PARTE TERCERA

EL HABEAS DATA EN LAS LEYES DE PROTECCION DE DATOS Y EN LAS TRANSPARENCIA Y ACCESO DE LA INFORMACION PÚBLICA

CAPITULO PRIMERO

I. El HÁBEAS DATA EN ALGUNOS ESTADOS DE AMERICA LATINA

1. ANOTACIONES PRELIMINARES

Hoy por hoy, las normas de desarrollo y reglamentación del Hábeas Data en los Estados de Latinoamérica, previamente a haber sido éste elevado a rango constitucional ha sobrevenido en algunos casos inmerso en las Leyes de protección de los datos o informaciones personales, cuya norma modelo es la regulada por en el derecho continental europeo, especialmente en las leyes teutonas de la década de los setenta, en forma general y las leyes protectoras de los datos de España, en forma particular. En otros eventos, la ley origen para el desarrollo legislativo del Hábeas Data, son las leyes denominadas de "transparencia y acceso a la información pública"; y otras pocas eventualidades, se regula el Hábeas Data separado de las leyes de protección de datos como de las leyes de transparencia y acceso a la información pública.

En el presente ensayo jurídico, abordaremos ejemplos típicos de legislaciones del Hábeas data perteneciente a cada uno de estas subdivisiones de origen que hemos planteado. No sobra advertir que si bien la Constitucionalización del Hábeas Data en Latinoamérica comenzó a finales de la década de los ochenta, en algunos pocos casos (v.gr. Brasil) y principios (v.gr. Colombia, Perú, Argentina y Ecuador) y finales de los noventa (v.gr. Bolivia y Venezuela; así como también principios del dos mil (v.gr. Panamá y Honduras), el desarrollo y reglamentación legal de la institución jurídico constitucional de igual forma se

ha dado en diferentes períodos de tiempo por variopintas razones que van desde las político-jurídicas (razones de seguridad de Estado y de las personas), pasando por la culturales, libertad de expresión, opinión y pensamiento hasta las de índole financiero, económico, comercial o bancario. Esas diferencias temporales en algunos casos han sido cortas desde la constitucionalización hasta la reglamentación de tipo legislativo, entre cinco y seis años (v.gr. caso Argentino); entre seis a diez años (v.gr. El caso de Brasil, Perú, Panamá, Uruguay, México y Honduras); y, de más de diez años (Casos en los cuales se tienen presentados varios proyectos de ley orgánica o estatutaria de Hábeas Data, pero que todavía no acaban de concretarse en leyes de cada Estado, v.gr. El Caso de Colombia, Ecuador, Bolivia, Venezuela; entre otros). Este último grupo de Estados será analizado en el capítulo segundo de esta tercera parte, en el presente capítulo abordaremos ejemplos tipos del primero y segundo grupo.

2. EL HABEAS DATA EN LAS LEYES DE PROTECCION DE DATOS DE LA REPUBLICA ARGENTINA

En la Argentina con una forma de Estado sui géneris: República Federal, existe normatividad general para la "nación", como ordenamiento jurídico para las regiones y ciudad autónoma de Buenos Aires. En tal virtud, veremos a continuación la Ley General de Protección de datos para la República Argentina, y las Leyes especiales de protección de datos para la ciudad autónoma de Buenos Aires y para la Provincia del Neuquem.

2.1. Ley de Protección de datos personales en la República de Argentina

2.1.1. Estructura formal de la Ley

La Ley 25.326 de Octubre 4 de 2000, que regula la protección de los datos personales en Argentina, tiene la siguiente estructura formal:

Capítulo I, relativo a las ***Disposiciones Generales***, compuesto por un objetivo de la ley (artículo 1º); unas definiciones utilizadas en el contexto de la ley y eminentemente técnicas, pero aplicables al derecho informático, tales como: Datos personales, Datos sensibles, Tratamiento de Datos, responsable del archivo, Datos informatizados, Titular de los Datos, Usuario de los Datos, Disociación de los Datos (artículo 2º).

Capítulo II, referente a ***los Principios generales relativos a la protección de datos****,* que son los que guían y orientan todo el proceso informatizado de datos de la persona humana y caracterizan a la ley como una norma especial aplicable a las personas físicas o naturales. Estos principios son: a) Licitud del archivo de datos (artículo 3º); b) Calidad de los datos (artículo 4º); c) Consentimiento (artículo 5º); d) Información (artículo 6º); e) categoría de los datos (artículo 7º); f) Datos relativos a la Salud (artículo 8º); g) Seguridad

de los datos (artículo 9º); h) Deber de confidencialidad (artículo 10º); i) Cesión (artículo 11); j) Transferencia internacional (artículo 12).

Capítulo III, relativa a los ***Derechos de los titulares de datos,*** que no son otros que las facultades inherentes al Hábeas Data que denominamos administrativa y el consecuente Hábeas Data jurisdiccional en el que desemboca. En efecto, se menciona en principio el derecho a la información que tiene toda persona para consultar sus datos (artículo 13); el derecho de acceso de sus propios datos recabados en bancos de datos públicos o privados (artículo 14º); contenido de la información, la cual debe ser clara, accesible, amplia, no vinculante de terceros y podrá suministrarse por escrito, medios electrónicos, de imagen u otro idóneo (artículo 15º); Derecho de rectificación, actualización o supresión de los datos, como derecho trípode y alternativo de toda persona que se hace efectivo frente al incumplimiento de los organismos o responsables de los bancos de datos, a través de la "*acción de protección de datos o de habeas data*" (artículo 16º); excepciones al acceso, rectificación, actualización o supresión de datos, por protección de la defensa nacional, orden y seguridad públicos, o de protección de derechos o intereses de terceros (artículo 17º); Comisiones legislativas de seguridad Interior e Inteligencia del Congreso (artículo 18º); se establece un principio adicional y concreto: el de gratuidad en las gestiones de rectificación, actualización o supresión de datos (artículo 19º); Impugnación de valoraciones personales contenidas en decisiones judiciales o actos administrativos, si revelan un perfil o personalidad del interesado (artículo 20º).

Capítulo IV, sobre los ***Usuarios y responsables de archivos, registros y bancos de datos*****.** Relaciona la inscripción en el Registro de datos, ante el cual debe realizarse por parte de todo responsable de archivos, registros o bancos de datos públicos o privados (artículo 21º); Archivos, registros o bancos de datos públicos (artículo 22º); bancos de datos especiales de particulares con fines administrativos para la seguridad nacional o pública: fuerzas armadas, de seguridad, organismos policiales y de inteligencia (artículo 24º); prestación de servicios informatizados de datos personales por cuenta de terceros (artículo 25º); prestación de servicios de información crediticia (artículo 26º); Archivos, registros o bancos de datos con fines de publicidad (artículo 27º); Archivos, registros o bancos de datos relativos a encuestas. En las encuestas de opinión, mediciones y estadísticas se aplica la Ley 17.622 (artículo 28º);

Capítulo V, sobre el ***Control*** de los datos personales del concernido**.** Contiene normas referentes al órgano de control, sus facultades, deberes y derechos frente a los titulares, usuarios y responsables del procesamiento de datos. Es un órgano con autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. Se designará por cuatro años, por el ejecutivo (artículo 29º); Códigos de conducta para asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada (artículo 30º).

Capítulo VI, relativo a las ***Sanciones***. Las sanciones administrativas son imponibles por el organismo de control, sin perjuicio de las penales o las de responsabilidad por daños y perjuicios derivados de la inobservancia de la ley (artículo 31º); Sanciones penales: se incorpora a la ley dos tipos penales al Código Penal Argentino (artículo 32º).

Capítulo VII, relativo a la ***Acción de protección de datos personales.*** Se relaciona la procedencia de la acción en dos casos: a) Para tomar conocimiento de los datos almacenados en bancos de datos públicos o privados; b) Cuando se presuma falsedad, inexactitud, desactualización, o durante el tratamiento de la información, para exigir la rectificación, supresión, confidencialidad o actualización (artículo 33º); legitimación activa de acción por parte del "afectado", tutores o curadores o sucesores de las personas físicas directamente o por apoderado. La Legitimación de "personas ideales", se hace por representante legal o apoderado. Coadyuva el Ministerio Público (artículo 34º); legitimación por pasiva. La acción se dirige contra los responsables y usuarios de los bancos de datos públicos y privados (artículo 35º); Competencia: Juez del domicilio del actor. La competencia federal, cuando se interponga en contra de archivos de datos públicos de organismos nacionales, o cuando los archivos de datos se encuentren interconectados interjurisdicciones, nacionales o internacionales (artículo 36º); Procedimiento aplicable a la acción de hábeas data, el del procedimiento de amparo común (artículo 37º); Requisitos de la demanda escrita (artículo 38º); Trámite: Admisión de la demanda, requerimiento a demandado, solicitud de informes, sí procede y resolución en 5 días (artículo 39º); Confidencialidad de la información, salvo en fuentes de información periodística y excepciones de ley (artículo 40º); contestación del informe: razones de su aceptación o negativa (artículo 41º); Ampliación de la demanda: 3 días (artículo 42º); Sentencia (artículo 43º); Ámbito de aplicación: De orden público y se aplica a todo el territorio nacional (artículo 44º); El ejecutivo reglamentará la ley (artículo 45º); Disposiciones transitorias (artículo 46º)

2.1.2. Comentarios sucintos a la Ley

2.1.2.1. Aspectos preliminares

Si bien la estructura de la norma especial argentina revela una cohesionada y bien intencionada ley de protección de los datos personales, dirigida a eliminar, restringir o minimizar la alta permeneabilidad que hoy por hoy, tienen los medios TIC y la informática en el pleno de derechos y libertades constitucionales y legales y especialmente del derecho a la intimidad, la imagen, el honor y la buena reputación. No es menos cierto, que dicha estructura normativa como las finalidades, objetivo, principios, mecanismos administrativos y jurisdiccionales para protegerlos, así como las autoridades creadas para tales fines y loables propósitos no pertenecen a la cultura y experiencia jurídica argentina, pues como

duramente lo sostiene *Moeykens*, la ley No. 25.326 de noviembre de 2000, "*no es mas que una triste copia mal efectuada de la vieja LORTAD española*" [1].

En efecto, la Ley de protección de datos argentina o de Hábeas Data para la época en que fue expedida debió el legislador, si esa era su técnica y estilo, apegarse al texto ya no de la LORTAD de 1992 que tantas críticas estructurales y de contenido había recibido en el derecho ibérico y en el comparado [2], sino a la nueva Ley de protección de datos personales de 1999 (L.O.15/99 o LOPDP) que corregía defectos de forma y fondo evidenciados por las varias demandas de constitucionalidad de personas, asociaciones o del propio defensor del pueblo español ante el Tribunal Constitucional; llenaba unos vacíos protuberantes sobre facultades efectivas de los titulares de derechos frente al tratamiento como al almacenamiento de datos, recabados, almacenados o comunicados ("transferidos" o "cedidos") en bancos de datos (sinónimos de bases, archivos, registros o ficheros de datos); reestructuraba las vías previas y procesales del procedimiento originado en la acción de Hábeas Data; así como también reedificaba la aplicabilidad de la normatividad sobre protección de datos tanto los bancos de datos de titularidad pública como de titularidad privada, con las pertinentes excepciones para unos y otros; entre otros aspectos que brevemente analizaremos *ut infra*.

Ante este proceder del legislador argentino, podemos decir, que la Ley de protección de datos argentina (LPDA) de 2000, acusa los mismos defectos y falencias de la LORTAD de 1992, y por supuesto, lo más gravé que desconoció las actualizaciones que la LOPDE de 1999 de España debió transponer como obligación de Estado miembro de la UE y previstas en las Directivas Europeas 95/46/CE y 97/66/CE.

Sin embargo y paradójicamente a nivel latinoamericano se pone a la vanguardia en legislación específica sobre la materia, pues acoge el modelo normativo europeo sobre protección de datos personales, al transliterar la LORTAD de 1992 al derecho argentino. Efectivamente la LORTAD recoge normativamente hablando, los lineamientos, objetivos, principios y normas procedimentales sobre protección de los datos personales contra los abusos del "*poder informático*" previstos en las normas aplicables a la Unión Europea, entre ellos, El Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981 y las recomendaciones de la OCDE de 1980, así como también de las normas alemanas y suizas de la década de los años setenta, sobre protección de datos personales.

---

(1) MOEYKENS, Federico Rafael. ***Derecho a la libertad informática: consecuencias del Habeas Data.*** Revista de Derecho Informático. Alfa-Redi No. 046, Mayo de 2002. Vía Internet.

(2) Vid. RIASCOS GOMEZ, Libardo O. ***El derecho a la Intimidad, la visión ius-informática y los delitos relativos a los datos personales*.** Tesis Doctoral, Universidad de Lleida, Lleida (España), p.30 y ss.

2.1.2.2. En relación al objeto y aplicabilidad de la ley

En relación al objeto de la ley, la LORTAD especificaba en el artículo 1º que ésta tenía por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. Con lo cual, el objeto resulta mucho más amplio que el propuesto por la Ley de protección de datos argentino. Objeto que fue parcialmente mutilado.

El Objeto de la nueva Ley orgánica de protección de datos española (LO.15/99), aclara de una buena vez, lo que en la LORTAD era objeto de interpretación y discusiones doctrinales y jurisprudenciales, vale decir que ésta sólo se dirige a proteger los derechos fundamentales de las personas naturales o físicas [3] *"y especialmente de su honor e intimidad personal y familiar"*, derechos personalísimos que se reputan del ser humano, pero no de las personas jurídicas, morales o "ideales", como se denominan en el derecho argentino.

La LPDA de 2000, estipula en el inciso segundo del artículo 1º, que la ley también será aplicable a las "*personas de existencia ideal*", previendo que también existe una especie de derecho al honor y la intimidad de las personas jurídicas que eventualmente pudieran ser vulnerados por los abusos del "poder informático" o los tratamientos informatizados de los datos de aquellas. Precisamente para evitar esa discusión que se dio en el derecho ibérico y ahora la revive el derecho argentino, la nueva ley española de protección de datos enfatizó en la protección de derechos fundamentales de la persona humana. Quizá la jurisprudencia de la Corte Suprema Argentina, examine a fondo este aspecto y pueda declarar inconstitucional, la extensión de la ley a las personas ideales.

2.1.2.3. En lo referente a las definiciones técnico-jurídicas de la ley

La LORTAD de 1992, tal como lo recoge la LPD argentina en el artículo 2º y lo mantiene la LOPDP de 1999, en el artículo 3º, se suministran unas definiciones técnico-jurídicas aplicables al tratamiento de datos personales y al mejor entendimiento del objeto y fines de la Ley de Protección de Datos. La principal diferencia entre la LPD de Argentina, es que considera dato personal, toda información concerniente a personas físicas e ideales, cuando la LORTAD de 1992 y la LOPDP española de 1999, solo consideran a los efectos de la ley, la información de las personas físicas.

El término "*Archivo, registro, base o banco de datos*", como el conjunto organizado de

---

(3) Ob., ut supra cit.

datos personales que son objeto de tratamiento o procesamiento, electrónico o no, cualquiera fuere la modalidad de su formación, almacenamiento, organización o acceso que relaciona el artículo 2º, inciso 3º de la LPD argentina, resulta más amplio y comprensible que término "*fichero automatizado*" [4] que traía el artículo 3º, literal b, de la LORTAD, pues como observábamos en su momento el tratamiento de datos no sólo puede darse por medios electrónicos, informáticos o telemáticos, sino también por medios mecánicos, escritos o tradicionales. La LOPDP española, en el artículo 3º, literal b, corrigió dicho error y sólo mención al término "fichero" (del francés "fichiers", sinónimo de banco o base de datos).

La LPD argentina en el artículo 2º, inciso 7º, define el término "*titular de los datos*", como toda persona física o persona de existencia ideal…cuyos datos sean objeto del tratamiento previsto en la ley. Esto en concordancia a lo dicho anteriormente que son sujetos destinatarios de la ley, no solo las personas físicas sino también las jurídicas.

La LORTAD de 1992, en su momento ya era criticada porque definía el solo el término "afectado", como a la Persona física titular de los datos que fueran objeto del tratamiento informatizado (electrónico o manual) previsto en dicha ley. Se cuestionaba la acepción negativa utilizado por la LORTAD para identificar al titular de algún derecho y por eso la LOPDP española adicionó a dicho término el calificativo de "*o interesado*", para incluir el lado positivo del concepto de titular de los datos.

La LPD argentina en el artículo 2º, inciso 2º, define una institución jurídica altamente permeable y de difícil concreción en una definición, como son los "datos sensibles". Así lo entendió la LORTAD de 1992 y lo ratificó la LOPDP de 1999, las cuales prefirieron regular la institución sin nominarla expresamente en diferentes normas relativas a los niveles potenciados de protección de ciertos datos especiales y en tal virtud, reglamentar lo relativo a la limitación, restricción o prohibición de aquellos, según la fase del tratamiento informatizado o no de los "*datos especialmente protegidos*" y como consecuencia ineludible de la aplicación del principio rector del tratamiento de datos, cual es el "consentimiento" de titular de los datos ("afectado o interesado", según la LOPD).

La LPD Argentina definió los "datos sensibles", como aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

La Exposición de Motivos de la LORTAD de 1992, sobre el tema propuesto, manifestaba:

---

(4) La LORTAD de 1992, definía así: "*Fichero automatizado: Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*".

Por su parte, el principio de consentimiento, o de autodeterminación, otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita; sus contornos, por otro lado, se refuerzan singularmente en los denominados «datos sensibles», como pueden ser, de una parte, la ideología o creencias religiosas -cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2- y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España.

Los demás términos definidos por el artículo 2º de la LPDA de 2000, son de idéntica transliteración a los relacionados en la LORTAD de 1992.

2.1.2.4. Los principios que orientan el tratamiento de datos

Los principios instituidos en toda ley o norma jurídica obedecen a la utilidad suprema que de estos se hace en el contexto de la norma y las finalidades que prestan para entender, interpretar o aplicar al caso concreto un inciso, artículo, capítulo o título de la ley. Estos principios sirven de guía y orientación al operador jurídico y por ello la denodada construcción del legislador al comienzo de cada norma jurídica.

Los principios o directrices interpretativas o integradoras de la protección de los datos personales en el derecho argentino se plasman en los artículos 3º a 12º de la Ley 25326 de 2000. Estos son: (i) licitud de las bases de datos, (ii) Calidad de los datos, (iii) consentimiento, (iv) Deber de información, (v) Categoría de datos, (vi) Datos relativos a la Salud, (vii) Seguridad de los datos, (viii) Deber de confidencialidad, (ix) Cesión, (x) Transferencia Internacional.

La LPD Argentina en estos temas transcribe en su integridad y extensión lo previsto en los artículos 4 a 11º de La LORTAD de 1992. Sin embargo, existen algunas diferencias, particularmente sobre lo siguiente:

a) La LPD individualiza el principio de la licitud de los “Archivos de datos” que la LORTAD lo incluye en el principio de la calidad de datos. La Ley Argentina, estima que tanto en la formación, como en el tratamiento y las finalidades las bases de datos no deben ser contrarios a la leyes o “*a la moral pública*”.

b) Si bien el principio del consentimiento se establece como regla general en todo procedimiento o tratamiento de datos personales en la LPD Argentina, como en la LORTAD de 1992, en la primera se instituyen unas excepciones numerus clausus, en los que no se requiere dicho consentimiento, al punto que la LORTAD enfatizó en las excepciones relativas a las fuentes accesibles al público, cuando se recolecte información para el ejercicio de las funciones de las “Administraciones Públicas” y las que surgen en las relaciones laborales [5].

Por su parte, la LPD Argentina, manifiesta en el artículo 5º , numeral 2º , que no se requerirá el consentimiento del concernido cuando: (i) los datos se obtengan de fuentes de acceso irrestricto, (ii) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, (iii) Se trate de listados cuyos datos se limitan a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio, (iv) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento, (v) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

El consentimiento en la LORTAD de 1992, según el numeral 3º del artículo 6º, *podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos*. Este derecho de capital importancia para el titular de los datos no fue previsto en la LPD Argentina.

c) El deber de la confidencialidad prevista en el artículo 10º de la LPD Argentina, se diferencia tan solo en el nombre utilizado por el artículo 10º de la LORTAD de 1992, pues en ésta se denomina “Deber de secreto”. En cuanto al contenido son idénticos. Resulta una

---

(5) El artículo 6º, numeral 2º de la LOPDP Española de 1999, amplia el listado en el cual no se requerirá el consentimiento del concernido, (i) cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; (ii) cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; (iii) cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley (Es decir, los datos de la salud para diagnóstico y prevención que afecte la vida del interesado); (iv) o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

adición válida la hecha por la LPD Argentina, cuando estipula en el numeral 2º del artículo mencionado, que "*el obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública*".

d) La LPD Argentina de 2000, instituye como principio importante del tratamiento de datos personales, "*la transferencia internacional*" que por regla general esta prohibida, si los países u organismos internacionales no ofrecen niveles de protección adecuada (y agregamos, y niveles de seguridad tecnológica y jurídica pertinentes). Se exceptúa en los siguientes casos: (i) Colaboración judicial internacional; (ii) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se aplique un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables; (iii) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicables; (iv) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; y, (v) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

La LORTAD de 1992, le dedica a este tema el Título V, relativo al "*Movimiento Internacional de datos*", y en el artículo 32, se establece la regla general de no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas. En cuanto a las excepciones a la regla, son de idéntico tenor a las previstas en el artículo 12º numeral 2º de la LPDA de 2000.

La LOPDP de 1999, acogiendo las críticas hechas a la LORTAD en su momento, reestructuró la norma y en el numeral 2º del artículo 33, agregó sobre el movimiento Internacional de Datos para estar acorde con las Directivas 95/46/CE y 97/66/CE, que el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las

medidas de seguridad en vigor en dichos países. Así mismo, aumento el listado de excepciones al previsto en la LORTAD de 1992 y que *ut infra* precisaremos.

2.1.2.5. Los derechos de los titulares de los datos personales

La doctrina ha clasificado los derechos y deberes [6] de las personas frente a la recolección, el almacenamiento, el tratamiento propiamente dicho y la comunicación ("circulación" o "transferencia") de datos, tal como lo confirma *Tanús*, al recoger un clasificación de Cifuentes de la siguiente manera: (i) Derecho oposición, (ii) derecho de información, (iii) Derecho de acceso, (iv) derecho de rectificación, cancelación o supresión; (v) Derecho de tutela, (vi) Derecho a la impugnación de valoraciones; y, (vii) Derecho de consulta. Y agregamos, el primero el derecho a conocer la información por parte del concernido, y el último en esta clasificación, el derecho a la oposición a la comunicación de los datos sensibles o a aquellos en donde no ha dado su consentimiento, siendo que éste se requiere expresamente.

Sin embargo, a efectos de nuestro ensayo nos referiremos a los derechos que aparecen en la ley. La LPDA, en los artículos 13 a 20, expresa que estos son: (i) Derecho a la Información, (ii) Derecho de acceso, (iii) Derecho de rectificación, actualización o supresión; y (iv) Derecho a la impugnación de valoraciones personales. Estos derechos son de idéntico tenor a los previstos en los artículos 12 a 17 de la LORTAD, con mínimas diferencias.

El Derecho a la información, es aquél que tiene toda persona para solicitar información al organismo de control (autónomo y descentralizado del ámbito del Ministerio de Justicia y Derechos Humanos de la Nación, en el derecho argentino) relativa a la existencia de bancos de datos personales, sus finalidades y la identidad de sus responsabilidades. Igual contenido tiene el artículo 13 de la LORTAD de 1992. La diferencia estriba en que la información se ha de solicitar al *Registro Nacional de Datos Personales* dependiente de la *Agencia de Protección de Datos española* (APDE), que es el organismo de control general de datos en todo el territorio español.

La información que suministre (en forma escrita o por medios electrónicos, teléfono, telemedia o cualquier otro medio idóneo) el organismo competente argentino debe ser clara, exenta de codificaciones y fuera necesario acompañada de una explicación, en

---

(6) Como deberes se establece: (i) Deber de secreto, (ii) Deber de inscripción, (iii) Deber de información, (iv) Deber de seguridad, (v) Deber de velar por la calidad de datos, (vi) Deber de dar acceso a los datos, (vii) Deber de rectificación, cancelación y supresión, (viii) Deber de bloqueo, (ix) Deber de controlar la cesión de datos a terceros, (x) Deber de información al cesionario. Cfr. TANUS, Gustavo D. ***Protección de datos personales: principios, derechos, deberes y obligaciones.*** En: http://www.protecciondedatos.com.ar

lenguaje accesible a todos. Así mismo, la información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aún cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aún cuando se vinculen con el interesado.

El Derecho de acceso de datos, lo tienen: (i) El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes; y (ii) El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Vencido el plazo estipulado en el numeral (ii), sin que se satisfaga solicitud de información, o si se expidiera el informe, éste no es completo, quedará expedita la acción de protección de datos o de Hábeas Data. Esta acción es gratuita y se ejerce a intervalos no inferiores a seis meses (12 meses en la LORTAD), salvo que se acredite un interés legítimo al efecto.

El derecho de rectificación, actualización, supresión ("cancelación" dice la LORTAD y así lo reconoce la doctrina argentina [7]) *y de confidencialidad* son aquellos derechos que tienen todas las personas, cuando sea concernidas con datos o informaciones que se hayan recabado, almacenados o administrados en bancos de datos de carácter público como de carácter privado. En tal virtud, el responsable o usuario del banco de datos, procederá a rectificar, actualizar, suprimir o conservar la confidencialidad de los datos personales del concernido, realizando las operaciones necesarias para conseguir dichos fines, dentro del plazo de cinco días hábiles a la recepción del reclamo o de detectado el error o la falsedad en los datos. Si se incumple éste término, habilita al titular de los datos para que ejerza la acción de protección de los datos o Hábeas Data.

En el evento de cesión o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

La supresión de datos no procede cuando pudiera causar perjuicios a terceros, o cuando

_____

(7) El derecho de cancelación permite eliminar del archivo o base de datos a aquellos datos personales que, por diversas circunstancias, no deben figurar en el mismo. Es importante poner de manifiesto que el término "cancelación" debe ser entendido en forma amplia como la acción tendiente a hacer irreconocibles los datos archivados, ya sea anulando, destruyendo, borrando, tornando ilegibles o declarando su nulidad. La metodología empleada diferirá de acuerdo a las circunstancias. Demás está decir que existen casos en los que, por cuestiones de interés público, será imposible eliminar completamente una información. Prueba de ello es la excepción a la destrucción física de los datos que la ley contempla en artículos al referirse al mecanismo de bloqueo de datos. Cfr. TANUS, Gustavo D. ***Protección de datos personales…*** Ob., ut supra cit.

existiera una obligación legal de conservar los datos.

Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que encuentra sometida a revisión.

Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

La LPDA de 2000, establece unas excepciones al derecho de acceso y de rectificación, actualización y supresión, por parte de los responsables o usuarios de los datos personas, mediante “decisión fundada” (o mejor, motivada y notificada) en los siguientes casos: (i) Cuando se trate de la función de protección de la defensa de la Nación, del orden y la seguridad públicas, o de la protección de los derechos o intereses de terceros; (ii) Cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. El derecho de acceso se permitirá en el evento que el titular del dato lo requiera para su defensa.

El derecho a la impugnación de valoraciones personales consiste en la facultad que tiene toda persona para impugnar una decisión judicial o un acto administrativo, cuando estas impliquen apreciación o valoración de la conducta humana y a la cual sólo se llegue como y único fundamento sea el resultado de un tratamiento informatizado de datos personales y configure un banco de datos público o privado. Será nulas las decisiones o actos que contravengan este derecho.

Sobre el tema en particular, el artículo 12 de la LORTAD, fue transvasado por la LPDA de 2000, hasta el punto que sólo se hace referencia a los actos administrativos o “decisiones privadas”, las que pueden impetrarse por el titular de los datos mediante los recursos administrativos o particulares pertinentes, pero no de las “decisiones judiciales”, pues éstas tienen otro tratamiento e impugnación jurídicos dentro de cada proceso jurisdiccional y que por su puesto no será pertinente o idóneo el recurso administrativo o particular. Igualmente se transvasa la LORTAD, cuando determina que los actos que contravengan las disposiciones de la LPDA, artículo 20, serán “*insanablemente nulos*”, pues esto no esta previsto en la LORTAD y jurídicamente resultaría improcedente el declaratoria de nulidad de una decisión judicial en la que se haga una valoración del comportamiento de una persona (que no “conducta humana”, como dice el artículo 20) que suministre un “perfil o personalidad del interesado”.

En efecto, el artículo 12 de la LORTAD, sostiene: "*El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad"*. La LOPDP española de 1999, amplia los supuestos en los que pudiera valorarse el comportamiento de una persona y el efecto jurídico que podría dársele a éstas en el artículo 13, pero en ningún caso la declaratoria de nulidad por una autoridad que no sería la competente para hacerlo. El numeral 4º del artículo 13 sostiene: *la valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.*

Bien sea por vía reglamentaria de la LPDA de 2000, o por vía de aplicación supletoria de la Ley de procedimiento Administrativa Argentina, el ejecutivo debería prever el procedimiento administrativo que se desata para ejercer los derechos de información, acceso y oposición, así como de rectificación, actualización y cancelación de los datos y igual forma del derecho a impugnación de la valoración del comportamiento humano mediante un tratamiento de datos, pues hasta que esto no se clarifique el titular de estos derechos y la autoridad competente que debe conferir y decidir, si fuere presentado un derecho de petición en concreto, pueden proceder conforme a derecho.

El ejercicio de estos derechos ante el organismo de control de la protección de datos, bien podría instituir lo que llamamos el Hábeas Data administrativo, pues una vez agotado los trámites, procedimientos o términos procesales, podrá acudirse al Hábeas Data jurisdiccional, que en la LPD Argentina de 2000, se posibilita no por agotamiento previo de esas vías administrativas, sino por incumplimiento de las autoridades competentes del control a resolver en el término prefijado por la LPDA, o por el simple transcurso del tiempo, sin resolución alguna, es decir, por la configuración de una especie de silencio administrativo negativo de plazo brevísimo: (i) Diez (10) días para ejercer la acción de Hábeas Data, cuando no se hace efectivo el derecho de acceso a la información del titular de los datos; (ii) Cinco (5) días para ejercer el Hábeas Data, cuando no se hace efectivo el derecho de rectificación, actualización o cancelación de los datos.

2.1.2.6. Sobre la prestación de servicios de solvencia patrimonial o crediticia

La LPDA de 2000, regula el tema de la "*prestación de servicios de información crediticia*" en el artículo 26 de parecida redacción al artículo 28 de la LORTAD y artículo 29 de la LOPDE de 1999, sobre *la prestación de servicios de solvencia patrimonial o crediticia.*

El dato financiero, como hemos tenido oportunidad de decirlo en otro de nuestros

trabajos[8], se entiende aquella información concerniente a una persona determinada o determinable tiene características económicas, comerciales, tributarias, o en general de índole financiera, bien sea en el ámbito privado o en el público, se puede decir genéricamente que el dato es financiero, pues según el diccionario el término financiero puede definirse como lo "*perteneciente o relativo a la Hacienda pública, a las cuestiones bancarias y bursátiles o a los grandes negocios mercantiles*" [9], con lo cual se entiende que los datos financieros engloban terminológicamente a los efectos de este ensayo, lo que entendemos por dato económico, comercial, bancario, bursátil y tributario público y privado.

Las Leyes de protección de datos española de 1992 y 1999, regulan esta clase especial de datos de la persona humana tan solo desde el ámbito privado, tal como lo confirma la ubicación de los artículos 28 y 29, respectivamente. En efecto, las normas hacen parte integrante del Título IV, relativo a la "Disposiciones Sectoriales", Capítulo II, "*Ficheros de titularidad privada*". En cambio, la LPDA al no ubicar formalmente bajo un título o capítulo de la ley que determine que clase de información financiera regula, deberá entenderse que lo hace en el ámbito privado y público, indistintamente, aunque los contenidos sigan siendo de la información financiera de carácter privado de la norma origen: la LORTAD.

La LPDA de 2000, expone en el artículo 26, que en la prestación de servicios de información crediticia sólo pueden tratarse los siguientes datos personales: (i) Los de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público (vale decir, los de dominio público, sin restricción o limitación alguna que no sea un pago por la contraprestación [10]) o procedentes de informaciones facilitadas por el interesado o con su consentimiento; y, (ii) Los relativos al cumplimiento o incumplimiento de las obligaciones de carácter patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

El tratamiento o procesamiento de estos datos financieros, en el derecho argentino deberán observar las siguientes reglas: (i) A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión; (ii) Sólo se podrán archivar, registrar o ceder los datos personales que sean signi-

---

(8) RIASCOS GOMEZ, Libardo O. ***Los datos personales de carácter financiero en los proyectos de ley estatutaria de Hábeas Data de origen parlamentario y gubernamental en Colombia.*** Ensayo jurídico para la Revista Electrónica Española de Derecom, Universidad de Valladolid (España). Vía Internet En: www.derecom.com.es

(9) Ob., ut supra cit.

(10) AA.VV. ***Microsoft® Encarta® 2007***. © 1993-2006 Microsoft Corporation. Reservados todos los derechos.

ficativos para evaluar la solvencia económica financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación debiéndose hacer constar dicho hecho; y (iii) La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Los datos personales de carácter privados recabados en los correspondientes bancos de datos, tanto en la legislación española de 1992 como en la legislación argentina de 2000, hacen énfasis en los realizados con fines de publicidad, los relativos a encuestas o investigaciones y los destinados a la prestación de servicios de información de solvencia patrimonial y crediticia. La LORTAD de 1992, incluía también los relativos a los abonados a los servicios de las telecomunicaciones y otros servicios prestados a la comunidad. Por su parte, la LOPD española de 1999, se ratifica los anteriores, reestructura los bancos de datos en los que se incluye información de acceso al público e incluye entre ellos, a los que figuren en el censo promocional, las listas de personas o grupos profesionales, los colegios profesionales, entre otros. Así como también los tratamientos con fines de publicidad y prospección comercial y censo promocional.

Sin embargo, es innegable que los asuntos que más nutren la jurisprudencia de la Corte Suprema de Justicia de la República argentina son los de índole financiero, especialmente en la labor crediticia de las entidades o instituciones bancarias privadas más que públicas, como tuvimos oportunidad de ponerlo en evidencia en el trabajo ut supra citado [11]. Todo por cuanto desde el nacimiento mismo de los proyectos de ley que trataban de regular el Hábeas Data como derecho y garantía constitucional previsto en las respectivas constituciones, el énfasis que se marcaba por la alta sensibilidad de los destinatarios de la información (usuarios, responsables de los bancos de datos y con mayor razón el titular de los datos personales), consistía en la información financiera [12]. Aunque también hay que reconocer que en unos Estados Latinoamérica, más que en otros, se ha convertido en un

---

(11) Según el artículo 3º de la LOPD de España de 1999, para evitar confusiones terminológicas definió a las fuentes accesibles al público en el literal j), así: "*Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación*".

(12) RIASCOS GOMEZ, Libardo O. ***Los datos personales de carácter financiero…*** Ob., ut supra cit.

obstáculo real a la hora de desarrollar y reglamentar legislativamente el Hábeas Data [13].

En Colombia por ejemplo, quizá el dato financiero haya sido la mayor piedra en el zapato, a la hora de expedir una Ley relativa a la reglamentación integral del Hábeas Data, aunque los diversos proyectos de ley de diferentes orígenes (parlamentario, gubernamental, defensoría del pueblo, entre otros), algunos no logren hacer el tránsito legislativo inicial, otros se queden en la etapa de control constitucional previo, por vicios de forma (por ser proyectos de ley estatutaria que tienen un procedimiento legislativo especial) y los últimos no logren el puntillazo legislativo final por errores o vicios de trámite legislativo, pero ninguno de ellos por estudio del contenido total o parcial. Esta labor la ha hecho la doctrina al develar los contenidos con muchas falencias, parcializados, descontextuados, con transliteraciones y mutilaciones de leyes extranjeras, o con exagerados énfasis de un solo tipo de dato personal: el financiero.

2.2. Ley de protección de datos personales de la Ciudad Autónoma de Buenos Aires

Mediante la Ley No. 1845, se reglamenta la protección de datos personales de la ciudad autónoma de Buenos Aires, la cual ha sido "vetada parcialmente" por el Decreto 1914 de 2006, de 29 de Diciembre.

2.2.1. Estructura formal de la Ley

La estructura formal de la ley es la siguiente:

Título I, relativo a las "***Disposiciones Generales***": El Objeto de la ley: la regulación del tratamiento informatizado de los datos de las personas físicas e "ideales" dentro de la ciudad de Buenos Aires (artículo 1º); Ámbito de aplicación: Se extiende a los bancos de datos públicos de entidades y organismos nacionales y descentralizados presentes en la ciudad de Buenos Aires, bien pertenezcan al poder ejecutivo, legislativo y judicial (artículo 2º); Definiciones de términos técnico jurídicos de: Datos personales, Datos sensibles, Archivos, Registros, Bases o Bancos de Datos, Tratamiento de datos, Titular de los datos,

---

(13) La historia legislativa sur y centro americana cuando de la reglamentación del derecho y garantía constitucional del Hábeas Data se trata, ha mostrado la propensión a reglamentarlo haciendo énfasis en el dato financiero, fiscal, tributario, tarifario o de servicios públicos más que en cualquier otra arista del dato personal. Así se demuestra en los variopintos proyectos de ley orgánica o especial que en su momento los Estados de Argentina, Perú, Chile, Uruguay, Paraguay, excepto el Brasil cuya motivación e inspiración constitucional del Hábeas Data hunde sus raíces en el Constitucionalismo Portugués y en el ámbito de la seguridad e información ciudadana, los secretos de Estado y las actividades desbordantes, por decirlo menos, de la policía política, a juicio de DE ABREU DALLARI, Dalmo. En: RIASCOS GOMEZ, Libardo O. ***Los datos personales de carácter financiero…*** Ob., ut supra cit.

Responsable del Archivo, Registro, Base o Banco de Datos, Encargado del Tratamiento, Usuario de Datos, Fuentes de Acceso Público Irrestricto (artículo 3º)

Título II, referente al ***"Régimen de los Archivos, registros o bases o bancos de datos"*** Creación de archivos, registros, bases o bancos de datos, con fines y propósitos lícitos y socialmente aceptados (artículo 4º); Tratamiento de datos personales efectuados por terceros. Vetados incisos 1º y 2º por del Decreto1914/05. El inciso 3º hace referencia a los contratos de prestación de servicios de tratamiento de datos personales deben contener niveles de seguridad exigidos por la ley (artículo 5º).

Titulo III, sobre los ***"Principios Generales de la protección de los datos personales"*:** (i) Calidad de los datos; (ii) consentimiento; (iii) Datos sensibles; (iv) Datos relativos a la salud; (v) Cesión de Datos; (vi) Transferencia interprovincial; (vii) Transferencia Internacional, artículos 6º a 12º.

Titulo IV, relativo a ***"Los derechos de los titulares de los datos personales"*,** estos son: (i) Derecho de información; (ii) Derecho de acceso; (iii) Derecho de rectificación, actualización y supresión; (iv) Excepciones: Orden o Seguridad pública, derechos o intereses de terceros. Artículos 13º a 15º.

Titulo V, referente a ***"Las obligaciones relacionadas con los datos personales asentados en archivos, registros o bancos de datos"*** Son: (i) confidencialidad; (ii) Seguridad; (iii) Obligaciones del responsable del banco de datos; (iv) obligaciones del encargado del tratamiento de datos; (v) Obligaciones del usuario de datos; (vi) valoraciones. Artículos 16º a 21º.

Titulo VI, concerniente al ***"Control":*** El defensor del Pueblo (artículo 22) Funciones de registro de la Defensoría: (i) Incisos 1º, 2º y 13º vetados por el decreto mentado; (ii) La demás vigentes (artículo 23). Conocimiento de los bancos de datos por toda persona (artículo 24º).

Titulo VII, concerniente a las ***"Infracciones"*:** infracciones administrativas que desconozcan los principios, obligaciones y derechos del tratamiento de datos personales por usuarios y responsables de los datos (artículo 25º).

Titulo VIII, relativa a las ***"Sanciones"***: (i) Responsabilidad de los responsables, usuarios o cesionarios de los bancos de datos del sector público de la ciudad de buenos Aires. (ii) Inmovilización de archivos, registros o bancos de datos. Artículos 26º y 27º

Titulo IX, sobre la ***"Acción de Protección de Datos"***: procede: (i) conocer los datos almacenados en bancos de datos del sector público en la ciudad de Buenos Aires; y (ii) En caso de infracción de la ley y la ley 25236, solicitar la rectificación, actualización, confidencialidad y supresión de datos. Exceptúan las fuentes periodísticas (Artículo 28º); Legitimación por activa: todo "afectado", curador, tutor y sucesores de las personas físicas; las personas "ideales", por representación legal o apoderado (artículo 29º); La legitimación por pasiva. Vetada por el decreto citado (artículo 30º); Jurisdicción y procedimiento aplicado (artículo 31º); Requisitos de la demanda (artículo 32º); Trámite (artículo 33º); confidencialidad de la información (artículo 34º); contestación del informe (artículo 35º); ampliación de la demanda (artículo 36º); Sentencia (artículo 37º).

Titulo X, concerniente a "***Las disposiciones particulares"*:** (i) Prestación de servicios sobre solvencia patrimonial y crediticia; (ii) Privacidad laboral en el ámbito del sector público de la ciudad de Buenos Aires; (iii) Disposiciones transitorias.

2.2.2. Comentarios sucintos a la ley

La Ciudad Autónoma de Buenos aires, reguló la protección de los datos en la Ley No. 1.845 de 2005 o LPD de CABA, siguiendo los parámetros y estructura de la Ley de protección de los datos de Argentina: Ley No. 25.326 de Octubre 4 de 2000. En tal virtud, los comentarios realizados a ésta ley son válidos para la presente. Sin embargo, se debe aclarar que la LPD de CABA, se expidió con el propósito claro de reglamentar el Hábeas Data solo en el sector público, tal como quedó plasmado en el objetivo y campo de aplicación de la ley (artículos 1º y 2º).

En efecto, la LPD de CABA, tiene por objeto y dentro del ámbito de la Ciudad de Buenos Aires, el tratamiento de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a ser asentados en archivos, registros, bases o bancos de datos del Sector Público de la Ciudad de Buenos Aires, a los fines de garantizar el derecho al honor, a la intimidad y a la autodeterminación informativa, de conformidad a lo establecido por el artículo 16 de la Constitución de la Ciudad Buenos Aires.

