UNIVERSIDAD NACIONAL AUTÓNOMA

DE MÉXICO

FACULTAD DE DERECHO

Seminario de Derecho Constitucional y de Amparo

EL EJERCICIO DE LOS DERECHOS "ARCO" FRENTE A LOS PARTICULARES: UN ESTUDIO COMPARATIVO DESDE EL DERECHO POSITIVO EN MÉXICO, ESPAÑA Y ARGENTINA.

TESIS

Que para obtener por el Título de

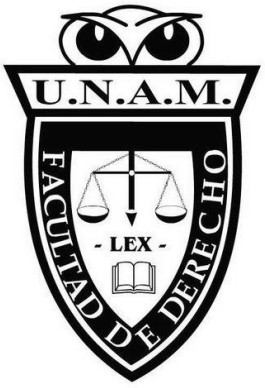
LICENCIADO EN DERECHO

Presenta:

VERÓNICA VÁZQUEZ MATA

Asesor

DR. PEDRO SALAZAR UGARTE



México, 2012

A Ana María Vázquez Pérez

In Memoriam

Agradezco…

A la Universidad Nacional Autónoma de México por brindarme la oportunidad de realizar mis estudios de licenciatura.

A la Facultad de Derecho, por el conocimiento jurídico y ético que en sus aulas aprendí, para poder ejercer tan noble profesión como la abogacía.

Al Doctor Pedro Salazar Ugarte por haber aceptado dirigir el presente trabajo, y por todas sus aportaciones que me permitieron concluirlo.

A la Lic. Yvonne G. Tovar por todo el apoyo que me brindó para poder concluir este trabajo, que sin sus aportaciones, dedicación y paciencia no hubiera sido posible concluirlo.

Al Lic. Jaime Zacarías por todos sus consejos y enseñanzas durante toda la carrera.

A Antonio Vázquez Mata por su apoyo y enseñanzas siempre.

A mis papás por todo su apoyo y dedicación, que han dado como fruto el término de esta etapa universitaria.

¡Gracias!

ÍNDICE

CAPITULO IV La protección de los Derechos ARCO

INTRODUCCIÓN

El tema de la protección de datos personales objeto de la presente investigación resulta de sumo interés atendiendo al contexto informático en el cual la sociedad se encuentra inmersa; si bien el tema no es nuevo, ha tomado un nuevo dinamismo atendiendo al desarrollo tecnológico principalmente en el sector de las comunicaciones, es decir hasta hace algunos años bastaba con una regulación estatal que protegiera la vida privada; sin embargo hoy en día se requiere de una regulación normativa enfocada plenamente a la protección de datos personales como un derecho autónomo del derecho a la intimidad, aunada a la cooperación internacional para hacer frente a las nuevas amenazas a la esfera de derechos de las personas derivadas de la inadecuada y excesiva utilización de datos.

Particularmente el tema en que se centra este trabajo es el referente a los mecanismos con que cuentan las personas para poder mantener un control sobre su información, incluyendo la posibilidad de reaccionar frente a una vulneración a sus derechos derivado de la inadecuada utilización de sus datos; tal es la función de los derechos “ARCO”, acceso, rectificación, cancelación y oposición.

A efecto de poder comprender el tema de una manera global, hemos recurrido a una investigación doctrinal, jurídica e histórica, analizando los postulados que la doctrina nos ofrece sobre los conceptos básicos en relación al tema, así como sus alcances; el campo jurídico es de vital trascendencia en este estudio, pues lo que pretendemos es hacer una comparación entre la normativa de un país europeo, uno latinoamericano y México, a efecto de conocer y fortalecer los aciertos y desventajas que nuestra reciente regulación representa para el desarrollo de la protección de datos personales. Así también recurrimos a la investigación histórica para comprender el desarrollo y evolución de la protección de datos personales.

La investigación se conforma de cuatro capítulos, en los que desarrollaremos diversos aspectos de la protección de datos personales mediante el ejercicio de los derechos “ARCO”, de manera genérica en los primeros tres capítulos y

finalmente en el cuarto haremos la separación correspondiente atendiendo a la normatividad establecida en cada uno de los países objeto de estudio.

