *Derecho Administrativo*. Parte General. Editorial Marcial Pons, Madrid, 1993, pág. 397.

además es necesario que se limiten a los estrictamente necesarios para cumplir el cometido funcionario en el cual se inserta el tratamiento. Esto debe entenderse en el marco de las disposiciones de la Directiva, que como vimos legitima a la autoridad a tratar datos personales en casos de que esté inserto en una "misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos". Siendo así, será la competencia general del organismo la que legitime este tratamiento, pero dentro de los parámetros de razonabilidad y proporcionalidad. Esta afirmación es válida para los datos públicos, pues tratándose de las categorías especiales de datos, la misma Directiva va más allá, calificando al interés público como *importante*, lo que deberá establecerse en la ley o ser determinado por la autoridad de control de datos personales. Siendo así, el tratamiento de los datos de perfiles de ADN en general deberán ser autorizados por ley, por tratarse de los datos de identificación señalados en el artículo 8 número 7 de ese mismo cuerpo legal.

En tercer lugar, la administración debe guiar toda su actuación bajo el principio de **transparencia**. En este sentido, y tratándose del tratamiento de datos personales, el administrador debe evitar en lo posible la obtención de datos personales a través de terceros, y en todo caso habrá de informar al afectado lo forma en que se han obtenido datos, los fines que tendrá el tratamiento, y las posibles consecuencias jurídicas a su respecto; cualquier excepción a este respecto debiera estar contemplada en la ley[30]. Por excepción la Directiva, en su artículo 11 número 2, exceptúa a los responsables del tratamiento de informar al afectado:

> Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.

[30] Así por ejemplo lo dispone la Ley Alemana de protección de datos personales de 20 de diciembre de 1990.

Sería el caso de la obtención de muestras de ADN en el marco de una investigación criminal y en el controvertido caso de las facultades de obtención de información respecto de terceros en el marco de una investigación administrativa.

No podemos olvidar que igualmente importante para la actuación del Estado es la satisfacción del principio de eficiencia administrativa, conforme al cual la Administración ha de disponer las medidas para que en colaboración se satisfagan las finalidades públicas con el menor desgaste institucional (financiero, humano, técnico). Como manifestación de este principio destaca en lo que nos interesa el deber de colaboración entre los distintos órganos, que supone de una parte la no interposición en las actividades y competencias de otros órganos y de otra la colaboración activa, por ejemplo, proporcionando la información necesaria para el cumplimiento de sus cometidos. Asimismo, ligado a lo anterior se impone el deber de coordinación de la actividad del Estado, conforme al cual no deben duplicarse esfuerzos. Siendo así, la pretensión del sistema integrado de datos personales vuelve a ser una aspiración legítima por parte del Estado. Sin embargo, creemos que en todo caso para que los datos sensibles y las categorías especiales de datos integren este sistema será necesario contar con autorización expresa en una norma de rango legal, por verse afectadas garantías fundamentales. En todo caso, el deber de cooperación y de colaboración no pueden interpretarse con prescindencia del deber de secreto y sigilo a que están sujetos los funcionarios públicos, conforme al cual deberán guardar secreto respecto de los datos que son objeto de tratamiento por la administración, obligación que en todo caso habrá de ser interpretada en concordancia con los derechos de los titulares de datos, especialmente el derecho de acceso a los datos que le conciernen.

Por supuesto que la legislación podrá disponer por excepción que ciertos datos personales estén cubiertos por el deber de secreto aún respecto de los titulares de datos. Es el caso de los datos recogidos dentro de una finalidad de defensa nacional, seguridad del Estado y seguridad pública, además del que nos ocupa: Art. 13 d) de la Directiva:

> la prevención, la investigación, **la detección y la represión de infracciones penales** o de las infracciones de la deontología en las profesiones reglamentadas.[31]

En todo caso, esta excepción debe entenderse en concordancia con las normas sobre debido proceso legal en general y en particular con el legítimo ejercicio a la defensa en juicio.

[31] Lo destacado es nuestro.