Cuando los datos se refieran a información pública y no a datos personales será de aplicación la ley 104 de la Ciudad de Buenos Aires, es decir, Ley No. 104 de 1998, relativa al acceso a la información pública, pues toda persona tiene derecho, de conformidad con el principio de publicidad de los actos de gobierno, a solicitar y a recibir información completa, veraz, adecuada y oportuna, de cualquier órgano del estado presente en la ciudad de Buenos Aires.

A efectos de los comentarios de la presente ley nos referiremos a dos temas no tratados en la LPDA de 2000. Estos son: (i) El organismo de control previsto en la ley para la

protección y garantía del Hábeas Data y los derechos fundamentales vinculados con éste; y (ii) Sanciones e Infracciones con motivo del tratamiento de datos.

2.2.2.1. La Defensoría del Pueblo como organismo de control de la protección de datos

La Ley de Protección de datos personales de la ciudad Autónoma de Buenos Aires (LPD de CABA, designa como organismo de control de los datos personales a la Defensoría del Pueblo.

Según el artículo 137 de la Constitución de la Ciudad Autónoma de Buenos Aires, de 1º de Octubre de 1996, la Defensoría del Pueblo es uno de los organismos de Control de la ciudad autónoma de carácter unipersonal e independiente con autonomía funcional y autarquía financiera, que no recibe instrucciones de ninguna autoridad.

Es su misión la defensa, protección y promoción de los derechos humanos y demás derechos e intereses individuales, colectivos y difusos tutelados en la Constitución Nacional, las leyes y esta Constitución, frente a los actos, hechos u omisiones de la administración o de prestadores de servicios públicos.

Por su parte, el artículo 22 de la LPD de CABA, al designar como organismo de control a la Defensoría del Pueblo le confiere unas atribuciones específicas sobre la protección de los datos personales, aparte de las funciones constitucionales previstas en el transcrito artículo.

Estas funciones son: (i) Llevar un Registro de los archivos, registros, bases o bancos datos creados por el Sector Público de la Ciudad de Buenos Aires. A tal fin, establecerá el procedimiento de inscripción, su contenido, modificación, cancelación, y la forma en que los ciudadanos podrán presentar sus reclamos, de conformidad con lo establecido en el art.4 inc.3 de la presente Ley; (ii) Garantizar el acceso gratuito al público de toda la información contenida en su Registro; (iii) Velar por el cumplimiento de las disposiciones de la presente ley y por el respeto de los derechos al honor, la autodeterminación informativa y la intimidad de las personas; (iv) Formular advertencias, recomendaciones, recordatorios y propuestas a los responsables, usuarios y encargados de archivos, registros, bases o bancos de datos del Sector Público de la Ciudad de Buenos Aires, a los efectos de lograr una completa adecuación y cumplimiento a los principios contenidos en la presente Ley; (v) Proponer la iniciación de procedimientos disciplinarios contra quien estime responsable de la comisión de infracciones al régimen establecido por la presente Ley; (vi) Recibir denuncias; (vii) Formular denuncias y reclamos judiciales por sí, cuando tuviere conocimiento de manifiestos incumplimientos de lo estipulado en la presente ley por parte de los responsables, usuarios y/o encargados de los archivos, registros, bases o bancos de

datos del Sector Público de la Ciudad de Buenos Aires; (viii) Representar a las personas titulares de los datos, cuando éstos se lo requiriesen, a fin de hacer efectivo el derecho de acceso, rectificación, supresión y actualización, cuando correspondiere, por ante el archivo, registro, base o banco de datos; (ix) Asistir al titular de los datos, cuando éste se lo requiera, en los juicios que, en virtud de lo establecido en la presente ley, entable por ante los tribunales de la Ciudad de Buenos Aires; (x) Elaborar informes sobre los proyectos de Ley de la Ciudad de Buenos Aires que de alguna forma tengan impacto en el derecho a la privacidad y protección de los datos personales; (xi) Elevar un informe anual a la Legislatura sobre el desarrollo de la protección de los datos personales en la Ciudad de Buenos Aires; (xii) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Por su parte, el Decreto 1914 de 29 de diciembre de 2006, vetó las siguientes funciones: (i) *Autorizar y habilitar la creación, uso y funcionamiento de los archivos, registros, bases y bancos de datos personales del Sector Público de la Ciudad de Buenos Aires de conformidad con lo preceptuado en la presente ley; (ii) Establecer los requisitos y procedimientos que deberán cumplimentar los archivos, registros, bases o bancos de datos del Sector Público de la Ciudad de Buenos Aires relativos al proceso de recolección de datos, diseño general del sistema, incluyendo los mecanismos de seguridad y control necesarios, equipamiento técnico, mecanismos adoptados para garantizar los derechos de acceso, supresión, rectificación y actualización así como demás extremos pertinentes; (iii) Colaborar con la Dirección Nacional de Protección de Datos Personales y con los correspondientes organismos de control provinciales en cuantas acciones y actividades sean necesarias para aumentar el nivel de protección de los datos personales en el Sector Público de la Ciudad de Buenos Aires.*

Estas funciones vetadas a la Defensoría del pueblo corresponden a los incisos 2º, 3º y penúltimo del artículo 22 de la LPD de CABA. Las razones jurídico constitucionales que suministra el Decreto 1914 para el veto, estriban en explicar que la Defensoría del Pueblo si bien es un organismo de control (no ejecutivo ni reglamentario) que no pertenece a las tres ramas del poder público, tiene su autonomía funcional y autarquía financiera y no recibe de instrucciones de ninguna autoridad. Además, se considera:

a) Que la gestión de gobierno en general hace indispensable la utilización de herramientas registrales o de bases de datos conforme lo permite el desarrollo tecnológico alcanzado, por lo que buena parte del instrumental que utilizan los tres poderes de Gobierno se nutre de la generación de bases de datos que, compartiendo con el espíritu de la ley, necesariamente deben ser controladas para evitar un avance estatal sobre la privacidad y derechos que la Constitución de la Ciudad garantiza a las personas que habitan en nuestro territorio, independientemente de la protección que otorga la Constitución y Ley Nacional;

b) Que no obstante lo expuesto, del análisis de los párrafos 2°, 3° y penúltimo del referido artículo se advierte que la norma ha conferido a la Defensoría del Pueblo de la Ciudad de Buenos Aires facultades propias del Poder Ejecutivo que exceden la natural esfera de control que debe ejercer el citado organismo, para incursionar en las correspondientes a la administración activa, relacionadas con la implementación y ejecución de las políticas gubernamentales;

c) Que las estipulaciones del mismo, al otorgar facultades ejecutivas al órgano de control -la Defensoría del Pueblo de la Ciudad de Buenos Aires-, a través de la creación del Registro de Datos Personales que funcionaría en su órbita, devienen exorbitantes, toda vez que el referido registro concentra la capacidad de autorizar y habilitar la creación, uso y funcionamiento de los archivos, registros, bases y bancos de datos personales del sector público de la Ciudad; estableciendo los requisitos y procedimientos que deberán cumplimentar dichos archivos, registros, bases y bancos de datos personales, relativos al proceso de recolección de datos, diseño general del sistema, mecanismos de seguridad y control, etc.;

d) Que en este aspecto, la ley que se analiza avanza sobre la competencia natural del órgano ejecutivo, al atribuir a la Defensoría del Pueblo de la Ciudad de Buenos Aires la capacidad de dictar la normativa reglamentaria, vulnerando de esta manera flagrantemente lo normado por el art. 102 de la Constitución de la Ciudad de Buenos Aires, que ha otorgado en forma expresa dicha atribución al Poder Ejecutivo;

e) Que según surge del artículo referido el registro que se crea, no sólo determinaría eventualmente qué conformación técnica deberían tener los registros o bases de datos del sector público de la Ciudad, sino que además debería habilitar su funcionamiento;

f) Que de no observarse el artículo 23 en los párrafos señalados, la Defensoría del Pueblo debería autorizar, sólo a modo de ejemplo el funcionamiento de las constancias de datos del Padrón de Contribuyentes y el Registro de Contribuyentes de la Dirección General de Rentas, las bases de prestatarios de servicios de taxis y remises; el Sistema de Seguimiento de Juicios de la Procuración General (SISEJ); las bases de permisionarios en cementerios; el Registro Único de Proveedores (RUP), todas las bases de datos del Registro Civil, el sistema único de mesa de entradas (SUME), etc.;

g) Que ello implicaría supeditar todo el funcionamiento de la administración a la autorización de un órgano de control independiente, la Defensoría del Pueblo;

h) Que si bien se comparte el espíritu de la ley sancionada, en cuanto al necesario control que debe instrumentarse en esta materia sobre la actividad administrativa del subsector estatal, e independientemente del poder de gobierno que esté a cargo de su

implementación, corresponde señalar que tanto la actividad de reglamentación del sistema, como la de habilitación de los registros o bases, atribuida a un "Registro" creado en la órbita de la Defensoría del Pueblo, podría subvertir el orden constitucional.

Sin embargo, la Defensoría del Pueblo, a tenor del artículo 24 de la LPD de CABA, está habilitada, ante el pedido de un interesado o de oficio ante la sospecha de una ilegalidad, a verificar el cumplimiento de las disposiciones legales y reglamentarias en orden a cada una de las siguientes etapas del uso y aprovechamiento de datos personales: (i) legalidad de la recolección o toma de información personal; (ii) legalidad en el intercambio de datos y en la transmisión a terceros o en la interrelación entre ellos; (iii) legalidad en la cesión propiamente dicha; y, (iv) legalidad de los mecanismos de control interno y externo del archivo, registro, base o banco de datos.

Todo lo anterior, por cuanto toda persona podrá conocer la existencia de archivos, registros, bases o bancos de datos personales, su finalidad, la identidad y domicilio del responsable, destinatarios y categorías de destinatarios, condiciones de organización, funcionamiento, procedimientos aplicables, normas de seguridad, garantías para el ejercicio de los derechos del titular de los datos así como toda otra información registrada.

2.2.2.2. Infracciones y Sanciones en el tratamiento de datos

A tenor del artículo 25 de la LPD de CABA, se consideran infracciones en el tratamiento de los datos personales, las siguientes de carácter administrativo:

1) Realizar el tratamiento de datos desconociendo los principios rectores del tratamiento, ut supra analizados en la Ley de Protección de Datos Argentina, que son los mismos de la presente ley, artículos 6º a 12º .

2) Incumplir las obligaciones de confidencialidad, seguridad, obligaciones del responsable del banco de datos, obligaciones del encargado del tratamiento de datos, obligaciones del usuario y valoraciones (artículos 16 a 21 de la ley)

3) No proceder a solicitud del titular de los datos, o del Organismo de Control a la supresión, rectificación y actualización de los datos personales en los supuestos, tiempo y forma establecidos en esta ley.

4) Obstaculizar o impedir el derecho de acceso reconocido en esta ley al titular o al Organismo de Control en los supuestos, tiempo y forma que la misma estipula.

5) Ceder datos personales en infracción a los requisitos que se establecen en el artículo 10º de la LPD de CABA.

6) Crear archivos, registros, bases o bancos de datos, ponerlos en funcionamiento y/o iniciar el tratamiento de datos personales sin el cumplimiento de los requisitos establecidos en la LPD de CABA.

7) No cumplimentar los demás extremos o requisitos que esta ley establece, así como aquellos que el organismo de control establezca en ejercicio de su competencia.

8) Obstruir las funciones que la LPD de CABA, le reconocen al organismo de control.

9) Tratar los datos de carácter personal de un modo que lesione, violente o desconozca los derechos a la privacidad, autodeterminación informativa, imagen, identidad, honor así como cualquier otro derecho de que sean titulares las personas físicas o de existencia ideal.

Estas sanciones, serán aplicadas de conformidad con las condiciones y procedimientos que al efecto se establezca en la reglamentación a la LPD de CABA. Dichas infracciones deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Por su parte, el artículo 26 de la LPD de CABA, establece un régimen sancionador correctivo y preventivo de carácter administrativo, cuando se constituya una de las infracciones anteriormente enlistadas.

Como régimen general de responsabilidad se establece que los responsables, usuarios, encargados o cesionarios de archivos, registros, bases o bancos de datos del Sector Público de la Ciudad de Buenos Aires que en forma arbitraria obstruyan el ejercicio de los derechos que la presente ley le reconoce a los ciudadanos serán considerados incursos en falta grave.

Consecuentemente, el régimen sancionatorio administrativo correspondiente deviene de la comisión de alguna de las infracciones tanto previstas en el LPD de CABA, como en las previstas en la Ley de Protección de Datos de Argentina (Ley 25.326). Esto sin perjuicios de las responsabilidades administrativas, por daños y perjuicios y/o de las sanciones penales que pudieran corresponder, el organismo de control dictará resolución recomendando al órgano del cual dependa jerárquicamente el archivo, registro, base o banco de datos en el que se hubiera verificado la infracción: (i) La adopción de las medidas que proceda adoptar para que cesen o se corrijan los efectos de la infracción. Dicha resolución se comunicará al responsable del archivo, registro, base o banco de datos, al órgano del cual dependa jerárquicamente, al titular del dato y, cuando corresponda, a los encargados del tratamiento y cesionarios de los datos personales; y (ii) La aplicación de las

pertinentes sanciones administrativas a los responsables de la infracción individualizando al responsable, los hechos y los perjudicados.

Si el que comete la infracción a la LPD de CABA, es un tercero encargado de realizar tratamientos de datos personales en virtud a un contrato celebrado de acuerdo a lo previsto por el art. 5º de la LPD de CABA [14], de acuerdo al tipo de infracción de que se trate, serán de aplicación con respecto al contratista infractor, las sanciones establecidas por la Ley Nacional Nº 25.326, su reglamentación y/o sus modificaciones.

Finalmente, aclara la LPD de CABA, que cumplida la recomendación del Organismo de Control, el Poder Ejecutivo deberá abrir un sumario administrativo para determinar si existió o no una infracción a la presente ley y dicha conclusión deberá ser informada a la Defensoría del Pueblo.

En los eventos constitutivos de infracción 5º y 6º, anteriormente relacionados (sobre cesión de datos y creación de bases de datos sin requisitos legales), según el artículo 27 de LPD de CABA, el organismo de control podrá requerir al órgano del cual dependa jerárquicamente el archivo, registro, base o banco de datos en el que se hubiera cometido la infracción, la cesación en la utilización o cesión ilícita de los datos personales y, en caso de corresponder, *la inmovilización del archivo, registro, base o banco de datos* hasta tanto se restablezcan los derechos de los titulares de datos afectados.

Esta inmovilización de bases de datos, técnica y jurídicamente constituye una especie de medida cautelar que podrá ser adoptada por el organismo de control del cual dependa jerárquicamente el administrador o responsable del banco de datos.

---

(14) Inciso 3º del artículo 5º de la LPD de CABA, sostiene:"*Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad exigidos por la ley, así como también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida y cumplir con todas las provisiones de la presente ley a los fines de evitar una disminución en el nivel de protección de los datos personales*". Por su parte los incisos 1º y 3º del Artículo 5º, fueron vetados por el Decreto 1914 de 2006, por idénticas razones jurídicas a las transcritas sobre las funciones de la Defensoría del Pueblo. Esos incisos sostenía: (i) *Cuando el responsable de un archivo, registro, base o banco de datos decida encargar a un tercero la prestación de servicios de tratamiento de datos personales, deberá requerir previamente la autorización del organismo de control, a cuyo efecto deberá fundar los motivos que justifican dicho tratamiento; y* (ii) *Los tratamientos de datos personales por terceros que sean aprobados por el organismo de control no podrán aplicarse o utilizarse con un fin distinto al que figure en la norma de creación de archivos, registros, bases o bancos de datos.*

2.3. La Ley de protección de los datos personales de la Provincia de Neuquen

Mediante la Ley No. 2.307 de 7 de Diciembre de 1999, se regula el ***"Régimen de la Acción de Hábeas Data"*** en la Provincia Argentina de Neuquen. Ley fue promulgada el 30 de Diciembre de 1999 y se publicó el 4 de febrero de 2000, fecha en la cual entró en vigencia

2.3.1. Estructura formal de la ley

El Régimen jurídico de la Acción de Hábeas Data, como intitula la ley, se halla reglamentado a nivel provincial, haciendo énfasis en *el objeto primordial de la ley*, por el cual sostiene que la acción de hábeas data procederá cuando se requiera conocer los datos de una persona que consten en forma de registro, archivo o banco de datos de organismos públicos o privados destinados a proveer informes, como así también para conocer la finalidad a que se destina esa información, si ha sido comunicada a terceros, a quiénes y a qué efectos y para requerir su ratificación, actualización o cancelación.

Asimismo, procederá contra la inclusión de aquellos datos que tiendan a discriminar a las personas afectadas y para requerir su supresión, rectificación, confidencialidad o actualización. Y agrega finalmente, que en ningún caso podrá afectarse el secreto de las fuentes y el contenido de la información periodística (artículo 1º).

La ley utiliza una estructura normativa de intitulado de normas, sin dividir o subdividirla en Libros, Títulos, Capítulos, como lo hacen las leyes de la República Argentina y la de Ciudad de Buenos Aires, sobre la protección de datos personales.

Están legitimados para ejercitar la acción de Hábeas Data, toda persona física o jurídica (artículo 2º), y es competente para conocerla todo Juez Civil del lugar donde se encuentre el banco de datos (artículo 3º), previa intimación al responsable del banco podrá accionarse ante el Juez (artículo 4º). El requirente estará asistido de asesores técnicos o jurídicos (artículo 5º), se entenderá silencio del requerido, si no contesta en el plazo de 5 días, si es persona privada, o 15 días si es persona pública (artículo 6º).

La acción se interpone dentro de los 60 días siguientes a la notificación de la negativa del responsable del banco de datos (artículo 7º). El trámite es el previsto en la ley y supletoriamente en el proceso "sumarísimo" del Código de procedimiento civil y comercial (artículo 8º). La demanda reúne unos requisitos formales mínimos (artículo 9º). A petición de parte o de oficio, pueden adoptarse medidas cautelares como la no publicación o cesión de datos a terceros, mientras se tramite el proceso (artículo 10º). Se puede ampliar la demanda en cualquier momento del proceso (artículo 11º). Se da traslado de la "acción" al demandado por 5 días (persona privada), o 10 días si es pública par que conteste (artículo

12º). Se abre a prueba el asunto por un término prudente, sino es de puro derecho (artículo 13º). Sin necesidad de alegatos previos, se produce la sentencia (artículo 14º). Se impondrá costas al vencido en el proceso (artículo 17º)

Dentro de los dos días hábiles de notificación de la sentencia o resolución de medidas cautelares se podrá interponer el recurso de apelación, según el C.P.C. y Co. (artículo 15º).

La acción de habeas data deja subsistente las demás acciones pertinentes que quepan en estos casos (artículo 16º). Esta exenta de tributo alguno y de sellado (artículo 18º)

2.3.2. Breves comentarios a la ley

El legislador provincial de Argentina haciendo uso de la reserva de ley para regular materias de ámbito nacional en todo aquello que no ha sido objeto de regulación integral, o mejor aún que no este reglamentado en forma clara, amplia o pertinente, expidió la Ley 2307 de Diciembre 7 de 1999, relativa al régimen de la acción de Hábeas Data en la provincia de Neuquen.

Efectivamente el legislador provincial entiende que la parte sustantiva de la Ley No. 23.326 de 2000, de Protección de datos de Argentina es amplio, claro y suficiente, sobre todo en el campo de aplicación de la ley a los titulares, usuarios y responsables o administradores de los archivos, registros o bancos de datos personales tanto los de titularidad privada como los de titularidad pública. Así mismo, lo referente al objeto y finalidades de la ley, como también a la infaltable relación de definiciones o conceptos utilizados en el tratamiento de datos personales y para conseguir un mejor entendimiento del objeto y fines de ley especial sobre datos o informaciones de la persona humana. Definiciones cerradas, técnica y jurídicamente comprensibles sobre Datos personales, datos sensibles; Archivo, registro, base o banco de datos; tratamiento de datos, responsable del banco de datos, datos informatizados, titular de los datos, Usuario de los datos y disociación de datos.

Igualmente, entiende el legislador provincial que es materia omni-comprensible lo atinente a los principios generales que deben observar quienes son sujetos destinatarios de la ley en todo tratamiento o procesamiento de datos personales de carácter público o de carácter privado. Principios que permean no solo el tratamiento propiamente dicho de los datos personales, sino todas las fases del tratamiento de datos (recolección, selección, almacenamiento y comunicación [15]), como sostuvimos en la segunda parte de este ensayo jurídico. Esos principios son: (i) Calidad de los datos, (ii) Consentimiento, (iii) Deber

---

(16) Vid. RIASCOS GOMEZ, Libardo O. ***El derecho a la Intimidad, la visión ius-informática y los delitos relativos a los datos personales*****.** Tesis Doctoral, Universidad de Lleida, Lleida (España), p.266 y ss.

de ser informado, (iv) categorización de datos, (v) Datos relativos a la salud, (vi) Seguridad de Datos, (vii) Cesión de datos, (viii) Transferencia internacional de datos.

La ley provincial de Neuquen se dedica a puntualizar aspectos procedimentales de la protección de datos personales, pues desde su intitulado clara e inequívocamente hace relación al régimen de la Acción de Hábeas Data y comienza por exponer el objeto de aquella, al exponer que ésta solo cabe en dos oportunidades: (i) Cuando se trata de la aprehensión y conocimiento de los datos del concernido y almacenadas en los bancos de datos públicos o privados; y (ii) Cuando el concernido, ha conocido previamente que los datos o informaciones almacenadas en un banco de datos público son inexactas, faltas o no conformes al ordenamiento jurídico, podrá ejercitar las facultades del Hábeas Data de rectificación, actualización y supresión de los datos.

La ley procesal de Hábeas Data de Neuquen a partir del artículo 2º hasta el 19º, puntualiza aspectos procedimentales del proceso "*sumarísimo*" originado en la acción de Hábeas Data, más desde el punto de vista de los breves lapsos de tiempo de cada una de las etapas jurisdiccionales (Etapas normales de: La litis contestatio: demanda y contestación; etapa probatoria, y etapa de juzgamiento, y la etapa contingente de "medidas cautelares") desarrolladas por el Juez civil del lugar donde se halle el banco de datos, que desde la reestructuración del proceso mismo, pues como lo sostiene la ley comentada, supletoriamente se aplica al proceso de Hábeas Data, las reglas y etapas del proceso "sumarísimo" previsto en el Código Procesal Civil y Comercial argentino.

Los brevísimos términos jurídicos que se establecen para cada etapa procesal comulgan con el espíritu, objeto y finalidades de la ley sobre datos personales tratados o informatizados en bancos de carácter público y privado; así como la efectividad, agilidad y pertinencia de las facultades inherentes al Hábeas Data ejercitadas por el concernido con las informaciones o datos personales. Este avenimiento de términos procesales es concordante con la actividad jurisdiccional que preferentemente avoca el conocimiento de esta clase de procesos en el cual se le suministra un margen de discrecionalidad temporal para la determinación de la etapa probatoria, así como un compás de discrecionalidad funcional para adoptar o no medidas cautelares en el proceso.

Las medidas cautelares en todo proceso jurisdiccional o administrativo, como mecanismos procesales que persiguen garantizar la terminación efectiva del proceso mediante sentencia, así como tutelar preventiva y realmente los derechos del demandante o titular de unos derechos o intereses jurídicos pendientes de decisión definitiva, pueden ser adoptadas a instancia de parte o *ex officio* por parte de la autoridad judicial o administrativa [16]. En el proceso originado por la acción de Hábeas Data, el juez dispone

_____

(16) Vid. RIASCOS GOMEZ, Libardo O. ***Las medidas cautelares en el procedimiento administrativo.*** Tesis doctoral, Universidad de Navarra, Pamplona (España), p. 430 y ss.

de la facultad discrecional de adoptar medidas cautelares en el proceso, si previamente no han sido solicitadas por el demandante o interesado. Al respecto, cabe exaltar la labor del legislador de Neuquen, porque efectiva y precautelativamente se tutela los derechos del concernido con los datos o también demandante en el proceso de Hábeas data, porque a pesar de ser un proceso brevísimo en trámites y términos procesales, la instauración de medidas cautelares precave daños y perjuicios mayores, suspende los que se estuvieren produciendo en menor escala o mejor aún, evita que pudieran producirse si el proceso "sumarísimo" demore más de lo debido y por diferentes razones aún las no imputables a las partes o al juez.

El Juez, a instancia de parte o de oficio, una vez presentada la demanda y en cualquier estado del proceso, podrá decretar precautelarmente medidas de no innovar a efectos que el demandado se abstenga de realizar publicidad o cesión de los datos a terceros; así como también, si procede, disponer el secuestro de los elementos que contengan la información hasta la terminación del proceso. Estas medidas cautelares documentales materiales de publicitación, comunicación y aprehensión de datos o informaciones personales buscan garantizar cautelar y eficazmente los derechos del concernido o titular de los derechos sobre los datos recabados en bancos de datos públicos y privados mientras dura el proceso (*pendentia litis*) y hasta su terminación efectiva mediante sentencia.

La Sentencia pronunciada por el Juez, en esta clase de procesos, se expedirá dentro del plazo de cinco (5) días de permanencia del expediente en el despacho judicial. La sentencia que admita las pretensiones del demandante, "librará el respectivo mandamiento que dispondrá: (i) la expresión concreta del particular, sea persona física o jurídica, o de la autoridad estatal a quien se dirija y con respecto a cuyos registros, archivo banco de datos se ha concedido la acción, (ii) la determinación precisa de lo que debe o no hacerse; y (ii) el plazo para su cumplimiento, que no podrá excederse de cuarenta y ocho (48) horas.

Vale decir, que el Juez en principio, deberá declarar e identificar inequívocamente al legitimado por pasiva: el usuario o al responsable del banco de datos, bien sea público o privado; y también, al legitimado por activa que será toda persona titular de un derecho o interés jurídico sobre los datos o informaciones que a él le conciernen, a efectos de viabilidad, pertinencia y declaratoria de derechos en el proceso originado por la acción de Hábeas Data. Así mismo, determinará a manera de condena, las actividades de hacer y no hacer respecto de los datos personales cautelados, y finalmente, ordena el cumplimiento de la determinación activa u omisiva en un lapso brevísimo de 48 horas, por parte de la autoridad, entidad u organismo del Estado, o de la persona privada, según fuere procedente y de conformidad con la sentencia.

3. EL HABEAS DATA EN LA LEY PROTECCION A LA VIDA PRIVADA O PROTECCION DE DATOS DE CARÁCTER PERSONAL DE CHILE

3.1. Notas preliminares: "*The right to privacy*"

Mediante la Ley No. 19.628 de Agosto 28 de 1999, el legislador del Estado Chileno expidió la "*Ley sobre Protección de la vida privada o protección de datos de carácter personal*" [17], en la cual se desarrolla y reglamenta el Hábeas Data, con el propósito central de proteger y garantizar a todas las personas el derecho a la intimidad personal y familiar o en términos de la primera etapa de regulación normativa del derecho europeo insular y anglosajón: *The right to privacy.* Derecho a la privacidad o vida privada que luego se trasladó a las leyes de protección de datos de la Europa continental, especialmente Francesa, Italiana, portuguesa y española. Sólo hasta la expedición de las Directivas Europeas de protección de los datos de carácter personal, Números 95/46/CE y 97/66/CE, se sustituyó el término de privacidad por el de derecho a la intimidad de las personas.

En el derecho latinoamericano, aún hace tránsito en las diferentes legislaciones, incluida la Chilena el término *ius civilista* del derecho a la privacidad, como un derecho personalísimo de todo ser humano que hunde sus raíces históricas en el trabajo doctrinal de los juristas norteamericanos *Warren and Brandeis,* quienes para estructurar *The right to privacy,* parten del análisis de uno de los fundamentales principios del *Common Law,* que sostiene: *todo individuo debe gozar de total protección en su persona y en sus bienes.* Así mismo, los juristas de la época se preguntaron si existía o no un principio common law que permita invocarse para amparar la *privacy*, y en tal virtud analizan estos aspectos: (i) La evolución de la concepción jurídica, efectos y alcances de los derechos a la vida, la libertad y la propiedad de todas las personas; (ii) La sentencia del Juez Cooley (1888), sobre el denominado derecho "a no ser molestado" –*The right to be alone--,* cuando se invaden *"los sagrados recintos de la vida privada y hogareña",* con la toma de fotografías por parte de empresas periodísticas sin el consentimiento de los fotografiados; y (iii) El escrito de *El Godkin, sobre "The rights of the cittizen: to his reputatation*" de junio de 1890, en donde se evidencia el peligro de una invasión de la privacidad por parte de los periódicos de la época, sobre todo, cuando se hacía comentarios sobre la vida personal y familiar del ciudadano Warren en detrimento de su reputación, poniéndolo "en ridículo" ante la sociedad o violando en términos más recientes, "su intimidad legal" [18].

---

(17) Texto completo de la ley En: http://www.sernac.cl/leyes/

(18) En nuestra tesis hacemos una evolución histórico-jurídica del derecho anglosajón The privacy hasta los actuales momentos, en los que se prefiere denominarlo derecho a la Intimidad y así ha sido constitucionalizado en la mayor parte de Constituciones americanas, europeas e incluso se comienza a denominarlo así en el derecho anglosajón contemporáneo. Cfr. RIASCOS GOMEZ, Libardo O. ***El derecho a la Intimidad, la visión ius-informática y los delitos relativos a los datos personales*****.** Tesis Doctoral, Universidad de Lleida, Lleida (España), p 11-12

Es clásica la distinción entre el término privacidad y el concepto intimidad, que salió a relucir en la Exposición de Motivos de la LORTAD de 1992 [19], más no en el contenido normativo de la misma, que siempre se refirió al derecho a la intimidad, tal como la Constitución Española de 1978, lo había hecho en su momento en el artículo 18-4. Hoy por hoy, la discusión es bizantina, pues el término privacidad ha quedado subsumido en una de las esferas más lejanas al núcleo del derecho a la intimidad. En su momento, la doctrina ibérica dominante evidenció la distinción y su poca utilidad a los efectos de la protección y garantía de un derecho fundamental de la persona humana, como lo era la intimidad y dentro de la cual se hallaba la concepción civilista de la privacidad (entre otros: *González Navarro, González Pérez, García de Enterría, Entrena Cuesta*). La E.M., de la LORTAD sostenía en uno de sus apartes: "*Nótese que se habla de la privacidad y no de la intimidad. Aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que se expresa sus sentimientos, por ejemplo-- , la privacidad constituye un conjunto, más amplio, más global, de facetas de la personalidad que aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado"*.

La ley de protección de los datos chilena, haciendo eco a esa primera etapa del derecho europeo en las que surgimiento la mayoría de las leyes de ese tipo, recogió el término de la vida privada y la privacidad como eje fundamental de su protección y garantía, y quizá por ello es la única a nivel latinoamericano, hasta el momento que intituló su ley con ese sello inconfundible de la protección a la vida privada, aunque en los actuales momentos debemos entender que se refiere al derecho a la intimidad, ya no solo personal sino también de carácter familiar, pues la evolución de la institución *The privacy* lleva más de un siglo.

3.2. Estructura formal de la ley

La Ley No. 19.628 de 28 de Agosto de 1998, "sobre protección a la vida privada o protección de los datos de carácter personal", está dividida en Títulos y artículos; artículos extensos sin titulación alguna y algo confusos en el contenido y redacción para un iniciado en derecho informático. La estructura es la siguiente:

Un **Título Preliminar,** relativo a las **"*Disposiciones Generales*",** artículos 1º a 3º, en los cuales se describe el objeto, campo de aplicación, algunas definiciones técnico-jurídicas

---

(19) E.M. LORTAD de 1992. AA.VV. ***Colección de discos compactos de Aranzadi***. Ed. Aranzadi, Pamplona, 1997.

de uso corriente en el contexto de la norma, tales como: (i) Almacenamiento de datos; (ii) Bloqueo de datos; (iii) Comunicación o transmisión de datos; (iv) Dato caduco; (v) Dato estadístico; (vi) Datos de carácter personal o datos personales; (viii) Datos sensibles, (ix) Eliminación o cancelación de datos; (x) Fuentes accesibles al público; (xi) Modificación de datos; (xii) Organismos públicos, las autoridades, órganos del Estado y organismos; (xiii) Procedimiento de disociación de datos; (xiv) Registro o banco de datos; (xv) Responsable del registro o banco de datos; (xvi) Titular de los datos; (xvii) Tratamiento de datos.

En el extenso titulo preliminar, también se hace referencia a la recolección de datos con objetivo de publicidad, censos promocionales o "sondeos de opinión pública", los que se advierte serán obligatorios o facultativos previo información, comunicación o notificación a los encuestados, preguntados o consultados. Deja a salvo los derechos de los titulares de esos datos y su derecho a la oposición, tanto en recolección como en la comunicación de los mismos.

El **Título I**, concerniente a "***la utilización de datos personales*"**, se trata en los artículos 4º a 11º. En estos se hace referencia al tratamiento y recolección de datos, al consentimiento por escrito requerido para ello, la revocabilidad de la autorización, la no exigencia del consentimiento para algunos tratamientos de datos (artículo 4º); requisitos para el tratamiento de datos a través de la comunicación o medios TIC ("Red electrónica"). No aplicabilidad a los datos accesibles al público (artículo 5º); sobre la eliminación, cancelación y bloqueo de datos personales (artículo 6º); Deber de secreto de los responsables de los bancos de datos (artículo 7º); Tratamiento de datos por "mandato escrito"--memorial poder-- (artículo 8º); Utilización de los datos para los fines previstos, salvo los de fuentes de acceso al público (artículo 9º); No son objeto de tratamiento los datos sensibles, salvo lo dispuesto en la ley o con el consentimiento del titular (artículo 10º); Diligencia de "cuidado" o conservación de los datos por los responsables de los bancos de datos (artículo 11º).

El **Título II,** relativo a **"*los derechos de los titulares de datos*",** se desarrolla en los artículos 12º a 16º. Derecho a la información que tiene toda persona, así como el derecho a la "modificación", si los datos son inexactos, erróneos, equívocos o incompletos. Así mismo a la eliminación, cancelación y bloqueo de datos (artículo 12º); Los anteriores derechos no pueden limitarse por acto o convención alguna (artículo 13º); derecho acceso al banco de datos administrado por diferentes organismos (artículo 14º); Excepciones a los derechos de información, acceso, eliminación o cancelación por tratarse de actividades fiscalizadoras del Estado, por seguridad o interés nacionales (artículo 15º); Acción y procedimiento de amparo ante las autoridades judiciales civiles competente, tras la negativa a contestar la petición de la información, la cancelación, el acceso o la eliminación de datos (artículo 16º).

El **Título III**, concerniente a "***la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial*****",** está contenido en los artículos 17 a 19. Deber de información de los responsables de los bancos de datos financieros a los usuarios o titulares, siempre que consten en títulos valores, documentos o contratos y éstos contengan obligaciones claras, expresas y exigibles (artículo 17º); No se podrá comunicar datos transcurridos 7 años después de haber sido exigible una obligación o 3 años después de haber ocurrido su pago o extinción por otro modo (artículo 18º); Caducidad de los datos (artículo 19º).

El **Título IV,** relativo al **"*tratamiento de datos por organismos públicos*"**, se desarrolla en los artículos 20º al 22º. El tratamiento de datos por organismos públicos se hace conforme a la ley y no requiere el consentimiento del particular (artículo 20º); No se podrán comunicar datos relativos a la condena por delitos, infracciones administrativas o faltas disciplinarias, salvo que estuviese prescrita la acción o la pena (artículo 21º); El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos (artículo 22º).

El **Título V**, concerniente a "***la responsabilidad por las infracciones a esta ley"*.** En el artículo 23, se reglamenta la responsabilidad por el daño moral y material devenida del indebido uso de los bancos de datos por parte de los destinatarios de la ley (usuarios y responsables de los bancos de datos), sin perjuicio de la responsabilidad administrativa, disciplinaria o penal a que hubiere lugar.

En las "***Disposiciones Transitorias"*,** se aclara que: (i) Los titulares de los datos personales registrados en bancos de datos creados con anterioridad a la entrada en vigencia de la presente ley tendrán los derechos que ésta les confiere; y (ii) Las normas que regulan el Boletín de Informaciones Comerciales creado por el decreto supremo de Hacienda Nº 950, de 1928, seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de esta ley.

3.3. Breves comentarios a la LPVP o PDP

La ley *"sobre Protección de la vida privada o protección de datos de carácter personal*" de 1998 o LPVP o PDP Chilena, desde su intitulado no se matricula en una escuela, doctrina o modelo de ley relativa a la reglamentación del Hábeas Data. Ni siquiera esta denominación se halla presente en el contexto de la ley, como tampoco, y esto sí es paradójico, la expresión "vida privada", "privacidad" o su homónimo contemporáneo: "La intimidad", que el objeto de tutela jurídica según el intitulado de la ley no se halla en la parte normativa de la ley en forma expresa.

Por la deficiente redacción de la ley de protección de datos Chilena, no podemos encuadrarla en el modelo europeo continental o insular o propio latinoamericano, pues hay

de todos un poco y nada exclusivamente de alguno de ellos. En momentos parecería seguir el modelo europeo continental, pues tiene elementos constitutivos de aquél, cuando acoge el sistema de definiciones técnico-jurídicas aplicables al tratamiento de datos, pero se aleja de éste, cuando no menciona en el título preliminar, los principios rectores de todo tratamiento (electrónico o manual) de datos personales, aunque en el contexto de las normas reiteradamente se refiere al "consentimiento" que lo asimila a la "autorización por escrito" dada por el titular de los datos; así como también, a la calidad de los datos, a la licitud, al secreto y la confidencialidad, a la categoría de datos (generales, especiales y sensibles), seguridad y comunicabilidad de los datos, entre otros, sin decir expresamente que son principios del tratamiento de datos, sino que implícitamente hacen parte de la redacción de la norma.

3.3.1. Objeto de la LPVP o PDP

A tenor del artículo 1º de la LPVP o PDP Chilena de 1998, tendrá por objeto regular todo tratamiento de datos de carácter personal que se recaben "*en registros o bancos de datos por organismos públicos o por particulares*", se exceptúan aquellos "*que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, Nº 12, de la Constitución Política*" de 1980, es decir, aquellas referidas a la libertad de expresión o a la libertad de prensa, pues del contenido de la norma constitucional citada devela aquellas libertades inmersas dentro de las de emitir opiniones y la de información, al expresamente mencionar los derechos, deberes y responsabilidades de los diferentes medios de comunicación (radio, televisión, periódicos, revistas, etc.,)

En ejercicio de la LPVP o PDP Chilena, toda persona "*puede efectuar el tratamiento de datos personales*", cuando la norma debería sostener que a través de todo tratamiento de datos se protege y garantiza "*el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce*", pues el titular de los datos o informaciones personales en principio es el sujeto principal de la protección y garantía de sus derechos y libertades, y aunque éste también tenga deberes constitucionales y legales no solo para con el tratamiento de datos sino para el derecho de los demás, el no abuso de los derechos y libertades propias, el Estado tiene como finalidad primera la protección y garantía de los derechos fundamentales a toda persona, natural o jurídica, nacionales o extranjeros, residentes o transeúntes.

Aunque se ha hecho un común denominador de todas la leyes de protección de datos de carácter personal el que se manifieste que la norma se expide para restringir o limitar el abuso del "poder informático" utilizado por las nuevas tecnologías de la información y la comunicación (TIC) y la informática, de cara a proteger expresos derechos constitucionales como la Intimidad, la honra, el honor, la buena imagen, la voz, la buena reputación, etc., la LPVP o PDP Chilena, a pesar de exponer en su intitulado la protección genérica de la "vida

privada", en éste punto de objeto de la ley no se manifiesta ni sobre su único objetivo de tutela constitucional, ni menos sobre el común denominador de derechos protegidos por las leyes de datos personales. Quizá interpretando los términos: "el pleno ejercicio de los derechos fundamentales de los titulares de los datos" que trae la LPVP o PDP Chilena que relaciona en la parte *in fine* del artículo 1º, que es de idéntico tenor al artículo 18-4 de la Constitución Española, podemos deducir, que genéricamente se halla protegida la vida privada y los demás derechos constitucionales mencionados. Por su parte, el artículo 19-4 de la Constitución Chilena de 1980, asegura la protección a toda persona de la "vida privada y pública", lo cual ratifica que por vía de interpretación sistemática se entienden tutelados los derechos fundamentales de la persona humana incluida la "vida privada" en concepto de las normas chilenas.

Objeto de especial atención le dedica la LPVP o PDP Chilena, a la información recabada por medio de encuestas, "*estudios de mercado o sondeo de opinión pública u otros instrumentos semejantes*", según el artículo 3º de la mencionada ley, pues dedica a éstas un reforzado cuadro de protección, al establecer por un lado, el derecho de toda persona involucrada en esta clase de tratamiento de datos personales en la fase de recolección, a ser informado sobre el carácter obligatorio o facultativo de las respuestas; y por otro lado, deberá manifestarse inequívocamente, "*el propósito para el cual se está solicitando la información*". Y además, por si fuera poco, deberá: (i) omitir las señas que puedan permitir la identificación de las personas consultadas, cuando se comuniquen los resultados de los instrumentos de encuesta, estudio, sondeo o semejantes; y, (ii) tener en cuenta que el titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

En el tratamiento de datos personales, la LPVP o PDP Chilena, establece como regla general el consentimiento de la persona para poder efectuarlo. Ese consentimiento o "autorización" deberá constar por escrito, aunque podrá ser revocado, sin efecto retroactivo o *ex nunc*, pero en todo caso la revocatoria también constará por escrito

Por excepción, según el artículo 4º de la mencionada ley, no se requiere autorización para aquel tratamiento de datos personales, en los siguientes casos: (i) cuando los datos que se recolecten provengan de fuentes accesibles al público; (ii) cuando sean de carácter económico, financiero, bancario o comercial; (iii) cuando se hallen en listas que sólo contengan la pertenencia de una persona a un grupo determinado, su profesión o actividad, sus títulos académicos, dirección o fecha de nacimiento; (iv) cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios; (v) cuando "*el tratamiento de datos personales que realicen personas jurídicas privadas para el, uso exclusivo suyo* (sic)*, de sus asociados y de las entidades a que están* (sic) *afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos*".