En el primer capítulo haremos referencia a la terminología general en torno a los datos personales, para generar un contexto que nos permita comprender el tema, así mismo referiremos a las características que engloban los datos personales, entre la que destaca su titularidad, pues como lo veremos, existe un debate en torno al titular de datos de naturaleza personal, es decir, si les son propios a personas jurídicas o solamente a personas físicas.

Una vez comprendido el contexto del tema de datos personales, en el capítulo segundo trataremos la importancia de protegerlos, dividiendo en dos apartados este capítulo, por un lado haremos referencia al ámbito económico en los que tiene presencia constante la utilización de datos personales; y por el otro el ámbito social que puede verse perjudicado a raíz de un uso desmesurado de los datos personales.

Vista la importancia de garantizar una adecuada protección de datos, en el tercer capítulo abordaremos el tema propiamente de los derechos ARCO, es decir aquellas prerrogativas de que dispone el titular de datos objeto de tratamiento, para poder acceder a información que le es propia y que se encuentra almacenada en una base de datos; en caso de encontrar que dicha información es errónea, desactualizada o incompleta proceder a su rectificación o cancelación; o en caso de no consentir el tratamiento de su información poder oponerse a ello.

Finalmente en el capítulo IV, abordaremos los antecedentes y conformación legislativa de la protección de datos personales en los tres países motivo de análisis del presente trabajo; cabe señalar que la designación de ellos se hizo en razón del grado de desarrollo legislativo y jurisprudencial que han tenido, por un lado España es uno de los países europeos que primeramente contó con un marco normativo sobre el tema y que ha servido de inspiración para la mayoría de países en Latinoamérica. En tanto que Argentina si bien no fue el primer país en Latinoamérica en proteger los datos personales si fue el primero de esta región en

ser reconocido por la Comunidad Europea como un país de destino con un nivel adecuado de protección de datos personales de acuerdo a las directrices europeas. Al término de este capítulo señalaremos los procedimientos establecidos por la legislación de cada país para el ejercicio de los derechos ARCO.

Habiendo esbozado el orden normativo que garantiza la protección de datos personales en cada uno de estos países, estaremos en posibilidad de poder evaluar los desafíos que aun necesito enfrentar México, quien recientemente ha incorporado diversas disposiciones al texto constitucional sobre el tema, así como la reciente creación de la Ley Federal de Protección de Datos en Posesión de Particulares.

CAPITULO I Generalidades en torno a los de datos personales

1.1 Concepto

Para estar en posibilidad de abordar el tema a desarrollar en el presente trabajo, primeramente es necesario definir lo que es un dato para después especificar qué se entiende por datos personales.

Por lo que respecta al aspecto gramatical, la palabra dato es de origen latín "*datum"* (lo que se da). El diccionario de la Real Academia de la Lengua Española define al dato como: 1. "El antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho. 2. "Documento, testimonio, fundamento" y 3. "Información dispuesta de manera adecuada para su tratamiento por un ordenador".[1]

Sin embargo, es evidente que la definición gramatical es insuficiente para comprender la naturaleza y alcances del vocablo "dato". Más aún esta definición no aporta los elementos necesarios para poder definir lo que son los "datos personales", y sus consecuencias jurídicas. En esa tesitura, es que consideramos necesario aludir a la doctrina, esto es a los estudios realizados por expertos en la materia, que nos permitirán tener una visión más aproximada de la esencia de un dato.

En primer término tenemos a Osvaldo Alfredo Gozaini, Doctor en Derecho y Ciencias Sociales, quien señala que *"el dato es una referencia. Puede ser descriptivo, indicador, dar una pauta, pero no se vincula a la información mientras el conocimiento no se trasmita".*[2]

Por otro lado Oscar Puccinelli, distinguido profesor universitario y magistrado argentino, afirma que el vocablo *"dato se refiere a un elemento circunscripto y aislado, que no alcanza a tener el carácter de información, pues para que se*

[1] *Diccionario de la Real Academia de la Lengua Española.* 22 ed. *http://buscon.rae.es/draeI/.*
[2] Gozaini, Osvaldo Alfredo, *Habeas data. Protección de datos personales*, Argentina, Rubinzal-Culzoni Editores, 2001, p. 113.

transforme en ella se requiere la interconexión de esos datos de manera que, vinculados, se conviertan en una referencia concreta".