3.3.2. Demasiadas definiciones técnico-jurídicas del tratamiento de datos

Si bien es una constante las definiciones de términos técnico-jurídicos en las leyes de protección de datos o de Hábeas Data, tal como lo hemos comentados *ut supra* desde las legendarias leyes de protección de datos de Alemania y Suiza en la década de los años setenta del pasado siglo; entre otras razones, porque este tipo de leyes conjugan aspectos de las tecnologías de la información y la comunicación (TIC), la informática jurídica (telemática, telegestión, cibernética y electrónica) y concepciones jurídicas sustantivas y procedimentales; no es menos cierto que el legislador deba abusar de ellas en el número y extensión de conceptualización, como aparece en la LPVP o PDP Chilena de 1998.

Si el propósito primero de las definiciones técnico-jurídicas de ésta clase de leyes, es aclarar la utilización y pertinencia de las mismas en el contexto de la ley, así como precisar conceptualmente cada una de las definiciones suministradas a fin de evitar confusiones, indebidas interpretaciones o equívocas aplicaciones por el operador jurídico de la norma, éstos propósitos de diluyen si se proporcionan demasiadas definiciones y de entre ellas pudiera presentarse colisiones conceptuales como parece suceder en la LPVP o PDP Chilena.

En efecto, la ley mencionada define lo que se entiende por dato personal, dato sensible, dato caduco, dato estadístico.

El dato personal, universalmente se ha entendido como toda información de la persona humana identificada o individualizada, como identificable. Esta información sólo se predica de las personas físicas o naturales. Se infiere entonces, que el titular de los datos, es la persona natural o física y no es necesario definir como la hace la ley Chilena, al "*titular de los datos*".

La regla general es la información o dato personal. Sin embargo existen, algunos datos sobre protegidos en la legislación mundial, porque afectan al núcleo esencial de la intimidad (o privacidad en términos de la Ley chilena), tales como el origen racial o étnico; tendencias políticas, religiosas, filosóficas, sindicales; circunstancias especiales de la salud, la vida sexual, entre otras, que se consideran como datos sensibles de la persona humana y por ello, los estados potencian los niveles de protección en estos casos, no permitiendo por ejemplo, la recolección y tratamiento posterior, libre del consentimiento del titular de los datos, o más aún está prohibido, aún con el consentimiento del titular. Como se observa aquí lo importante es definir que entendemos por consentimiento del titular, más que cuántos ejemplos podemos dar de datos denominados esenciales como se empeña en relacionar la Ley Chilena, pues existen legislaciones de protección de datos, como la española por ejemplo, donde el consentimiento se convierte no sólo en una simple definición, sino un principio rector del tratamiento de datos que lo ilumina y determina en todas sus fases. En la ley Chilena esta definición de consentimiento no aparece

expresamente en el artículo 2º dedicado a las definiciones, pero si se utiliza en varios artículos de la Ley con el nombre de “autorización del titular”.

En cuanto al dato caduco, definido por la Ley Chilena como aquel “*que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiere norma expresa, por el cambio de los hechos o circunstancias que consigna*”, es una construcción que se originó en la jurisprudencia del Tribunal Constitucional Español y que ha ido variando con el fortalecimiento de la jurisprudencia, que hoy considera que los datos no caducan sino que se transforman de positivos a negativos, o de éstos a neutros, con el simple transcurrir del tiempo.

De otra parte, caducan sólo las acciones o recursos procesales jurisdiccionales o administrativos por la no utilización de aquellos por su titular o por quien demuestre interés legítimo dentro de un término preestablecido por la ley. Por ello, no pueden caducar los datos o informaciones personales, porque estas *per se* son intemporales, el valor agregado que le damos de ser información positiva, negativa o neutra a nuestros intereses, tiene una connotación altamente subjetiva que puede fundarse en intereses financieros, políticos, sociales, culturales, científicos, etc., aunque en el ámbito de las leyes de protección de datos siempre se ha hecho énfasis en el valor agregado estrictamente financiero (económico, comercial, bancario, bursátil, etc.,), pues es en el ámbito donde más tiene aplicabilidad el concepto de “caducidad del dato” o “dato caduco”. Más aún, ni siquiera en éste solo ámbito del valor agregado, las legislaciones universales se han puesto de acuerdo en qué término exactamente se produce la caducidad del dato; unas mencionan 3, 5, 7 o 9 años después de cumplida una condición resolutoria determinada, del pago del crédito, de notificado el cumplimiento de la obligación, entre otras posibilidades de cumplimiento o incumplimiento de una obligación económico-jurídica.

En consecuencia, la definición del “dato caduco” al ser altamente cambiante en la doctrina y la jurisprudencia sobre el tema, no parece conveniente petrificarla, como se hace en el artículo 2º de la comentada ley.

Con el dato estadístico, definido por la LPVP o PDP Chilena, como “*el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable”*, resulta pleonástico e innecesario, pues como la mayoría de leyes de protección de datos del mundo, incluida la Ley Chilena, definen que debe entenderse como “procedimiento de disociación de datos” (“*todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o indeterminada*”) de donde se infiere que el dato estadístico es un ejemplo de aplicabilidad de dicho procedimiento de disociación, con lo cual resulta intrascendente pronunciarse nuevamente cuando ya se ha definido en que consiste la disociación de datos.

Resulta cuando menos, sorprendente que la Ley Chilena se esmere en definir el dato estadístico que constituye una excepción a la aplicación del principio rector del tratamiento de datos denominado del consentimiento de las personas y deje de lado la conceptualización del dato financiero, al cual le dedica el Título III y tres extensos artículos de la LPVP o PDP. No solo sorprende porque también el dato financiero está excluido del principio general del consentimiento o "autorización" del titular de los datos para el tratamiento de cualquier dato de carácter personal, como lo está el dato estadístico de menos valor agregado y de perfil más bajo, por ser un dato disociado, que el del dato financiero, que es un dato personal individualizado o individualizable, sino además porque sólo protege al dato financiero en la fase de comunicación (circulación, transferencia o cesión) de datos y no en la recolección, selección, almacenamiento y registro de datos, pues en esta no se requiere "autorización" expresa y escrita del titular de los datos.

Por otro lado, resultan innecesarias las definiciones de "organismos públicos", entidades o instituciones del Estado, cuando no son términos técnico-jurídicos aplicables exclusivamente a la LPVP o PDP Chilena y son de conocimiento y aplicación general al derecho chileno, más aún existe una norma de ámbito nacional que explica, la estructura, organización y funcionamiento del Estado en desarrollo y regulación de la Constitución sobre el tema, es la Ley Nº 18.575, *"Orgánica Constitucional de Bases Generales de la Administración del Estado*", que explica con más amplitud y profundidad lo que debe entenderse por organismos públicos e instituciones, organismos o entidades del Estado, que una ley específica en datos personales que tiene otros objetivos y fines programáticos.

4. EL HABEAS DATA EN LAS LEYES DE TRANSPARENCIA EN LA GESTION PUBLICA DE LA REPUBLICA DE PANAMA

La República de Panamá mediante la Ley 6º de 22 de Enero de 2002, expidió la ley que intitula: "normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y otras disposiciones" [20]. Con lo cual es la única ley en Latinoamérica que regula el fenómeno jurídico de Hábeas Data en una misma ley que incorpora dos derechos fundamentales autónomos como son, por un lado, el derecho a la información y la garantía constitucional de su acceso a cualquier medio mediante el cual se recabe, recolecte o almacene (electrónico, informático o manual o escrito); y por otro, el derecho y garantía constitucional de Hábeas Data. En varios países latinoamericanos como Argentina, Perú, Ecuador, Chile, Uruguay e incluso Colombia que prepara desde hace años su Ley de Hábeas Data, regulan los mencionados derechos constitucionales en estatutos jurídicos diferentes.

_____

(20) Texto completo En: http://www.defensoriadelpueblo.gob.pa/

Veamos a continuación que ventajas y desventajas trae la regulación integral del derecho a la información y su garantizado acceso público y privado y el derecho de Hábeas Data.

4.1. Estructura de la LTGP y HD

Ley No.6 de 22 de enero de 2002, se estructura formalmente en Capítulos y artículos sin intitulados.

En el artículo 1º de la Ley para "*la transparencia en la gestión pública, establece la acción de Hábeas Data y otras disposiciones*" de Panamá (o LTGP y HD), relaciona un amplio catálogo de definiciones jurídicas relativas al derecho de la información y sus derechos fundamentales conexos, pero omite hacer sobre las definiciones técnico-jurídicas aplicables al tratamiento de datos o informaciones personales o al conjunto de facultades inherentes al Hábeas Data, que según el intitulado es también objeto de protección y garantía jurídica de la ley, aunque por la omisión parecería más un tema que raya la ajenidad con la norma su inclusión.

En efecto, se define el Código Ético, como el "*conjunto de principios y normas de obligatorio cumplimiento, con recomendaciones que ayudan a los miembros de una organización a actuar correctamente"; el* Derecho de Libertad de Información, como aquel "*que tiene cualquier persona de obtener información sobre asuntos en trámites, en curso, en archivos, en expedientes, documentos, registros, decisión administrativa o constancias de cualquier naturaleza en poder de las instituciones incluidas*" en la LTGP y HD de Panamá.

Luego profundiza, sin a nuestro juicio necesario hacerlo, en las definiciones de "ética", "información", "información confidencial", "información de acceso libre", "información de acceso restringido", "institución", "persona", "principio de acceso público", "principio de publicidad", "rendición de cuentas" y "transparencia". Definiciones todas que en una ley que regula el derecho de acceso y transparencia de la información públicas, sin el aditamento del Hábeas Data, es válido y hasta cierto punto explicable, pero igualmente en este punto, retórico.

En el ***Capítulo II,*** relativo a la ***"Libertad y Acceso a la Información",*** la LTGP y HD de Panamá, describe en los artículos 2º a 7º, la titularidad, legitimidad, características, requisitos, autoridades y formas de acceso del derecho a la información que tiene toda persona, bien sea por escrito, en forma verbal o a través de los nuevos medios de información y comunicación electrónica o informática. Así mismo, explica como los funcionarios encargados de recepcionar las peticiones de información, están obligados a contestar por escrito en el término de treinta (30) días calendario.

En el ***Capitulo III,*** concerniente a la "***Obligación de Informar por Parte del Estado",*** en los artículos 8º a 12º, se regula los deberes y las obligaciones de informar al público en general, y a los peticionarios en particular, por parte de las entidades, organismos y dependencias del Estado, en especial sobre Contratación Pública del Ministerio de Economía y Finanzas y de la Contraloría General de la República. Así mismo, se establece los mecanismos y canales de información entre los particulares y el Estado; los instrumentos de información tradicional, documental escrita o electrónica y la forma de entregar información por escrito, en formularios o por vía Internet.

En el ***Capítulo IV,*** referente a la "***Información Confidencial y de Acceso Restringido",*** prevista en los artículos 13º a 16º, la LTGP y HD de Panamá, relaciona la no revelación o divulgación (o "descubrimiento", como se dice en el derecho anglosajón) de la información confidencial de las personas humanas que hacen parte tanto del núcleo "duro" o esencial de la intimidad, como las concernientes a la "vida privada" de las personas, a los asuntos penales, policivos, médicos, correspondencia escrita y electrónica y a las conversaciones telefónicas, entre muchas otras informaciones. En el caso de la información judicial, se establece la reserva salvo el caso del concernido y las partes que intervienen en éste.

La información de acceso restringido, es decir, "*todo tipo de información en manos de agentes del Estado o de cualquier institución pública, cuya divulgación haya sido circunscrita únicamente a los funcionarios que la deban conocer en razón de sus atribuciones*", no podrá ser revelada por un período de diez (10) años, "*contado a partir de su clasificación como tal, salvo que antes del cumplimiento del período de restricción dejen de existir las razones que justificaban su acceso restringido".*

Se relaciona como información de acceso restringido, la relativa a: (i) la seguridad del Estado; (ii) los secretos comerciales; (iii) la información sobre procesos realizados por el Ministerio Público, las fuerzas militares y de policía, la Dirección de Aduanas y la Contraloría General de la Nación; (iii) información sobre yacimientos mineros y petrolíferos; (iv) información documental diplomática; (v) procesos y documentos judiciales penales y policivos; (vi) documentos e información de la Presidencia, Vicepresidencia y "gabinete" ministerial; (vii) Transcripciones y documentos de la Asamblea Legislativa.

La negación de entrega de información de información de acceso restringido o reservada, deberá ser motivada y por escrito por parte de la entidad del Estado que así proceda [21].

_____

(21) Que según el artículo 1º, numeral 5º , la conforma: "Todo tipo de información en manos de agentes del Estado o de cualquier institución pública que tenga relevancia con respecto a los datos médico y psicológicos de las personas, la vida íntima de los particulares, incluyendo sus asuntos familiares, actividades maritales u orientación sexual, su historial penal y policivo, su correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad. Para efectos de esta Ley, también se considera como confidencial la información contenida en los registros individuales o expedientes de personal o de recursos humanos de los funcionarios".

En el ***Capítulo V****,* concerniente a la "***Acción de Hábeas Data"*** contenida en los artículos 17 a 19, La Ley panameña, describe la legitimación del Hábeas Data para toda persona natural o física, cuando solicita información a él concernida y se encuentren en "manos" de las entidades del Estado o sea tratadas o procesadas por éstas a través de mecanismos electrónicos y ésta información sea negada o insuficiente o inexactamente entregada. Así mismo, menciona a las autoridades judiciales competentes y el procedimiento constitucional de amparo específico o de Hábeas Data informativo. Finaliza, indicando que el proceso será sumario, sin formalidades y sin presencia de abogado y respecto a la sustanciación, impedimentos, notificaciones y apelaciones, se aplicarán las normas que para estas materias se regulan en el ejercicio de "*la acción de Amparo de Garantías Constitucionales".*

En el ***Capítulo VI*****,** relativo a las "***Sanciones y Responsabilidades Personales de los Funcionarios",*** previsto en los artículos 20º a 23º describe la responsabilidad del funcionario judicial que desatiende "el recurso de Hábeas Data", sancionándolo la primera vez con multa por desacato, y con destitución, sí reincide. El perjudicado con la negativa de información por Hábeas Data, podrá demandar civilmente al funcionario público por daños y perjuicios, sin perjuicio de las acciones penales o disciplinarias que quepan.

En el **Capítulo VII,** concerniente a la "***Participación Ciudadana en las Decisiones Administrativas y sus Modalidades*****"**, contenidas en los artículos 24º y 25º, describen los mecanismos de participación ciudadana en las acciones y gestiones públicas de las entidades del Estados, especialmente en obras civiles, valorización, zonificación, tarifas y servicios públicos. Así mismo establece las modalidades tales como la consulta y audiencias públicas, foros, talleres y participación directa ante la Instituciones públicas. Por los contenidos del capítulo bien podría tratarse de una norma que quebranta el principio de "*unidad legislativa y de materia*", pues si bien en la solicitud y entrega de información se requiere la participación efectiva de la ciudadanía, no necesariamente debería haberse legislado sobre éste tópico en forma como lo hizo la Ley de acceso a la información y Hábeas Data de Panamá, pues constituye un "*mico legislativo*".

En el ***Capítulo VIII****,* relativo a la "***Fiscalización del Cumplimiento por el Órgano Legislativo",*** previsto en el artículo 26º, la ley obliga a las entidades del Estado que anualmente incorporen en su memorias de informe al órgano legislativo, el número de peticiones de información resueltas y negadas, así como la listas de los actos administrativos en los que tuvo participación la ciudadanía.

En el ***Capítulo IX****,* concerniente al "***Código de Ética",*** previsto en el artículo 27º, se establece la obligatoriedad de todas las entidades del estado, pertenecientes a cualquiera de las tres ramas del poder público, del nivel nacional, regional y local, para que en el término de seis (6), si ya no lo tienen, adopten un Código de Ética para el correcto ejercicio de la función pública que será publicada en la Gaceta Oficial.

En el ***Capítulo X****,* relativo a las "***Disposiciones Finales",*** previsto en los artículos 28º y 29º, establece la tabla de vigencia de la ley.

4.2. Breves comentarios de la ley

4.2.1. La acción o "recurso" de amparo específico de Hábeas Data

La LTGP y HD de Panamá en el Capítulo V, regula lo que inicialmente denomina "*Acción de Hábeas Data*", pero que en el contenido normativo del capítulo cambia su denominación por "*recurso de Hábeas Data*".

Esta ley panameña, como se ha dicho antes hace énfasis en la regulación amplia del derecho de acceso a la información pública contenida en documentos escritos, tradicionales y electrónicos (archivos o bases de datos), por parte de cualquier persona concernida con ésta y tan solo cuando ésta información es negada o entregada insuficiente o inexactamente por parte de la entidad, organismo, institución o dependencia del Estado, perteneciente a una cualquiera de las tres ramas del poder público u organismos autónomos o semiautónomos, nace para el peticionario, el consultante o solicitante de información, la posibilidad de accionar o recurrir ante las entidades jurisdiccionales, en Hábeas Data, para hacer respetar y garantizar su derecho a la información en los términos que establece el ordenamiento jurídico vigente, a través de un procedimiento breve y sumario, sin formalidades mayores que las que establece la LTGP y HD de Panamá y sin necesidad de abogado.

Esto por cuanto, como lo explica el Presidente de la Asamblea Legislativa Panameña, la "*nueva ley es un instrumento moderno que reconoce el derecho de cada uno de ustedes a exigir la información que sea del caso, sin tener que dar justificación o explicación sobre esa petición, y en un plazo no mayor de 30 días que, salvo algunas situaciones específicas, podría extenderse sólo otros 30 días"* [22]*.* Cuando la información que es el derecho privilegiado en el derecho panameño es desconocido o quebrantado por las organismos, entidades, autoridades o dependencias del Estado, toda persona tiene derecho a recurrir al Hábeas Data, "*que no es más que un mecanismo que tendría el ciudadano para "garantizar su derecho de acceso a la información", cuando el servidor público titular "no le haya suministrado lo solicitado" o le haya entregado algo de manera "insuficiente o en forma incorrecta"* [23].

---

(22) ***Mensaje del Excelentísimo Señor Presidente de la Asamblea Legislativa, Rubén Arosemena, en torno a la Ley de Transparencia en la gestión Pública***. En: http://www.defensoriadelpueblo.gob.pa/

(23) En dirección electrónica, ut supra cit

Por su parte, a Presidenta del Gobierno Panameño [24], al comentar la LTGP y HD, reconocía la importancia de esta ley, en particular cuando crea "*la acción jurisdiccional de Habeas Data mediante la cual, cualquier persona, podrá recurrir ante la justicia ordinaria y exigir el respeto a su derecho a ser informado de una actuación pública",* de las gestiones y realizaciones públicas en contratación estatal, en servicios públicos, en actividades tributarias, de valorización, de tarifas e incluso de gestiones efectivas contra la corrupción y las actividades ilegales, todo ello en beneficio de la mayor transparencia del Gobierno y las entidades del Estado para con sus ciudadanos y personas que pudieran ser afectadas por acción, omisión o extralimitación de funciones públicas.

La acción o recurso de Hábeas Data regulado en la LTGP y HD, se introdujo en el derecho público panameño, para proteger y garantizar primigéneamente el derecho de acceso a la información pública que tiene toda persona humana, pero también para garantizar de contera, "*la imagen, la privacidad, el honor, el derecho a la autodeterminación de la información y libertad de información de una persona*" [25].

Como analizamos en la Parte Segunda de este ensayo jurídico, la Constitución Panameña con la reforma de 2004, resulta mucho más avanzada que la Ley que la reglamentó, pues los artículos 43 y 44 de la Constitución garantizan el derecho de acceso a la información tanto pública o de interés colectivo como de carácter privado siempre que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos y que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación.

Pero además y en forma integral y completa, la Constitución Panameña, confiere a toda persona el derecho de promover "acción de Hábeas Data", en los siguientes casos: (i) con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información; (ii) para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución; y, (iii) podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal.

La reglamentación y desarrollo legal de los artículos 43 y 44 de la Constitución en la LTGP y HD de Panamá, es parcial porque por un lado, sólo desarrolla el acceso a la información

---

(24) La Sra. Presidente de Panamá en la época, Mireya Moscoso. En: http://www.defensoriadelpueblo.gob.pa/

(25) Según el Colegio de Abogados de Panamá. En: http://www.defensoriadelpueblo.gob.pa/

pública por toda persona; y por otro establece el mecanismo jurisdiccional del Hábeas Data con algunas reglas procesales mínimas propias y otras, que son las mayoritarias nacen en la remisión legislativa al "Código Judicial de Panamá", libro IV, Titulo III, sobre "Amparo degarantías Constitucionales", en lo que "*respecta a la sustanciación, impedimentos, notificaciones y apelaciones"*, como lo dispone el artículo 19 de la LTGP y HD.

El legislador panameño, perdió la oportunidad de reglamentar en forma amplia, integral y verdaderamente efectiva el proceso sumario originado en la acción de Hábeas Data, tal como se había facultado por la reforma constitucional de 2004, en el inciso *in fine* del artículo 44 y procedió en su entender mejor a la labor remisoria que a la tarea de creación legislativa de un proceso breve, expedito y altamente garantísta de los derechos fundamentales *ut supra* mencionados. En tal virtud, el proceso constitucional originado en la acción de Hábeas Data actualmente es de naturaleza jurídica mixta, pues por un lado, la Constitución estableció que éste sería sumario y sin necesidad de apoderado judicial y que serían competentes los tribunales judiciales que determine la ley; y por otro, según la LTGP y HD, en cuanto a la sustanciación, impedimentos, notificaciones y apelaciones del "proceso sumario", se regirán por los artículos 2615 a 2632 del Código Judicial que regulan el proceso de amparo de garantías constitucionales.

El proceso de amparo específico de Hábeas Data en consecuencia tiene una naturaleza jurídica de *tertium genus,* porque se estructura inicialmente como un "proceso sumario" específico para el Hábeas Data, pero que se complementa por un proceso judicial apto para la protección y garantía de derechos fundamentales a través de instituciones jurídico-procesales aplicables al proceso de amparo, cuyas características y peculiaridades en el derecho público panameño, como lo hemos observando al leer los artículos mencionados del Código Judicial, no son prenda de garantía de la mayor eficacia, sumariedad, claridad normativa y más aún, de ser un instrumento jurisdiccional expedito para garantizar y proteger los derechos fundamentales de la persona sólo contra entidades u organismos del Estado [26], con el mínimo de formalidades procedimentales y sin necesidad de apoderado judicial.

---

(26) Actualmente la acción de amparo no procede contra los acciones, actos o decisiones de los particulares cuando desconozcan o quebranten el ordenamiento jurídico vigente, tal como sí es posible en el derecho comparado. El autor en su obra, señala como "en el Derecho Constitucional tradicional, se consideraba que los derechos y garantías que la Constitución consagra a favor de los habitantes de una nación se establecían como una protección a los mismos frente a posibles abusos del Estado. Es decir, se estimaba que sólo el Estado podía violar los derechos fundamentales de los particulares y por ello, nuestra Carta Magna, entre muchas otras del área, señala que el Amparo cabe contra órdenes de hacer o no hacer dictadas por funcionarios. Pero, en la actualidad, se ha hecho evidente que los particulares pueden también violar los derechos de otros particulares". Y por eso cuestiona el actual sistema jurídico panameño que no permite elevar acciones de amparo frente a la actividad contraria al derecho realizada por parte de las entidades o personas particulares. En: BLANDON FIGUEROA, José. ***El amparo contra particulares.*** **http://www.pa-digital.com.pa/**

Según una autorizada doctrina, "*La acción de amparo de garantías constitucionales lejos de cumplir su función protectora de los derechos individuales, incumple su misión por la multiplicidad de presupuestos legales y jurisprudenciales que se le han incorporado y que han desnaturalizado su razón de ser, así como la voluntad del constituyente*" [27]. Se ha convertido en una "acción inaccesible" por parte de las personas que hacen uso de ella para tutelar sus derechos fundamentales y especialmente el de Hábeas Data que venimos comentando.

En efecto, como lo constata el abogado y docente universitario *De León Batista*, al respecto sostiene: "*venimos observando que la mayoría de las acciones de amparo de garantías constitucionales ni siquiera las admite el tribunal competente de la causa por el hecho de que no cumplen una serie de formalidades o requisitos"* [28].

En la Parte Segunda de este ensayo, analizamos brevemente los cuadros estadísticos relacionados por el tratadista *Pérez Jaramillo* [29], en los que demuestra que desde la entrada en vigencia de la LTGP y HD de Panamá hasta Mayo de 2003, se había rechazado sesenta (60) acciones de Hábeas Data por parte de la Corte Suprema de Justicia, basado en diversos argumentos, casi todos de índole formal, pues a título de ejemplo, se rechazaron por: (i) Once, porque no demostró "el interés legítimo, es decir, no es persona interesada"; (ii) Nueve, no se "solicita información y solicita otra petición"; (iii) Cinco, porque la "autoridad ha respondido la solicitud, aunque el peticionario no lo considera así"; (iv) Cinco, porque "al interponer la acción de Hábeas Data no se presentaron originales sino copias y se omiten formalidades"; (v) Tres, porque "la autoridad alega no tener la información y dice que corresponde a otra entidad"; (vi) Tres, porque "el peticionario presentó Hábeas Data, antes de 30 días"; (vii) Tres, porque "la autoridad a la que se hace petición no es funcionario público, aunque labore para una empresa mixta"; (viii) Tres, porque la "información fue calificada de ´acceso restringido´.

Según el artículo 18 de la LTGP y HD, tienen competencia y jurisdicción para avocar y resolver acciones de Hábeas data de carácter público, de conformidad con el nivel de la entidad administrativa y del funcionario titular o responsable del banco de datos, así: (i) los Tribunales Superiores que conocen de la acción de Amparo de Garantías constitucionales, cuando el funcionario titular o responsable de registro, archivo o banco de datos, tenga mando y jurisdicción a nivel municipal o provincial; y (ii) El Pleno de la Corte

_____

(27) PORCELL D., Kenia I**. *El Amparo de Garantías Constitucionales, una Acción Inaccesible (Parte I y II)*** Abogada Asistente Secretaría de Asuntos Legales, Procuraduría General de la Nación. En: http://www.ministeriopublico.gob.pa/

(28) DE LEON BATISTA, Hernán. ***Amparo de garantías: ¿un recurso muy especial?.*** *En:* **http://mensual.prensa.com/**

(29) PEREZ JARAMILLO, Rafael. ***El Hábeas Data no admitidos y argumentos de rechazo conforme a los fallos de la Corte*****. Vía Internet.**

Suprema de Justicia, en el evento de que el titular o responsable del registro, archivo o banco de datos tenga mando y jurisdicción en dos o más provincias o en toda la República.

Vale decir entonces, que los órganos judiciales competentes para conocer el proceso de amparo originado en la acción de Hábeas Data en Panamá, son de naturaleza colegiada o plural, bien sea que el asunto se conozca a nivel local y regional, o bien se trate de asuntos interprovinciales o nacionales. Las autoridades judiciales individuales a nivel de jueces municipales, provinciales o de Circuito, entre otros, están ausentes de esta clase de procesos según la ley comentada. Sin embargo, se hace necesario un reglamentación urgente sobre este tópico, pues así la naturaleza del proceso sumario de amparo de derechos fundamentales que pretende ser expedito debería prever el conocimiento y resolución judicial por jueces individuales que están mas cerca de la población y a los asuntos que aquejan a los ciudadanos o personas a quienes se les niega, desconoce, limita o restringe el derecho de acceso a la información, por ahora sólo pública.

5. El HABEAS DATA URUGUAYO EN LA LEY DE PROTECCION DE DATOS PERSONALES DE CARÁCTER FINANCIERO

La República del Uruguay mediante la Ley No. 17938 de Octubre 1º de 2004, reglamentó y desarrolló legislativamente el Hábeas Data para la protección de los datos personales de carácter financiero, constituyéndose así en una de las más recientes leyes suramericanas que enfatiza en el dato financiero, como una especie del género de datos de la persona humana.

5.1. Estructura de la LPDP_HDU

La Ley No. 17938 de Octubre 1º de 2004 o "*Ley de protección de datos personales para ser utilizados en informes comerciales y el Hábeas Data*" del Uruguay (LPDP_HDU), esta estructurada en títulos, capítulos y artículos que regulan los siguientes contenidos:

En el **Título I, Capítulo I,** relativo a la **"*Protección de datos personales de informes comerciales",*** la LPDP_HDU, en los artículos 1º y 2º regula objeto de la ley y sus excepciones. La ley tiene como objetivo reglamentar las fases del tratamiento de datos personales (el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración), cuando se hallen en archivos, bases de datos, u otros "medios similares autorizados" (se entenderá en escritos, documentos tradicionales, o "informes"), sean éstos públicos o privados, "*destinados a brindar informes de carácter comercial*".

Por oposición, se exceptúan del anterior objeto, los siguientes datos o informaciones de la persona humana: (i) los datos de carácter personal que se originen en el ejercicio de las

libertades de emitir opinión y de informar; (ii) los relativos a encuestas, estudios de mercado o semejantes; y, (iii) los datos sensibles sobre la privacidad de las personas

En el **Capitulo II,** concerniente a los **"*Principios Generales",*** la ley uruguaya describe a espacio, en los artículos 3º a 7º los principios rectores que rigen al tratamiento de datos de las personas físicas y jurídicas, tales como: (i) De licitud de los datos; (ii) El consentimiento de los titulares, como regla, con sus excepciones *numerus clausus o* taxativas [30]; (iii) Proporcionalidad y finalidad de los datos; (iv) Utilización adecuada y proporcionada de datos; (v) Secreto o sigilo profesional de los datos.

En el **Capítulo III**, concerniente al "***Tratamiento de datos personales relativos a las obligaciones de carácter comercial",*** previsto en los artículos 8º a 11º se precisa que el tratamiento de datos personales regulado en la LPDP_HDU abarca el cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permiten evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor sin consentimiento del titular.

El registro de los datos comerciales sólo podrá estar registrado en las bases de datos por el término de cinco años.

Cuando se cancele una obligación, el acreedor estará obligado a comunicarla al responsable del banco de datos en un plazo máximo de diez (10) días. El receptor de esta información tiene un plazo máximo de tres (3) días para actualizar la información.

En el **Título II**, referente al *"**Hábeas Data y Órgano de Control"*,** Capítulo I sobre el "*Hábeas Data"*, previsto en los artículos 12º a 16º de la ley, se define la acción de Hábeas Data como un derecho ejercitable por toda persona física y jurídica y se describe su objeto así: (i) Tomar conocimiento de los datos personales de carácter comercial; (ii) Se averigua la finalidad y el uso dado a dichos datos; (iii) Si se trata de datos amparados por el secreto, el Juez "apreciará" el levantamiento del mismo según el caso y circunstancias; y (iv) A la

---

(30) Según el artículo 4º de la Ley No.17.838, No requiere previo consentimiento el registro y posterior tratamiento de datos personales cuando: (i) Los datos provengan de fuentes públicas de información, tales como registros, archivos o publicaciones en medios masivos de comunicación; (ii) Sean recabados para el ejercicio de funciones o cometidos constitucional y legalmente regulados propios de las instituciones del Estado o en virtud de una obligación específica legal; (iv) Se trate de listados cuyos datos se limiten a nombres y apellidos, documento de identidad o registro único de contribuyente, nacionalidad, estado civil, nombre del cónyuge, régimen patrimonial del matrimonio; (v) fecha de nacimiento, domicilio y teléfono, ocupación o profesión y domicilio; (vi)

rectificación, actualización y la eliminación o supresión de los datos personales que le conciernan, cuando estando incluidos en bases de datos, éstos lo estén por error o falsedad en la información.

En el **Capítulo II,** relativo a la *"Acción de protección de datos personales",* contenida en los artículo 17º a 19º, se describe la titularidad de la acción para toda persona física o jurídica, los casos en los que puede impetrarse y las normas del proceso a seguirse: (i) normas del Código General del Proceso; y (ii) Normas especiales de la LPDP_HDU y las previstas en la Ley No. 16.011 de 19 de diciembre de 1998, es decir, en la Ley de amparo uruguaya [31].

En tal virtud, la acción de Hábeas Data para la protección de datos financieros constituye adjetivamente hablando configura una acción de amparo específica que genera un proceso jurisdiccional de amparo especial, con formas y ritualismos generales previstos en el Código General del Proceso y con ritos especiales previstos en la Ley de amparo.

En el **Capítulo III**, concerniente a los "***Órganos de Control"***, describe en los artículos 20º a 21º, la competencia y jurisdicción del Ministerio de Economía y Finanzas del Uruguay, el cual está asesorado por una comisión consultiva compuesta por integrantes del Ministerio de Economía, del Ministerio de Educación y Cultura, La Cámara Nacional de Comercio y la Liga de defensa Comercial. Además, se puntualiza las funciones y las diversas sanciones que puede aplicar a quienes incumplieren los predicamentos de la LPDP_HDU. Sanciones que van desde el apercibimiento hasta la clausura de la base de datos.

En el **Título III**, referente a las "***Disposiciones finales y transitorias"***, previstas en los artículos 22º a 26º, se describe además de la tabla de vigencia de la ley, siguientes aclaraciones: (i) que la LPDP_HDU, no rige para los registros públicos y similares creados por leyes especiales; (ii) que los responsables de bancos de datos públicos y privados existentes tendrán un plazo de 90 días, a partir de la promulgación de la ley, para inscribir dichos bancos en el Registro General; (iii) Igual término, tendrán los responsables de los bancos de datos, para actualizar la información y en el evento de los "datos caducos" para eliminarlos; (iv) Los acreedores de obligaciones ya canceladas dispondrán del término de 10 días hábiles para comunicar dicha eventualidad a los responsables de los bancos de

---

(31) A tenor del artículo 1º de la Ley de Amparo, "Cualquier persona física o jurídica, pública o privada, podrá deducir la acción de amparo contra todo acto, omisión o hecho de las autoridades estatales o paraestatales, así como de particulares que en forma actual o inminente, a su juicio, lesione, restrinja, altere o amenace, con ilegitimidad manifiesta, cualquiera de sus derechos y libertades reconocidos expresa o implícitamente por la Constitución (artículo 72), con excepción de los casos en que proceda la interposición del recurso de "habeas corpus". La Acción de amparo uruguaya es de carácter jurisdiccional y subsidiaria. Conocen de ella, los Jueces letrados de primera instancia de la materia que corresponda el acto, hecho u omisión impugnados y el lugar donde estos produzcan sus efectos. Es subsidiaria, porque sólo podrá interponerse cuando no existan otros medios judiciales o administrativos que permitan obtener el mismo resultado de ésta acción.

datos; y (v) El poder ejecutivo dispondrá de 180 días para reglamentar la ley.

5.2. Breves comentarios a la LPDP_HDU de 2004

5.2.1. Notas preliminares. En particular, el proyecto de Hábeas Data de 2002

Uruguay como la mayoría de países de América Latina, antes de expedir una norma sobre protección de datos personales, experimentó con una cantidad de proyectos de diferente origen y matriculados a diferentes escuelas normativas globales que regulan estas materias técnico-jurídicas. Los anteproyectos y proyectos que regulaban la protección de datos en forma genérica, o el derecho de Hábeas Data en forma específica, tenía como común denominador, desarrollar legislativamente conjuntamente con aquellos, el derecho al acceso a la información pública o de interés colectivo y la información privada. Todo por cuanto, los datos de la persona humana tratados a través de las nuevas tecnologías de la información y la comunicación (TIC), la informática y el derecho público posibilitaban una nueva y específica reglamentación que más temprano que tarde debían abordar los Estados no sólo latinoamericanos sino del mundo.

Cierto es, como sostiene algún sector de la doctrina [32], que Uruguay era el único Estado del MERCOSUR que no había expresamente elevado a rango constitucional el Hábeas Data, pero eso no impedía que por vía de interpretación sistemática de la Constitución, toda persona tenga derecho a solicitar tutela del Estado para la protección de los datos personales que le conciernen cuando se hallen recolectados, almacenados o comunicados en bancos de datos, por error, inexactitud, falsedad o cuando se hayan realizado sin el consentimiento del titular o sin la“ previa conformidad de los titulares”, como dijera más tarde el inciso in fine del artículo 2º de la LPDP_HDU.

Un proyecto de Hábeas Data, publicado en la Internet [33], deja ver cómo la intención del legislador uruguayo en el año 2002, era reglamentar la protección de los datos personales recabados en bases o bancos de datos tanto de carácter público, como de carácter privado, a la par con el derecho de acceso a la información y el derecho de petición en interés particular, en interés general, al igual que el derecho de petición de informaciones y de consulta de actos y contratos administrativos (o mejor “estatales”) de la administración nacional, regional y local. Esto último para ponerse a tono con los países vecinos del cono sur de América en lo relativo a leyes de transparencia en la gestión pública y la implantación de mecanismos idóneos contra la corrupción pública.

---

(32) DAPKEVICIUS, Rubén Flórez. ***Protección de Datos Personales de Informes Comerciales: Ley 17838 de Uruguay.*** **Invitado en el WEB: El Derecho Público Mínimo. En: http://www.udenar.edu.co/derechopublico**

(33) En: http://www.privacyinternational.org/countries/uruguay/Proyecto-ley-Habeas-Data-1002.pdf.

La regulación del derecho de acceso a la información, el derecho de petición y la protección de datos de carácter personal en el proyecto de 2002, era amplia, genérica y aplicable a toda clase de datos personales, salvo los del “núcleo duro” de la intimidad o privacidad que estaban exentos de tratamiento de datos o de tratamientos restringido con potenciación en la protección en algunas fases del tratamiento, como por ejemplo, la comunicación de datos, tal como existe en el derecho continental europeo y en particular en las normas de protección de datos española de 1992 y 1999.

El proyecto además, reglamentaba la acción de Hábeas Data en dos estadios de su existencia, como lo hemos sostenido ut supra en este ensayo jurídico; es decir, en el ámbito administrativo y en el jurisdiccional. Así se desprende de la lectura de los artículos 12º y 13º del proyecto citado cuando sostiene que “el peticionante” podrá ejercer la acciones de Hábeas Data en los siguientes casos: 1) Cuando hayan transcurrido quince días corridos a contar desde la resolución denegatoria de la información solicitada ; y, 2) Cuando se haya agotado el plazo a que se refiere el artículo 8 º (es decir, “la petición que recibiere deberá expedirse en un plazo máximo de cuarenta y cinco días hábiles de recibida la misma“) sin pronunciamiento de la autoridad requerida.

Una vez conocida por los interesados la información relacionada con su persona y archivada por organismos estatales o personas públicas de derecho privado, nacionales o departamentales, ya sea por resolución de los mismos o por orden judicial, aquellos, si consideren que la información es errónea o su recolección y archivo fuera ilegal, o la posesión o uso de la misma pueda causar perjuicio, lo que harán saber a los organismos o personas antes indicados en plazo que no podrá exceder los quince días hábiles a contar desde el siguiente al de su conocimiento.

Y agregaba el inciso 2º del artículo 13º del proyecto que vencido el plazo sin contestación, o si ésta fuera negativa, los interesados podrán promover la acción de “Hábeas Data” con el fin de modificar o eliminar la información errónea o ilegal, la que se interpondrá dentro de los plazos y se sustanciará según las formalidades previstas en esta ley.

El legislador Uruguayo de 2004, finalmente se decidió por expedir una Ley de Protección de datos personales y Hábeas Data, con expreso énfasis en los datos de carácter financiero, aunque la norma alude al término comercial, como pasamos a ver.

5.2.2. Ley de protección de datos de carácter financiero

La LPDP_HDU de 2004, es una típica ley que enfatiza en la protección de los datos financieros de la persona no sólo física o natural, sino de la persona moral, “ideal” o jurídica. Quizá por ello, en el ámbito latinoamericano es la primera de las últimas leyes dictadas con ese claro sabor económico, basado el legislador uruguayo, a buen seguro, en

el fenómeno de la globalización de la economía, el tracto financiero público y privado cada vez más decisivo en la gestión y acciones estatales como las del ámbito particular individual o empresarial, así como en los crecientes, fructíferos y productivos negocios de capitales, bienes y servicios en los cuales están involucrados entidades públicas, privadas y mixtas del sector bancario, bursátil y crediticio y llueven –si nos permiten el término— obligaciones constantes en títulos valores, bonos del estado y dinero líquido.

Hoy en día, el pago de un medio de transporte, la compra de un inmueble o acción, la venta de un servicio hotelero, el pago y/o cobro de un tributo, el pago y/o cobro de un servicio público doméstico o el crédito personal de tarjeta, son muestran inequívocas del impacto que actualmente tiene las acciones, gestiones o actividades financieras en la vida de las personas humanas y jurídicas, y como tal cada una de ellas genera una huella, un dato o una información que puede ser recolectada, seleccionada, almacenada, registrada o comunicada a través de un procedimiento o tratamiento de datos tradicional o escrito, o electrónico o informático.

Estos entronques de las finanzas públicas y privadas con las nuevas tecnologías de la información y la comunicación (TIC) y la informática (telegestión, telemática o electrónica), es lo que ha cautivado últimamente a los Estados del mundo, para expedir normas proteccionistas de derechos o libertades fundamentales que pudieren verse afectadas por el abuso, extralimitación o exageración del llamado “poder informático”. Uruguay en Suramérica es de los primeros países que quedó impactado por el fenómeno jurídico y las finanzas y por ello se decidió en legislar sobre ese entronque anotado, antes que por la protección genérica de los datos de la persona humana y jurídica no financieros. Más aún en la LPDP_HDU esta clase de datos han quedado excluidos expresamente en el artículo 2º, cuando sostiene:

Quedan excluidos de la aplicación de la Ley, los siguientes datos: (i) los datos de carácter personal que se originen en el ejercicio de las libertades de emitir opinión y de informar; (ii) los relativos a encuestas, estudios de mercado o semejantes, los que se regularán por las leyes especiales que les conciernan y que al efecto se dicten; y (iii) los datos sensibles sobre la privacidad de las personas, entendiéndose por éstos, aquellos datos referentes al origen racial y étnico de las personas, así como sus preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o información referente a su salud física o a su sexualidad y toda otra zona reservada a la libertad individual.

Aclara la Ley de 2004, que solo será procedente recolectar y aplicar el tratamiento o procesamiento de datos en estas clase de datos no comerciales, cuando el titular lo consienta en forma “expresa y previa”, luego que sean informados del “*fin y alcance del registro en cuestión*”. Esto porque obviamente son datos que pueden afectar el “núcleo duro” de la intimidad o los derechos fundamentales de la persona humana.

Con estas exclusiones y aclaraciones expresas de la Ley uruguaya de 2004, se entiende que el legislador postergó la tarea de reglamentación y desarrollo legal de la protección de datos personales no comerciales o financieros. Por ahora, se ha legislado sobre el tema de actualidad mundial: las finanzas públicas y privadas.

La LPDP_HDU de 2004, desde el intitulado y el contenido mismo de la norma, se marca la impronta de ser una ley reguladora de datos financieros, aunque se empecina en nominarlos como datos comerciales.

El dato financiero como anotábamos *ut supra*, es aquélla información concerniente a una persona determinada o determinable que tiene características económicas, comerciales, tributarias, o en general de índole financiera, bien sea en el ámbito privado o en el público. Genéricamente esto dato financiero, pues según el diccionario el término financiero puede definirse como lo *perteneciente o relativo a la Hacienda pública, a las cuestiones bancarias y bursátiles o a los grandes negocios mercantiles"*, con lo cual se entiende que los datos financieros engloban terminológicamente a los efectos de este ensayo, lo que entendemos por dato económico, comercial, bancario, bursátil y tributario público y privado.

En la Ley Uruguaya para que no quepa la duda de si se puede o no someter a tratamiento manual o electrónico los datos financieros de las personas humanas o jurídicas, determinó en el artículo 8º que queda "*expresamente autorizado el tratamiento de datos personales*", bien sea sobre el cumplimiento o el incumplimiento de obligaciones de carácter comercial o crediticia. Con lo cual legalmente se excluye el consentimiento de las personas concernidas con dicha información, que a partir de la Ley de datos financieros de 2004, pueden tratarse sin la "conformidad", "autorización" o consentimiento escrito y expreso del concernido.

Esta apertura uruguaya al tratamiento de datos financieros, tiene como objetivos inmediatos el que las entidades financieras puedan recabar la información pertinente dentro de este mundo globalizado de la economía y la rapidez y efectividad de la información que se necesita en toda clase de actividades donde medie el capital, para evaluar la concentración de negocios en general, la conducta comercial (no la valoración subjetiva del titular de los datos) o la capacidad de pago del titular de los datos, siempre y cuando la información se obtenga de "fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor, aparte de las eventualidades que la regla general, sin el consentimiento del titular de los datos.

El dato financiero tiene unas características especiales en todas las fases del tratamiento o procesamiento de datos personales, aparte de las anotadas en la fase de recolección.

En la fase de registro de la información, el dato financiero tendrá un plazo de cinco (5) años, contados a partir de su incorporación a la base, fichero o banco de datos respectivo. Solo en el evento en que la obligación persista en el incumplimiento, el acreedor podrá solicitar válidamente al responsable del banco, treinta días antes del vencimiento del plazo inicial, la permanencia por otros cinco (5) años más improrrogables, según el artículo 9º de la LPDP_HDU. Este plazo inicial y el de la prórroga generan la vigencia y la vida útil del dato, pues ningún dato o información deberá ser perenne, ni por tiempo indefinido.

Por esta razón, las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción, según lo dispone el inciso *in fine* del artículo 9º.

Cuando se haga efectiva la cancelación de cualquier obligación incumplida registrada en una base de datos, el acreedor deberá en un plazo máximo de diez días hábiles de acontecido el hecho, comunicarlo al responsable de la base de datos correspondiente.

Una vez recibida la comunicación por el responsable, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación.

6. EL HABEAS DATA PERUANO EN EL CODIGO PROCESAL CONSTITUCIONAL DE 2OO4

6.1. Notas preliminares

El lunes 31 de Mayo de 2004, con demasiados bombos y platillos el Estado Peruano, estrenó la única norma en su género en el ámbito Latinoamericano, conocida como “Código Procesal Constitucional”, el cual compila sistemática y coherentemente los procedimientos constitucionales generados por las acciones de Hábeas Corpus, Amparo, Hábeas Data y de cumplimiento; así como también las acciones de inconstitucionalidad y acciones populares. De igual forma, la jurisdicción y competencia, reglas generales y especiales que las autoridades judiciales deben observar al avocar, desarrollar y resolver los procedimientos correspondientes.

La Ley No. 28237 de 2004, tuvo origen en diferentes motivaciones de tipo doctrinal, jurisprudencial e incluso legislativo, sobre las cuales los juristas peruanos han escrito obras jurídicas de relevancia. En nuestro criterio, el Código Procesal Constitucional peruano o CPCP, tiene inequívocas finalidades de concentración temática al compilar instrumentos adjetivos idóneos para proteger y garantizar derechos fundamentales, así mismo objetivos normativos de unidad jurídica de acciones, recursos o instrumentos procesales diferentes

en su origen, pero homologables o equiparables a través de un mismo hilo procedimental o *iter procesalis* genérico que admite peculiaridades o reglas especiales para todas o cada una de las instituciones que no pierden su autonomía y diferencia. Esta nueva técnica legislativa de compilación de instituciones jurídicas diferentes en su origen pero equiparables en sus procedimientos es loable, práctica, altamente eficiente para el operador jurídico y relevantemente pedagógico para el titular de un derecho o interés legítimo que lo estime amenazado, vulnerado, limitado o restringido por un acto, hecho u omisión de una autoridad, entidad u organismo del Estado o por los particulares con funciones o servicios públicos, por excepción.

Como es apenas obvio, el CPCP de 2004, reglamenta y desarrolla la garantía y acción constitucional de Hábeas Data, en el ámbito estrictamente procedimental. Por ello, para analizar la institución jurídica del Hábeas Data en forma integral, hay que recurrir a la Ley de Transparencia y Acceso a la información Pública peruana (LT y AIP) o Ley No.27806 de 13 de Julio de 2002, la cual tiene por finalidad además de promover la transparencia de los actos, contratos, gestiones y acciones del Estado, la encomiable labor de reglamentar el derecho fundamental de acceso a la información consagrada en el numeral 5º del artículo 2º de la Constitución Peruana, es decir, el derecho de toda persona a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

En efecto, la LT y AIP de 2002 [34], regula la parte sustantiva del Hábeas Data, pues allí el legislador peruano regula el derecho fundamental de información en general y en particular sobre la información de acceso público [35], la legitimación por activa y por pasiva de la información, las autoridades o entidades del Estado obligadas a dar cumplimiento al acceso a la información pública, los principios rectores de la información veraz, oportuna, lícita, clara, exacta que deben entregar las entidades estatales y a su vez, recibirla los titulares o concernidos con la misma; el régimen de sanciones y responsabilidades que asumen titulares, usuarios y administradores de la información; los extensísimos y quizá cuestionables regímenes excepcionales al acceso a la información pública, cuando ésta se considera “secreta”, “reservada” y “confidencial”; la regulación amplia y pormenorizada de

---

(34) Texto completo de la norma En: http://www.pcm.gob.pe/Transparencia/

(35) El Artículo 10 de la LT y AIP, considera la Información de acceso público, aquella que las entidades de la Administración Pública tienen la obligación de proveer la información requerida si se refiere a la contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro formato, siempre que haya sido creada u obtenida por ella o que se encuentre en su posesión o bajo su control. Agrega, el inciso 2º Asimismo, para los efectos de esta Ley, se considera como información pública cualquier tipo de documentación financiada por el presupuesto público que sirva de base a una decisión de naturaleza administrativa, así como las actas de reuniones oficiales.

la información de las finanzas, el régimen fiscal y presupuestal del Estado; entre muchas otras aristas del derecho a la información.

La LT y AIP posibilita el ejercicio de la acción de Hábeas Data, solo cuando se ha agotado el no fácil y expedito "procedimiento" común o administrativo de acceso a la información pública.

En efecto, el artículo 11º de la mentada ley, sostiene que el acceso a la información pública esta sujeta al siguiente procedimiento: (i) Toda solicitud de información debe ser dirigida al funcionario designado por la entidad de la Administración Pública para realizar esta labor. En caso de que éste no hubiera sido designado, la solicitud se dirige al funcionario que tiene en su poder la información requerida o al superior inmediato; (ii) La entidad de la Administración Pública a la cual se haya presentado la solicitud de información deberá otorgarla en un plazo no mayor de siete (7) días útiles; plazo que se podrá prorrogar en forma excepcional por cinco (5) días útiles adicionales, de mediar circunstancias que hagan inusualmente difícil reunir la información solicitada. En este caso, la entidad deberá comunicar por escrito, antes del vencimiento del primer plazo, las razones por las que hará uso de tal prórroga, de no hacerlo se considera denegado el pedido. En el supuesto de que la entidad de la Administración Pública no posea la información solicitada y de conocer su ubicación y destino, esta circunstancia deberá ser puesta en conocimiento del solicitante; (iii) La denegatoria al acceso a la información se sujeta a lo dispuesto en el segundo párrafo del artículo 13º de la presente Ley; (iv) De no mediar respuesta en los plazos previstos en el inciso b), el solicitante puede considerar denegado su pedido; (v) En los casos señalados en los incisos c) y d) del presente artículo, el solicitante puede considerar denegado su pedido para los efectos de dar por agotada la vía administrativa, salvo que la solicitud haya sido cursada a un órgano sometido a superior jerarquía, en cuyo caso deberá interponer el recurso de apelación para agotarla; (vi) Si la apelación se resuelve en sentido negativo, o la entidad correspondiente no se pronuncia en un plazo de diez (10) días útiles de presentado el recurso, el solicitante podrá dar por agotada la vía administrativa; (vii) Agotada la vía administrativa, el solicitante que no obtuvo la información requerida podrá optar por iniciar el proceso contencioso administrativo, de conformidad con lo señalado en la Ley Nº 27584 u optar por el proceso constitucional del Hábeas Data, de acuerdo a lo señalado por la Ley Nº 26301.

Por ahora nos dedicaremos al estudio del proceso constitucional originado en la acción de Hábeas Data, o dicho de otro modo, a la visión jurisdiccional o procedimental del Hábeas Data.

6.2. Estructura de la Ley No. 28237 o Código Procesal Constitucional del Perú

Si bien vamos a relacionar la estructura general del CPCP de 2004, eso no obsta que hagamos énfasis en aquellos apartes referidos a la acción o "proceso constitucional" de Hábeas Data, que es el objeto general de nuestro ensayo jurídico.

El CPCP tiene una estructura de extenso *Codex* y está dividió en Títulos, Capítulos, Artículos, numerales, literales y parágrafos. Contiene un Título preliminar y trece Títulos, y por su puesto disposiciones transitorias y tabla de vigencia.

El **Título Preliminar** en los artículos I a IX, regula el alcance, fines y principios de los procesos constitucionales; los órganos del poder judicial competentes; el entendimiento que debe darse a la interpretación constitucional y el control difuso; la sentencia del Tribunal constitucional como precedente en el derecho público peruano y la aplicación supletoria de los Códigos procesales de la materia objeto del cuestionamiento constitucional.

En el **Título I,** relativo a las ***"Disposiciones generales de los procesos de Hábeas Corpus, Amparo, Hábeas Data y cumplimiento"***, en el artículo 1º al 24, hace referencia a la finalidad, procedencia frente a actos basados en normas o respecto de resoluciones judiciales, las causales de improcedencia, la cosa juzgada, la representación procesal del Estado, la responsabilidad del agresor, la ausencia de etapa probatoria, las excepciones y defensas previas, la integración decisiones, el turno, la tramitación preferente, notificaciones, medidas cautelares, extinción de la medida cautelar, sentencia, recursos de agravio constitucional y de queja, el pronunciamiento del Tribunal Constitucional, la incorporación de medios probatorios sobre hechos nuevos al proceso, actuación de sentencias, procedencia durante los regímenes de excepción y agotamiento de la jurisdicción nacional.

El **Título II,** concerniente al "***Proceso de Hábeas Corpus",*** *c*ontiene dos capítulos. En **el Capítulo I**, sobre los ***"Derechos protegidos"***, en el artículo 25º, relaciona "enunciativamente" los derechos a la libertad individual de las personas protegidas por Hábeas Corpus. En el Capítulo II, sobre "***el Procedimiento"***, en los artículos 26º a 36, relaciona las partes y fases del proceso, la legitimación activa y pasiva, trámite y recursos.

El **Título III,** relativo al **"Proceso de Amparo"**, contiene dos capítulos. En el Capítulo I, relativo a los "***Derechos protegidos",*** en los artículos 37º a 38º , enumera los derechos en los que procede el amparo; entre otros, el honor, la información, la intimidad, las informaciones inexactas o agraviantes, la libertad de cátedra, etc. En el Capítulo II, referente al ***"Procedimiento"***, en los artículos 39 a 60, menciona la legitimación, la representación procesal, la procuraduría oficiosa, requisitos y plazo para interposición de la demanda, acumulación subjetiva de oficio; el no menos discutible aspecto de "agotamiento

de las vías previas" y excepciones al mismo; la improcedencia liminar; inadmisibilidd, abandono y reconvención; Juez competente, plazos para decidir, trámites y recursos.

El **Título IV**, referente al ***"Proceso de Hábeas Data"***, en los artículos 61 a 65, describe los derechos protegidos a través de este mecanismo constitucional y que se concreta en los siguientes: (i) Acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material; (ii) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros; y (iii) a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

Así mismo, se relacionan en éste capítulo los requisitos especiales que debe reunir la demanda en ejercicio de la acción de Hábeas Data; también una especie de medidas cautelares, que el legislador peruano, llama "ejecución anticipada"; la acumulación de pretensiones de conocer y acceder a la información, con las de actualizar, rectificar o eliminar información o de impedimento de entrega de informaciones; y finalmente, la homologación del procedimiento de amparo al procedimiento de Hábeas Data.

El **Título V**, relativo al ***"Proceso de cumplimiento"***, en los artículos 66 a 74 describe el objeto, la legitimación activa y pasiva, representación, requisitos especiales de la demanda, causales de improcedencia, desistimiento de las pretensiones, contenido de la sentencia, ejecución de la sentencia y aplicabilidad del procedimiento de amparo a la acción de cumplimiento.

El **Título VI,** concerniente a "***Disposiciones generales de los procesos de acción popular e inconstitucionalidad"***, en los artículos 74º a 83, referencia la finalidad y procedencia de la acción popular y la de inconstitucionalidad, principios de interpretación, efectos de la sentencia, cosa juzgada y efectos de la irretroactividad.

El **Título VII,** referente a la ***"Acción Popular",*** en los artículos 84 a 97, relaciona la legitimación activa y pasiva, la competencia, requisitos de la demanda, admisibilidad e improcedencia, emplazamiento y publicación de la demanda, contestación, vista de la causa, recursos, medidas cautelares y sentencia.

El **Título VIII**, relativo a la ***"Acción de Inconstitucionalidad"***, en los artículos 98 a 108, menciona la legitimación y competencia de la acción, representación *ad procesum*; la demanda, anexos, inadmisibilidad y su improcedencia *Ad limine*; improcedencia de medidas cautelares, trámite y sentencia.

El **Título IX**, concerniente al ***"Proceso competencial"***, en los artículos 109º a 113, relaciona los procesos generados por los conflictos de competencias administrativas entre los órganos del Estado. Así mismo, sobre las pretensiones, medidas cautelares, causales de improcedencia y efectos de la sentencia.

El **Título X**, referente a la "***Jurisdicción Internacional"***, en los artículos 114º a 116º, hace mención a los organismos internacionales competentes para tutelar los derechos fundamentales de los peruanos, cuando han agotado las vías administrativas y jurisdiccionales internas, el Comité de Derechos Humanos de las Naciones Unidas, la Comisión Interamericana de Derechos Humanos de la Organización de Estados Americanos, por ejemplo.

El **Título XI**, relativo a las "***Disposiciones generales aplicables a los procedimientos ante el Tribunal Constitucional"***, en el artículo 117º al 121º, menciona la acumulación de procesos, numeración de sentencias, solicitud de información del Tribunal a los organismos del Estado, subsanación de vicios de procedimiento y el carácter inimpugnable de las sentencias del Tribunal.

El **Titulo XII**, concerniente a las "***Disposiciones finales"*** de la primera a la séptima, se mencionan aspectos que por técnica legislativa no pudieron incrustarlos en los títulos referidos a disposiciones, reglas o principios generales o aspectos que deberían ir en el título preliminar. Por ello, se menciona "las denominaciones empleadas" a lo largo de la ley, los jueces especializados, publicación de sentencias, aspectos de pedagogía constitucional en centros educativos y la gaceta constitucional.

El **Título XIII**, referente a las "***Disposiciones Transitorias y derogatorias".*** Se derogan expresamente 15 leyes y se dispone la vigencia después de 6 meses de la publicación.

6.3. Breves comentarios a la parte pertinente del Hábeas Data en el CPCP de 2004

El CPCP le dedica específicamente el Título IV al Hábeas Data, pero también le dedica inmerso con otras acciones constitucionales, el Título I, para hacer mención a las disposiciones generales que rigen al proceso constitucional originado en la acción o garantía constitucional de Hábeas Data, aunque por disposición final (Titulo XIII), sostiene que se "denominará" proceso de Hábeas Data a la acción de Hábeas Data. Asimilación

terminológica que parece conllevar el cambio de naturaleza jurídica del Hábeas Data peruano.

Por eso, en el presente aparte haremos un análisis sucinto de los aspectos relacionados en los artículos 61 a 65 del CPCP, con las consiguientes remisiones a la Constitución Peruana de 1993.

6.3.1. El procedimiento de amparo específico o de Hábeas Data

Desde el punto de vista procedimental es aplicable al Hábeas Data según el artículo 65 del CPCP, el Título III relativo al "*Proceso de Amparo*" en toda su extensión (artículos 39 a 60 ibidem), es decir en cuanto a la iniciación, desarrollo, sustanciación, recursos y sentencia del procedimiento de Hábeas Data, éste se tramitará conforme a las formas y ritualidades del proceso de amparo, salvo lo previsto en forma específica en los artículos 61 a 64 del CPCP, vale decir sobre objeto de la acción de Hábeas Data, las medidas cautelares y la acumulación de pretensiones, propias del proceso de Hábeas data. Lo cual quiere decir, que el proceso de Hábeas Data es mixto en el derecho peruano y está compuesto por parte genérica aplicable todos los procesos de amparo, y una parte específica, aplicable en forma exclusiva y excluyente al proceso de Hábeas Data.

El procedimiento constitucional de amparo peruano, lejos de ser un proceso sumario, expedito y altamente garantizador del derecho fundamental y garantía constitucional de Hábeas Data, se erigió en el CPCP, con una serie de etapas normales y contingentes para todo procedimiento constitucional ordinario, digno de estudiarse en una obra jurídica autónoma y separada a la presente. En tal virtud por ahora, solo nos permitimos relacionar casi gráficamente las etapas de dicho proceso para demostrar nuestra crítica.

Tiene unas etapas normales u obligatorias del proceso como son la de litis contestatio y la de juzgamiento. La etapa de *litis contestatio,* compuesta por la: (i) demanda con requisitos generales y especiales, plazo para su interposición, agotamiento de vías previas y excepciones mínimas a éste; y, (ii) Contestación de la demanda. La Etapa de Juzgamiento constituida por la sentencia, salvo que se haya formulado solicitud de informe oral.

Tiene como etapas contingentes o facultativas: (i) Inadmisibilidad de la demanda; (ii) desistimiento; (iii) impedimentos del juez; (iv) intervención litisconsorcial; (v) Adopción de medidas cautelares; y, (vi) procedimiento para represión de actos homogéneos; además de las circunstancias procesales contingentes de acumulación subjetiva de terceros y acumulación de procesos.

6.3.2. El Objeto del procedimiento constitucional de Hábeas Data

Sobre el objeto y el extravasamiento del CPCP, respecto de la reglamentación de la garantía constitucional del Hábeas Data, previsto en el artículo 200 de la Constitución Peruana, ya nos hemos referido al hacer los comentarios pertinentes a ésta en la Parte Segunda de esta obra, y por ello, sólo adicionemos aquí, que el CPCP concreta un objetivo amplio que puede ser mejorado, si se reglamenta el artículo 200-3º en su integridad (no sólo los numerales 5º y 6º del artículo 2º de la Constitución incorporado al artículo 200-3º y reglamentado en el artículo 61 del CPCP, sino también el numeral 7º [36] que es omitido en dicha reglamentación legal) pues hoy por hoy, la acción de Hábeas data sólo procede en las fases de conocimiento y acceso de la información, de solicitud de actualización, rectificación y cancelación de la misma y en las eventualidades de solicitar la supresión de las informaciones o de impedir que sean sometidas a tratamiento de datos, ciertas informaciones sensibles o privadas cuando con ellas se amenacen, vulneren o desconozcan derechos fundamentales de la persona.

El numeral 5º del artículo 2º de la Constitución Peruana de 1993, sostiene que toda persona tiene derecho: "A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional". Y agrega el inciso 2º: "El secreto bancario y la reserva tributaria pueden levantarse a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado".

Por su parte, el numeral 6º del artículo 2º constitucional, sostiene que toda persona tiene derecho: "*A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*".

Tanto en el numeral 5º como en el 6º, la Constitución preserva bienes jurídicos y derechos fundamentales tales como el derecho de acceso a la información pública o de interés colectivo y privada o de interés individual y el derecho a la intimidad personal y familiar. Derechos constitucionales autónomos que gozan de protección *per se,* por sus

---

(36) El numeral 7º del artículo 2º de la Constitución sostiene que toda persona tiene derecho: "Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Agrega el inciso 2º, "Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley". Pues en este caso también procede la acción de Hábeas Data como mecanismo idóneo y potenciado de protección y garantía constitucional y legal de los mencionados derechos fundamentales, más cuantos se hace mención a informaciones inexactas o agraviantes por cualquier medio TIC. Esto sin perjuicio e independencia que éstos derechos fundamentales tienen en ejercicio de su autonomía, protección y garantía constitucionales por medio de la acción de amparo. Si se hubiese éste numeral 7º en el artículo 61 CPCP, los derechos fundamentales allí mencionados gozaran hoy de una protección ultrapotenciada que la necesitan ante el avance y la alta porosidad de las TIC y la informática en el derecho.

connotaciones especiales, su caracterización de derechos de la persona humana y jurídica (el de la información) o de personalísimos del ser humano (el de intimidad), por ser de aplicación inmediata y por estar garantizados por el Estado a toda persona habitante, residente o transeúnte en el país. Además gozan de la protección reforzada a través del mecanismo administrativo del derecho de petición ante cualquier autoridad del Estado y del mecanismo jurisdiccional de la acción de amparo, según el CPCP. Pero además, tienen un ámbito de ultraprotección, por disposición del artículo 200-3º de la Constitución, cuando entran en entronque el abuso, irregular, indebido o ilegal tratamiento de datos o informaciones personales por medios TIC y la informática (abuso del "poder informático"). Es entonces, en este momento que los derechos fundamentales enunciados en los numerales 5, 6 y 7º del artículo 2º obtienen una ultraprotección constitucional y legal que le es negada parcialmente al los derechos constitucionales del numeral 7º , por omisión del legislador peruano o por disposición y a sabiendas de su exclusión. La doctrina peruana tiene la palabra sobre este punto.

6.3.3. Requisitos especiales de la demanda de Hábeas Data

Ahora bien, en cuanto a los requisitos de la demanda en el "proceso constitucional de Hábeas Data", el CPCP, redirige en principio a los requisitos generales previstos para la acción de amparo, los cuales están previstos en el artículo 42 en forma enunciativa, al emplear el término "*cuando menos*" para referirse a que la demanda por escrito, con sus "datos y anexos", podrá ser presentada por quien se halle legitimado para hacerla y cuando reúna los siguientes requisitos: (i) La designación del Juez ante quien se interpone; (ii) El nombre, identidad y domicilio procesal del demandante; (iii) El nombre y domicilio del demandado, sin perjuicio de lo previsto en el artículo 7 del CPCP, sobre representación procesal del Estado; (iv) La relación numerada de los hechos que hayan producido, o estén en vías de producir la agresión del derecho constitucional; (v) Los derechos que se consideran violados o amenazados; (vi) El petitorio, que comprende la determinación clara y concreta de lo que se pide; (vii) La firma del demandante o de su representante o de su apoderado, y la del abogado.

Estos requisitos son los que normalmente se exigen para la presentación de cualquier tipo o clase de demanda ante autoridades jurisdiccionales, en cualquier Estado del mundo.

Agrega el inciso in fine del artículo mencionado, que "*en ningún caso la demanda podrá ser rechazada por el personal administrativo del Juzgado o Sala correspondiente*". Nos parece que debió decir, que no podrá ser rechazada por el jueces o jueces que son los funcionarios con jurisdicción y competencia para pronunciarse sobre la admisión, inadmisión o rechazo de la demanda, mediante providencia o decisión judicial correspondiente.

El CPCP en el artículo 62, establece unos requisitos especiales de la demanda que debe reunir la acción de Hábeas Data, además de los requisitos generales para la demanda en acción de amparo. Estos son: (i) que el demandante previamente haya reclamado, por documento de fecha cierta, el respeto de los derechos de conocimiento y acceso a la información, de actualización, rectificación o eliminación de la información inexacta, erróneo o ilegal, o de supresión o impedimento de la publicación de información sensible o privada que afecte derechos constitucionales; (ii) que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud tratándose del derecho reconocido por el artículo 2 inciso 5) de la Constitución, o dentro de los dos días si se trata del derecho reconocido por el artículo 2 inciso 6) de la Constitución. Excepcionalmente se podrá prescindir de este requisito cuando su exigencia genere el inminente peligro de sufrir un daño irreparable, el que deberá ser acreditado por el demandante. Aparte de dicho requisito, no será necesario agotar la vía administrativa que pudiera existir.

Estos requisitos denominados especiales por el CPCP, en verdad, son trámites administrativos previos que debe agotar el titular de los datos o persona concernida con éstos, pues ese es el significado que debe dársele al solicitar el artículo 62 la demostración de haber reclamado, “por documento de fecha cierta”, es decir, de haber ejercido el derecho de petición ante las autoridades, organismos o instituciones del Estado, o ante personas físicas o jurídicas de carácter particular y esperar que unas u otras, según el caso, hayan o no respondido expresa o tácitamente (una especie de “silencio administrativo” de petición), en forma oportuna o extemporánea, dentro o no de un lapso de tiempo cierto. En fin, el primer requisito, parece sólo pedir que se demuestre que se reclamó mediante un memorial o documento, con la sola presentación y atestamiento de la autoridad o persona que recibió el memorial con sello de hora, día y fecha que de fe a la presentación.

El requisito especial segundo del artículo 62 del CPCP, parece aclarar el requisito primero. En efecto, solicita que el impetrante en acción de Hábeas Data, deba demostrar que la entidad o persona, pública o privada que lo denomina anticipadamente “demandado” cuando todavía no lo es técnica ni procesalmente y según el caso, que ésta o éstas, se han ratificado en su incumplimiento o no hayan contestado así: (i) dentro de los diez días útiles siguientes a la presentación de la solicitud (o petición más claro) tratándose del derecho de acceso a la información pública o privada; (ii) dentro de los dos días si se trata del derecho de la intimidad personal o familiar.

Excepcionalmente, agrega el artículo citado, se podrá prescindir de este requisito especial cuando su exigencia genere el inminente peligro de sufrir un daño irreparable, el que deberá ser acreditado por el demandante. La prueba idónea que se exige al “interesado o afectado” con el tratamiento de datos, parecería exagerada, pues la calificación de los

hechos, actos, sucesos u omisiones, sí constituyen o no “inminente peligro” debe darse por el funcionario jurisdiccional que admite el amparo específico de Hábeas Data, cuando no esté regulado previamente en el ordenamiento jurídico vigente, o más aún en el CPCP, pues la carga de la prueba en estos casos debería soportarla el Estado o la persona privada que vulnere el tratamiento de datos, a falta de regulación expresa.

Como se observa, sí existen vías previas antes de la acción de Hábeas Data en el derecho peruano, que el CPCP, se empeña en decir, en el inciso *in fine* del artículo 62 que “*no será necesario agotar la vía administrativa*”. Si bien es cierto, no existen recursos administrativos contra la decisión expresa o tácita al derecho de petición (“solicitud”, “reclamo”, como lo denomina el CPCP), elevados por el interesado, afectado o titular de los datos frente a las personas o entidades públicas o privadas; no es menos cierto, que las peticiones incoadas por aquél cuando se trata de los derechos fundamentales previstos en los numerales 5º y 6º del artículo 2º de la Constitución Peruana, reciben una contestación tácita negativa que genera un silencio administrativo de peticiones de 10 días en el caso del derecho de acceso a la información y de dos días en el caso del derecho a la intimidad; es decir, que hay una respuesta tácita negativa, que en todo caso genera una vía administrativa --mal llamada en Colombia “gubernativa”-- que ineludiblemente debe agotarse para acudir en Hábeas Data, pues el artículo 62 expone que estos son requisitos especiales adicionales a los generales de la presentación de la demanda en acción de amparo específico o de Hábeas Data.

6.3.4. Las medidas cautelares en el procedimiento de amparo específico de Hábeas Data

En el Título I, concerniente a las “*Disposiciones generales de los procesos de Hábeas Corpus, Amparo, Hábeas Data y cumplimiento”* del CPCP, y más concretamente en el artículo 15, se sostiene que son viables las medidas cautelares y de suspensión del acto violatorio en los procesos de amparo, Hábeas Data y de cumplimiento, indicando con ello, que respecto al proceso de amparo específico o de Hábeas Data son viables como etapa contingente del proceso las medidas cautelares como la suspensión de la eficacia o de los efectos jurídicos del acto (particular o administrativo) acusado [37] .

Para la adopción de las medidas cautelares en esta clase de procesos constitucionales sumarios, el legislador peruano impuso a la autoridad jurisdiccional que se comprobara *ab initio* los requisitos caracterizadores de las medidas cautelares: (i) la apariencia del derecho o también conocido como elemento *fumus boni iuris* [38]; (ii) el peligro en la demora o

---

(37) Vid. RIASCOS GOMEZ, Libardo O. ***Las medidas cautelares en el procedimiento administrativo.*** Tesis Doctoral, Universidad de Navarra, Pamplona (España), 1986, p. 15 y ss.
(38) Ob., ut supra cit.

periculum in mora [39]; (iii) que el pedido cautelar sea adecuado para garantizar la eficacia de la pretensión o como lo denominamos, el elemento de la *pendentia litis* [40]; y (iv) se dictan sin audiencia de la contraparte.

Efectivamente, los anteriores elementos caracterizadores de toda medida cautelar se deben reunir al momento de la solicitud de la medida cautelar por el interesado o afectado, pero es el Juez quien en el momento de la adopción de la medida mediante providencia idónea quien evalúe y compruebe su existencia y pertinencia luego de leer los argumentos fácticos, jurídicos y probatorios esgrimidos por el solicitante, en memorial escrito conjunto o separado de la demanda y de comprobar si existe una violación o vulneración irrefragable (“*palmaria” o “prima facie”*, como se solicita en el derecho público colombiano en los procesos de nulidad de actos administrativos ante la jurisdicción contencioso administrativa) entre el acto acusado y el ordenamiento jurídico vigente.

La procedencia, trámite y ejecución de las medidas cautelares, según el artículo citado dependen del contenido de la pretensión constitucional intentada y del aseguramiento de la decisión final.

Tienen competencia para avocar y decretar medidas cautelares en esta clase de procesos, si la solicitud de medida cautelar tiene por objeto dejar sin efecto actos administrativos dictados en el ámbito de aplicación de la legislación municipal o regional, en primera instancia por la Sala competente de la Corte Superior de Justicia del Distrito Judicial correspondiente.

En cuanto al trámite para la adopción, ejecución y recursos de las medidas cautelares, se seguirá el previsto en los incisos 3º y 4º del mentado artículo; es decir, se aplicará el *iter procesalis* del CPCP, como norma especial y el Código Procesal Civil Peruano (Título IV de la Sección Quinta), como norma subsidiaria para llenar los vacíos o lagunas legales del CPCP. En efecto, ab initio el trámite es el siguiente: De la solicitud se corre traslado por el término de tres días, acompañando copia certificada de la demanda y sus recaudos, así como de la resolución que la da por admitida, tramitando el incidente en cuerda separada, con intervención del Ministerio Público. Con la contestación expresa o ficta la Corte Superior resolverá dentro del plazo de tres días, bajo responsabilidad salvo que se haya formulado solicitud de informe oral, en cuyo caso el plazo se computará a partir de la fecha de su realización. La resolución que dicta la Corte será recurrible con efecto suspensivo ante la Corte Suprema de Justicia de la República, la que resolverá en el plazo de diez días de elevados los autos, bajo responsabilidad.

---

(39) Ob., ut supra cit.
(40) Ob., ut supra cit.

La medida cautelar se extingue, según el artículo 16 del CPCP de pleno derecho cuando la resolución que concluye el proceso ha adquirido la autoridad de cosa juzgada.

Si la resolución final constituye una sentencia estimatoria, se conservan los efectos de la medida cautelar, produciéndose una conversión de pleno derecho de la misma en medida ejecutiva. Los efectos de esta medida permanecen hasta el momento de la satisfacción del derecho reconocido al demandante, o hasta que el juez expida una resolución modificatoria o extintiva durante la fase de ejecución.

Si la resolución última no reconoce el derecho reclamado por el demandante, se procede a la liquidación de costas y costos del procedimiento cautelar. El sujeto afectado por la medida cautelar puede promover la declaración de responsabilidad.

De verificarse la misma, en modo adicional a la condena de costas y costos, se procederá a la liquidación y ejecución de los daños y, si el juzgador lo considera necesario, a la imposición de una multa no mayor de diez Unidades de Referencia Procesal.

La resolución que fija las costas y costos es apelable sin efecto suspensivo; la que establece la reparación indemnizatoria y la multa lo es con efecto suspensivo.

CAPITULO SEGUNDO

II. El HABEAS DATA EN LAS LEYES DE PROTECCION DE DATOS DE CARÁCTER PERSONAL EN EL DERECHO CONTINENTAL EUROPEO

2.1. PRELIMINARES.

Nos parece oportuno en esta parte del trabajo, hacer mención a los diferentes cuerpos normativos que regulan el tratamiento informatizado de los datos de carácter personal, a efectos de exaltar, entre otros aspectos, por un lado, la labor que vienen cumpliendo los legisladores en los diferentes Estados de Europa continental (a título de ejemplo en Alemania, España y la Unión Europea) por puntualizar y establecer un marco de garantías y medias de protección a los derechos involucrados en dicho tratamiento (con mayor énfasis en el derecho a la intimidad y subsidiariamente de la información, la expresión, el honor y la imagen, entre otros); y por otro, analizar, estudiar y puntualizar el derecho del *Hábeas Data* prevista en las principales leyes de protección de datos personales, clasificadas inicialmente en *tres generaciones*, según sus contenidos y evolución en la regulación del fenómeno informático en entronque con el derecho. Ampliaremos luego una cuarta generación y otra en transición, atendiendo además de lo dicho, al factor temporal, los avances significativos de *iusinformática* y la consideración de los Estados "*paraísos informáticos*" técnica como legislativamente.

En la ***primera generación*** de estas leyes se hallan las denominadas *leyes pioneras* en la regulación y tratamiento (informatizado o no) de datos de carácter personal: La *Ley Federal alemana de protección de datos personales* y Ley Sueca "*Data Lag"* de 11 de mayo de 1973 [41]**.** Según *Mirabelli* [42], estas leyes son tendencialmente restrictivas puesto que se sujetan al requisito de "la autorización previa" para la creación de los *"ficheros"* o bancos de datos, limitando excesivamente la recolección de los "datos sensibles" e instituyendo organismos con funciones y estructura cuasi jurisdiccional para la concesión y el ejercicio del control de los mencionados banco de datos [43]. Sin embargo, como veremos más adelante la Ley Alemana, --que tomamos como prototipo de análisis de esta primera generación-- por contra, se caracteriza por ser la primera en el tratamiento integral de tratamiento informatizado o no de datos personales, así como de demarcar una nueva técnica legislativa en materia de definiciones técnico-jurídicas, estructurar por vez primera los "*procesos de datos*" públicos y privados y crear la figura del Comisario de Protección de datos para la vigilancia, garantía y protección de los derechos fundamentales, las libertades públicas e intereses legítimos de los titulares de datos personales.

En una *segunda generación de leyes* protectoras de los datos personales se destacan la de Francia en 1974, Noruega en 1978, Luxemburgo en 1981, etc. Por paralelo y con idénticos propósitos, surgen normas de ámbito internacional (La Recomendación de la OCDE de 1980) y Comunitario Europeo propuestas por el Consejo de Europa (El Convenio de Estrasburgo de 1981). Las leyes en esta etapa se caracterizan por el sistema de "la notificación" y no de la autorización como requisito *a priori* para crear bancos de datos. Además, se introduce la figura del responsable del fichero o banco de datos [44], se ingresa en la técnica legislativa de la conceptualización de los términos técnico cerrados y abiertos utilizados en las nuevas tecnologías de la información y la comunicación (TIC) que inciden en el derecho y se instituye, a partir de éstas, los denominados "principios fundamentales de la protección de datos", tanto en el tratamiento, almacenamiento, difusión como en la

---

(41) La Data lag Sueca, según el profesor ORTI, "estableció un sistema de Registro de ficheros informatizados, exigiéndose la inscripción con carácter constitutivo, necesaria para obtener la autorización para crear un fichero, y a la que se condicionaba la inclusión en el Registro. Este requisito fue sustituido más tarde por el sistema de la mera notificación e inscripción registral, que es el seguido en la ley española" Cfr. ORTI VALLEJO, Antonio. ***Derecho a la intimidad e informática*** *(Tutela de la persona por el uso de ficheros y tratamiento informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*. Ed. Comares, Peligros (Granada), 1994, p.14.

(42) MIRABELLI, ***"Banche dati e contemperamento degli interessi"****, Bance dati telematica e diritti della persona,* Cedam, Padova, 1984, pág. 160. Citado por ORTI V. Ob. cit., p. 11.

(43) En ésta etapa de clasificación de normas de protección de datos personales, nacieron por doquier varias leyes en Europa y América.. Se destacan entre ellas la Ley Francesa de 6 de Enero de 1978, conocida como "*Loi relative à l´informatique, aux fichiers et aux libertés",* y la "*Privacy act* de 31 de diciembre de 1974, que fueron el prototipo de otras que les siguieron. Entre ellas, la Ley Noruega de Junio 9 de 1978, la de Luxemburgo de 30 de Marzo de 1979, la Suiza de 1981.

(44) Ob. ut supra cit. p. 11.

"libre circulación de datos de carácter personal". Aspectos capitales en el procedimiento informatizado de datos que se evidenciaron más en las normas de ámbito internacional y comunitario, antes que en las leyes estatales, como precisaremos.

Por ello, tomaremos de ésta generación dos prototipos de legislación sobre el tratamiento informatizado de datos: La Recomendación del Consejo de la OCDE de Septiembre 30 de 1980, *por la que se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales* y El Convenio Europeo de Estrasburgo de 28 de Enero de 1981", relativo a la *"protección de las personas con respecto al tratamiento automatizado de datos de carácter personal".* Convenio incorporado por todos los Estados Europeos en sus respectivos ordenamientos jurídicos internos a través de normas jurídicas de trasposición. En España, el Convenio se ratificó mediante instrumento de Enero 27 de 1984 (BOE. 15-11-1985, núm. 274) e ingresó al ordenamiento jurídico interno no sólo como mecanismo de interpretación de derechos humanos (art.10.2 CE), sino como una verdadera norma jurídica con fuerza legislativa desde aquélla época (art.96.1 CE).

En la "*tercera generación"*, se ubican las normas jurídicas nacidas en la década de los noventa, muy a pesar de que las propuestas e iniciativas venían manejándose desde la década anterior. En esta se ubican la *"La ley española de regulación del tratamiento automatizado de datos de carácter personal"*, de 29 de Octubre de 1992, conocida también como LORTAD, reformada en 1999, por la "*Ley Orgánica de Protección de Datos*" o LOPD, Ley 15 de 1999; como también la *"Privacy and data Protection Bill 1994 (NSW) o Ley de protección de la intimidad y los datos personales en Australia.* Esta generación de leyes se caracteriza según *Orti Vallejo* [45], siguiendo a *Pérez Luño,* por ser más "*liberalizantes del uso de ficheros de datos personales*" y establecer un amplio marco de principios, derechos y obligaciones para las personas naturales, jurídicas, públicas y privadas.

Una *cuarta generación* de normas surge con la expedición de la Directiva 95/46/CE del Parlamento Europeo 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.* Esta generación se caracteriza por plantear como epicentro el principio-derecho de la libre circulación de datos personales entre los países miembros de la Unión Europea e incluso entre países terceros, previo el lleno de unos requisitos *sine qua nom;* la consagración de principios, derechos (como el de información y de Hábeas data) y obligaciones en todas las fases, etapas o ciclos informáticos del procedimiento informatizado de datos, cuando se realiza con soportes, medios y aplicaciones informáticas

---

(45) ORTI VALLEJO, A. Ob. cit., p. 18

electrónicas y telemáticas y la plasmación del llamado *derecho de oposición al tratamiento informatizado* de datos personales, como un derecho personalísimo de los titulares de los datos personales.

Finalmente, una *quinta generación* o *generación de leyes protectoras de datos específicas en tránsito*, constituida por Estados que no disponen de normas especiales en la protección de datos personales, pero en cambio disponen de diversas normas jurídicas generales, mecanismos, procedimientos administrativos (iniciados por el derecho de petición y desarrollados y concluidos con los recursos ordinarios y extraordinarios de reposición, apelación, queja y revocatoria, respectivamente) y procedimientos jurisdiccionales de índole constitucional, contencioso-administrativo, civil y penal dirigidas a proteger los datos personales. Si bien estos Estados no se halla en Europea continental e insular, ello no obsta para que los mencionemos por ahora en esta clasificación, pues como veremos en el la última parte de este ensayo jurídico, han adelantado la defensa y protección de derechos y libertadas fundamentales con base en la aplicación directa de la Constitución que elevó a rango constitucional el Hábeas Data como acción, recurso, garantía o proceso constitucional. Colombia es un ejemplo tipo de esta generación.