Olga Estadella Yuste, profesora titular de Derecho Internacional Público de la Universidad Autónoma de Barcelona, aclara que los términos "información" y "datos" responden a tiempos diferentes de creación. *Datos* pertenece a la era informática, e *información* a la era preinformática. Las directrices de la ONU hablan indistintamente de "informaciones personales" y de "datos personales".[3]

A partir de estas definiciones, vemos que los tres autores hacen una diferenciación entre lo que es un dato y la información; sin embargo, esa diferencia cada autor la funda en elementos diferentes, el primero de ellos, refiere a que los datos deben ser transmitidos, el segundo a que los datos deben ser interconectados, y la ultima autora refiere a la evolución de la informática.

Para englobar los elementos que consideramos nos ayudan a continuar con el análisis del concepto propiamente de datos personales, concluyamos diciendo que el dato es una referencia a algo, sea esta una descripción o un señalamiento del mismo, cuyo enlazamiento con otros datos, genera una fuente de información.

Una vez establecido el significado del vocablo dato, estamos en posibilidad de avanzar al siguiente concepto; los datos personales. Por lo que se refiere a la doctrina, José Luis Piñar Mañas, Doctor en Derecho y autor de numerosas publicaciones sobre Derecho de Protección de Datos, señala que los datos personales son "*cualquier dato personal, no solo los íntimos, ni los que afecten a la privacidad, sino cualquier tipo de dato personal, el contenido del derecho implica que cada ciudadano es dueño de sus datos personales, sean estos o no íntimos, por tanto hablamos de datos personales que estén sometidos a tratamiento*

[3] *Ibídem,* p. 319.

informatizado o no informatizado, es decir, estén incorporados a un fichero, sea este informatizado o no".[4]

Alonso Gómez-Robledo, Investigador titular "C" de tiempo completo en el Instituto de Investigaciones Jurídicas de la UNAM, refiere a una definición más concreta al señalar que *"los datos personales son el conjunto de informaciones sobre una persona física".*[5]

Por su parte Javier Nájera Montiel, quien cuenta con un Máster en informática y derecho, conceptúa al dato personal como *"la unidad mínima del conocimiento, de naturaleza indeterminada, referente al hombre y su dignidad humana, que representa externamente los pensamientos, creencias, emociones y sensaciones que conforman el ámbito íntimo de reserva de las personas. El dato personal es una unidad mínima del conocimiento, la unidad del saber que al momento de estar sujeta a un procesamiento transmuta en información".*[6]

Como complemento podemos citar la definición que nos proporciona el Instituto Federal de Acceso a la Información y Protección de Datos Personales, es decir, *"toda aquella información relativa a una persona que la identifica o la hace identificable. Entre otras cosas, le dan identidad, la describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Pero también, describen aspectos más sensibles o delicados, como su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros aspectos".*[7]

Como podemos ver cada definición nos aporta elementos que podemos ir concatenando a fin de obtener una idea más clara respecto a lo que son los datos

---

[4] Piñar Mañas, José L., *IV Encuentro iberoamericano de protección de datos personales*, México, IFAI, 2005, p. 22.

[5] Gómez-Robledo, Alonso y Órnelas Núñez, Lina, *Protección de datos* personales en México: *el caso del Poder Ejecutivo Federal,* México, Instituto de Investigaciones Jurídicas, UNAM, 2006, p. 16.