En todo caso, estos Estados con este conjunto de normas e instituciones jurídicas, propenden por la efectiva protección de los derechos fundamentales, en todos los ámbitos incluidos aquellos que se presentan en el tratamiento informatizado de datos. Quizá por ello, en puridad jurídica no existen *"Estados paraísos informáticos*" por el sólo hecho de no tener normas específicas que regulen la tensión-relación de la informática, los medios TIC y los derechos humanos, pues el vacío normativo específico lo han llenado con normas procesales y sustantivas generales aplicables al tratamiento de datos personales en desarrollo jurisprudencial suministrado al Hábeas Data por los Tribunales o Corte Constitucional en sus variados fallos de defensa y tutela de los derechos a la intimidad, la imagen, la información, el buen nombre entre otros (v.gr. Sentencias de la Corte Constitucional: T-414-1992, Ago.T-444-92 de 7Jul.,T-127-1994, de 15 de Mar, T-022/1993, de 29 Ene., T-413-1993, de 29 de Sep., T-097/1995, de 3 de Mar, SU-082 y 089/1995, de 1 de Marz., C.C. Sent.T-552/1997, de 30 de Oct, entre muchas otras citadas ut supra y las que citaremos ut infra.

A continuación no referiremos a las Leyes de protección de datos Alemana, Española y las que rigen en la Unión Europea (UE).

2.2. ALEMANIA: LA LEY FEDERAL DE PROTECCION DE DATOS DE 27 DE ENERO DE 1977 [46].

Esta Ley Federal es el resultado de la estructuración y promulgación de la Ley perteneciente al *Land de Hesse* de 7 de Octubre de 1970, primera en regular todo lo atinente al tratamiento informatizado de datos que "*utilizaban los servicios administrativos del Land*" y de la ley de la Renania-Palatinado [47]

La Ley Federal de protección de datos, no sólo fue la pionera a nivel internacional en regular legislativamente el tratamiento informatizado de los datos personales, sino que es la primera y la única, incluso hasta épocas actuales, en tratar integralmente todo lo atinente al tratamiento informatizado los datos personales, tanto en el ámbito público como privado; así como también en regular los aspectos civiles, penales y derecho público derivados del ejercicio, protección y transgresión de los derechos que ostentan los titulares de los datos, ante las autoridades civiles, administrativas y punitivas.

2.2.1. Estructura de la LFAPD

La Ley Federal Alemana de protección de los titulares de los datos, el 20 de diciembre de 1990, recibió una nueva redacción en su texto y que en esencia su contenido y su "concepción sigue siendo igual a la de 1997" [48]. Por ello, estudiaremos brevemente el texto de 1977. Esta ley (en adelante LFAPD), tiene cinco secciones de las que destacaremos los aspectos que tienen que ver con el objeto de nuestro trabajo. Son:

SECCION PRIMERA*: Disposiciones generales*: En las que se refiere a los cometidos y objeto de la ley, definiciones, admisibilidad del "proceso de datos", derechos del "afectado"; y "secreto de los datos, medidas técnicas y de organización".

SECCION SEGUNDA*: Proceso de datos de autoridades y otros servicios públicos*: ámbito de aplicación; elaboración de datos personales por cuenta ajena; almacenamiento y modificación de datos; comunicación de datos dentro del sector público; comunicación de datos a "entes" ajenos a un sector público; Publicidad de los datos almacenados; Facilitación de información "al afectado"; Rectificación, bloqueo y cancelación de datos; Ejecución de la protección de datos en la Administración Federal; Disposiciones administrativos de carácter general; nombramiento de un Comisario Federal de Protección de datos; situación jurídica del Comisario Federal de Protección de Datos; Funciones del

---

(46) Texto completo en AA.VV. ***Documentación informática***. Serie Amarilla. Tratados Inter. núm.2.
(47) ORTI VALLEJO, A. Ob. cit. pág. 12
(48) Según Heredero Higueras, citado por ORTI VALLEJO, Ob. ut supra cit., pág. 12-13.

Comisario Federal de Protección de Datos; Reclamaciones del Comisario Federal de Protección de Datos; y, Recurso ante el Comisario Federal de Protección de Datos.

SECCION TERCERA: *Proceso de datos de entes no público para uso interno:* Ámbito de aplicación; modificación de datos; facilitación de información al afectado; Rectificación, bloqueo y cancelación de datos; Designación de un Comisario de Protección de Datos; Funciones del Comisario de Protección de Datos; y, Autoridad de tutela.

SECCION CUARTA*: Proceso de datos realizado con finalidad mercantil para entes no públicos:* Ámbito de aplicación; Almacenamiento y comunicación de datos; modificación de datos; facilitación de información al "afectado"; Rectificación, bloqueo y cancelación de datos; elaboración de datos personales para su difusión en forma "anonimizada" (o simplemente anónima); elaboración de datos personales por cuenta ajena; Comisario de Protección de Datos; Deber de denuncia; y, Autoridad de tutela.

SECCION QUINTA: *Normas punitivas y sancionadoras:* Acciones punibles, y, Infracciones de Policía.

SECCION SEXTA: *Disposiciones transitorias y finales:* Disposiciones finales; Aplicación de la Ley de Procedimiento Administrativo; Disposiciones subsistentes; "Cláusula Berlinesa"; y entrada en vigor.

2.2.2. Comentarios sucintos a la LFAPD de 1977

Son muchos y variados los temas los que aborda la Ley alemana, sin embargo, destacaremos a nuestros efectos investigativos los siguientes, los cuales los dividiremos así: a) Las definiciones técnico-jurídicas o ius-informáticas; b) El Comisario de Protección de los Datos; y c) El Sistema Punitivo y Sancionador en materia de datos.

2.2.2.1. Definiciones técnico-jurídicas o ius informáticas

La Ley Federal Alemana del tratamiento de datos personales, inaugura en su condición de pionera, la técnica legislativa que posteriormente se extendiera en toda norma jurídica estatal y comunitaria de iniciar el texto legislativo con un glosario de términos técnico-jurídicos cerrados, cuyas definiciones son de aplicación necesaria para todo operador jurídico de la ley. Las definiciones contenidas en la Ley de 27 de Enero de 1977, son *ius-informáticas*, por referirse a la órbita jurídica tanto al derecho público como al derecho privado y en particular, al tratamiento informatizado de datos dominado por la informática.

Las diversas definiciones las podemos agrupar por su contenido y afinidad con el fenómeno tecnológico de la informática (entendida como la ciencia del tratamiento lógico,

sistematizado e informatizado de cualquier unidad de información o datos) y el derecho, en los siguientes: a) Definiciones sobre los sujetos del tratamiento de datos; b) Definiciones aplicables al "*Habeas Data*" y al proceso de datos personales; y, c) Definiciones aplicables al procedimiento informatizado de datos.

2.2.2.1.1. Definiciones sobre los sujetos del tratamiento de datos

Pertenecen a este grupo las definiciones de "Datos personales", "tercero" y "ente almacenante". *Datos personales* se consideran las indicaciones concretas acerca de condiciones personales o materiales de una persona natural determinable (o "afectado" aunque en puridad mejor llamado sería: el interesado o titular de los datos). Estos datos personales como información perteneciente a cualquier persona física, incluye tanto la contenida en método no informáticos, como en aquellos a los que se les ha aplicado la técnica, tratamiento o procedimientos informatizados o "*procedimientos automáticos*", como lo denomina la Ley Federal Alemana de Protección de Datos. Se excluyen no del concepto de datos personales sino del ámbito de aplicación de la LFAPD, los datos personales elaborados por empresas auxiliares de la prensa, radio o cinematografía, exclusivamente para uso interno en relación con la difusión (Art. 1 *in fine* LFAPD), salvo en lo atinente a las "medidas técnicas y de organización" que éstas deben implementar para garantizar los derechos e intereses legítimos de los titulares de los datos de conformidad con LFAPD [49].

---

(49) "Si se elaboraren automáticamente datos personales, deberá adoptarse para la aplicación de los preceptos de la presente ley medidas que en función de la índole de los datos personales que hubieren de ser protegidos fueren idóneas para: l. impedir a personas no autorizadas el acceso a los equipos de proceso de datos con los cuales fueren elaborados los datos personales (control de acceso a los equipos); 2. Impedir que las personas ocupadas en la elaboración de datos personales retiren sin autorización soportes de información (control de salidas); 3. Impedir la introducción no autorizada en memoria de datos personales, así como la toma de conocimiento, modificación o cancelación no autorizadas de datos personales ya almacenados (control de memorias); 4. Impedir que personas no autorizadas utilicen sistemas de proceso de datos a partir de los cuales se comunicaren datos personales valiéndose de dispositivos automáticos o en los cuales se introdujeren datos personales valiéndose tales dispositivos (control de usuarios); 5. Garantizar que las personas con derecho a usar un sistema de proceso de datos puedan acceder mediante dispositivos automáticos exclusivamente a los datos personales que estuvieren comprendidos dentro del ámbito de su facultad de acceso (control de acceso a los datos) ; 6. Garantizar que se pueda comprobar y determinar en que puntos es posible comunicar datos personales valiéndose de dispositivos automáticos (control de la comunicación); 7. Garantizar que se pueda comprobar y determinar a posteriori que datos personales, en que momento y por quien fueron introducidos en sistemas de proceso de datos (control de la introducción en memoria); 8. Garantizar que en los datos personales que fueren elaborados por cuenta ajena sólo puedan serlo de conformidad con las instrucciones del comitente (control de encargos); 9. Garantizar que en los supuestos de comunicación de datos personales, así como en los casos de transporte de los correspondientes soportes de información, estos no puedan ser leídos, modificados o cancelados sin autorización (control del transporte de datos); 10. Configurar la organización interna de las autoridades o empresas de tal manera que la misma responda a las exigencias de la protección de datos (control de la organización)". ANEXO ARTICULO 6, PRIMER PARRAFO, PROPOSICION PRIMERA.

Tercero, es toda aquella persona o entidad ("ente") ajena a la entidad almacenante, a excepción de los interesados o de aquellas personas y entidades (Autoridades públicas, personas jurídicas, sociedades u otras agrupaciones, etc.) que obraren por "encargo" dentro del ámbito de vigencia de la LFAPD.

Y, finalmente, *Entidad Almacenante*, se consideran como tales cualquiera de las personas naturales o jurídicas o entidades que almacenaren datos por sí mismo o encomendare a otro su almacenamiento. Estas son: a) Las diversas Autoridades o entidades públicas (pertenecientes al Estado, a los Municipios, mancomunidades de municipios y cualesquiera otras personas jurídicas de derecho público sujetas a tutela estatal. Art. 7 LFAPD); y, b) Personas naturales o jurídicas, sociedades u otras agrupaciones de personas de derecho privado, para uso interno (se exceptúan de ésta aparte las personas de derecho privado que desempeñan "funciones propias de la Administración Pública". Art.22 LFAD), o las que realicen "con carácter regular y por cuenta ajena" actividades con "finalidad mercantil" (en esta se incluyen las empresas de derecho público, con idéntica finalidad. Art. 31 LFAPD).

2.2.2.1.2 Definiciones aplicables exclusivamente al Hábeas Data y al proceso de datos personales

Si bien como recuerda el profesor *González Navarro*, citando a *Heredero Higueras* [50], el derecho de acceso, aún antes de la promulgación de las leyes de protección de datos, fue bautizado como *habeas data*, por considerarlo como una modalidad de acción exhibitoria análoga a la del *habeas corpus* del derecho anglosajón, no debemos olvidar que el derecho de acceso a los datos, sobre todo los informatizados o sometidos en parte o en todo a tratamiento o procedimientos "automatizados", conlleva un grupo de derechos concomitantes y subsiguientes al ejercicio del derecho de acceso, tales como: el derecho a conocer la existencia de datos que le conciernan a la persona y que se hallen almacenados ("storage") y contenidos en un fichero, banco de datos o simplemente en un "archivo" o registro informatizado (o simplemente "*file*" anglosajón), bien sean procesados con o sin su consentimiento; así como también el derecho a consultarlos, si fuere del caso, por cualquier método, técnica o medio informático, electrónico o telemático, dentro de conformidad con el ordenamiento jurídico vigente sobre la materia. Como consecuencia, de ello podrá, independientemente de los recursos (básicamente jurisdiccionales), solicitar la revisión, rectificación, actualización, modificación y, llegado el caso, la cancelación, borrado y bloqueo de los datos personales que le conciernen.

En consecuencia, pertenecen a este segundo grupo de definiciones, las siguientes: alma-

---

(50) GONZALEZ NAVARRO, Francisco. ***Derecho administrativo español.*** Ed. Eunsa, 1a., ed., 1987 y 2a., ed., 1994, Pamplona, p. 179

cenar, comunicar, modificar y cancelar datos personales.

Almacenar datos personales, en términos iusinformáticos, consiste en recoger, registrar o conservar en un soporte de información con miras a su ulterior utilización. El "almacenamiento" de datos, según la LFAPD constituye una fase del procedimiento informatizado de datos que abarca una etapa previa, como es la recolección; una etapa concomitante, como es la del registro; y una etapa posterior, como es la conservación de datos. Todas ellas interdependientes, pues faltando una de éstas no se puede completar el fenómeno o actividad de almacenamiento.

La LFAPD, establece la subsidiariedad de ésta, cuando existan leyes especiales federales sobre los datos personales almacenados en registros informatizados (art.45), destacando con ello la etapa de almacenamiento y tratamiento informatizado de los datos. Así a título de ejemplo, se aplicará la ley especial sobre la general en la guarda de secreto sobre noticias obtenidas oficialmente o en el ejercicio profesional; p. e., el art. 12 de la Ley de Estadísticas para fines Federales, de 3 de septiembre de 1953 **[51]**.

La LFAPD, al hacer mención a los derechos que tiene el "afectado" (por titular de los datos, en términos positivos y no en términos negativos, tal y como lo prevé la ley) dentro del llamado "proceso de datos", se hace expresa referencia a los derechos derivados del acceso y consulta de la información y subsecuente, todos ellos componentes del derecho fundamental del *habeas data.* Los derechos subsecuentes son: a) La información acerca de los datos almacenados en relación con la persona; b) La Rectificación de los datos almacenados en relación con su persona, cuando los mismos fueren inexactos; c) El bloqueo de los datos almacenados en relación con su persona cuando no pudiere determinarse su exactitud o inexactitud, o cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento; y d) La cancelación de los datos almacenados en relación con su persona, si su almacenamiento no había sido admisible o bien --a elección, además del derecho de cancelación-- cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento.

_____

(51) Otros ejemplos son: a) Sobre limitación del examen de documentos por terceros; p. e., el articulo 61, párrafo segundo y tercero de la ley de estado civil de las personas; b) Sobre examen del expediente personal por los funcionarios o empleados; p e., el articulo 90 de la ley federal de funcionarios; el articulo 83 de la ley de Organización de Empresas; c) Sobre el deber de las autoridades de informar a los ciudadanos de los datos almacenados acerca de los mismos; p. e., el articulo 1.325 de la Ordenanza Imperial del Seguro; g) Sobre difusión, rectificación y cancelación de los datos referidos a personas incluidos en Registros públicos; p. e., los artículos 19, 23, 27, segundo párrafo; y d) Sobre la obligación de elaborar datos referidos a personas en la rendición de cuentas, comprendidas la contabilidad y otras anotaciones; p.e., los artículos 38 a 40, 42 a 47 del Código de Comercio. Texto completo de la LFAPD., en AA.VV. ***Documentación Informática****.* Serie Amarilla. Tratados Internacionales núm. 2º

Comunicar, en términos de la LFAPD, es una especie cualificada (dirigida a “terceros”) del género *informar* (que la ley denomina derecho de “facilitación de información al afectado”, considerado como un derecho fundamental, no absoluto que tiene el titular de los datos personales, tanto en el proceso de datos público [52], como en el privado [53], puesto que se prevé expresas excepciones al ejercicio del mismo), puesto que comunicar se entiende la acción de dar a conocer a terceros datos almacenados u obtenidos directamente mediante un proceso de datos, tanto si fueren datos difundidos por el ente almacenante, como si son datos conservados por la entidad para su examen, en especial para su búsqueda automática (art. 4-2). En este sentido, la *comunicación* de datos personales, con el lleno de los requisitos previstos en la ley, bien puede hacerse a personas como entidades públicas tanto en los procesos de datos de carácter público (art. 11), como en los procesos de índole privada (art. 32).

---

(52) Se facilitará al afectado, si así lo solicitare, información acerca de los datos almacenados con relación a su persona. En la solicitud deberá detallarse la índole de los datos personales sobre los cuales deba facilitarse la información. El servicio o ente almacenante determinará el procedimiento, en especial la forma de facilitar información según las conveniencias del servicio... No precederá la facilitación de la información en los siguientes supuestos: 1. si la información perjudicare el legítimo cumplimiento de las tareas comprendidas en la competencia del servicio almacenante; 2. si la información perjudicare a la seguridad o al orden públicos o causare detrimento a la Federación o a un Estado; 3. si los datos personales o el hecho de su almacenamiento hubieren de ser mantenidos en secreto en virtud de norma jurídica o por razón de su esencia, en especial en razón del interés legítimo preponderante de un tercero ; 4. si la información hiciere referencia a la comunicación de datos personales a las autoridades mencionadas en el articulo 12, segundo párrafo, apartado 1. La facilitación de la información estará sujeta al devengo de una tasa... (art. 13 LFAPD).

(53) Si se almacenaren por primera vez datos referentes a la persona del afectado, deberá este ser informado de ello, a menos que hubiera tenido conocimiento del almacenamiento por otros medios. El afectado podrá exigir información acerca de los datos almacenados con relación a su persona. Si los datos fueren objeto de tratamiento automático, el afectado podrá exigir asimismo información acerca de las personas y servicios a los cuales fueren transmitidos regularmente sus datos. Deberá señalar la clase de los datos personales sobre los cuales debiere ser facilitada la información. La información se facilitara por escrito, siempre que no procediere otra forma de facilitación de información en razón de especiales circunstancias. Podrá exigirse por la información una retribución, la cual no Podrá exceder de los gastos directamente imputables a la facilitación de la información. No Podrá exigirse retribución en los casos en que por circunstancias especiales existiere motivo fundado para creer que se ha llevado a cabo un almacenamiento inexacto o ilícito de datos personales, o en los casos en que la información facilitada hubiera revelado que los datos personales debieren ser rectificados o, en virtud de lo dispuesto en el articulo 27, tercer párrafo, proposición segunda, semi-proposición primera, hubieren de ser cancelados. Los párrafos primero y segundo no regirán en la medida en que: 1. el dar a conocer datos referidos a personas pudiera crear un peligro considerable para el objeto social o los fines del ente almacenante, y no obstaren a ello intereses legítimos del afectado, 2. el servicio publico competente con relación al ente almacenante hubiere observado que el dar a conocer datos referidos a personas podría poner en peligro la seguridad o el orden públicos o causar otros perjuicios para el bien de la Federación o de un Estado, 3. los datos personales hubieren de ser mantenidos en secreto en virtud de una norma jurídica o por razón de su esencia, en especial a causa de intereses legítimos preponderantes de una tercera persona, 4. los datos personales hubieren sido tomados de fuentes de acceso general, 5. los datos personales que, en virtud de lo dispuesto en el articulo 27, segundo párrafo, proposición segunda, estuvieren bloqueados porque sobre la base de disposiciones legales, estatutarias o contractuales, no pudieren ser cancelados a tenor de lo dispuesto en el articulo 27, tercer párrafo, proposición primera (art. 26 LFAPD).

Cancelar, es la acción de hacer irreconocibles datos ya almacenados: cualquiera que fuere el procedimiento empleado a tal efecto. En tanto *modificar*, se considera la acción de transformación del contenido de datos ya almacenados (art. 4-3 y 4-4). En el caso de los datos de carácter privado, la *modificación de los datos* personales será admisible dentro del marco de los fines de una relación contractual o de una relación de confianza análoga a la relación contractual creada, respectivamente con el titular de los datos, o en la medida en que fuere necesaria para salvaguardar intereses legítimos de la entidad almacenante, y no existiere motivo fundado para creer que de ello pudieren resultar perjuicios para los intereses dignos de protección del interesado (art. 25).

La *Rectificación, bloqueo y cancelación de datos*, son tres acciones íntimamente ligadas y subsecuentes por la consideración de sí los datos almacenados, son: a) inexactos o se duda sobre su exactitud. El *in dubio pro date*, como podríamos llamarlo siempre favorece al titular de los datos. b) Si han sido almacenados de forma ilícita, c) Si los datos dejado de ser necesarios para los fines para los cuales fueron almacenados; y, d) porque así "lo exige" el titular de los datos ("afectado").

Sin embargo, la rectificación de los datos sólo es procedente en el caso de no ser exactos los datos personales (art. 14 y 27 *ab initio*).

Se procederá al bloqueo de datos, cuando su exactitud fuere discutida por el titular de los mismos y no fuere posible determinar su exactitud ni su inexactitud. Igualmente serán bloqueados los datos cuando su conocimiento hubiere dejado de ser necesario para que el servicio almacenante pueda cumplir debidamente las tareas a éste encomendadas, a menos que fueren imprescindibles para fines científicos, para fines probatorios, "intereses preponderantes del servicio almacenante o de un tercero", o por consentimiento del titular de los datos. Esto rige para los datos con carácter público como los de carácter privado

La cancelación de datos, en los datos de carácter público, procederá cuando su conocimiento hubiera dejado de ser necesario para que el servicio almacenante pueda cumplir debidamente las tareas comprendidas dentro de su competencia y no existieren motivos fundados para creer que la cancelación pudiera causar perjuicio a intereses dignos de protección del titular. Igualmente serán cancelados los datos si su almacenamiento hubiere sido ilícito o cuando así lo exigiere el interesado. En los datos de carácter privado, además de los anteriores casos, procederá la cancelación cuando así lo exigiere el interesado, en los datos referentes a condiciones de salud, acciones punibles, infracciones de policía, así como a concepciones religiosas o políticas, si su exactitud no pudiere ser probada por la entidad almacenante (art.14 y 27 *in fine*).

El *habeas data* y el grupo de derechos subsecuentes rigen para los titulares de datos cuando sean almacenados tanto en un "proceso de datos de autoridades y otros servicios

públicos" (art.7 y ss LFAPD), o procesos informatizados de carácter público, como en los "procesos de datos de entes no públicos para uso interno" (art. 22) y los "procesos de datos realizados con finalidad mercantil para entes no públicos", vale decir de carácter privado o que se reputan privados a los efectos de la LFAPD, respectivamente (v.gr. el caso de las "empresas públicas de derecho público", art.31).

2.2.2.2. Definiciones aplicables al proceso informatizado de datos

La LFAPD, estructura tres procesos de datos, a saber: a) El Proceso de datos de autoridades y servicios públicos (arts. 7 a 21); b) El proceso de datos de "entes" no públicos para uso interno (arts. 22 a 30); y c) El proceso de datos realizado con finalidad mercantil para entes no públicos (arts. 31 a 40). En estos procesos de datos de naturaleza jurídica de derecho público y de derecho privado, respectivamente, rige por igual etapas o fases, principios, derechos y deberes de los titulares de los datos, a pesar de estar regulados por separado, pues la misma norma reiterada como innecesariamente los reglamenta para cada uno, con específicas diferencias. V.gr. sobre el derecho de "facilitación de información al afectado" (arts. 14, 27 y 34), con cuasi similar contenido para cada uno de los procesos.

Interesa a los propósitos de la investigación, desentrañar las etapas ínsitas en dichos procesos, cara a la estructuración del procedimiento informatizado de datos informáticos.

En efecto, las etapas o fases inmersas en el *proceso alemán de datos* inmersa en las tres clases de procesos de datos son: a) La etapa de recolección o de "elaboración" de datos; b) La etapa de almacenamiento; c) La etapa de conservación e inscripción en un registro (público, privado o mixto, según fuere el caso); y d) La transmisión o comunicación de datos; y e) Rectificación, bloqueo y cancelación de datos.

La LFAPD, al hablar del proceso de datos, en general, estipula que a éste debe someterse los titulares de los datos o interesados, si así esta previsto en una ley o norma jurídica en forma expresa o si el interesado así lo consiente en forma escrita, "siempre que no procediere otra forma en razón de especiales circunstancias" (art. 3 LFAPD).

Igualmente, interesa aquí destacar los conceptos estructurales del derecho de habeas data y el de "archivo informatizado" que están íntimamente ligados con el concepto de proceso de datos. En efecto, se considera *archivo informatizado*, una colección de datos estructurados de manera homogénea, susceptibles de ser obtenidos y ordenados de conformidad con determinadas características y, en su caso, reordenados y explotados de conformidad con otras características determinadas, cualquiera que fuere el procedimiento empleado a tal efecto, sin se consideren comprendidos los expedientes y las colecciones

de expedientes, a menos que los mismos pudieren ser reordenados y explotados por procedimientos automáticos (art. 1-3).

Ahora, pasemos a ver otros aspectos capitales del procedimiento informatizado de datos alemán que aún hoy, tienen relevancia y discusión doctrinal no pacífica.

2.2.2.3. El Comisario de protección de datos: Un Ombudsman [54] en el sector público y un veedor ciudadano en el sector privado

La figura del Comisario de datos personales en el proceso de datos alemán se estructura, cualifica y funciona, según la clase de proceso (público o privado) ante el cual se nombra o se designa por parte de las autoridades públicas federales o las personas privadas competentes, según fuere el caso y ámbito competencial.

2.2.2.3.1. El Comisario Federal de protección de datos en el sector público

El nombramiento del Comisario Federal de protección de datos en “los procesos de datos de autoridades y otros servicios públicos”, se realiza por el Presidente Federal a propuesta del Gobierno Federal. El nombramiento se extingue por expiración del plazo de mandato y por destitución, previo trámite legal y la entrega de un “instrumento fehaciente” extendido por el Presidente Federal.

El designado como Comisario prestará su juramento y cumplirá un plazo de cinco (5) años y su régimen jurídico será el de derecho público. Jerárquicamente depende el Ministerio Federal del Interior, quien podrá entre otras atribuciones, encomendar a un sustituto del Comisario, cuando el titular se viere impedido para ejercer el cargo.

El Comisario Federal de Protección de Datos, tiene las siguientes funciones:

a) *De cumplida ejecución y de asesoramiento sobre leyes de protección de* *datos*. En consecuencia, velará por la observancia y cumplimiento de la LFAPD; así como de otros preceptos sobre protección de datos a los cuales están obligados las autoridades públicas y otros servicios públicos de la Federación, para corporaciones, instituciones y fundaciones de derecho público, etc. Se exceptúa de esta previsión los Tribunales, en la medida en que estos no conocieren de negocios contencioso-administrativos. A este efecto podrá formular recomendaciones en orden al mejoramiento de la protección de datos, pudiendo en especial asesorar al Gobierno Federal y a los distintos Ministros, así como a las restantes autoridades públicas en todo lo tocante a la protección de datos.

---

(54) ORTI VALLEJO, A. Ob. ut supra cit., pág. 13

b) *De Emisión de dictámenes e informes*. Si fuere requerido a ello por “la Dieta Federal Alemana“ o por el Gobierno Federal, el Comisario Federal deberá emitir dictámenes e informes. Asimismo elevara anualmente a la Dieta Federal Alemana una memoria de sus actividades.

c) *De solicitud de auxilio a autoridades y servicios públicos*. El Comisario podrá solicitar a las autoridades y servicios públicos le faciliten información en relación con las preguntas que éste formulare, así como facilitarán el examen de toda clase de documentos y expedientes que guardaren relación con la elaboración de datos referidos a personas, especialmente los datos almacenados y los programas de ordenador. Y, como consecuencia, permitirán en todo momento el acceso a todos los locales oficiales.

d) *De Registro*. El Comisario Federal llevará un registro de los archivos explotados automáticamente, en los cuales se almacenaren datos referidos a personas. Dicho registro se limitará a contener un cuadro general de la naturaleza de los archivos y de los fines para los cuales fueren empleados. El registro podrá ser examinado por toda persona. Las autoridades, servicios y entidades públicas, estarán obligadas a denunciar al Comisario Federal los archivos explotados automáticamente por las mismas. Quedan exentos de esta obligación: La Oficina Federal de Defensa Constitucional, el Servicio Federal de Investigación y el Servicio de Contraespionaje Militar (art. 19).

e) *De reclamaciones*. Si el Comisario Federal de Protección de Datos observare que con ocasión del proceso de datos personales se atenta contra LFAPD, o contra las normas jurídicas de protección de datos, formulará una reclamación ante la autoridad suprema federal competente, si se tratare de la Administración Federal; ante la Dirección del Ferrocarril Federal, si se tratare de este; ante la Dirección o, en su caso, ante el órgano que tuviere atribuida la representación, si se tratare de corporaciones, instituciones o fundaciones de Derecho publico directamente dependientes de la Federación, así como si se tratare de agrupaciones de tales corporaciones, instituciones y fundaciones; y la intimara a que se pronuncie dentro de un plazo que el mismo fijara (art. 20).

f) *De protección de los derechos de los titulares de datos personales*. Toda persona podrá acudir al Comisario Federal de Protección de Datos si fuere de la opinión de que en el curso del tratamiento de sus datos personales realizado por las autoridades, servicios y entidades públicas, a excepción de los Tribunales, siempre que estos no conocieren de negocios contencioso-administrativos, han lesionada los derechos de aquellas (artículo 21).

2.2.2.3.2. El Comisario de protección de datos en el sector privado

La LFAPD, si bien distingue los “procesos de datos de entes no públicas para uso interno” y los “procesos de datos realizados con finalidad mercantil para entes no públicos”, no

procede de idéntica manera, cuando menos, respecto de las funciones generales y especiales que el Comisario de Protección de los datos en el sector privado debe cumplir en uno y otro procesos.

En efecto, cuando se trata de procesos de datos de entes no públicos para uso interno, la designación del Comisario de Protección de datos se realizará, según el art. 28 de la LFAPD, por las personas, sociedades y otras agrupaciones de personas de derecho privado que sometan a tratamiento (o elaboraren) automáticamente datos personales y a tal efecto ocuparen con carácter permanente, por regla general, a cinco trabajadores por lo menos, deberán nombrar por escrito, lo mas tarde dentro de un mes después de iniciar su actividad, a un Comisario de Protección de Datos. Igual se procederá si se ocupare con carácter permanente a veinte trabajadores.

El Comisario de Protección de Datos dependerá directamente del propietario, de la Dirección, del gerente o de otra persona a quien correspondiere la dirección en virtud de disposición legal o estatutaria. En la aplicación de su pericia profesional en materia de protección de datos no estar sujeto a instrucciones superiores. No podrá ser objeto de perjuicios por razón del cumplimiento de sus funciones.

El Comisario de Protección de Datos, cuando se trata de “procesos de datos realizados con finalidad mercantil para entes no públicos”, se designará por las personas, sociedades y otras agrupaciones de personas de derecho privado, o en su caso, por las empresas de derecho público que concurrieren en el mercado, según el art. 38 de la LFAPD. En cuanto a las funciones generales y especiales, éste Comisario cumplirá, en cuanto fuere procedente, las que se atribuyen al Comisario en el proceso de datos de entes no públicos para usos internos.

En tal virtud, El comisario de Protección de Datos, para uno y otro proceso de datos, cumple en su ámbito competencial idénticas funciones generales a las atribuida al Comisario Federal de Protección de Datos; vale decir, que velará por la observancia, cumplimiento y conocimiento de la LFAPD; así como de otras disposiciones relativas a la protección de datos. A tal efecto podrá acudir en casos de duda a la Autoridad de tutela (autoridades administrativas o jurisdiccionales, según el caso).

Como funciones especiales tendrá: ii) *De veeduría y vigilancia de datos, fines, destinatarios y equipos.* En tal virtud, llevará un estado de la clase de los datos personales almacenados, así como del objeto social y los fines para cuya realización o cumplimiento fuere necesario conocer tales datos, de sus destinatarios regulares y la clase de los equipos de tratamiento automatizado de datos que estuvieren instalados; (ii) *De veeduría de medios informáticos.* Velará por la regularidad de la aplicación de los programas de ordenador con cuya ayuda debieren ser tratados los datos personales; y, (iii) *De veeduría profesional.* Prestan

asesoramiento en la selección de las personas que se hubieren de ocupar en el tratamiento de datos los personales.

2.2.2.3.3. El sistema punitivo y sancionador en materia de datos previsto en la LFAPDE

Siendo la LFAPD, una ley de ámbito federal, su carácter es de ley general, por tanto, se aplicará subsidiariamente en caso de ausencia de ley especial o para llenar vacíos o lagunas legislativas si existieren otras leyes de protección de datos de ámbito federal (art. 45). En materia punitiva se aplicarán preferentemente a la LFAPD, a título de ejemplo las siguientes disposiciones: a) Sobre el derecho a negarse a extender certificaciones o a facilitar información por razones personales o profesionales en procedimientos judiciales (arts. 52 a 55 de la Ordenanza Procesal Penal); b) Sobre la obligación, limitación o prohibición del almacenamiento, difusión o publicación de indicaciones pormenorizadas sobre personas (art. 161 de la Ordenanza Procesal Penal); y, c) Secreto profesional (v.gr. secreto médico. Art. 203 Código Penal).

Sin embargo, la LFAPD, se aplicará con carácter general en los casos expresamente previstos como hechos punibles (delitos y contravenciones) contra el tratamiento (informatizado o no) de datos personales.

1. Delitos (art. 41 LFAPD):

a) *Atentados contra los datos personales que no son de dominio público.*

Se considera como hecho punible investigable a instancia de parte el que sin la debida autorización: 1. comunicare o modificare, o 2. recuperare o se procurare a partir de archivos encerrados en depósitos adecuados, datos referidos a personas y protegidos por la LFAPD, que no fueren de dominio público, será castigado con pena de privación de libertad de un año como máximo o con pena de multa.

b) *Tipo Agravado por el lucro o por perjuicio a otro.*

Si el autor, realizare una cualesquiera de la anteriores conductas y además obrare por precio o con el propósito de procurarse a si mismo o a otro un lucro o de causar perjuicio a otro, la pena será privativa de libertad de dos años como máximo o de multa.

2. Contravenciones o "Infracciones" de policía (art. 42 Ibídem). Obra con dolo o culpa quien:

a) ***Por falta de información al interesado de almacenamiento de datos que le conciernen***. No informar al interesado ("afectado"), sobre el almacenamiento de datos personales que le conciernen por primera vez, a menos que hubiere tenido conocimiento del almacenamiento por otros medios. Igual incumplimiento se dará, si por primera vez fueren comunicados datos acerca de la persona interesada, siendo que debía ser informada de su almacenamiento, a menos que hubiere tenido noticia de éste por otros medios.

b) ***Por falta de designación, teniendo la obligación de hacerlo, de un Comisario de Protección de datos***. Por incumplimiento de designar un Comisario de Protección de datos, por parte de las personas, sociedades y agrupaciones de derecho privado que sometan a tratamiento informatizado datos personales y que ocuparen permanentemente trabajadores (cinco o veinte)

Igual, sucederá cuando se incumple la obligación de designar Comisario de Protección de datos por parte de las personas, sociedades y agrupaciones de derecho privado dentro de los procesos de datos realizado con finalidad mercantil para entes no públicos.

c) ***Por falta de adjunción de motivos que justifiquen un interés legítimo para la comunicación de datos***. Si el destinatario no justificare los motivos y la existencia de un interés legítimo y los medios que lo acreditaren en forma fidedigna y detallada para que sea admisible la comunicación de datos personales.

d) ***Por falta de cumplimiento del "deber de denuncia".*** Cuando las personas, sociedades y otras agrupaciones de personas de derecho privado, así como sus filiales y sucursales, teniendo la obligación de formular en tiempo oportuno (un mes) denuncia, no lo hacen. Igual incumplimiento se verificará, si estas personas no facilitaren al formular tal declaración los datos necesarios o no los facilitaren correctamente o de manera incompleta. Estos datos se refieren a la determinación del propietario, directiva, gerente u otro director designado en virtud de disposición legal o estatutaria, y sobre personas encargadas de la dirección del tratamiento de datos y sus direcciones (art.39-2 y 3 LFAPD)[55].

---

(55) *LFAPD. ART. 39. Deber de denuncia*. Las personas, sociedades y otras agrupaciones de personas que se mencionan en el artículo 31, así como sus filiales y sucursales, deberán dar cuenta de la iniciación de su actividad ante la autoridad de tutela competente dentro del plazo de un mes. Al Llevar a cabo la denuncia, deberán comunicarse al Registro llevado por la Autoridad de tutela los siguientes datos: 1. nombre o denominación del ente; 2. propietario, directiva, gerente u otro director designado en virtud de disposición legal o estatutaria, y personas encargadas de la dirección del tratamiento de datos; 3. dirección; 4. objeto social o fines del ente y del tratamiento de datos; 5. naturaleza de los equipos utilizados para el tratamiento automatizado de datos; 6. nombre del Comisario de Protección de Datos; 7. naturaleza de los datos personales almacenados por el ente o por encargo suyo; 8. en caso de comunicación regular de datos personales, destinatarios y naturaleza de los datos comunicados. El primer párrafo regirá en cuanto fuere procedente para la terminación de la actividad, así como para la modificación de los datos facilitados en virtud de lo dispuesto en el segundo párrafo.

2.3. LA EUROPA DE 1980: EL COMIENZO DE UNA DECADA CLAVE EN LA NORMATIZACION Y HOMOLOGACION DE LOS REGIMENES JURIDICOS DE TRTAMIENTO DE DATOS PERSONALES

Si bien es cierto Alemania, Suecia, Francia; entre otros Estados europeos, habían afrontado no solo teórica sino prácticamente el complejo mundo del tratamiento informatizado o no de datos de carácter personal, como el movimiento, flujo o circulación de datos entre países, expidiendo leyes sobre la materia; no es menos cierto también, que éstos esfuerzos legislativos resultaban aislados e incomprensibles incluso en el contexto de una Europa unida, pregonada y defendida desde hacía tres décadas antes con la suscripción de Francia y Alemania con la llamada "declaración o Plan Shuman" de 1950, y subsiguientemente la suscripción del "Tratado del Carbón y el Acero" de 1951--CECA--, por los países bajos, Italia, Bélgica, Luxemburgo y la entonces República Federal Alemana (RFA). Mucho más, resultaba incomprensible cuando dichos Estados habían apostado por una Comunidad de Estados europeos, de origen económico sí, pero luego su radio ampliado a los aspectos sociales, laborales, culturales, políticos, legislativos; y en fin, en un futuro no muy lejano, alcanzar lo que siempre buscaron: un gran Estado Europeo unido con una sola Constitución, como lo teorizaba el profesor alemán de la Universidad de Münster, *Martín Seidel* [56].

Pese a ello, el profesor *Davara* [57], sostiene que desde 1967 en Europa existía "conciencia europea sobre protección de la privacidad" (por la traducción literal de la "privacy" anglosajona) y para ello relaciona varias recomendaciones surgidas en el seno del Consejo de Europa, el cual constituyó una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad a los más elementales derechos de la persona, entre los que estaba la Intimidad. Entre las más destacadas están: (i) La Resolución 509 de 1958, de la Asamblea del Consejo de Europa, sobre "Derechos Humanos y los nuevos logros científicos y técnicos", (ii) Las recomendaciones del Comité de Ministros del Consejo de Europa de 1973 y 1974, sobre la creación de bancos de datos en el sector privado y público, respectivamente, (iii) En Septiembre de 1980, la Recomendación de la OCDE, sobre el flujo internacional de datos, protección a la intimidad y las libertades fundamentales, (iv) Recomendación del 30 de abril de 1980, relativa a la enseñanza, la investigación y la formación en materia de "informática y derecho", (v) La Recomendación del 18 de septiembre de 1980, relativa al intercambio de informaciones jurídicas en materia de protección de datos, (vi) La Recomendación del 23 de enero de 1981, relativa a la regla-

---

(56) Vid., RIASCOS GOMEZ, Libardo O. ***Los denominados recursos ante los tribunales de Justicia de la UE y Andino.*** Ed. UNED, Universidad de Nariño, Pasto (Colombia), 1995, pág. iii y 1.
(57) DAVARA RODRIGUEZ. Miguel A. ***Manual de derecho informático***. Ed. Aranzadi S.A., Pamplona (Nav.), 1997, pág. 56-61.

mentación aplicable a los bancos de datos médicos automatizados, (vii) La Recomendación del 23 de Septiembre de 1983, relativa a la protección de los bancos de datos de carácter personal utilizados con fines de investigación científica y de estadísticas, (viii) La Recomendación de 23 de enero de 1986, relativa a la protección de los datos de carácter personal utilizados con fines de seguridad social".

Con base en éstos o por inspiración de aquellos, algunos Estados Europeos expidieron sus propias normas de ámbito nacional, relativas al tratamiento informatizado de datos, con marcadas diferencias tanto en la conceptualización de los términos técnico-jurídicos (datos, fichero, banco de datos, tratamiento "automatizado", etc.), como en lo referente a la enunciación y enumeración de principios, derechos, deberes y excepciones al tratamiento y la protección de los datos, lo cual indicaba que no existía univocidad en los temas referidos, en el grado y categorías de protección que estilaban dispensar a los datos de carácter personal sometidos a tratamiento informatizado en uno y otro país, ni menos el ámbito de los derechos fundamentales que en éste se involucraban si no era únicamente el de la intimidad.

Orti Vallejo [58] , estima que esta etapa de legislación estatal de protección de datos, se caracteriza por la preocupación de tutelar la intimidad de la persona, como lo acredita el hecho de que se protejan las informaciones consideradas sensibles, que son aquellas que tienen una más inmediata incidencia sobre la vida privada y sobre el datos produjo dos enclaves actualmente vigentes: por un lado, el matrimonio de las leyes de protección de datos aparentemente únicamente con el derecho a la intimidad, produjo a partir de ésta época una identificación casi plena sustentada en la argumentación de que la informática atentaba directa y plenamente a la intimidad y no al conjunto de derechos y libertades fundamentales, tal como se revelaría en las diversas normas protectoras de datos personales; y por otro lado, considerar al derecho de *habeas data* como una sola emanación del derecho anglosajón del *habeas corpus* y de aplicación exclusiva al tratamiento de la información manual o mecanizada, sino también, a todo procedimiento de tratamiento de datos personales de carácter informatizada. Esto replanteaba el tradicional de "derecho de acceso" a la información que tiene toda persona sobre los datos que le conciernen, así como los facultades subsecuentes, de conocimiento, consulta, rectificación, bloqueo y cancelación de información o datos personales que sean erróneos, inexactos o ilegales.

De ésta época, tomaremos como prototipo de análisis y estudio las normas supraestatales o comunitarias de protección de datos personales que tendieron desde aquella época

---

(58) ORTI VALLEJO. A. Ob. ut supra cit., pág. 15

hasta los actuales momentos por la normatización y normalización del tratamiento informático de datos personales, la protección integral de los derechos, libertades públicas (o “individuales”) e intereses legítimos. En efecto, abordaremos la Recomendación del Consejo de la OCDE, del 23 de Septiembre de 1980, cuyo ámbito se extiende a los Estados de la Comunidad Europea (hoy, UE) y los algunos Estados de Oriente y Occidente. Así mismo, el Convenio de Estrasburgo de 28 de Enero de 1981, el cual creo un espíritu normalizador de todo cuanto existía en Europa sobre tratamiento informatizado de datos personales.

2.3.1. La recomendación del Consejo de la OCDE, de Septiembre de 1980

La OCDE (Organización de Cooperación y Desarrollo Económico), creada en 1948, como organización de cooperación preferentemente económica entre Estados Europeos que hoy forman la UE (Unión Europea), EE.UU y Canadá (1960), Japón (1964), Finlandia (1969), Australia (1971) y Nueva Zelandia (1973). Sin embargo, las funciones de esta organización internacional de Estados también se dirige desde su nacimiento hasta la actualidad a proyectar, planear, desarrollar, emitir conceptos, sugerencias y recomendaciones sobre diferentes aspectos de la vida que inciden de alguna manera en lo económico, tales como las estrategias, políticas y directrices sobre la protección de derechos fundamentales, libertades públicas e intereses legítimos de las personas naturales, jurídicas, públicas o privadas, según fuere el caso, con miras esencialmente ha facilitar la armonización de las legislaciones nacionales de los diferentes Estados que componen la OCDE.

En éste último orden de ideas, la OCDE recomendó a sus Estados Miembros, sin perjuicio de sus legislaciones internas sobre la materia [59], unas directrices sobre la protección de todo derechos fundamentales, como el de la intimidad, las “libertades individuales”, y sobre el derecho a la información que tiene toda persona y “ conciliar valores fundamentales

---

(59) El artículo 5 del Convenio de 14 de diciembre de 1969, de la OCDE, expresa: "Con miras a alcanzar sus objetivos, la Organización, podrá: a) adoptar decisiones que, salvo disposición en contrario, vincularan a todos los miembros: b) formular recomendaciones a los miembros; c) concertar acuerdos con sus miembros, con Estados no miembros y con organizaciones internacionales". Por su parte, el articulo 18 del Reglamento de Procedimiento de la OCDE, de julio de 1976, dispone: "a) Las decisiones de la Organización, adoptadas de conformidad en los artículos 5, 6 y 7 del Convenio, podrán ser: (i) decisiones obligatorias para sus miembros, y que estos ejecutarán previo cumplimiento de los procedimientos que requieren sus constituciones; (ii) decisiones por las que fueren aprobados acuerdos concertados con sus miembros, con Estados no miembros y con organizaciones internacionales; (iii) decisiones de orden interno relativas al funcionamiento de la Organización, que se denominaran resoluciones; (iv) decisiones por las que se hicieren comunicaciones a Estados no miembros o a organizaciones. b) *Las Recomendaciones* de la Organización, formuladas de conformidad con lo dispuesto en los artículos 5, 6 y 7 del Convenio, serán sometidas a la consideración de los miembros para que estos procedan a su ejecución si lo estimaren oportuno, c) los textos de las Decisiones o de las Recomendaciones a que se alude en los apartados a), (i) y b) que anteceden, deberán incluir una referencia al articulo 4- a) o al articulo 5- b), respectivamente". Citado por RIVERA LLANO, A. Ob.cit., p.178.

aunque susceptibles de entrar en conflicto, tales como la intimidad y el libre flujo de la información" (Preámbulo del Convenio). Esta recomendación previos los proyectos y estudios, por parte de las comisiones y subcomisiones de expertos respectivas se concretó en lo que se conoce como "Recomendación Adoptada por el Consejo de la OCDE (con base en los arts. 1 (c), 3 (a) y 5 (b) del Convenio relativo a la OCDE, de 14 de diciembre de 1960) del 23 de Septiembre de 1980, *"por la que se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales".*

El Texto de la Recomendación propuesto al Consejo por el Comité de Política Científica y Tecnológica, fue aceptado por los Estados Miembros de la OCDE, entre los que Estaba España, Alemania Occidental, Austria, Bélgica, Dinamarca, EE.UU., Finlandia, Francia, Grecia, Italia, Japón, Luxemburgo, Noruega, Nueva Zelandia, los Países Bajos, Portugal, Suecia y Suiza; en tanto que, Islandia, Turquía y el Reino Unido adhirieron a la Recomendación, el 21 de enero de 1981 y el 27 de Octubre de 1981, respectivamente, no sin mantener su abstención por lo que se había sostenido en la sesión de 23 de Septiembre de 1980.

La Recomendación de la OCDE, constituye un documento de capital importancia para aquella época e incluso con plenas y claras incidencias en la actualidad, tanto en las legislaciones internacionales como en las comunitarias europeas [60]. El documento preparado por un grupo heterogéneo de expertos de diferentes Estados de Occidente y Oriente del mundo, es un fiel, serio, oportuno y claro diagnóstico y recetario de los innumerables hechos, sucesos, problemas, conflictos y proposición de sugerencias y soluciones a los mismos, sobre todo lo atinente al *flujo internacional de datos* entre países miembros de la OCDE y la protección de los derechos fundamentales como el de la intimidad (aunque no en todo su contexto, pues sólo se destaca la visión iusinformática de la intimidad), como hace énfasis el preámbulo, el texto y contexto y las Memorias Explicativas (en adelante M.E.) de la Recomendación; además del conjunto de las llamadas *libertades individuales* (surgidas en la historia del constitucionalismo del liberalismo anglo-francés, y que hoy se consideran como un ámbito importante de los dere-

---

(60) El profesor destaca esa importancia de la Recomendación de la OCDE, pero más dirigida a la vocación legislativa de los Estados Miembros que con vocación europeísta, y más aún, internacionalista, tal y como fue su origen y presentación. DAVARA RODRIGUEZ, Miguel. ***Manual de Derecho Informático****.* Ob.cit., pág. 57.

chos fundamentales) [61], dentro de las cuales se encuentra el hoy llamado "derecho de habeas data", el derecho a la información y los derecho de impugnación y recurso que tiene toda persona contra decisiones administrativas o judiciales.

La Recomendación de la OCDE, en el anexo correspondiente a las "*directrices sobre protección de la intimidad y de los flujos de datos de carácter personal a través de las fronteras"*, estructura las cinco partes en las que se compone. Estas están referidas a las generalidades, Los principios fundamentales a aplicar en el ámbito interno, los principios fundamentales aplicables en el ámbito internacional: libre circulación y restricciones legítimas, la aplicación de los principios en el ámbito interno; y, la cooperación internacional.

A nuestros efectos destacaremos, los siguientes temas: a) las definiciones en el tratamiento informatizado de los datos personales y, b) los principios y excepciones fundamentales del tratamiento informatizado de los datos, tanto en el ámbito nacional como en el ámbito internacional, y dentro de éste especialmente, el principio denominado de la *libre circulación de datos personales* y las restricciones legítimas.

---

(61) La importancia mundial que han adquirido los derechos fundamentales en el ámbito del derecho constitucional español a tenido relevancia muchísimo antes del reconocimiento constitucional en 1978, tal y como lo sostiene *SEMPERE*, al referirse a la "Tutela constitucional de los derechos fundamentales de la personalidad", y en especial *al derecho a la intimidad* prevista en el art. 18 CE, que en el momento de la entrada en vigor del texto constitucional ya existía un cuerpo consolidado de doctrina y jurisprudencia con el reconocimiento y tutela de los derechos del honor, la intimidad, la imagen; entre otros. En igual forma, se suma a ello, que con carácter preconstitucional la protección de los derechos fundamentales, tanto en el ámbito penal (doctrina del T.C., sobre los delitos de injurias y animus iniuriandi y una nueva regulación del C.P.) como en el ámbito de la tutela civil (L.O.1/1982, de 5 de Mayo), así como en relación con la compatibilidad de uno u otro tipo de tutela y la posibilidad de elección, entre ellos, por el interesado. Tal reconocimiento determina, al menos, cuatro consecuencias a destacar: 1. El reconocimiento de los derechos privados de la personalidad mencionados en el artículo 18 como derechos fundamentales. El mismo conlleva una doble consecuencia. Por un lado, afirmar que ya no tiene mucho sentido hablar de estos dere*chos como derechos subj*etivos de naturaleza privada, sino como derechos fundamentales de la personalidad, tal como lo sostiene *DIEZ PICAZO*. Por otro lado, en el ejercicio y limitaciones de estos derechos debe aplicarse la doctrina del T.C., sobre los derechos fundamentales. 2. Exigencia de garantía frente al legislador ordinario. Se concretaría en el respeto por parte de las leyes que reg*ulen el ejercicio* de estos derechos, de un contenido mínimo esencial (art. 53.1 CE). Concepto éste jurídicamente indeterminado cuyo control corresponde, en últ*imo término, al TC (*art.12), a través del recurso de inconstitucionalidad, recurso con el que se garantiza la primacía de la C.E. -- arts. 161.1. a) CE y 27 y 55.2 de la L.O.T.C. 3. *Cualificación de la interven*ción del legislador: reserva de la ley orgánica. Implica que la ley que desarrolle el ejercicio de estos derechos, tanto en su aprobación como modificación, se ajuste a un procedimiento y quórum especiales (art. 168 CE), dado que se trata de leyes orgánicas (art. 81 y 82 CE). 4 . Habilitación de tutela especial ante el Tribunal Constitucional: Recurso de amparo.... SEMPERE RODRIGUEZ, Cés*ar. **Artículo 18: Derecho al honor, a la intimidad y a la imagen.*** Ob.ut supra cit. p. 390 y ss.

2.3.2. Definiciones básicas en el tratamiento informatizado de los datos personales

Siguiendo el criterio --generalizado en la década de los ochenta-- la Recomendación de la OCDE, prevé una serie de definiciones ius-informáticas, tales como, Responsable del fichero, datos de carácter personal y flujos internacionales de datos de carácter personal. Se abstiene de definir lo que debe entenderse como "tratamiento automático de datos", pese a que en el preámbulo y en el apartado tercero referido a los "grados de sensibilidad de los datos", se menciona expresamente. Las razones, entre muchas otras, son: limitar al máximo las definiciones; y en el caso específico, porque resulta difícil hacer una distinción clara entre tratamiento "automático y no automático de la información" [62] y porque las directrices no están dirigidas exclusivamente al tratamiento de datos de carácter personal con "ordenadores" (o "automático"), aunque curiosamente esto fue la punta del iceberg que convocó la reunión, estudio y planteamiento de las recomendaciones ahora comentadas [63].

La persona física a la que se refiere la definición tiene que gozar de una habilitación legal para decidir, sobre el contenido y utilización de los datos, independientemente de si los datos han sido o no obtenidos, registrados, tratados o difundidos por dicha persona o por una persona que obra en su nombre. El responsable del fichero puede ser una persona física o jurídica, una autoridad u organismo público.

---

(62) Cfr. MEMORIA EXPLICATIVA (M.E) Punto 34. "*Tratamiento automático y no automático de datos"*. Las actividades que la OCDE había venido dedicando a la protección de la intimidad y a otros ámbitos conexos estaban centradas en el tratamiento automático de la información y en las redes de ordenadores. El grupo de expertos considero con especial atención la cuestión de si el alcance de estas directrices debía o no quedar limitado al tratamiento automático e informatizado de los datos de carácter personal. Este enfoque puede justificarse por razones diversas, tales como los especiales peligros que llevan consigo para las libertades individuales la automatización y los banco de datos informatizados, el creciente predominio de los métodos de tratamiento automático de la información, en especial en el contexto de los flujos internacionales de datos, así como el marco especifico de la política de la información, de la informática y las comunicaciones, dentro del cual hubo de cumplir su mandato el grupo de expertos. AA.VV. ***Documentación Informática.*** Serie Amarilla. Tratados Internacionales núm. 2.

(63) M.E. Punto 35. "Así, por ejemplo, existen sistemas mixtos de tratamiento de la información y hay también ciertas etapas del tratamiento de la información que pueden o no ser susceptibles de automatización. Estas dificultades pueden agravarse aun mas como consecuencia de los continuos progresos técnicos, tales como la aparición de métodos semiautomáticos perfeccionados basados en la utilización de microfilmes o de microordenadores, que podrán ser empleados cada vez más para fines meramente privados, a la vez inofensivos e incontrolables. A mayor abundamiento, si las directrices se centraran únicamente en los ordenadores podrían dar lugar a incoherencias y lagunas, del mismo modo que podrían crear para los responsables de ficheros posibilidades de obviar las normas de aplicación de la directrices con sólo utilizar medios no automáticos para fines que podrían ser nocivos". Ibídem Ob. ut supra cit.

La definición excluye, por tanto a: a) las autoridades competentes para conocer autorizaciones o licencias y los organismos que autorizan el tratamiento de la información pero son competentes para decidir sobre que actividades deben llevarse a cabo y para que fines; b) las empresas de servicios informáticos que realizan actividades de tratamiento de la información por cuenta de terceros; c) las autoridades competentes en materia de telecomunicaciones y los organismos análogos; d) los *usuarios dependientes*, que si bien pueden acceder a los datos, no están sin embargo autorizados para decidir sobre que datos deberían ser registrados o cuales utilizados (M.E. núm.40).

Los *Datos de carácter personal*, o simplemente datos personales, se considera cualquier información relativa a una persona física identificada o identificable --o también interesado-- (R.1-b). Las directivas se aplicarán tanto a los datos personales en el sector público como en el sector privado, siempre que acarrearen un peligro para la intimidad y las libertades individuales, a causa de la manera en que fueren elaborados o por razón de su naturaleza o del contexto en que fueren usados (R.2). En esta aplicación deberá observarse: a) las medidas de protección a las diversas clases de datos tanto en la obtención, almacenamiento, elaboración o difusión. b) que no se excluyen ni siquiera datos de carácter personal que de manera manifiesta no ofrecieren riesgo alguno para la intimidad y las libertades individuales [64], y c) que no se limitará la aplicación de las directrices a la "elaboración automática" de datos personales (R.3).

Los *flujos internacionales de datos de carácter personal,* se consideran a los movimientos de datos de carácter personal a través de las fronteras nacionales (R.1-c). Aunque hace referencia a los flujos internacionales, las directrices no tienen en cuenta problemas hacia el interior de los Estados Federales. Los movimientos de datos tendrán lugar a menudo mediante la transmisión electrónica, pero también pueden servirse de otros medios de transmisión, así como por vía satélite (M.E. núm. 42).

2.3.3. Principios y excepciones fundamentales del tratamiento informatizado o no de los datos personales

---

(64) M.E. Punto 1 a 3. Los problemas prioritario que detectaron las comisiones y subcomisiones de expertos se refieren principalmente al derecho a la intimidad; la informática, la tecnología (de ordenadores, redes de comunicación), las telecomunicaciones, el derecho a la información y el de "habeas data", aunque en el texto de la Recomendación y las M.E., se hace mención genérica al derecho de acceso a la información, a conocer, actualizar, cancelar o modificar los datos de carácter personal por el titular o interesado; el "tratamiento automático de la información. En particular se refieren a la intimidad en un concepto más amplio que el tradicional derecho de "sólo dejar a sola" --el "The Right to Privacy" anglosajón--, y algo que se convertirá en la cantinela de proposición de toda la Recomendación, al decir: "con la expresión intimidad y libertades individuales constituye el aspecto más controvertido" de todos cuantos se tratan en la Recomendación de la OCDE de 1980.

Las partes segunda, tercera y cuarta de la Recomendación de la OCDE, se destinan a hacer referencia a los principios fundamentales a aplicar en el ámbito interno, los principios fundamentales a aplicar en el ámbito internacional: libre circulación de los datos y restricciones legítimas y aplicación de los principios en el ámbito interno, que no es más que un aparte reiterativo de las gestiones administrativas, jurídicas, legislativas "y de otra índole" que los Estados Miembros de la OCDE deben adelantar para implementar los medios y mecanismos idóneos para aplicar los principios en sus ámbitos legislativos internos y hacer efectivas las medidas de protección del derecho a la intimidad y las libertades individuales[65].

Los principios fundamentales aplicables al tratamiento informatizado o no de los datos personales en el ámbito nacional, según la directiva son: a) limitación de la colecta de los datos, b) calidad de los datos, c) especificación del fin, d) restricción del uso, e) garantía de la seguridad, f) transparencia, g) participación del individuo y h) responsabilidad.

En el plano internacional, los principios básicos aplicables al tratamiento (informatizado o no) de los datos personales, constituyen un complejo grupo de principios y límites que estructuran a su vez, el principio fundamental denominado: *libre circulación de datos personales* dentro de un flujo o movimiento internacional de los mismos.

2.3.4. Principios del tratamiento de datos en el ámbito nacional

Aunque se hace una distinción de los principios tanto en el ámbito nacional y el ámbito internacional, y dentro del primero en cada una de las fases del tratamiento de los datos personales (recolección, almacenamiento, registro, difusión y flujo), lo cierto es que dichos "principios son interdependientes y en parte se entrecruzan y traslapan. Por ello, las distinciones que con relación a los principios se hacen entre las actividades y las fases del tratamiento de datos son artificiales y no deben impedir que los principios sean tratados conjuntamente y estudiados como un todo" (M.E.50). Esto se evidenció además, al analizar que los diferentes Estados Miembros de la OCDE, en sus diferentes iniciativas legislativas internas para la protección de la intimidad y las libertades individuales tienen

---

(65) P.IV: *"APLICACION DE LOS PRINCIPIOS EN EL AMBITO INTERNO*. 19. Los países miembros al aplicar en su ámbito interno los principios (parte II y III) deberán crear mecanismos jurídicos, administrativos y de otra índole, o instituciones, tendentes a proteger la intimidad y las libertades individuales con respecto a los datos de carácter personal. En especial, los países miembros deberán: a) promulgar una legislación interna idónea, b) fomentar y apoyar las reglamentaciones autónomas, bien en forma de códigos de deontología, bien en otra forma, c) poner a disposición de las personas físicas medios idóneos para ejercer sus derechos, d) instaurar sanciones y recursos para los supuestos de inobservancia de medidas de aplicación de los principios que se detallan en las partes II y III. e) Velar porque no exista discriminación desleal alguna contra los interesados".

muchos rasgos comunes, así como intereses, valores básicos y principios fundamentales[66] que guían y orientan las fases o ciclos del tratamiento de los datos personales.

Analicemos brevemente los mencionados principios:

1. El *Principio de limitación de la colecta de datos*, hace referencia a aquellos datos personales que, debiendo ser obtenidos por medios legítimos y leales, y en el caso en que fuere procedente, con el conocimiento o el consentimiento del interesado, dichas actividades deberán ser limitadas (R.7).

Este principio hace referencia a dos aspectos: a) los límites que han de fijarse a la colecta de aquellos datos que debieren ser considerados como especialmente datos *sensibles*[67] a causa de la manera en que hubieren de ser tratados, su naturaleza, el contexto en el cual hubieren de ser utilizados, y b) las condiciones que deben cumplir los métodos de colecta de datos.

En cuanto al primer aspecto, hay que resaltar lo siguiente: Se deberá poner fin a la colecta indiscriminada de datos personales, y más aún cuando se trata de universalizar la consideración de qué datos se consideran sensibles. Para esto, la Recomendación suministra una serie de pautas que sirvan para determinar la índole de tales límites. Estas

---

(66) Esos rasgos comunes se sintetizan así: a) "poner límites a la colecta de datos personales, de conformidad con los objetivos del que hace acopio de tales datos y con otros criterios", b) "restringir el uso de los datos, de tal forma que se acomode a unos fines claramente expuestos; c) adoptar los medios necesarios para que el individuo conozca la existencia y el contenido de los datos y pueda requerir la corrección de los datos, y d) determinar las personas responsables del cumplimiento de las disposiciones y resoluciones de protección de la intimidad y de las libertades individuales que fueren aplicables. "En términos generales, las leyes de protección de la intimidad y de las libertades individuales con relación a los datos de carácter personal tienden a cubrir las sucesivas etapas del ciclo que comienza con la colecta inicial de los datos y termina con la cancelación u otras medidas semejantes, y a garantizar en lo posible el conocimiento, participación y control del individuo con respecto a dicho ciclo". M.E. núm. 5.

(67) Dado que por aquel entonces y hasta ahora, determinar el Agrado de sensibilidad de los datos" resulta un labor titánica, aún cuando se acude a circunstancias específicas de potencialidad del riesgo, se consideró por los expertos de la Recomendación de la OCDE, hacer mención genérica de los "datos sensibles" para que sean los Estados Miembros quienes determinen cuáles se pueden considerar como tales. Se hacía mención por ejemplo, que mientras en unos países los "identificadores personales universales" (tarjeta de identidad o cédula de ciudadanía, número de identificación profesional, de seguros, etc.), se consideran inocuos y útiles; en otros, se consideran algo delicado. Así mismo, se puso en evidencia, la disparidad de las legislaciones sobre qué datos se consideran o no sensibles. En efecto, en "las legislaciones europeas existen precedentes al respecto --es decir, considerar datos sensibles a los datos referidos a la-- (raza, creencias, religiosas, registros de condenas, p.e.). Pero también se puede argüir que ningún dato es intrínsecamente privado o sensible, sino que puede llegar a serlo según su contexto y el uso que del mismo se haga. Esta opinión se refleja en la legislación de los Estados Unidos de protección de la intimidad, por ejemplo.(M. E. 50).

son: a) los aspectos cualitativos de los datos (es decir, que deberá ser posible extraer de los datos obtenidos una información de una calidad suficientemente buena, y que los datos deberán ser obtenidos dentro de un marco informativo apropiado); b) la finalidad del tratamiento de la información (es decir, que sólo deberán ser obtenidos determinados datos y, a ser posible la colecta de datos se limitará al mínimo necesario para lograr la finalidad prevista): (i) Identificación mediante "marcas" de aquellos datos que según las tradiciones y actitudes propias de cada país miembro fueren especialmente sensibles; (ii) actividades de colecta de datos de determinados responsables de datos; (iii) preocupaciones relativas a los derechos humanos (M.E. núm. 51).

En cuanto al segundo aspecto, es decir las condiciones de los métodos de colecta de datos, se advierte contra ciertas prácticas que implican, por ejemplo, el uso de dispositivos ocultos de registro de datos, tales como magnetófonos u otros que inducen a error a los interesados, moviéndoles a facilitar información. La necesidad de poner los datos en conocimiento del interesado (que puede estar representado por un tercero, como en el caso de los menores de edad o personas “deficientes mentales”, etc.) o de obtener su consentimiento para registrarlos, constituye una norma básica, y el conocimiento, la exigencia mínima. Sin embargo, por razones prácticas, no es posible siempre exigir el consentimiento. p.e. las investigaciones criminales y la actualización periódica de las listas de distribución de correspondencia (M.E. núm. 52).

2. El *Principio de calidad de los datos*. Los datos personales deben ser pertinentes con respecto a los fines para los que fueron usados, y, en la medida en que fueren necesarios para tales fines, deberán ser exactos y completos, debiendo asimismo ser actualizados constantemente (R.8) .

La calidad de los datos hace relación a dos aspectos claramente definidos para toda información, más cuando ésta es de carácter personal. En efecto; uno, es el cumplimiento en todo el tratamiento (informatizado o no) de datos desde la recolección misma hasta la fase de difusión, recuperación o transmisión acerca de la finalidad con que han sido tratados los datos y su correspondiente utilización posterior; y otro, como verificación de lo anterior, el de que los datos tratados deberán ser exactos, completos y constantemente actualizados. Estos aspectos están interrelacionados, puesto que no se puede exceder en la utilización de los datos la finalidad para las cuales fueron tratados (informatizada o no) en su momento. v.gr. En los datos relativos a opiniones pueden fácilmente inducir a error si se utilizan para fines con los cuales no guardan relación alguna. Lo mismo puede decirse con respecto a los datos valorativos.

Sin embargo, se evidencia que en alguna clase de datos personales el criterio de la finalidad, lleva consigo el problema de si se puede o no causarse perjuicio a los interesados por falta de exactitud, de completud y de actualidad. Tal sería, el caso de las

investigaciones de las ciencias sociales que llevan aparejados los llamados estudios "longitudinales" de la evolución de la sociedad, de investigaciones históricas y de actividades de archivo (M.E.núm. 53).

3. El *Principio de especificación del fin.* Los fines para los cuales se obtuvieren datos personales deberán ser precisados en el momento de la colecta de datos, debiendo su subsiguientemente uso limitarse al cumplimiento de tales fines o de aquellos otros que, sin ser incompatibles con los mismos, fueren especificados cada vez que fueren modificados (R.9).

Este principio reitera, complementa y concreta el anterior principio, poniendo énfasis en la relación utilización y finalidades previstas para el tratamiento (informatizado o no) de datos, los cuales deben precisarse desde el momento mismo de la recolección.

Los fines pueden ser definidos de maneras diversas y complementarias, principalmente por medio de declaraciones públicas, o bien informando a los interesados, por medio de la legislación, resoluciones administrativas y autorizaciones otorgadas por los organismos de tutela.

Así, cuando los datos hubieren dejado de estar subordinados a un fin y, siempre que fuere posible, podrá ser necesario hacerlos destruir (borrar) o darles forma anónima. Esto por cuanto, los datos dejan de tener interés, sucede que se pierde el control sobre ellos y pueden surgir nuevos riesgos, tales como, “el hurto, reproducción no autorizada o de otras acciones ilícitas” (M.E. núm. 54 *in fine*).

4. El *Principio de restricción del uso*. Los datos personales deberán ser revelados, facilitados o, en general, usados para fines que no fueren los que se especificaren de conformidad con el anterior principio, excepto en los siguientes supuestos: a) previo el consentimiento del interesado, b) previa habilitación legal al efecto (R.10).

Este principio que limita el uso de los datos en ciertos y precisos casos, no es más que un principio bisagra de los principios relativos a la calidad y la determinación del fin, y como tal, juega un papel de inmovilizador de las facultades discrecionales que tuvieran las autoridades competentes, responsables de un fichero o incluso usuarios de los datos personales tanto en la revelación o divulgación como en el mera uso de los mismos. Por ello, se limita la divulgación o el uso de los datos que impliquen desviaciones con respecto a las finalidades previamente determinadas.

La regla general, por la cual todo tratamiento de datos debe tener previamente determinadas sus finalidades desde el momento mismo de la recolección, precisa dos excepciones, a saber: una, por el consentimiento del interesado (o de su representante, en

el caso de menores, etc.); y otra, por disposición normativa. Estas excepciones son *numerus clausus*, y por tanto, no cabe excepciones interpretativas según este principio.

En tal virtud, podría destinarse datos personales a fines de investigación, estadísticos y de planificación social, que inicialmente se han obtenido con miras a tomar decisiones de tipo administrativo, sin que medie para ello, el consentimiento o así lo determine una norma jurídica.

5. El *Principio de garantía de la seguridad*. Deberán preverse medidas adecuadas de seguridad para proteger datos personales contra riesgos tales como la pérdida o el acceso, destrucción, uso, modificación o divulgación de los mismos sin la oportuna autorización (R.11).

Este principio constituye el epicentro de las medidas de protección del derecho a la intimidad y de las libertades individuales, cuando se ha sometido a tratamiento (informatizado o no) datos personales por quienes están involucrados en dicho tratamiento. Para concretar las denominadas “garantías adecuadas”, contra los riesgos tales como, la pérdida de datos (que incluye el borrado a causa de accidente, la destrucción de soportes de información y el “hurto” de tales soportes), el acceso no autorizado para destruir, modificar o divulgar datos, o más aún, el uso indebido o no autorizado de los mismos (que incluye la reproducción no autorizada de datos), deberán las autoridades competentes implementar medidas idóneas proporcionales a los riesgos que los titulares de los datos pueden sufrir.

El grupo de expertos de la Recomendación de la OCDE, a título de ejemplo, propuso una serie de “garantías adecuadas”, tales como, las de índole material (cerrojos en puertas y tarjetas de identificación, por ejemplo), *medidas de organización* (niveles jerárquicos en relación con el acceso a los datos, así como la obligación que tiene el personal responsable del tratamiento de la información de *respectar el carácter confidencial de los datos*), y sobre todo en los sistemas informáticos, *medidas relacionadas con la información* (encriptación, control de actividades inusitadas capaces de constituir un peligro y medidas tendentes a hacerles frente). (M.E. núm. 56).

6. El *Principio de transparencia*. Deberá adoptarse una norma general de transparencia en cuanto a las innovaciones, prácticas y criterios existentes con respecto a los datos personales. Deberá ser posible disponer fácilmente de medios que permitan determinar la existencia y naturaleza de los datos personales, el fin principal de su uso y la identidad del responsable de los datos y la sede habitual de sus actividades (R.12).

Como lo expone el grupo de expertos de la OCDE, el principio de transparencia puede ser considerado como condición previa del principio de participación individual. Como tal se

considera una condición *sine qua nom*, para que pueda darse cabal y recto cumplimiento a uno de los principales principios con relación al tratamiento de datos, cual es el de la participación individual.

7. El *Principio de participación del individuo*. Toda persona física gozará de los siguientes derechos: 1) obtener del responsable del fichero o de otra instancia la confirmación de si el responsable de datos tiene datos acerca de su persona. 2) Requerir que se le comuniquen los datos que hicieren referencia a la misma, y ello: i) dentro de un plazo prudencial, ii) previo abono, en su caso, de una tasa que no fuere excesiva, iii) de manera razonable, iv) de manera directamente inteligible. 3) ser informado de la motivación de la resolución denegatoria de la petición formulada al amparo de los apartados *a*, y *b*, y poder recurrir contra la denegación. 4) impugnar datos que hicieren referencia a la misma y, en el supuesto de que la impugnación fuere fundada, requerir que los datos fueran cancelados, rectificados, completados o modificados (R.13).

Este principio fundamental esta estructurado por una serie de derechos y deberes que tienen y deben cumplir los sujetos interactuantes en el tratamiento o procedimiento (informatizado o no) de la información o datos. En efecto, se establecen los derechos que goza toda persona física en el transcurso del tratamiento de datos desde la recolección misma, así como las obligaciones que tienen que cumplir los responsables del fichero o autoridades competentes para proteger, respetar y hacer respetar esos derechos. Todo ello, dirigido a garantizar la protección de la intimidad y las libertades individuales.

Cuando en el principio se hace mención a los derechos que tiene toda persona para acceder, conocer, impugnar, y en su caso solicitar, la cancelación, rectificación, complementación o modificación y actualización de los datos personales que le conciernen, simple y llanamente estamos haciendo referencia al derecho denominado de A*habeas data*@, por el cual la persona puede tener control de sus propios datos. Obviamente este derecho, como todo derecho fundamental, no es absoluto y está sometido a limitaciones previstas en las propias normas jurídicas.

Por ello, los expertos de la OCDE, concretaron lo siguiente:

a) El derecho de acceso deberá ser, en general, fácil de ejercitar. Esto puede significar, entre otras cosas, que debería formar parte del conjunto de las actividades cotidianas del responsable del fichero o del que hiciere sus veces y no requerir proceso judicial o medida análoga alguna. En algunos casos podría quizá ser conveniente prever un acceso intermedio a los datos; así, por ejemplo, en la esfera médica el médico podrá servir de intermediario.

b) La condición de que los datos sean comunicados dentro de un plazo razonable puede ser cumplida de modos diversos. Así, el responsable de un fichero que facilite información a los interesados a intervalos regulares puede ser dispensado de la obligación de responder inmediatamente a las peticiones formuladas individualmente. Normalmente, el plazo deberá ser computado desde la recepción de una petición. Su duración podrá variar en cierta amplitud de una situación a otra en función de circunstancias tales como la índole del tratamiento de la información.

c) La comunicación de tales datos *de manera razonable* significa, entre otras cosas, que debe presentarse la debida atención a los problemas de la distancia geográfica, cuando menos.

d) El derecho a ser informado de las razones, en los términos previstos en el apartado 3, es limitado en cuanto que se constriñe a situaciones en las cuales hubieren sido desestimadas peticiones de información.

e) El derecho a impugnar, contemplados en los apartados 3 y 4, tiene una gran amplitud, y comprende las reclamaciones formuladas en primera instancia ante los responsables de los datos y asimismo los subsiguientes recursos presentados ante tribunales, organismos administrativos, órganos profesionales u otras instituciones, siguiendo los cauces previstos en los reglamentos internos de procedimiento. El derecho a impugnar no implica que el interesado pueda decidir cuáles sean los recursos o reparaciones disponibles (rectificación, incluso de una anotación que precise que los datos son objeto de litigio, etc.); tales cuestiones serán resueltas aplicando el Derecho interno y los cauces procesales internos (M.E. núm. 58 a 61).

8. El *Principio de responsabilidad*. El responsable del fichero deberá responder de la observancia de las medidas tendentes a dar cumplimiento a los principios que anteceden (R.14).

Este principio dirigido al responsable de los ficheros constituye el principal principio-deber de éste y principio-derecho de los titulares de los datos personales para demandar su efectividad. Este responsable no será dispensado de tales obligaciones ni siquiera cuando el tratamiento de datos es “llevado a cabo por su cuenta por un tercero, como una oficina de servicios, por ejemplo. Más aún, es probable deducir responsabilidad” al personal de las oficinas de servicios, a los *usuarios dependientes* y a otras personas. Por ello, las sanciones impuestas por incumplir la obligación de *confidencialidad* podrán afectar a todas las personas, físicas o jurídicas, encargadas del tratamiento de los datos de carácter personal (M.E.núm.62).

2.3.5. Principios del tratamiento de datos en el ámbito internacional: Libre circulación y restricciones legítimas

Este grupo de principios que se concreta en el *Principio fundamental de la Libre circulación de los datos*, está previsto en la parte III, apartados 15 a 18 de la Recomendación de la OCDE. Decimos grupo de principios porque la Recomendación no deslinda uno a uno, como sí lo hace en el ámbito nacional, los principios aplicables al ámbito internacional. En los apartados mencionados se dan pautas que unidas concretan el principio fundamental que se quiere resaltar, el de la libre circulación de los datos. Sin embargo, no debemos olvidar que siendo la transferencia, flujo o movimiento de datos uno de los ciclos posibles del tratamiento de datos personales, es lógico pensar que a esta clase de información transmitida en el ámbito internacional se tengan que aplicar los principios generales para todo el tratamiento de la información, es decir, los que hemos comentado en el apartado anterior, para el nivel nacional. Esta tesis se ve reforzada en el texto de la Recomendación misma, pues "los países miembros deberán tender a la formulación de unos principios en el plano interno e internacional que rijan el derecho aplicable en los supuestos de flujos internacionales de datos personales" (R.22), debiendo tener en cuenta estos países "las implicaciones que para otros países miembros tuvieran el tratamiento interno de datos personales y su reexportación" (R.15).

Para conseguir la incardinación de dichos principios e implementar las medidas de seguridad necesarias a nivel internacional, "los países miembros deberán adoptar las medidas razonables oportunas para que los flujos internacionales de datos personales, incluso el tránsito por un país miembro, sean ininterrumpidos y seguros" (R.16); es decir, que deben estar protegidos contra los accesos desautorizados, la pérdida, destrucción, modificación o cancelación de datos. Esta protección debe extenderse a todos los datos personales, incluso a los "*datos en tránsito*", o sea, aquellos que transitan de un país a otro sin ser utilizados o almacenados en éste con finalidades de posterior uso o consulta [68].

---

(68) "El compromiso general que se contempla en el apartado 16 deberá ser considerado, por lo que respecta a las redes de ordenadores, dentro del contexto del Convenio Internacional de Telecomunicaciones de Málaga-Torremolinos (25 de Octubre de 1973). En virtud de este convenio, los miembros de la Unión internacional de Telecomunicaciones (UIT), entre ellos los países miembros de la OCDE, acordaron entre otras cosas, adoptar las medidas oportunas para crear los canales e instalaciones necesarios con el fin de asegurar un intercambio rápido e ininterrumpido de las telecomunicaciones internacionales. A mayor abundamiento, los países miembros de la UIT acordaron adoptar todas la medidas posibles y compatibles con el sistema de telecomunicación empleado, con objeto de garantizar el secreto de la correspondencia internacional. En cuanto a las excepciones, los miembros se reservaron el derecho de suspender el servicio de las telecomunicaciones internacionales, así como el derecho de comunicar la correspondencia internacional a las autoridades competentes, con el objeto de garantizar la aplicación de su legislación interior o la ejecución de los convenios internacionales en los cuales fueren parte los países miembros de la UIT. Estas normas se aplicarán tan pronto como los datos fueren transmitidos por medio de las lineas de telecomunicación. Dentro de su contexto propio, las directrices constituyen un medio suplementario de garantizar que los flujos internacionales de datos de carácter personal tengan lugar sin interrupción y con plena seguridad" (M.E. núm. 66).

Todo ello, por cuanto a nivel interno, los Estados miembros de la OCDE, presentaban diferentes problemas que no podía resolver aisladamente y surgidos por la adopción de medidas que amparan a la persona con respecto al flujo o movimiento de datos personales a través de sus fronteras [69]. Además porque, este flujo había crecido, a la par con la creación de *bancos internacionales de datos* (entendiendo como tales, los conjuntos de datos almacenados para poder ser recuperados y para otros fines). Esto no sólo justificaba la necesidad de cooperación internacional entre los Estados para resolver estos problemas, para velar porque los procedimientos aplicables al flujo internacional de datos personales y la protección de la intimidad y de las libertades individuales sean seguros y compatibles con los de otros países miembros, sino que consecuentemente fundamentaba el *libre flujo de la información*, así como el grupo de principios que éste conlleva, pues hasta ahora la libre circulación de datos "con frecuencia debe ser mitigado en aras de la protección de datos y de las oportunas limitaciones con respecto a su colecta, tratamiento y difusión" (M.E.7).

Se establece como regla general, la libre circulación de los datos personales, como un principio-derecho, no absoluto, y por tanto limitada en los siguientes casos:

a) Todo país miembro deberá abstenerse de restringir los flujos internacionales de datos personales que tuvieren lugar entre su territorio y el de otro país miembro, excepto en el supuesto de que este no observare sustancialmente las presentes directrices o cuando la reexportación de dichos datos permitiere soslayar la aplicación de su legislación interna de protección de la intimidad y de las libertades individuales (R.17 *Ab initio*).

b) Todo país miembro podrá asimismo imponer restricciones con respecto a determinadas clases de datos personales para las cuales su legislación interna de protección de la intimidad y de las libertades individuales previere regulaciones normativas específicas basadas en la naturaleza de tales datos, siempre que el otro país miembro no les otorgare una protección equivalente (R.17 *In fine*). Con ello no se quiere que los países tengan regímenes de protección idénticos (en forma y fondo), sino que sus efectos puedan considerarse en esencia idénticos entre los Estados que intervienen en el movimiento de datos (Emisor/Transmisor de datos. Aunque la Recomendación utiliza una terminología ius-mercantilista criticable de Importador/Exportador de datos).

---

(69) "Otras razones para completar la reglamentación del tratamiento de datos personales a nivel internacional, son: a) los principios en juego hacen referencia a ciertos valores que varios países ansían preservar y ver respetados; b) pueden contribuir a ahorrar gastos en la circulación internacional de datos; c) los países tienen un interés común en evitar la creación de enclaves en los cuales fuera fácil hurtarse al cumplimiento de las reglamentaciones nacionales internas relativas al tratamiento de la información" (M.E.9).

c) Los países miembros deberán abstenerse de dictar disposiciones legales, formular directrices políticas o crear prácticas que, concebidas en nombre de la protección de la intimidad y de las libertades individuales, excedieren las exigencias de dicha protección y fueren por ello incompatibles con la libre circulación de datos personales a través de las fronteras (R.18). Sin embargo, esta restricción impuesta a nivel interno no significa que se limite la actividad legislativa de los Estados sobre flujos transfronterizos en el marco comercial, tarifas aduaneras, empleo y "a otros factores económicos conexos que condicionan el tráfico internacional de datos" (M.E.núm. 68).

2.3.6. Excepciones a las Directrices

La regla general que se establece en la Recomendación para estructurar las excepciones a las Directrices, es la de que éstas constituyen en el ámbito de aplicación de los Estados Miembros de la OCDE, "pautas mínimas susceptibles de ser completadas con medidas adicionales de protección de la intimidad y de las libertades individuales" (R.6).

Si bien, ni técnica ni jurídicamente la Recomendación *sin fuerza ejecutiva*, expone un listado de los supuestos que deben considerarse como excepciones, como se hace en las legislaciones a nivel interno, no debe desdeñarse el hecho de plantear unas pautas generales para su aplicabilidad, partiendo de la expuesta regla general. En efecto, se entiende entonces que las excepciones serán las mínimas posibles y deben darse a conocer al público por medios idóneos (p.e. publicación en diario oficial). Dentro de ese *exceptionis mínimum*, la Recomendación destaca tres supuestos genéricos: La Soberanía y la Seguridad nacionales y el orden público. Aspectos estos que en las diferentes legislaciones de los Estados, aún ahora, han sido definitivos para construir un sistema de excepciones, aún vigente.

El sistema de excepciones propuesto por la Recomendación no fue *númerus clausus* ni concentrado. Lo primero, por lo que se ha dicho anteriormente; y lo segundo, por cuanto no sólo constituyen eventos de excepciones a la regla general del tratamiento (informatizado o no) de datos, ni a la aplicación de los principios que propenden por su protección y garantía, sino porque en el contexto de la Recomendación se exponen supuestos con el nombre de "limitaciones", "restricciones legítimas", etc., que en puridad jurídica constituyen casos de excepciones. Bástenos mirar las llamadas restricciones legítimas al flujo internacional de datos.

2.4. El CONVENIO DE ESTRASBURGO DE ENERO 28 DE 1981

Una armonización legislativa internacional en los Estados Europeos sobre la protección de los datos personales sometidos a tratamiento informatizado por medios idóneos, constituía la aspiración capital del Convenio 108 del Consejo de Europa de 28 de Enero de 1981.