[6] Nájera, Javier, "El aspecto axiológico de los datos personales en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental", *Revista de Derecho Comparado de la Información, México*, núm. 11, enero-junio de 2008, *http://www.juridicas.unam.mx/publica/rev/decoin/cont/11/art/art5.htm*

[7] *http://www.ifai.gob.mx/InformacionGeneral/informacion*

personales. La primera definición nos aclara que los datos personales no son solamente los relativos a la intimidad de la persona, la segunda hace la precisión que los datos personales sólo engloban a las personas físicas (postura que en otro apartado analizaremos con detenimiento); por lo que respecta a la tercera, especifica que el dato representa el mínimo de información que de una persona se puede saber; finalmente la cuarta nos da un panorama mucho más amplio, ya que refiere por un lado a los datos que externamente caracterizan a la persona, así como a los datos relacionados propiamente con la intimidad de la misma.

Para seguir clarificando el concepto de datos personales, pasemos a analizar las definiciones que nos proporciona el ordenamiento normativo de cada país analizado en la presente investigación.

Comencemos con el ámbito europeo; el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, así como 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, han definido los datos personales, como aquella información relativa a una persona física identificada o identificable, es decir, relativa a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación, o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

La Ley Orgánica 15/1999 de España, y su Reglamento, añaden a la definición de datos personales, que éstos pueden ser cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

La ley 25.326 de Argentina define los datos personales como aquella "*Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables".*

En tanto la Ley Federal de Protección de Datos Personales en Posesión de Particulares los define como "*cualquier información concerniente a una persona física identificada o identificable".*

Podemos resaltar de las legislaciones, que el marco europeo hace una definición más minuciosa al precisar qué aspectos que caracterizan a la persona pueden considerarse como datos personales, así como la manera de representar a los datos; la particularidad de la legislación argentina es que engloba dentro de su definición a las personas jurídicas; en cuanto a México solo retoma elementos dados por la legislación española.

Una vez que conocemos las posturas adoptadas tanto por la doctrina como por la legislación estamos en posición de aportar una definición para datos personales; los cuales entendemos como aquellos elementos de cualquier naturaleza que caracterizan a una persona en su aspecto interno como externo.

1.2 Características

Definidos los datos personales, corresponde analizar cada una de las características de éstos. Por su parte Marcela I. Basterra, Magister en Derecho Constitucional y Derechos Humanos, señala que lo que caracteriza al dato personal es la posibilidad de identificar con alguna precisión a la persona, física o jurídica, a la que el dato pertenece.[8]

Es precisamente esa posibilidad lo que hace necesario que el dato esté jurídicamente protegido, en razón de que nos permite confeccionar un perfil tanto físico como conductual del titular de los datos. Por lo cual no es necesario que la información que proporciona se refiera a la vida intima del titular, tal como lo señala la autora española Ana Garrida al puntualizar que lo importante es la

[8] *Cfr.* Basterrra, Marcela I., *Protección de datos personales. Ley 25.326 y Dto. 1558/01 comentados.* Argentina. Editorial Ediar. 2008, p. 94.

posibilidad de relacionarlo con otros.[9] Así como tampoco es necesario que el dato sea falso, inexacto o discriminatorio, basta con que su titular no quiera que sea conocido por terceros porque pertenece a su fuero más íntimo, como es el caso de los datos sensibles[10].

Dentro del concepto genérico de datos personales, podemos identificar a los datos sensibles, los cuales en palabras de Osvaldo Alfredo Gozaini son aquellos datos "*que de difundirse ponen en conocimiento de quien los conoce datos de contenido privado que, salvo manifestación expresa del afectado, socavan la intimidad de las personas. El dato sensible se refiere a la salud, la condición racial y social, los pensamientos, hábitos y costumbres de la persona*". [11] El mismo autor divide a los datos sensibles en tres grupos:

1. Datos especialmente sensibles: son los que se refieren a cuestiones de ideología, religión o creencia.
2. Datos relativos a los antecedentes penales.
3. Datos derivados de la raza, la salud y la vida sexual, los cuales también requieren consentimiento de su titular para poder ser tratados. Al respecto cabe señalar que el Consejo de Europa emitió la Recomendación 81/1, donde se insiste en que los datos médicos forman parte de la esfera de la intimidad de las personas, de manera que su trasmisión o divulgación solamente puede hacerse en temas y problemas muy puntuales y restringidos.[12] El dato de salud puede ser actual o pasado o referir a una característica que tuvo una persona fallecida. En ningún caso existen diferencias de trato. El dato sexual se vincula con la actividad o las preferencias que distinguen una costumbre diferente. La información

[9] *Cfr.* Garrida Domínguez, Ana, *Tratamiento de datos personales y derechos fundamentales*, 2ª ed., España. Editorial Dykinson S.L., 2009, p. 30.
[10] *Cfr.* Armagnague, Juan (Dir.), *Derecho a la información, habeas data e internet*, Argentina, Ediciones La Rocca, 2002, p. 484.
[11] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 2, pp. 233-234.
[12] *Ibídem,* P. 245.

compila el comportamiento sexual del individuo así como la ausencia de dicha actividad, y las consecuencias derivadas[13].

Esta clasificación consideramos es un tanto extensiva del concepto de datos sensibles, pues incluye a los datos relativos a los antecedentes penales, que si bien es cierto forman parte de la intimidad de la persona, también lo es que no pueden considerarse dentro del concepto de datos sensibles, ya que son de interés general.

En cuanto a la legislación, tanto la española, la argentina y la mexicana de manera unánime definen los datos sensibles como aquéllos relacionados con el origen racial y étnico; opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual; es decir, son aquellos datos personales que afecten a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

Después de haber puntualizado lo referente a los datos sensibles, sigamos con el análisis de la clasificación de los datos personales. Una primera clasificación es la que la Fiscal argentina Alejandra Gils nos señala respecto de la ley 25.326 de Argentina, en la cual a partir del tipo de datos de que se trate, varía el nivel de protección jurídica que le brinda.[14]

a) Los datos que son de libre circulación, como los de identificación: nombre, apellido, documento de identidad, identificación tributaria, ocupación, fecha de nacimiento y domicilio, porque en principio, están excluidos de la exigencia del consentimiento para su recolección y cesión, al cumplir un papel esencial para la vinculación de las personas, sobre todo en el área de negocios y ante el Estado, con relación al ejercicio de los derechos y deberes individuales.

[13] *Ibídem,* p. 247.
[14] *Cfr.* Gils Carbó, Alejandra M., *Régimen legal de las bases de datos y hábeas data*, Argentina, Editorial La Ley, 2001, p. 167.

b) Los de circulación restringida a un sector o actividad determinada, que son susceptibles de tratamiento en tanto se presente una causa de justificación legitima y con las limitaciones que resulten de esa especialidad (crediticios, de publicidad o tributarios)
c) Los de recolección prohibida porque afectan la intimidad personal o familiar, que son los denominados datos sensibles.

Por otro lado Osvaldo Alfredo Gozaini tomando distintos criterios, realiza la siguiente clasificación:

- *Por la identificación del titular del dato* se dividen en:[15]

  a) Nominativo: es el dato de una persona física o jurídica conocida e identificada.
  b) Anónimo: es el dato de uso estadístico o científico que no identifica a persona alguna porque la información archivada no se refiere a él sino a sus actividades.

- Por la *confidencialidad de la información* pueden ser:

  a) *Datos que no afectan la sensibilidad de las personas:*[16] se trata de aquella información irrelevante que por las características que tiene no permiten herir los sentimientos más íntimos de la persona ni afectar su derecho a la privacidad. Es el dato rutinario, el que se ofrece sin complicaciones o se obtiene de fuentes fácilmente accesibles.
  b) *Datos que afectan la sensibilidad de las* personas: son los datos sensibles.