Esto es lo que se pretendió con el Convenio de Estrasburgo, y en efecto se logró. El Convenio Europeo de 1981, como también se le conoce, relativo a la *protección de personas en relación con el tratamiento automatizado de datos de carácter personal*, fue ratificado por España el 27 de Enero de 1984, con lo cual a partir de allí perteneció a los Estados con leyes de protección de datos de la *segunda generación.* Este texto, aparte de constituir norma jurídica de derecho interno en España, por el ingreso al ordenamiento jurídico (art.96.1 CE) y ser un eficaz instrumento de interpretación de los derechos humanos, en lo referente al "uso de la informática" (STC 254/1993, de 20 de Julio), ha servido de modelo normativo (en forma y contenido no muy fiel, como veremos) a la *Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal española --LORTAD--*: L.O.5/1992, Oct. 29 [70]. Incluso a la vigente Ley 15 de 1999.

En el Preámbulo del Convenio de Estrasburgo, se establecen las líneas directrices y programáticas para todos los Estados Miembros del Consejo de Europa, así como las posturas jurídicas a observar por los dichos Estados, respecto a la protección de los derechos y libertades fundamentales, en general, y al derecho a la intimidad (aunque conceptualmente se refiera a "la vida privada"), en especial. Esta particularidad ha hecho que la protección en el tratamiento informatizado de datos personales sea inmediatamente identificada en su vulnerabilidad con el derecho a la intimidad, tal como lo hicieran otras normas comunitarias y estatales de protección de datos. Así mismo se confirmó varios postulados y principios previstos en la Recomendación de la OCDE de 1980, pero especialmente sobre la *Libre circulación de datos, la libertad de información y la conciliación y respeto mutuo de derechos y libertades fundamentales.*

Estas Directrices capitales son: a) Propender por una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; b) Ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados; c) Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras; y d) Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos.

Muy a pesar de que el preámbulo en todo cuerpo normativo tiene efectos materiales y jurídicos vinculantes sobre el contexto o articulado, el Convenio prefirió pasar de reiterativo

---

(70) Las infidelidades de la LORTAD, fueron causa de recursos de inconstitucionalidad incoados por asociaciones y por la Defensoría del Pueblo Español. El autor destacaba la inspiración de contenido del Convenio seguido por la LORTAD. Vid. ORTI VALLEJO. A. Ob. ut supra cit., p. 17.

y volvió a plasmar estas directrices en forma resumida en el artículo primero, confirmando con ello la protección en el tratamiento informatizado de datos personales de todos los derechos, libertades públicas e intereses legítimos, no única y exclusivamente el derecho a la intimidad.

El Convenio está dividido en siete capítulos, a saber: 1. *Disposiciones Generales*: Objetivo y fin, definiciones, y ámbito de aplicación; 2. *Principios fundamentales de la protección de datos:* Obligaciones de las partes, calidad de los datos, clases especiales de datos, seguridad de los datos, garantías complementarias para el interesado, excepciones y restricciones, sanciones y recursos, y ampliación de la protección; 3. *De los flujos internacionales*: flujos internacionales de datos de carácter personal y derecho interno; 4. *Del Mutuo Auxilio:* Cooperación entre las partes, asistencia a los interesados residentes en el extranjero, garantías referentes a la asistencia prestada por las autoridades designadas, desestimación de peticiones de asistencia, gastos y tramitación de la asistencia; 5. *Del Comité Consultivo:* Composición del Comité, funciones del Comité, procedimiento; 6. *De las Enmiendas:* Enmiendas; y, 7. *Cláusulas Finales:* Entrada en vigor, adhesión de estados no miembros, cláusula territorial, reservas, denuncia y notificación.

De este variopinto contenido, abordaremos el análisis de los siguientes temas: a) Las definiciones nucleares en el tratamiento informatizado de datos personales y, b) Los principios y excepciones fundamentales en el tratamiento y circulación de datos.

2.4.1. Definiciones nucleares en el tratamiento informatizado o no de datos personales

El *poder de la informática* desde la expedición del Convenio y mucho antes, hacía gravitar sobre los usuarios de los sectores públicos y privado la consiguiente responsabilidad social. En la sociedad moderna, gran parte de las decisiones que afectan a los individuos descansan en datos registrados en ficheros o bases de datos (v.gr. Nóminas, expedientes de seguridad social, historiales médicos, judiciales, policiales, etc.). En los años que siguieron a aquella época, el tratamiento informatizado de la información continuó imponiéndose en el ámbito administrativo y de gestión, entre otras cosas, a causa del abaratamiento de los costes del tratamiento informático de los datos, de la aparición en el mercado de dispositivos de tratamiento inteligente y de la creación de nuevos sistemas de telecomunicaciones para la transmisión de los datos, tal como lo destacaba también la Memoria Explicativa del Convenio (M.E.).

Un cierto halo de temor que rondaba a los operadores jurídicos (abogados, jueces, administradores, etc.) al aplicar cuerpos normativos jurídico-técnicos, como lo era el Convenio Europeo de 1981, inspiraba a los legisladores a implementar un capítulo preliminar que funcione como glosario técnico-jurídico que guía y orienta a los operadores

jurídicos del Convenio. Así, se paliaba ese temor, que aún ahora subsiste en todas las normas que regulan el fenómeno tecnológico de la información y la comunicación (TIC), unido a la informática.

En tal virtud, el Convenio definió los siguientes términos nucleares en todo tratamiento informatizado de los datos: Datos personales, persona identificable, interesado, “fichero automatizado”, “tratamiento automatizado” y “autoridad controladora”, entre otros.

Los datos de carácter personal (o datos personales), se consideran cualquier información relativa a una persona física identificada o identificable ("persona concernida", como insiste el Convenio).

Se deduce de esta definición, que el concepto de *persona concernida*, a los efectos de determinar de identificación dentro de un procedimiento informatizado de datos, no solamente abarca los rasgos de identificación de la persona de carácter jurídico (como los registros de nacimiento, médico, etc., documento de identificación personal v.gr. Documento Nacional de Identidad DNI en España o Documento de Identidad Nacional DIN o Cédula de ciudadanía en Colombia, Pasaportes, etc.), sino también de carácter físico interno v.gr. Exámenes sanguíneos, de líquidos humanos diferentes a la sangre (semen, orina, etc.), exámenes morfológicos (color de piel, facial, dentales, ópticos, de estatura, etc.); o de carácter físico externo, con fotografías y huellas humanas y/o tecnológicas (códigos, password o firmas digitalizadas). Estas huellas, se consideran como rasgos diferenciadores de una persona humana de carácter morfológico o tecnológico con incidencia jurídica.

Esta identificación del ser humano o de la “persona concernida” es la que a la luz del Convenio constituye el núcleo central del concepto de datos de carácter personal, muy a pesar de que se sostiene en la E.M., del Convenio, que “persona identificable”, es aquella “persona que puede fácilmente ser identificada”, sin necesidad de “identificación de personas por métodos complejos” [71]. Quizá en aquella época en que surgió la norma europea, tal proposición pudiera ser válida parcialmente, pero hoy no, pues dicha identificabilidad de las personas, antes y ahora debe incluir métodos y procedimientos científico-técnicos idóneos, máxime si se refiere al tratamiento informatizado de datos personales --con o sin el consentimiento del titular--, que relacionan datos personales contenidos en documentos jurídicos, registros de estado civil, médicos, judiciales, económicos o financieros, etc., en todos los cuales para una debida identificación de la persona se debe emplear medios idóneos de tipo técnico-científicos irrefutables previos al asiento o registro informático o concomitante con éste.

---

(71) Memoria Explicativa del Convenio 108 de 1981. M.E.núm.28. Compilados por HEREDERO HIGUERAS, Manuel. ***Legislación Informática.*** Ed. Tecnos, Madrid, 1994, p.570

Hoy, el ser humano tiene un derecho a *la identificación* sico-física, como persona humana dotada de cuerpo, mente e inteligencia, válido o validable en todo ámbito social, cultural, político, económico, y sobre todo jurídico o iusinformático. Por lo tanto, no se puede desdeñar ningún método científico-técnico para la plena identificación en todo procedimiento que tenga incidencia en el pleno ejercicio de los derechos y libertades fundamentales de una persona. El Convenio recoge este parecer cuando sostiene que su objetivo prioritario es "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" (M.E.núm. 1).

El concepto de persona concernida también se extiende al de persona "*interesada"*, que el Convenio utiliza en varios artículos. Así, *interesado*, "expresa *la idea* según la cual toda persona tiene un derecho subjetivo sobre la información relativa a sí misma, aún cuando tal información haya sido reunida por otras personas (cfr. la expresión inglesa *data subjetc*)[72]

El "*fichero automatizado*" o bancos de datos. Significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado. Aunque en la E.M., del Convenio eufemísticamente se dice que se prefiere el nombre de fichero al de Banco de datos, porque esta expresión se utiliza "hoy en un sentido más especializado: el de un fondo común de datos accesibles a varios usuarios" [73]. Sin embargo, la diferencia hoy por hoy es simplemente terminológica y de origen idiomático (Banco de datos término anglosajón "*database*" o, Fichero informatizado del término francés "*Fichiers*".

Los Estados Miembros del Consejo de Europa eran conscientes de que día a día crecían por la irrupción de la tecnología TIC y la informática, maneras y formatos de recolectar y almacenar información de todo tipo (incluida las denominadas "personales") con medios informáticos, electrónicos o telemáticos, y que se materializaban en los llamados ficheros o bancos de datos, por regla general. Eran también, conscientes de que los diversos Estados tenían en sus sistemas jurídicos regulaciones sobre el derecho a la intimidad de las personas, la responsabilidad civil, el secreto o la confidencialidad de ciertas informaciones sensibles, etc. Sin embargo, se echaban de menos unas reglas generales sobre el registro y la utilización de informaciones personales y en "especial sobre el problema de como facilitar a los individuos el ejercicio de un control sobre informaciones que, afectándoles a ellos, son colectadas y utilizadas por otros" (M.E.núm.3). En tal virtud, se decidió concretar además de el concepto de datos de carácter personal, qué debe entenderse por fichero o banco de datos para proteger los derechos y libertades fundamentales de la persona y

---

(72) Ibídem., p. 570.

(73) El M.E. núm. 30 *ab initio*, sostiene que la "expresión ´fichero automatizado´ ha sustituido a la de ´banco de datos electrónico´ utilizada anteriormente en Resoluciones (73)22 y (74)29 y en algunas leyes nacionales. Por ello, en el transcurso de la investigación utilizaremos indistintamente fichero o banco de datos para referirnos al mismo concepto.

facilitar el autocontrol de los mismos por parte de la persona concernida.

El concepto de fichero o banco de datos informatizados, comprende “no solamente ficheros consistentes en conjuntos compactos de datos, sino a si mismo conjuntos de datos dispersos geográficamente y reunidos mediante un sistema automatizado para su tratamiento” (M.E.núm. 30 *ab initio*).

La definición de fichero “automatizado” para diferenciarlo del fichero o banco de datos mecánico o manual, resulta reiterativo cuando menos desde el punto de vista terminológico, cuando al final sostiene que ese conjunto de informaciones deben estar sometidas a un tratamiento igualmente “automatizado” (que mejor sería decir informatizado[74]). Sin embargo, esta observación es de menor entidad, frente a la significancia de la inclusión de un término imprescindible en el tratamiento lógico de entrada (E/) y salida (/S) de información por medios informáticos, como lo es el de fiche- ro o banco de datos informatizados. Esta aclaración delimita a su vez, el ámbito de aplicación del Convenio, al tratamiento informatizado de los datos o información de carácter personal, a diferencia de la Recomendación de la OCDE de 1980, que abarcaba incluso el tratamiento no informatizado de datos personales, aunque la definición siguiente desmienta tal diferenciación, al menos en toda su integridad.

En efecto, por *"tratamiento automatizado",* se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión (art. 2, c). Este tratamiento de datos se extiende a los datos de carácter personal en los sectores público y privado (art. 3-1, del Convenio) [75]

---

(74) Preferimos decir “informatizado”, porque entre otras razones que se dan a lo largo de la investigación, existen estrechos vínculos entre la información obtenida (cualquiera sea esta, y más si es de tipo personal) con “la informática documental”, según los términos del profesor *LOPEZ MUÑIZ-GOÑI,M* (En: ***Informática Jurídica Documental***) que utiliza métodos y procedimientos informatizados en el tratamiento lógico, sistemático y analítico de la información que ésta proporciona y no solamente un tratamiento robótico o “automático” de la información, tal como lo hacen los cajeros electrónicos, sistemas electrónicos de detección de personas o cosas, etc. Es un tratamiento logicial con medios informáticos, electrónicos o telemáticos y no simplemente cibernético o robótico aunque éste sea la base del mismo.

(75) El Convenio se aplica al sector público y privado. “Si bien es cierto que la mayor parte de la circulación internacional de datos tiene lugar dentro del marco del sector privado, el convenio reviste, no obstante, gran importancia para el sector público y ello por dos razones: en primer lugar, el art. 3 impone a los Estados miembros la obligación de aplicar los principios de la protección de datos aun en el caso del tratamiento de ficheros públicos --que es el supuesto normal-- totalmente dentro de sus fronteras nacionales. En segundo lugar, el convenio ofrece asistencia a los interesados que deseen ejercer su derecho a ser informados del registro que de ellas lleve una autoridad pública en un país extranjero. La distinción sector público- sector privado no aparece en las demás disposiciones del convenio, sobre todo porque esta nociones pueden tener significados distintos de un país a otro...” (M.E. núm. 33).

Las acciones de tratamiento lógico de la información, que se traducen en fases o ciclos informatizados, según la definición de tratamiento automatizado del Convenio puede efectuarse total o parcialmente con procedimientos informáticos, con lo cual se introducen métodos de tratamiento mixtos de la información, en los cuales participan acciones mecánicas o manuales e informáticas.

El concepto técnico-jurídico abierto de *tratamiento de datos personales*, abre la posibilidad a la interpretación de que el Convenio no sólo regule el tratamiento informatizado de la información, sino también el no informatizado siempre y cuando contenga alguna parte, acción o fase de carácter informática. Esto es posible cuando la fase inicial o de recolección de información en un tratamiento lógico o informatizado es carácter mecánico o manual.

Las fases o ciclos del tratamiento informatizado, según el Convenio se inician con el *registro de datos* y frente a él todas las acciones (u "operaciones aritméticas", guardando con ello más relación al tratamiento robótico de la información que al lógico o sistémico) subsiguientes que pueden realizarse: modificación, borrado, extracción o difusión de la información [76]. Todas estas acciones a excepción de la última, son componentes de una acción eminentemente tecnológica realizable con los datos (o "files": archivos o registros), más que jurídica; puesto que, sí se quería referir a las acciones técnico-jurídico realizables con cualquier tipo de datos, debió hacerse mención a las fases de recolección, almacenamiento, registro, conservación, rectificación, bloqueo y cancelación de la información, tal como lo hiciera la LFAPD de 1977, y posteriormente, la Recomendación de la OCDE de 1980.

Sin embargo, el contexto del Convenio aclara la deficiente definición de *tratamiento automatizado*, cuando se refiere: a) a los principios y derechos que tiene toda persona cuando han sido sometidos a tratamiento informatizado los datos personales que le conciernen y, b) al hacer mención expresa a la fase de recolección (en los artículos 5-a y 12 del Convenio [77]) y de transmisión "internacional" (o fase de comunicación) de datos, como fases ineludibles y/o posibles del tratamiento informatizado o no de datos. Esto a pesar de la insistencia de la E.M., núm. 31 *ab initio* del Convenio al excluir la fase de recolección o colecta de información "de la noción de tratamiento" de datos, con unos

(76) La voz "difusión", según la E.M. núm. 31 ab initio, "es un término genérico que abarca tanto la revelación de información a una persona (o a varias personas), como la consulta de la información por tales personas"

(77) El Convenio utiliza los términos "obtener" o "reunir", para hacer mención a la fase inicial de recolección o colecta de datos. En efecto, el art. 5, a), expresa: "Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) *Se obtendrán* y tratarán leal y legítimamente", y el Art.12., al referirse a los "Flujos transfronterizos de datos de carácter personal y el derecho interno : 1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado *o reunidos* con el fin de someterlos a ese tratamiento".

argumentos poco convincentes [78]

La *Autoridad "controladora del fichero",* se considera a la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero informatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les deberá aplicar.

La definición contiene un concepto ampliado del *ente almacenante* que trae la LFAPD, en el art. 1-1., y a la vez, una conceptualización casi idéntica a la de "responsable del fichero" contenida en la Recomendación de la OCDE de 1980, art.1-a. En efecto, la entidad almacenante atribuible a cualquier persona, entidad, servicio o institución pública o privada, tiene como función primordial el almacenamiento (que incluye según la ley alemana, las fases de recolección, registro y conservación) de datos por sí mismo o por encargo a otro.

En cambio, "el responsable del fichero", tanto en el la Resolución de la OCDE, como en el Convenio 108 de 1981, abarca otros ciclos o fases como funciones del tratamiento informatizado de los datos o informaciones personales, tales como la transmisión de datos, la determinación de la finalidad del fichero, la categorización de los datos, el registro y hasta "cuáles operaciones se les aplicarán" (art. 2, d), del Convenio), respectivamente.

El *Responsable del fichero* se diferencia en uno y otro cuerpo normativo (OCDE y Convenio) en la circunstacia de que el "responsable del fichero", en el Convenio es única y "exclusivamente la persona o ente que en última instancia responde de la gestión del fichero, pero no aquellas otras personas que llevan a cabo las operaciones del tratamiento de conformidad con las instrucciones del responsable del fichero" (M.E.núm.32).

Este concepto de *Responsable del fichero*, cuando menos, determina dos aspectos importantes en el tratamiento informatizado de datos: por un lado, la exclusión de cualquier grado o nivel de responsabilidad de los que realizaran actividades de tratamiento por encargo; y de otra, que la determinación del responsable del fichero, lleva aparejada una garantía para las personas concernidas con el tratamiento de dato personales, la cual es, que puedan en todo momento identificar plenamente al responsable del fichero [79].

---

(78) Se dice que "ante el rápido desarrollo de la tecnología del tratamiento de la información, se consideró conveniente enunciar una definición bastante general de "tratamiento automatizado", susceptible de una interpretación flexible". Y según, la autointerpretación del legislador comunitario del Convenio, la colecta queda excluida del concepto "tratamiento".

(79) En efecto, el art. 8., del Convenio 108 de 1981, al hacer referencia a las denominadas "Garantías complementarias para la persona concernida", sostiene que cualquier persona deberá poder: "a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como *la identidad* y la residencia habitual o el establecimiento principal de *la autoridad controladora del fichero.*

2.4.2. Principios y excepciones fundamentales en el tratamiento y circulación datos personales

El Convenio 108 del Consejo de Europa de 1981, sobre protección de las personas en relación con el tratamiento informatizado de datos personales, no sólo "refuerza" la protección jurídica de los individuos en relación al tratamiento informatizado de información de carácter personal, tal como se prevé en el preámbulo, la E.M., núm. 1, y en el propio texto (art. 1); sino que además propone una armonización normativa en el ámbito competencial del Consejo de Europa. Quizá uno de los aspectos capitales en los cuales el Convenio más apuesta por la armonización normativa a nivel europeo, es precisamente en la estructuración de los principios y excepciones fundamentales, así como en los derechos subsecuentes para los titulares de datos personales que de aquellos se derivan. En efecto, el Convenio persigue homogeneizar todo lo atinente a la regulación de la protección de los titulares de los datos prevista en las leyes protección de aquellos dictados hasta ese entonces (v.gr. Alemania, Suecia, Suiza, Francia, Noruega, Luxemburgo, Portugal, etc.), como también aquellas otras leyes que se dictaron a su amparo y guía, como es el caso de la Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal española (L.O. 5/1992, de 29 de Oct.).

En efecto, las Comisiones y subcomisiones encargadas del estudio, análisis y proposición del texto definitivo del que luego fuera el Convenio Europeo de 1981, reestructuró los principios inmersos en las leyes europeas de protección de datos y en forma mancomunada abordó la tarea de su proposición final con el grupo de expertos del Comité respectivo de la OCDE [80]. Especial atención le dedicó a los principios de la libre circulación y seguridad de los datos [81]. Quizá por ello, los principios como excepciones al tratamiento informatizado de datos personales en uno y otro cuerpo normativo comunitarios resultan coincidentes, con la diferencia de que en el Convenio de Estrasburgo, estos y aquellas tienen una especial regulación que los convierte en la columna vertebral del tratamiento informatizado de datos personales.

En efecto, el Convenio Europeo como regla general establece que los principios y excepciones al tratamiento informático de datos, rigen en todo el tratamiento o procedimiento informatizado de datos personales y no en forma exclusiva y/o excluyente de una fase o etapa de dicho tratamiento (v.gr. recolección, almacenamiento, registro, conservación, etc.). Así se deduce de la redacción dada a los arts. 5 a 9 del Convenio. El

---

(80) M.E. núm. 14, "Cooperación con la OCDE y con la CEE".

(81) M.E. núm. 16. "La comisión de las Comunidades Europeas, que ha llevado a cabo estudios sobre la armonización de las legislaciones nacionales dentro del marco de la Comunidad con relación a los flujos internacionales de datos y las posibles distorsiones de la concurrencia, así como sobre los problemas vinculados a la seguridad de los datos, mantuvo estrecho contacto con el Consejo de Europa"

sistema de principios y excepciones están ligados entre sí, pues unos y otros tienden a garantizar y proteger los derechos, libertades públicas, intereses legítimos “y los valores fundamentales en una sociedad democrática” (M.E. núm. 55).

Es aquí donde halla eco y sentido el denominado “*núcleo irreductible*”[82] , basado en la catalogación de los principios y excepciones fundamentales del tratamiento informatizado de datos personales, con capitales fines y objetivos de protección y garantía de derechos y libertades fundamentales (no sólo el derecho a la intimidad, como se ha generalizado), el debido y oportuno cumplimiento que los Estados deben observar en la implementación en el ordenamiento jurídico interno (es decir, armonización legislativa) y la reducción al mínimo de los posibles conflictos de las leyes o de jurisdicción.

2.4.2.1. Principios fundamentales en el tratamiento y transmisión de datos personales

Ahora bien, hagamos referencia a los principios en relación con las fases del tratamiento informatizado de datos que es donde tienen aplicabilidad y vigencia.

2.4.2.1.1. Fase de recolección de datos

En la *fase inicial o de recolección de los datos personales*, son aplicables los principios siguientes: a) De lealtad y legitimidad (art.5-a,); b) De Prohibición excepcionada a la recolección de datos pertenecientes al “núcleo duro de la privacy” anglosajona [83] (art. 6); y, c) De información en la recolección, sobre los objetivos y fines de la misma (art. 8).

Estos principios se hallan en el Convenio bajo los epígrafes de “calidad de los datos”, “categorías particulares de los datos” y “garantías complementarias para la persona concernida”.

El principio de lealtad y legitimidad, como principio de causa y efecto entre el objeto del tratamiento (datos) y su actividad (recolección), se entiende que los datos que se van a obtener, recoger o recolectar debe pertenecer a una persona identificada o identificable, procesarse con métodos informáticos idóneos que permitan no vulnerar los derechos y libertades fundamentales del titular de los mismos y se proceda de conformidad con el

---

(82) Institución de derecho público que se explica en relación con los principios y *per se.* En efecto, “los principios del ´núcleo irreductible´ reconocen a los interesados en todos los Estados en los cuales se aplique el Convenio un determinado mínimo de protección con relación al tratamiento automatizado de datos de carácter personal” M.E. núm. 20 *in fine*).

(83) Comentado por el profesor MORALES PRATS, Fermín. *Comentarios a la parte especial del Derecho Penal.* En: ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.*** Ed. Aranzadi, Pamplona, 1996, p. 310 y ss.

ordenamiento jurídico vigente en cada Estado y en concordancia con las normas comunitarias. Queda proscrita toda recolección de datos en forma ilícita, ilegítima, indebida, inoportuna o expresamente prohibida. Quizá por esto último resulta incompleta la calificación de este principio como "principio de legalidad" de los datos, que algún sector de la doctrina ibérica lo nomina (*Castells, Souviron, López*, etc.), pues la ley queda transvasada, cuando se involucra el interés estatales o personal, el criterio de la oportunidad del tratamiento, etc.,

En principio, está prohibida la recolección de datos de carácter personal denominados "sensibles" [84] que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales (artículo 6).

2.4.2.1.2. Fase de Almacenamiento de datos

En *la fase de almacenamiento* de datos, serán aplicables los principios de: a) Exactitud del contenido (o "veracidad", según *Souvirón* [85]) y de sujeción a la revisión y actualización (art. 5-d); b) De prohibición excepcionada de los datos denominados "sensibles" (art.6); y c) De información en el almacenamiento de datos sobre los objetivos y fines del mismo (art. 8).

2.4.2.1.3. Fase de Registro de datos

En la *fase de registro de los datos personales*, que es la etapa sobre la cual más incide el Convenio Europeo, quizá por las implicaciones de tipo socio-jurídico que se derivan de dicha actividad informatizada de datos, pues ésta sobreviene con carácter definitivo en tanto no haya causas para suspenderla, suprimir o cancelarla de conformidad con el ordenamiento jurídico vigente. Pareciera, por la redacción inicial del Convenio que la protección de los titulares de los datos se inicia con el registro de los mismos y no antes. Sin embargo, una recta interpretación del Convenio extiende la protección al momento mismo de la recolección de datos, haciendo énfasis en la etapa del registro porque supuestamente más afloran los síntomas de vulnerabilidad, aspecto éste que es más apariencia que realidad, como se ha visto.

---

(84) Según *E. Vilariño*, datos sensibles son "aquellos datos personales que se refieren a las características morales o físicas que, en principio, no son de interés para los demás y no afectan en general a la sociedad y cuyo conocimiento, en cambio, puede perjudicar injustificadamente los derechos e intereses legítimos de esas personas", p. 54. Citado por SOUVIRON, José M. ***En torno a la juridificación del poder informático del Estado***. R.V.A.P. Núm. 40, Sep-Dic., Bilbao, 1994, cita núm. 67 p.153.

(85) SOUVIRON, José M. Ob. cit. ut supra. pág. 152.

Los principios aplicables a esta etapa del tratamiento informatizado son: a) De compatibilidad de las finalidades (art. 5-b); b) De adecuación, pertinencia y no excesibilidad de las finalidades (art. 5-c); c) Prohibición excepcionada del registro de datos personales denominados “sensibles” (art.6); d) Principio de información en el registro de datos (art. 8); y e) Principio de “Seguridad de los datos” (art. 7).

Se destacan en esta etapa los principios de información y seguridad de los datos, por cuanto, en puridad jurídica es aquí donde nace el derecho de *habeas data* [86] y los subsecuentes derechos que este conlleva. Efectivamente, tras el ejercicio el derecho de la información y conocimiento por parte del titular de los datos, de terceros, de personas autorizadas o no, las personas naturales, jurídicas, públicas o privadas encargadas del tratamiento (o responsables) de datos toman las necesarias medidas de seguridad para la protección de datos de registrados en ficheros informatizados, a fin de evitar la destrucción accidental o no autorizada, la pérdida accidental o el acceso, la modificación o la difusión no autorizados.

En tal virtud, aquí se ponen en juego las que el Convenio en el artículo 8, llama “Garantías complementarias para la persona concernida”, dentro de las cuales cualquier persona podrá: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos de “calidad de los datos” y “categoría particular de datos”; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, luego de conocer la existencia de un fichero con los datos del concernido o de obtener a “intervalos razonales” la confirmación de tal existencia o no.

---

(86) Se considera un derecho fundamental, que según *Fairen Guillen*, “ya no (solo) es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de *habeas data.* Tales son las ideas generalmente admitidas hoy entre juristas y en el Derecho comparado, que ofrece una de las vías para determinar el contenido esencial de un derecho fundamental (S.T.C. 11/1981)” en el derecho español. Cfr. FAIREN GUILLEN, Víctor. ***El Hábeas Data y su protección actual sugerida en la Ley Española de Informática de 29 de Octubre de 1992***. En: Revista de Derecho Procesal. Núm.3, Madrid, 1996, p. 530.

2.4.2.1.4. Fase de conservación de datos

En la *fase de conservación de los datos,* se aplicará los siguientes principios: a) De identificación del concernido y de compatibilidad de las finalidades. En ejercicio de este principio, se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado (art. 5-e,); b) De Prohibición excepcionada en la conservación de datos personales considerados "sensibles" (art.6); c) De Seguridad de los datos (art. 8); y d) De información en la conservación de datos.

2.4.2.1.5. Fase de transmisión de datos. En particular, "el flujo internacional de datos" [87]

En la *fase de transmisión, flujo o movimiento de los datos,* a la que el Convenio también le ha prestado especial cuidado y tratamiento, rigen los principios previstos bajo los epígrafes de "calidad de datos", "categoría particular de datos", "Seguridad de datos" y "garantías complementarias para la persona concernida", que antes hemos referenciado, pues al fin y al cabo la transmisión de datos es otra fase más del tratamiento de datos, tal como lo sostiene el art. 12.1 del Convenio Europeo [88]. Pero además, se aplicará un principio fundamental y específico para esta fase del tratamiento informatizado de datos personales, cual es la "*libre circulación de datos*" [89], que desde la Recomendación de la OCDE de 1980, ya había sido planteado y sustentado.

Esta fase del tratamiento informatizado de datos personales es tan importante como delicada, pues los Estados que poseían medidas legislativas protectoras de dicho trata -

---

(87) La M.E. del Convenio Europeo especifica el alcance de la noción de *flujos internacionales*, ha sido redactado de tal manera que tenga en cuenta la gran diversidad de los factores determinantes del modo en que los datos son transferidos: modalidad de representación (texto libre o codificado), soporte (papel, tarjeta perforada, cinta perforada, cinta magnética, disco, etc.), medio de transporte (transporte físico, correo, enlace de telecomunicación conmutada por circuito o paquetes), interfaz (ordenador con terminal, ordenador con ordenador, manual con ordenador, etc.), el circuito dedicado (directo desde el país de origen al país de destino, o a través de uno o varios países de tránsito), las relaciones entre el emisor y el destinatario (pertenecientes ambos a una misma organización o a distintas organizaciones), etc. (M.E. núm. 63).

(88) Artículo 12. "Flujos transfronterizos de datos de carácter personal y el derecho interno 1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal *que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento"* (Cursivas nuestras).

(89) Este principio fundamental en el tratamiento y transmisión de datos personales, tanto para los individuos como para los Estados, se erigió, "habida cuenta de la rápida evolución de las técnicas de tratamiento de la información y del desarrollo de la circulación internacional de datos...(y de que era) conveniente crear unos mecanismos a escala internacional que permitan a los Estados tenerse informados mutuamente y consultarse entre sí en materia de protección de datos" (E.M. núm. 11 *in fine*).

miento habían preparado y aplicado sus normas hacia el interior de sus zonas geográficas, pero no estaban preparados inicialmente para afrontar las dificultades sobrevenidas por la transferencia de datos entre Estados. La creación de “bancos de datos internacionales”, con diferentes fines, objetivos y actividades evidenció más aún dichas dificultades, pero a la vez, con la generalización de las transferencias internacionales en los ámbitos sociales, políticos, culturales, jurídicos y sobre todo económicos de la UE, se puntualizó y potenció toda clase de medidas de seguridad, eficacia, oportunidad y celeridad de la transmisión/emisión de datos personales, para eliminar las dificultades y aumentar el flujo necesario de información entre Estados, sin mayores riesgos que los sobrevenidos de actividades indebidas, ilegales o no autorizados, tanto de tipo técnico como jurídico. En efecto, así ocurrió con las variopintas transacciones comerciales (v.gr. agencias de viajes, operaciones bancarias, cajeros automáticos: tarjetas de crédito, debido, etc.), las transferencias en actividades personales privadas o públicas (.v.gr. Bancos de datos médicos, investigativos, bibliotecológicos, estadísticos, etc.); o en fin, para transmitir información de un lugar geográfico transfronterizo a otro sin las debidos controles (técnicos o jurídicos, según la M.E. núm. 8), con fundamento en los adelantos de las telecomunicaciones, la informática, o la unión de las dos: la comunicación electrónica o telemática.

En especial, --se decía en el E.M.núm.9-- existe el temor de que los usuarios se sientan tentados a “hurtarse” a los controles impuestos por la protección de datos desplazando sus operaciones, en todo o en parte hacia “paraísos de datos”, es decir, a países que tengan leyes de protección de datos menos rigurosas o que carezcan de leyes de protección de datos. Aunque algunos otros Estados para evitar estos riesgos han previsto en su Derecho interno controles jurídicos especiales, como las “autorizaciones de exportación de datos”, las cuales pueden resultar excesivos o insuficientes, frente a la avalancha de crecimiento de las transmisiones electrónicas de datos entre Estados.

El Convenio, en consecuencia, establece que un Estado no podrá “prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio” de otro Estado, so pretexto “de proteger la vida privada”, salvo: a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación del otro Estado (*o Parte*) establezca una protección equivalente; b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otro Estado, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación del Estado a que se refiere el comienzo del presente párrafo (art. 12 *in fine*).

En estas transmisiones interestatales, el mayor flujo de circulación de datos lo ocupan las transferencias de datos de carácter personal, por ello, el Convenio plantea como regla general, la *libre circulación de información* , como principio fundamental, tanto para los individuos como para los Estados (o "pueblos", según la E.M.núm.9) y como excepciones, las directrices previstas con carácter de *numerus clausus* para algunas categorías de datos personales (básicamente los denominados *sensibles*) o ficheros que los contengan y para aquellas transmisiones triangulares entre Estados y uno de los cuales no pertenezca al Consejo europeo.

Si no fuese así, "tales controles (como el de la autorización, p.e.) podrían crear trabas a la libre circulación de la información", erigida como principio fundamental en el tratamiento y transmisión de datos personales entre Estados. "Había que encontrar, por tanto, una fórmula que garantizara que la protección de datos a escala internacional no vulneraría este principio" (M.E. núm. 9 *in fine*). Se trata en últimas de conciliar [90] dos aspectos capitales en el tratamiento y transmisión de datos personales, que tienen la particularidad de ser concurrentes y aparentemente excluyentes: por un lado, la protección de datos; y por otro, la libre circulación de los mismos. Concurrencia que se consigue cuando toda transmisión o flujo de datos debe prever cierto mínimo de garantías o de protecciones, pero no de controles especiales ni menos rigurosos que pudieran excluir la libre circulación de los datos. De ahí el establecimiento de una regla general con sus taxativas excepciones.

La E.M., del Convenio sustenta una serie de características especiales referentes a los flujos internacionales de datos, las cuales en su conjunto reafirman la regla y excepciones anotadas.

En efecto, se establece que con base en el principio del *núcleo irreductible* que reconoce a los interesados en todos los Estados en los cuales se aplique el Convenio un determinado mínimo de protección con relación al tratamiento informatizado de datos, y como tal, al obligarse a aplicarlos los Estados y miembros, "tienden a suprimir entre ellos las restricciones de los flujos internacionales de datos, evitando que el principio de libre circulación de datos sea puesto en tela de juicio por alguna forma de proteccionismo" (M.E. núm. 20 *in fine*).

Respecto de la transmisión o flujos de datos personales calificados de sensible (relativos al origen racial, origen racial, las opiniones políticas, las convicciones religiosas u otras

---

(90) Ese es el objeto principal del art. 12 del Convenio de Europa, "conciliar las exigencias de protección eficaz de los datos con el principio de la libre circulación de la información independientemente de la existencia de fronteras, consagrado por el artículo 10 del Convenio Europeo de los Derechos del Hombre" (E.M. núm. 62).

convicciones, la salud [91] o a la vida sexual, según el art. 6 del Convenio) se establece, al menos dos directrices para que un Estado justifique la derogación de las garantías que el Convenio ofrece a esta clase especial de datos personales. Estas son:

a) Cuando las medidas específicas de protección de tales datos fueren sensiblemente distintas de las disposiciones del derecho de los demás Estados que hicieren referencia a tales datos y, en especial, cuando tales medidas ofrecieren, de conformidad con el art. l1, (es decir, que ninguna de las disposiciones del capítulo II, se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Estado, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio) un nivel de protección que transcendiere las normas mínimas contenidas en el Convenio.

b) Cuando determinados datos o ficheros que no estuvieren previstos dentro de los denominados datos sensibles, estuviesen sujetos a garantías especiales.

No será lícita la derogación, en estos casos, si el Estado destinatario ofreciere una protección equivalente. v.gr. Si un Estado somete los flujos internacionales de datos a una autorización especial, no puede negarse otro Estado, so pretexto de razones de protección de la intimidad, a conceder una tal autorización si el país receptor concede una protección equivalente (E.M. núm. 69 *in fine*).

Respecto de la *transferencias triangulares de datos personales*, o sea, aquellas que tienen lugar en dirección a un Estado no contratante a través de un Estado contratante, la derogación sólo puede ser invocada si está previsto que los datos transferidos se encuentren en un Estado contratante sólo en tránsito. No deberá ser invocada sobre la base de la mera presunción o expectativa de que los datos transferidos a otro Estado contratante pudieran, en su caso, ser transferidos a un Estado no contratante (E.M. núm. 70).

2.4.2.2. Excepciones al tratamiento informatizado de datos y a los principios. "Las Restricciones"

Para establecer un régimen jurídico de excepciones en un ámbito interestatal, se debe

---

(91) Los datos de carácter personal relativos a la salud, fue cuidadosamente estudiado por el Comité de expertos de protección de datos dentro del contexto de sus trabajos sobre los bancos de datos médicos. Tal noción abarca las informaciones concernientes a la salud pasada, presente y futura, física y mental, de un individuo. Puede tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas (E.M. núm. 45).

tener en cuenta, al menos dos reglas primordiales: el objeto y fin de la norma jurídica y la taxatividad en la enunciación de los supuestos de excepciones. Todo ello, para que los Estados no “tropiecen con dificultades en cuanto a la interpretación de la excepción, pues ello podría obstaculizar gravemente la aplicación del Convenio” (E.M. núm. 35 *in fine*).

Por lo primero, el Convenio Europeo, según el art. 1., establece que su objeto y fin es garantizar, en los territorios de los Estados miembros, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus *derechos y libertades fundamentales*, concretamente su derecho a la intimidad (o “vida privada”), con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos").

Respecto de lo segundo, es decir, la regulación *numerus clausus* de los supuestos de excepciones, están previstas en el art. 9 del Convenio, con las siguientes anotaciones:

La regla general, para las excepciones al tratamiento informatizado de datos, consiste en la no admisión de excepción alguna contra los principios fundamentales previstos para las fases o etapas del tratamiento informatizado de recolección, almacenamiento, registro y conservación de datos personales, salvo que estuviere: prevista en el ordenamiento jurídico vigente del Estado miembro y constituya una medida necesaria en una *sociedad democrática*, para: a) la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; y, b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

Estas excepciones a la excepción de los principios fundamentales del tratamiento informatizado, están inspiradas en el Convenio Europeo de los Derechos del Hombre (arts. 6, 8, 10 y 11). Así mismo, la expresión “medida necesaria” en una sociedad democrática, constituye una noción fruto de los acuerdos de la Comisión y el Tribunal de los Derechos Humanos, por la cual, resulta claramente que los criterios de tal concepto no pueden ser fijados para todos los Estados y en todo momento, sino que deberían ser considerados a la luz de la situación dada en cada Estado **[92]**.

Las excepciones a la regla general tienen como fuente dos grandes ramales, a saber: los intereses fundamentales de los Estados y los intereses particulares de la persona humana.

En efecto, la enumeración taxativa dentro de las causales exceptivas al tratamiento y principios fundamentales de los datos obedece básica y exclusivamente a la delimitación

---

(92) Las excepciones se limitan a las que son necesarias para proteger los “valores fundamentales en una sociedad democrática”. (E.M. núm. 55).

conceptual de los que se consideran intereses principales de los Estados, es decir, de aquellas instituciones socio-jurídicas ; tales como, la seguridad del Estado [93], seguridad pública , intereses monetarios del Estado [94] e infracciones penales [95]; y por su puesto, a fin de evitar que en la aplicación del Convenio los Estados puedan tener un "margen de maniobra demasiado amplio" en la interpretación y aplicación de las mismas y conserven la facultad de "rehusar" [96] la aplicación del Convenio en casos concretos por motivos de importancia ponderada (E.M. núm. 56).

En cuanto a la enunciación taxativa de las causales de excepción al tratamiento y principios básicos de los datos previstas en el literal b), sobre protección de la persona concernida están fundadas en los intereses particulares de la persona humana, tales como los del *interesado* (p.e., información psiquiátrica) o de *terceros* (p.e., la libertad de prensa, secretos del comercio, etc.).

Conjuntamente con este marco de excepciones, el Convenio presenta las que llama "restricciones" al ejercicio de los ciertos derechos de la persona concernida y presentes en los "ficheros automatizados" de datos personales que se utilicen con fines estadísticos o de investigación científica [97], cuando no existan manifiestamente riesgos de atentado a la intimidad ("vida privada") de las personas concernidas (art. 9-3)

Jurídicamente están restricciones no se consideran excepciones, sino limitaciones al ejercicio de algunos derechos impuestas por razones expresamente previstas en el orde-

---

(93) Se entiende por *Seguridad Pública*, en el sentido tradicional de protección de la soberanía nacional contra amenazas internas o externas, incluida la protección de las relaciones internacionales del Estado (E.M. núm. *56 in fine*).

(94) *Intereses monetarios del Estado*, comprende todo aquello que contribuye a facilitar al Estado los recursos financieros de su política. v.gr. La recaudación de los impuestos y al control de cambios. (E. M. núm. 57 *ab initio*).

(95) *Represión de los delitos*, comprende tanto la investigación de los delitos como su persecución (E.M. núm. 57 *in fine*).

(96) *Artículo 16. Denegación de peticiones de asistencia*. Una autoridad designada, a quien se haya dirigido una petición de asistencia con arreglo a los términos de los artículos 13 ("Cooperación entre Estados) o 14 (Asistencia a las personas concernidas que tengan su residencia en el extranjero) del presente Convenio, solamente podrá negarse a atenderla si: a) La petición es incompatible con las competencias, en materia de protección de datos, de las autoridades habilitadas para responder; b) la petición no está conforme con lo dispuesto en el presente Convenio; c) atender a la petición fuese incompatible con la soberanía, la seguridad o el orden público de la Parte que la haya designado, o con los derechos y libertades fundamentales de las personas que estén bajo la jurisdicción de dicha Parte.

(97) En los ficheros o banco de datos estadísticos la posibilidad de limitar el ejercicio de los derechos de los interesados, se centra en las "operaciones de proceso de datos que no llevaren aparejado riesgo alguno... en la medida en que se trate de datos presentados en forma agregada y separada de los identificadores. Igual los ficheros de datos científicos de conformidad con una recomendación de la Fundación Europea de la Ciencia". (E.M. núm. 59 *in fine*).

namiento jurídico, y como tal, pueden ser preventivas (*in tempore*) o modales (eliminación del riesgo o vulnerabilidad). Sin embargo, en la *praxis,* estas restricciones pueden esconder verdaderas instituciones nugatorias de derechos, aún cuando fueren preventivas o modales.

Las restricciones al ejercicio de algunos derechos en las circunstancias y para ciertos ficheros o bancos de datos previstos en el Convenio, se extiende a aquéllos derechos de la persona concernida que como "garantía complementaria" ostenta en el transcurso del tratamiento informatizado de datos personales. Esos derechos son los componentes del derecho de *habeas data* que inicia con el de información*.* En efecto, se admite la restricción al ejercicio de los siguientes derechos: a) *De confirmación* de la existencia o no de un fichero con datos del concernido, así como el de comunicación de dichos datos; b) *De rectificación* o borrado de datos, según fuere el caso, si se desconoce los principios fundamentales del tratamiento informatizado de datos (recolección, almacenamiento, registro y conservación) o la consideración de ser datos sensibles; y c) *De recurso*, ante las autoridades competentes, si no se atiende o se desconoce los anteriores derechos.

2.5. ESPAÑA: LEY ORGANICA DE PROTECCION DE LOS DATOS PERSONALES DE 1999 o LOPDP.

2.5.1. Notas preliminares

Antes de la vigencia de LOPDP de 1999, en España rigió la Ley orgánica de regulación del tratamiento automatizado de datos de carácter personal, L.O. 5/1992, Oct. 29 o LORTAD, la cual a su vez terminaba con la existencia de la disposición transitoria primera de la Ley Orgánica 1/1982, de 5 de mayo, de *protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen,* a través de la cual se aplicaba la mencionada ley, aunque en un ámbito de comprensión legislativa y aplicabilidad hermenéutica restringidos (pues sólo se refería "*a las intromisiones ilegítimas derivadas del uso de la informática*") a todos aquellos aspectos referentes al tratamiento informatizado de datos personales, la protección de los derechos y libertades fundamentales e intereses legítimos y el uso de la informática, según lo estipulaba la disposición única derogatoria de la LORTAD.

La vida y derogación jurídicas de unas normas jurídicas que regulan el tratamiento informatizado de datos personales en España, estaba marcada no sólo temporal sino espacialmente de una etapa fructífera de cariz legislativo comunitario y estatal europeos en materia de protección de los titulares de los datos personales, más que de los datos *per se,* cuando son sometidos a procesos informáticos con soportes y medios informáticos, electrónicos o telemáticos. Quizá eso motivó en su momento la reforma y derogación

parcial de la Ley Orgánica 1/82, y también la derogación total de la LORTAD de 1992 por la nueva Ley de protección de los datos personales de 1999.

España como Estado Miembro de la Unión Europea debía no sólo tener una Ley de protección de datos como la LORTAD, sino que debía adecuarla, homologarla a las normas comunitarias de protección de datos a efectos regular técnica y jurídicamente los instrumentos o mecanismos idóneos que compatibilizaran con los de los demás Estados de la Unión. Esta técnica legislativa comunitaria se conoce como "transposición normativa". España entonces debía transponer las dos últimas directivas comunitarias que se había expedido para el tratamiento de datos personales y la protección de derechos y libertades fundamentales de la persona humana (no jurídica) y del derecho a la intimidad esencialmente. Esas Directivas eran la 95/46/CE y 97/66/CE, normas comunitarias que constituyeron junto con las normas europeas de 1980 y 1981, ut supra analizadas, el fundamento de la nueva Ley Orgánica de Protección de Datos Española de 13 de Diciembre 1999 o LOPDP.

2.5.2. Estructura de la LOPDP de 1999

La LOPDP se compone de Títulos, Capítulos y Artículos, así:

El **Título I**, relativo a las ***"Disposiciones Generales",*** en los artículos 1º a 3º hace mención al objeto de la ley que consiste en garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

También hace relación a ámbito de aplicación de la ley, referido al tratamiento de datos personales de carácter público y privado. Al igual que la LORTAD, la LOPDP, trae una relación *numerus clausus* de los ficheros o bancos de datos a los cuales no se aplica la ley. Estos son: (i) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; (ii) A los ficheros sometidos a la normativa sobre protección de materias clasificadas; (iii) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos o APD.

Aclara en el numeral 3 de artículo 2º de la LOPDP, que se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: (i) Los ficheros regulados por la legislación de régimen electoral; (ii) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública; (iii)

Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del Régimen del personal de las Fuerzas Armadas; (iv) Los derivados del Registro Civil y del Registro Central de penados y rebeldes; (v) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Y finalmente, en el artículo 3º relaciona un listado básico de términos técnico-jurídicos que se aplican en el tratamiento de datos personales: (i) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables; (ii) Fichero; (iii) Tratamiento de datos; (iv) Responsable del fichero o tratamiento; (v) Afectado o interesado; (vi) Procedimiento de disociación; (vii) Encargado del tratamiento; (viii) Consentimiento del interesado; (ix) Cesión o comunicación de datos; y, (x) Fuentes accesibles al público.

En el **Título II**, concerniente a "***Los principios de protección de los datos***", en los artículos 4º a 12º, relaciona los siguientes principios: (i) Calidad de los datos; (ii) Derecho de información en la recogida de datos; (iii) Consentimiento del afectado; (iv) Datos especialmente protegidos; (v) Datos relativos a la salud; (vi) Seguridad de los datos; (v) El deber de secreto; (vi) Comunicación de datos; (vii) Acceso a los datos por cuenta de terceros.

En el **Título III**, referente a ***"Los Derechos de las personas"*** en los artículos 13º a 19, menciona los siguientes: (i) Impugnación de las valoraciones; (ii) Derecho de consulta al Registro General de los datos; (iii) Derecho de Acceso; (iv) Derecho de rectificación y cancelación; (v) Procedimiento de oposición, acceso, rectificación o cancelación; (vi) Tutela de derechos; (v) Derecho a indemnización.

En el **Título IV**, relativo a "***Las Disposiciones sectoriales",*** compuesto de dos capítulos. En el Capítulo Primero dedicado a *"Los Ficheros de titularidad pública",* en los artículos 20 a 24, hace mención a lo siguiente: (i) creación, modificación o supresión; (ii) Comunicación de datos entre administraciones Públicas; (iii) Ficheros de las Fuerzas y Cuerpos de Seguridad; (iv) Excepciones a los derechos de acceso, rectificación y cancelación; (v) Otras excepciones a los derechos de los afectados.

En el Capítulo Segundo, destinado a *"Los Ficheros de titularidad privada"* en los artículos 25º a 32º, relaciona lo siguiente: (i) Creación; (ii) Notificación e inscripción registral; (iii) Comunicación de la cesión de datos; (iv) Datos incluidos en las fuentes de acceso público; (v) Prestación de servicios de información sobre solvencia patrimonial y crédito; (vi) Tratamiento con fines de publicidad y prospección comercial; (vii) Censo promocional; y, (viii) Códigos tipo.

En el **Título V**, concerniente al ***"Movimiento Internacional de Datos"*** en los artículos 33º a 34º, menciona las normas generales y las excepciones a dicho movimiento.

En el **Título VI,** referente a la "***Agencia de Protección de los Datos"*** en los artículos 35º a 42, se menciona lo siguiente: (i) naturaleza y régimen jurídico; (ii) El director y sus funciones; (iii) El Consejo consultivo; (iv) El Registro General de Protección de Datos; (v) Potestad de Inspección; (vi) Órganos correspondientes de las Comunidades Autónomas; (vii) Ficheros de las comunidades autónomas en materias de su exclusiva competencia.

En el **Título VII**, relativo a las ***"Infracciones y sanciones"*** en los artículos 43º a 49º menciona lo siguiente: (i) Responsables; (ii) Tipos de infracciones (relaciona más de una veintena); (iii) Tipos de Sanciones; (iv) Infracciones de las Administraciones Públicas; (v) Prescripción; (vi) Procedimiento Sancionador; y, (vii) Potestad de inmovilización de ficheros.

Además establece seis "***Disposiciones Adicionales***", relativas a los siguientes aspectos: (i) Sobre ficheros preexistentes; (ii) Ficheros y Registro de Población de las Administraciones Públicas; (iii) Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social; (iv) Modificación del artículo 112.4 de la Ley General Tributaria; (v) Competencias del Defensor del Pueblo y órganos autonómicos semejantes; (vi) Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Tres "***Disposiciones Transitorias***", referentes a lo siguiente: (i) Tratamientos creados por Convenios Internacionales; (ii) Utilización del Censo Promocional; (iii) Subsistencia de normas preexistentes.

2.5.3. Comentarios sucintos a la LOPDP

Dada la complejidad y amplitud temática de la LOPDP, a los efectos del presente trabajo tan solo abordamos y comentamos los siguientes temas: a) Las definiciones técnico-jurídicas; b) Los principios fundamentales aplicados a las fases del tratamiento informatizado de datos personales; y c) Los órganos de protección de los datos personales.

2.5.3.1. Definiciones Técnico-jurídicas de la LOPDP

Con los antecedentes legislativos de Estados europeos como Alemania, Suiza, Francia, entre otros, y con los antecedentes normativos comunitarios, básicamente de la Recomendación de la OCDE de 1980 y el Convenio de Estrasburgo o Convenio de Europeo de 1981, el Estado Español introdujo en su ordenamiento jurídico, una legislación

homogénea, pero no plena en el tratamiento (informatizado o no) de datos de carácter personal de titularidad pública y de titularidad privada, con cierto retraso frente a la legislación estatal europea existente sobre la materia y sobre todo, con los avances tecnológicos del fenómeno TIC e informática [98], que se concretó inicialmente en la L.O. 5/1992, de 29 de Octubre conocida como LORTAD y luego 7 años después se expidió la L.O. de 13 de Diciembre de 1999, o Ley de Protección de Datos de España o LOPDP ajustándola a las Directivas Comunitarias de 1995 y 1997 sobre protección de datos personales, garantía de los derechos y libertades constitucionales y especialmente de la Intimidad personal y familiar y del honor. Transposición normativa comunitaria de la LOPDP que también tuvo retraso de cuatro y dos años respectivamente.

Retraso normativo inicial morigerado, según se ha sostenido porque desde 1984, se conocía "un conjunto de normas heterogéneas que no siempre distinguían entre ficheros automatizados y ficheros convencionales" [99] y porque en nuestro criterio, se aplicaba teóricamente la Ley Orgánica núm. 1 de 5 de Mayo de 1982, relativa a la protección civil de los derechos del honor, la intimidad y el propia imagen, como norma jurídica subsidiaria en todos los asuntos relacionados con las intromisiones ilegítimas derivadas del uso de la informática (Disposición Primera Transitoria).

Este antecedente referencial legislativo, condujo a la LORTAD en 1992 y a la LOPDP en 1999, a decantar y mejorar varias definiciones técnico-jurídicas aplicables al tratamiento informatizado de datos personales y la estructuración de procedimientos técnicos informáticos, a fin de hacerlas más inteligibles al operador jurídico, pero principalmente al juzgador que debe aplicar e interpretar la norma jurídica.

---

(98) La LORTAD, "se ha demorado quince años, pero finalmente está ya publicada", para destacar el epígrafe sobre "riesgos para los derechos de la personalidad que pueden derivar del acopio y tratamiento de datos por medios informáticos". Cfr. GONZALEZ NAVARRO **Francisco. *Derecho Administrativo Español.*** Ed. Eunsa, 1a., ed. de 1987 y 2a., ed., Pamplona, 1994, p. 166. En igual sentido, CASTELLS, quien sostiene: "La aparición de España de una red de tráfico de datos personales obrantes en registros públicos a comienzos de la década de los 90, reveló lo que una política puramente promocional del fenómeno informático, sin suficientes alertas en el plano cautelar, podía ocasionar, *Pérez Luño* ha mencionado "*la paradoja dramática"*, consistente en compensar el retraso en la incorporación al desarrollo tecnológico, con la vanguardia mundial en la piratería del "software", la delincuencia informática y las agresiones informáticas a la libertad". Vid. CASTELLS ARTECHE, José M., ***Derecho a la privacidad y procesos informáticos: Análisis de la LORTAD****. R.V.A.P.* Bilbao, 1997, p. 251.

(99) El autor cita como ejemplos de dichas normas, entre otras, las siguientes: la LGT (arts. 111 y 112, modificado en 1985 y 1990), la ley 19 /1988 de 12 de julio, de auditoría de cuentas (arts. 13 y 14), y la ley 30/1984, de 2 de agosto, de Medidas para la reforma de la función pública (que prohibía registrar datos "sensibles" en los expedientes de personal). Refiriéndose ya específicamente a ficheros automatizados cabe citar la legislación electoral y la ley de la Función estadística pública, de 1982. Vid. GONZALEZ NAVARRO, Francisco. ***Derecho..*** *Ob. cit.*, p. 168.

En la LORTAD, se incluyeron las siguientes definiciones: (i) Datos de carácter personal, (ii) Fichero automatizado, (iii) Tratamiento de datos, (iv) Responsable del fichero, (v) Afectado, y (vi) Procedimiento de disociación.

En la LOPDP de 1999, el listado de términos aumentó porque la doctrina y jurisprudencia ibérica había hecho serios reparos son la terminología pendular empleada por titulares, usuarios, responsables de los ficheros y hasta los mismos órganos de control de los datos, como la Agencia de Protección de datos. Para corregir la ambigüedad en la terminología aplicable al tratamiento de datos personales, la nueva ley definió con precisión los siguientes términos:

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento de datos respectivo.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: 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.

h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

A continuación comentaremos a espacio los siguientes términos:

Datos de carácter personal o simplemente datos personales, se considera cualquier información concerniente a personas físicas identificadas o identificables. Esta definición es idéntica a la prevista en el Convenio de 1981, por ello son válidas las observaciones realizadas en aquél aparte. Sin embargo, la LOPDP incluye entre sus definiciones la de "afectado o interesado", para indicar que se trata de una persona física titular de los datos que sean objeto del tratamiento informatizado, con lo cual abunda sin necesidad sobre el concepto de persona física (identificada o identificable) con el *inri* de que dicha persona no es en *strictu sensu* un *afectado* como lo sostenía la LORTAD*,* sino también un interesado como adicionó la LOPDP, pues la persona física es el titular de los datos personales o concernido en un tratamiento o procedimiento informatizado que tiene derechos y también deberes, no simplemente obligaciones o cargas como sugería el concepto de solo "afectado".

El titular de datos personales o interesado, contextua la idea de toda persona que tiene derechos subjetivos sobre la información relativa a sí misma, aún cuando tal información haya sido reunida por otras personas. Esta visión no sería posible si le anteponemos el calificativo de afectado para referirnos a esa misma persona.

La LOPDP, como lo hiciera en su momento la LORTAD, destaca las definiciones de los conceptos de "*tratamiento de datos*" informatizado o no y de "*fichero*" (que la LORTAD le adicionaba un apellido de "automatizado", que resultaba innecesario y equívoco, porque excluía a los ficheros manuales, mecánicos o escriturales).

Quizá por ello, la LOPDP al eliminar el término automatizado dado a fichero terminó con el equívoco anotado, puesto que en la definición actual quedan involucrados en el término

genérico, los ficheros, bases o bancos de datos tanto los manuales o escritos, como los electrónicos o informáticos, al decir, que el fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

La LOPDP al definir el *"Tratamiento de datos"* retomo en su integridad el suministrado por la LORTAD. En efecto, se dice que el Tratamiento de datos son aquellas *operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*, extiende el tratamiento a todo procedimiento técnico no informatizado y estructura el procedimiento de datos personales, a través de un *iter* compuesto de etapas o fases que encadenadas por un tratamiento informático, vale decir, con soportes y medios informáticos, electrónicos o telemáticos se dirigen a producir un dato informatizado, con el cual los responsables de la gestión, los titulares de los datos o los usuarios puedan desarrollar cualquier acción jurídico-técnica posible. v.gr. grabación, almacenamiento, bloqueo o interconexión. La definición de tratamiento de datos, destaca el iter informático que en su conjunto produce un proceso de igual carácter, es decir, un proceso informatizado de datos compuesto de fases o etapas, tales como las iniciales, de desarrollo y terminación. Estas fases, se estructuran con base en los principios fundamentales de la protección de los titulares de los datos personales.

En las definiciones anteriores se exaltan las etapas o fases del tratamiento informatizado de datos personales que conforman un procedimiento ibídem. En efecto, se destaca las fases de recolección, almacenamiento, registro, conservación y la comunicación (Emisión/transmisión y cesión) de datos personales. En tanto, que las acciones informáticas de revisión, actualización, rectificación, bloqueo y cancelación son originadas tras el ejercicio del derecho de información y acceso que tiene toda persona concernida con datos personales; vale decir, tras el ejercicio del derecho de *habeas data.*

Por ello*,* "la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia", según lo destacaba en su momento la Exposición de Motivos de la LORTDA en el numeral 1º .

El ***Responsable del fichero o tratamiento*****,** se considera a la *persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad contenido y uso del tratamiento*. La LOPDP, al definir al responsable del fichero o

tratamiento, retoma la definición de la LORTAD, pero solo agregándole el término "o tratamiento" que esta no lo tenía.

En esencia, esta definición contiene los elementos de la definición inmersos en el concepto de *"autoridad controladora del fichero*", previsto en el Convenio Europeo de 1981, con la diferencia que en éste se especifican las funciones decisorias acerca de cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán a los ficheros, en tanto que la LOPDP, engloba y amplia el radio de acción, al expresar que dichas decisiones se extienden a "*la finalidad, contenido y uso del tratamiento*" y no simplemente a la existencia *per se* de los ficheros o el tratamiento, en particular.

Efectivamente, como lo sostiene el profesor *González Navarro* [100], aparte de los dos sujetos (titular de los datos y el responsable del fichero), en el tratamiento de datos puede intervenir un tercer sujeto que es "*el contratista o comisionista*" que presta sus servicios de tratamiento informatizado de datos personales dentro de un procedimiento ibídem. Por su parte, la Ley Federal alemana de protección de datos personales (LFADP) extiende los efectos del principio de responsabilidad en el tratamiento de datos de los denominados "responsables del fichero" a las personas físicas o jurídicas, públicas o privadas que actúan como terceros en el mismo (v.gr. Oficinas de servicios informáticos), tanto de los deberes-derechos que estos tienen, como de las sanciones y la obligación de guardar la confidencialidad de los datos.

Por ello, la LOPDP al llenó el vacío existente en la LORTAD, al crear y definir al ***Encargado del tratamiento,*** como 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.

De otra parte, la LOPDP recoge la misma definición dada en la LORTAD al "***procedimiento de disociación",*** definido como *todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable*.

Este derecho-garantía para el titular de los datos personales y el Estado que debe regular, el tratamiento, uso y utilización de los mismos conforme a derecho, tiene aplicación prác-

---

(100) Este tercero, según el art. 27 no puede aplicar o utilizar los datos obtenidos con un fin distinto del que figura en el contrato de servicios, ni cederlos a otras personas ni siquiera para su conservación. Igualmente, una vez cumplida la prestación contractual, los datos personales deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se presten tales servicios, porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años. Ob. ut supra cit., p. 170.

tica, así: En la distinción de *dato anónimo* [101], "*dato reservado*" [102], comúnmente empleado en las normas jurídico-penales y ius-administrativistas españolas. En efecto, a pesar de ser ambos datos de carácter personal deducibles de una persona física, se diferencian en que éste último se predica única y exclusivamente de una persona identificada o identificable, so pena de desvirtuarse, y más aún, no haber existido, si alguna vez eso ocurrió. Tal es el caso, en el ámbito penal y más concretamente al referirse a los delitos contra la intimidad en el título X, Libro II del Código Penal Español de 1995. Igualmente, en el ámbito administrativo, al referirse a las infracciones al tratamiento informatizado de datos previsto en la LOPDP (arts. 43 y 49).

De igual manera, tiene la aplicabilidad práctica el procedimiento de disociación cuando se refiere a los datos anónimos, a los efectos de hacerles perder la determinabilidad de una persona humana a la que le conciernen los datos de carácter personales. p.e., en los datos estadísticos, históricos, científicos, investigativos, publicitarios, etc.

2.5.3.2. Principios fundamentales aplicables a las fases del tratamiento de datos personales

La institucionalización de "*los principios reguladores de la recogida, registro y uso de datos personales*", según sostenía la Exposición de Motivos de la LORTAD, en su momento y agregamos, como en las demás fases o etapas del tratamiento informatizado o no de datos personales, tales como el almacenamiento, conservación y comunicación constituyen una garantía para el derecho al honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos y libertades constitucionales en el derecho público ibérico. Por ello, la existencia de los principios fundamentales del tratamiento informatizado de datos personales sólo encuentra validez, eficacia y presentación en la estructuración de sus fases o etapas, tales como la de recolección, almacenamiento, re-

---

(101) Los *datos anónimos*, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general. v.gr. como pueden ser los registros de la propiedad o mercantiles. Por ello, al determinar el ámbito de aplicación de la LORTAD, ésta excluía en el artículo 2-a la aplicación del tratamiento informatizado de datos personales, a los ficheros de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.

(102) De la interpretación doctrinal de los arts. 197.2 y 200 del Código Penal Español de 1995, se pueden deducir varios conceptos de dato reservado, a saber: 1. "Dato reservado es cualquier información concerniente a personas físicas identificadas o identificables cuyo conocimiento esta limitado a los usuarios del archivo, registro o fichero automatizado o convencional de acceso restringido. 2. Dato reservado es aquel que es indispensable libremente por terceros, requiriéndose para ello autorización de su titular. 3. Dato reservado es aquel que potencialmente puede lesionar el derecho a la intimidad de su titular; en lo que respecta a las personas físicas, y cuyo descubrimiento o revelación debe incidir en la esfera "personal o familiar" de su titular... Vid. BAJO FERNANDEZ, Miguel et all. ***Compendio de derecho penal (Parte Especial)***. Vol. II. Ed. Centro de Estudios Ramón Areces, S.A. Madrid, 1998, p. 201-202

registro, conservación y comunicación de datos personales, reguladas por la LOPDP e inmersos en el Título II, en los artículos 4º a 12º. Estos son: (i) Calidad de los datos; (ii) Derecho de información en la recogida de datos; (iii) Consentimiento del afectado; (iv) Datos especialmente protegidos; (v) Datos relativos a la salud; (vi) Seguridad de los datos; (v) El deber de secreto; (vi) Comunicación de datos; (vii) Acceso a los datos por cuenta de terceros.

La LOPDP, agregó a la lista de principios que traía la LORTAD, los relativos a "*La comunicación de datos*" y "*el acceso a los datos por cuenta de terceros*", pues estos estaban previstos en las Directivas comunitarias de 1995 y 1997 y se requería su urgente transposición a las normas internas de protección de datos personales a efectos de normalizar u homologar los textos normativos comunitarios con los textos normativos de Espala.

El artículo 11 de la LOPDP, al regular el principio de comunicación de datos, estipuló lo siguiente:

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. Este consentimiento exigido no será preciso: (i) Cuando la cesión está autorizada en una Ley; (ii) Cuando se trate de datos recogidos de fuentes accesibles al público; (iii) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique; (iv) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas; (v) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; (v) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad

a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la LOPDP de 1999.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Por su parte el artículo 12 de la LOPDP, al reglamentar el principio de **"*Acceso a los datos por cuenta de terceros",*** sostuvo:

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la LOPDP que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Ahora veamos brevemente la aplicación de los demás principios en las diferentes fases o etapas del tratamiento de datos.

2.5.3.2.1. Fase Inicial de recolección de datos

En la fase inicial de recolección de los datos, se aplicarán los principios de *la congruencia y racionalidad*, según lo sostenía la Exposición de Motivos de la LORTAD.

Además es aplicable a esta fase del tratamiento de datos, *el principio de calidad*. En efecto, según el artículo 4-1 de la LOPDP, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Concordantemente con lo anterior, el numeral 7º del mencionado artículo "prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos".

Por el principio del *consentimiento, o de autodeterminación* (artículo 6 LOPDP), todo tratamiento de datos de carácter personal, y por su puesto, la recolección de los mismos, "*requerirá el consentimiento inequívoco*" del titular, interesado o persona concernida, pues con él, se "otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del titular o interesado para que la recogida de datos sea lícita".

Sin embargo, según el numeral 2 del artículo 6 de la LOPDP, no será preciso el consentimiento, en los siguientes casos: (i) cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; (ii) cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; (iii) cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la LOPDP [103]; (iv) cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

---

(103) No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo (datos especialmente protegidos: "núcleo duro" de la Intimidad), cuando dicho tratamiento 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 se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Por el *principio de información,* previo al principio del consentimiento y concomitante con el ejercicio de algunos derechos (v.gr. derecho de acceso a la información) y posterior con el ejercicio de otros, tales como el de habeas data, el titular de los datos personales puede informarse plenamente y en forma *a priori,* de qué datos suyos pudieran ser recolectados y sometidos a tratamiento informatizado o no.

Este principio fundamental que también es un derecho subjetivo de la persona concernida, porque le permite al titular de los datos "ser previamente informado de modo expreso, preciso e inequívoco" (artículo 5-1 LOPDP), cuando sean solicitados datos a él referentes y vayan a ser objeto de recolección y tratamiento informatizado. Quizá, por esto es uno de los principios de importancia capital para el pleno ejercicio del derecho de *Hábeas data* y los demás derechos y libertades fundamentales, y se aplica no sólo a la fase de recogida de datos sino al conjunto de fases o etapas del tratamiento de datos.

2.5.3.2.2. Fase de almacenamiento de datos

En la *fase de almacenamiento de datos* se aplicarán los siguientes: a) *El principio de adecuación, pertinencia y no excesibilidad de los datos* con relación al ámbito y las finalidades legítimas (artículo 4-1 LOPDP). Este principio que es válido para la recolección de los datos, lo es también para el almacenamiento, por cuanto, éste se requiere para todo dato personal que sea "sometido a tratamiento" informatizado o no , y obviamente el almacenamiento posterior a la recogida de datos es una fase ineludible del tratamiento; b) El *principio del consentimiento* (artículo 6-1 Ibid), con igual razonamiento al precedente, se aplica este principio a la fase del almacenamiento de los datos, pues el consentimiento del titular se requiere durante todo el tratamiento; c) *El principio de veracidad de la información*. Los datos personales serán exactos y puestos al día de forma que respondan con veracidad a la situación real del titular (artículo 4-3 Ibid); d) *El principio de información* (artículos 5º Ibid), que opera en todo el tratamiento informatizado de la información y que le permite al titular de los datos ejercer los derechos de acceso, habeas data e impugnación contra actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento o personalidad.

El principio del consentimiento en esta fase del tratamiento es importante, porque "otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes", niveles que "se refuerzan singularmente en los denominados *´datos sensibles´*, como pueden ser, de una parte, la ideología o creencias religiosas --cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2-- y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según

exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece *la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características*. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España".

2.5.3.2.3. Fase de Registro de Datos

En *la etapa del Registro de los datos*, se aplica: a) El *principio de exactitud y completud de los datos*. Si los datos personales registrados resultaren ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que los titulares de los mismos devenidas del ejercicio del derecho de *Hábeas Data* --llamados por la LOPDP "derechos de rectificación y cancelación" , artículo 16-- (artículo 4-4 Ibid) [104]. Así mismo, por aplicación de éste principio, podrán ser cancelados los datos "*cuando hayan dejado de ser necesarios o pertinentes para la finalidad para cual hubieren sido recabados o registrados*" (artículo 4-5 Ibid).

Igualmente se aplicarán los principios del consentimiento, principio de información y el *principio de seguridad de datos*. Este último, como condición *sine qua nom* para el registro de datos, puesto que no se registrarán datos personales en ficheros informatizados o no que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas (artículo 9-2 Ibid) .

---

(104) **Artículo 16. Derecho de rectificación y cancelación.** 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.
Cumplido el citado plazo deberá procederse a la supresión.
4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación .
5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Por *el principio de la confidencialidad de los datos*, aplicable a todo el tratamiento informatizado de datos, pero particularmente a las fases de registro, conservación y comunicación de datos, el responsable del fichero y quienes intervengan en "cualquier fase del tratamiento de los datos" personales están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo (artículo 10 Ibid).

2.5.3.2.4. Fase de conservación de los datos

En esta fase del tratamiento informatizado se aplicará:

a) El *principio de la temporalidad de los datos*. Aplicable en dos formas: 1. no se serán conservados en forma que permita la identificación del titular de los datos durante un período superior al necesario para los fines en base a los cuales hubieran, salvo que deban mantenerse en su integridad atendiendo al valor histórico que los datos puedan tener de conformidad con el ordenamiento jurídico vigente (artículo 4-5 Ibid); y 2. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el titular de los mismos.

b) Por el *principio de seguridad de los datos,* el responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural (artículo 9-1 Ibid).

c) Por *el principio de tutela de derechos del titular de los datos*, integrado por los anteriores principios y los referentes al derecho de *habeas data,* el titular podrá ejercer el derecho de acceso, a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes --artículo 15-3—

2.5.3.2.5. Fase de comunicación de datos

Esta fase del tratamiento informatizado se estructura en la emisión y transmisión de los datos personales, a través de soportes y medios informáticos, electrónicos o telemáticos idóneos para la comunicación o la cesión de los mismos. Se entiende por *cesión de datos*, toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero; y sobre todo, la actividad de interconexión con otros ficheros y la

comunicación de los datos realizada por una persona distinta del titular de los datos personales.

En consecuencia, serán aplicables los principios de consentimiento, información, confidencialidad y seguridad de los datos, por tener aplicabilidad en todas las fases del tratamiento informatizado.

La LOPDP, en el artículo 11º ut supra transcrito mejoró la redacción y entendimiento que la LORTAD, le daba a la "cesión de datos", cuando en el fondo se estaba refiriendo a un fenómeno técnico jurídico más genérico como era la "comunicación de los datos", el cual tiene concordancia con el fenómeno regulado en las Directivas Comunitarias y últimamente en la LOPDP en los artículos 33 y 34, sobre el "Movimiento Internacional de Datos".

El *principio de libre circulación de datos,* aplicable a las comunicaciones de datos personales denominado por la LOPDP, como "*movimiento internacional de datos*" (artículo 33). En este punto, la Ley traspone la norma del artículo 12 del Convenio 108 del Consejo de Europa, apuntando así una solución para lo que ha dado en llamarse flujo transfronterizo de datos. La protección de la integridad de la información personal se concilia, de esta suerte, con *el libre flujo de los datos*, que constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la autorización de la Agencia cuando tal sistema no exista pero se ofrezcan garantías suficientes. Con ello no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias.

2.5.3.3. Órganos de Protección de los datos personales

La LOPDP establece como órganos de la protección de los datos personales a los siguientes: a) La Agencia de protección de datos, que como organismos de régimen jurídico *sui géneris* cuenta con un Director asesorado con un "Consejo Consultivo"; b) El Registro General de protección de datos, como órgano integrado a la Agencia; la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia (artículo 11-3, R.D.núm.428/1993, de 26 de Marzo).; y c) Órganos de protección de datos de las Comunidades autónomas.

2.5.3.3.1. La Agencia de Protección de Datos o APD

La Agencia de Protección de Datos Española, es la entidad pública, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones, con un régimen jurídico *sui géneris* (integrado por la LOPDP y por un Estatuto propio dictado por el Gobierno R.D.núm.428/1993, de 26 de Marzo).

La Agencia, tiene como objetivo prioritario velar por el cumplimiento de la legislación en materia de protección de datos personales informatizados en España, pero particularmente, la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de Diciembre, sobre *la Protección los Datos de Carácter Personal* y los derechos y libertades fundamentales e intereses legítimos implicados en ella.

La Agencia se caracteriza por la absoluta independencia de su Director en el ejercicio de sus funciones, independencia que trae causa, en primer lugar, de un expreso imperativo legal, pero que se garantiza, en todo caso, mediante el establecimiento de un mandato fijo que sólo puede ser acortado por un numerus clausus de causas de cese.

La Agencia de Protección de datos, según el artículo 37 de la LOPDP tendrá como funciones, las siguientes:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46 (“Infracciones de las Administraciones Públicas”.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2.5.3.3.2. El Director de la Agencia de Protección de Datos

El *Director de la Agencia de Protección de Datos*, dirige la Agencia y ostenta su representación. Prioritariamente el Director hará cumplir y cumplirá todo lo atinente a la legislación sobre tratamiento informatizado de datos personales y en su carácter de funcionario ejecutor de las políticas, recomendaciones y sugerencias de la Agencia de Protección de Datos, velará y controlará el ejercicio de los derechos de información, *Hábeas Data* (acceso, actualización, rectificación, bloqueo y cancelación de datos) y el pleno de derechos y libertades fundamentales e intereses legítimos.

El Director será nombrado, de entre quienes componen el consejo Consultivo, mediante Real Decreto, por un período de cuatro años. Cesará antes de la expiración del período, por las siguientes causas: 1. A petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes

miembros del Consejo Consultivo; 2. Por incumplimiento grave de sus obligaciones, 3. Por incapacidad sobrevenida para el ejercicio de su función, y, 4. por incompatibilidad o condena por delito doloso.

El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

El Director de la Agencia, tiene una gama variopinta de funciones, tales como las de Dirección, de Gestión y designación, que apuntan a determinar que su cargo se desempeña con dedicación absoluta, plena independencia y total objetividad, y por ello no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna.

2.5.3.3.3. El Registro de Protección de Datos

El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

Serán objeto de inscripción en el Registro General de Protección de Datos:
a) Los ficheros de que sean titulares las Administraciones Públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones a que se refiere la LOPDP.
d) Los códigos tipo a que se refiere el artículo 32 de la LOPDP.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

Según el numeral 3º del artículo 39 de la LOPDP, por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

2.6. LAS DIRECTIVAS 95/46/CE y 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 1995 Y 1997, RESPECTIVAMENTE

Las Directivas comunitarias hacen referencia, la primera de 1995, a los principios, derechos y garantías de los titulares de los datos personales generales y sensibles y las fases del proceso informatizado o no de los datos y a la “circulación de datos”. La segunda de 1997

hace referencia a la fase de comunicación del proceso informatizado de datos y en los principios y garantías de tutela de los titulares de los datos personales.

2.6.1. LA DIRECTIVA 95/46/CE, sobre *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*

La Directiva 95/46/CE., en materia de *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,* contiene una estructura normativa *sui géneris* muy propia de las normas comunitarias europeas, pertenecientes a las fuentes del llamado Derecho Derivado Comunitario [105]

La Directiva esta dividida en dos grandes partes: una, de carácter interpretativo o hermenéutico; y otra, de carácter normativo propiamente dicho, y por ende con efectos jurídicos, dividida en capítulos, secciones y artículos. La primera parte, contiene un amplísimo número de considerandos, 72 en total, los cuales constituyen la exposición de motivos de la norma jurídica; vale decir, la parte de interpretación hermenéutica plasmada por el propio legislador comunitario a fin de desentrañar y justificar el cuerpo del texto normativo.

La segunda parte, se estructura así: Capítulo I. *Disposiciones Generales*: Objetivo de la Directiva (art.1), Definiciones (art.2), Ámbito de aplicación (art.3), Derecho nacional aplicable (art.4). Capítulo II. *Condiciones generales para la licitud del tratamiento de datos personales:* Secc. I. Principios Relativos a la Calidad de datos (art. 6). Secc. II. Principios Relativos a la Legitimación del Tratamiento de datos (art. 7). Secc. III. Categorías Especiales de tratamiento (arts.8 y 9). Secc. IV. Información del interesado (arts.10 y 11). Sec. V. Derecho de Acceso del interesado a los datos (art.12). Secc. VI. Excepciones y limitaciones (art.13). Secc.VII. Derecho de Oposición del interesado (art. 14 y 15). Secc. VIII. Confidencialidad y Seguridad del Tratamiento (arts. 16 y 17). Sec. IX. Notificación (arts. 18 a 21). Capítulo III. *Recursos Judiciales, Responsabilidad y Sanciones* (arts. 22 a 26). Capítulo IV. *Códigos de Conducta* (art.27). Capítulo VI. *Autoridad de control y grupo*

---

(105) Este derecho escrito es el creado por los organismos comunitarios (El Parlamento, La Comisión y El Consejo, especialmente). Comprende en primer término, los actos jurídicos expresamente previstos en los Tratados de creación de la CE (hoy UE, Unión Europea); actos que contienen reglamentaciones obligatorias para los Estados Miembros. Estos son: los Reglamentos, LAS DIRECTIVAS, y las Decisiones dirigidas a particulares y al Estado Respectivo; así como las Recomendaciones o razones que emanan del Tratado de la CECA, y los Acuerdos Internacionales que conciernen a la Comunidad Europea. Mis trabajos: ***Las fuentes del derecho comunitario europeo.*** En: Revista FORO UNIVERSITARIO. Ed. UNED, Univ. de Nariño, Núm. 15, Pasto, 1988, p.65-75; y, ***Los denominados recursos ante los Tribunales de Justicia de la CE y Andino.*** Ed. UNED, Universidad de Nariño, Pasto (Colombia), 1995, p. 11 y ss.

de protección de las personas en lo que respecta al tratamiento de datos personales (arts. 28 a 30). Cap. VII. *Medidas de ejecución comunitarias* (art. 31). *Disposiciones Finales* (art.32 a 34).

Los principios de protección a las personas físicas (identificadas o identificables, no anónimas [106]) en el tratamiento informatizado o manual (aunque sólo extensible a los denominados *ficheros* no a las *carpetas* de datos) [107] de datos personales, previstos en la Directiva, tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos. Estas obligaciones, se refieren en particular, a la calidad de datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento. De otra parte, estos principios hacen referencia a los derechos otorgados a las personas cuyos datos sean objeto de tratamiento, tales como, el de ser informados acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias [108].

2.6.2. LA DIRECTIVA 97/66/CE, *relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas*

La fase informatizada de comunicaciones (o "telecomunicaciones" como prefiere, la Directiva) de datos personales con el desarrollo constante y revolucionario de las nuevas

---

(106) En similar sentido, los considerandos 25, 26, 68 y 72 de la Directiva.

(107) Según el considerando 27 de la Directiva sostiene que "La protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su *tratamiento manual*; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los *ficheros,* y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva".

(108) Para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. Por tanto, los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado. Los códigos de conducta con arreglo al art. 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado (Considerando 26).

las nuevas tecnologías de la información y comunicación (TIC) [109] , día a día, se va super especializando cara a los intereses, derechos y libertades fundamentales dignos de protección y garantía por parte del Estado e incluso de los mismos particulares; así como el de preservar los principios de *la libre circulación de los datos* y la confidencialidad de las comunicaciones [110] que transiten entre los Estados de la UE, conjuntamente con los cada vez, paradójicamente por el mismo avance, espectros de riesgo y vulnerabilidad que crecen geométricamente y se concretan; entre otras actividades, en el acceso, la transformación o la interceptación no autorizada de datos personales y continentes en bases de datos públicas o privadas, a través de medios muy sofisticados de tipo informático, electrónico o telemático. Acciones humanas indebidas, abusivas o ilegales que generan reproche social y normativo que en España van, desde las sanciones administrativas por infracciones (o contravenciones) al régimen del tratamiento informatizado o no de datos personales, previsto en la LOPDP, hasta las sanciones penales por estar incursos en formas delictuales contra los derechos y libertades fundamentales (entre ellos, la intimidad, la imagen y el honor, la información, etc.) [111].

La Directiva 97/66/CE, constituye una norma jurídica comunitaria que refuerza, amplía y concreta el régimen previsto en la Directiva 95/46/CE, sobre protección a los derechos y libertades fundamentales (particularmente, el derecho a la intimidad) de las personas humanas, cuando sus datos han sido tratados con medios informáticos, electrónicos o telemáticos, haciendo énfasis en la fase de transmisión (emisión/recepción) de datos. En tal virtud las normas de la Directiva 95/46/CE, se aplicarán por extensión, en cuanto a los recursos judiciales, régimen de responsabilidad y sanciones (art. 14-2); así mismo se po-

---

(109) En efecto, son los Estados de la UE, quienes mediante sus disposiciones normativas, garanticen, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicaciones y de los servicios públicos de telecomunicaciones. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente (Considerando 5).

(110) El Parlamento Europeo y el Consejo de la Unión Europea (UE), consciente de dichos avances y de que la Directiva 95/46/CE, constituye un buen instrumento, pero jamás suficiente, de defensa de los derechos y libertades fundamentales de la persona humana, ha venido trabajando una propuesta común que se concrete en una Directiva Comunitaria que refuerce y especialice la protección de esos intereses y derechos, ya que "en la actualidad están apareciendo en la UE nuevas redes digitales públicas avanzadas de telecomunicación que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios; que el desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de telecomunicaciones; que el desarrollo transfronterizo de estos servicios, como el vídeo por pedido o la televisión interactiva, depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad" (C. 2). Texto Completo de la Proposición Común (CE) No. 57/96, relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales. En: www.cc.cec *Database CELEX.*

(111) RIASCOS GOMEZ, Libardo Orlando. ***El delito informático contra la Intimidad de las personas: Una visión constitucional y penal.*** En: Revista FORO UNIVERSITARIO No. 22 de Noviembre de 2004, ISSN 1692-7923, Universidad de Nariño, Pasto, p. 9 a 40.

drá limitar el alcance de las obligaciones y derechos previstos en los denominados por la Directiva 95, “Principios relativos a la calidad de datos” (art.5 y 6), y los datos de “categorías especiales de tratamiento” (art. 8-1 a 8-4), cuando dichas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicaciones (art. 14-1).

La Directiva consta de una parte interpretativa y hermenéutica (26 considerandos) y un cuerpo normativo, con los siguientes temas: Objetivo y ámbito de aplicación (art. 1), Definiciones (art. 2), Servicios regulados (art.3), Seguridad (art.4), Confidencialidad de las comunicaciones (art. 5), Tráfico y facturación (art.6), Facturación desglosada (art. 7), Presentación y limitación de la identificación de la línea llamante y conectada (art. 8), Excepciones (art. 9), Desvío automático de llamadas (art.10), Guías (11), llamada no solicitada (art. 12), Características técnicas y normalización (art. 13), Extensión del ámbito de aplicación de determinadas disposiciones de la Directiva 95/46/CE (art. 14), Aplicación de la Directiva (art.15), y Destinatarios (art. 16).