- Por la mayor o menor complejidad para lograr el dato se clasifican en:

[15] *Cfr.* Gozaini, Osvaldo Alfredo, *op. cit.,* nota 2, pp. 231 y 232.
[16] *Ídem.*

a) Datos públicos o fácilmente conocidos[17]: la información que se encuentra disponible para cualquier interesado por encontrarse en registros o lugares de fácil acceso al público.
b) Datos privados, secretos y confidenciales:[18]

- Dato privado: aquél que la persona quiere conservar en la esfera de su intimidad. Es el dato oculto que sólo conoce el titular y que será secreto únicamente mientras esté en el reducto de lo personal, exento de toda curiosidad. Es este un dato imposible de filtrar y por ello no cuenta en el problema de protección o defensa que merece.
- Dato secreto: debe custodiarse en la medida en que el deber de secreto constituye una de las manifestaciones del derecho a la intimidad. El secreto implica la ocultación de algo, pero la misma se ha de efectuar en relación a un grupo de personas. Se traduce en la existencia de una comunicación que se pretende preservar.
- Dato confidencial: es el que por su alta sensibilidad no se puede divulgar ni transmitir a terceros. Cuando el dato está en un banco o archivo la reserva es una obligación que convierte en responsable directo a quien produce la revelación.

❖ *Por la subjetividad o pertinencia de los datos* se clasifican en:[19]

a) Datos personales existenciales: aquéllos que se relacionan con definidores de la personalidad tales como el natalicio, lugar de origen, estado civil, domicilio actual y profesional, entre otros.
b) Datos personales no existenciales: son aquéllos vinculados con el patrimonio económico y con la pertinencia de cosas que identifican. Relacionados con cosas o bienes de las personas.

❖ Por el secreto que guardan:

[17] *Ibídem,* p. 235.
[18] *Ibídem,* p. 239.
[19] *Ibídem*, pp. 240-241.

a) Profesionales: al estar en una base de datos que supervisa y ordena quien ha recibido la información como consecuencia de su desempeño en una profesión determinada.
b) Militar: cuando pone en riesgo operaciones de logística o comprometer la seguridad del Estado al hacer público el armamento disponible, la campaña diseñada, el planeamiento estratégico, la adquisición de material, etc.
c) Documentos oficiales: los que quedan restringidos del derecho de acceso con la excepción que se otorgue especificaciones para ello.

Finalmente por el tipo de derecho que podemos ejercer sobre ellos, los datos los podemos clasificar en:

- Erróneo**:** es aquel que no corresponde con la realidad presente o pasada de las cosas. Procede el derecho de rectificación.
- Desactualizado: es aquel que en un momento pasado fue correcto, pero que ha devenido en incorrecto por no reflejar la situación existente al presente. El tipo de derecho que podemos ejercer es el de rectificación.
- Discriminatorios o sensibles**:** los que tienen un contenido étnico, racial, religioso, político, filosófico y sexual, es decir, definen la personalidad de una persona. Procede tanto el derecho de oposición como de cancelación
- Caduco: es el dato que por efecto del transcurso del tiempo ha perdido virtualidad, ha devenido intrascendente a los efectos de cualquier jurídico relativo a la ejecución.[20] En este caso procede el derecho de cancelación.

1.3 Titularidad de los datos personales

En este apartado analizaremos a quién pertenece la titularidad de los datos personales, pues los criterios considerados por las distintas legislaciones no son unánimes en este tema; por un lado se reconoce como único titular a las

[20] *Ibídem,* p. 438.

personas físicas, mientras que por el otro se extiende la titularidad a las personas jurídicas. Así lo podemos constatar al referirnos a la legislación de México, España y Argentina.

La Ley Federal de Protección de Datos Personales en Posesión de Particulares de México y la Ley Orgánica 15/1999 de España definen al titular como *"la persona física a quien corresponden los datos personales".*

Mientras que la Ley 25.326 de Argentina señala que es *"la persona física o de existencia ideal, con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto de tratamiento…"*

A partir de estas dos definiciones podemos establecer la existencia de una dicotomía entre las corrientes normativas, debido a que los datos personales suelen entrañarse como una manifestación de la intimidad y de la vida privada de las personas, lo que hemos visto no siempre es así, pues los datos que se refieren a estos tópicos, son los datos sensibles, mas no los datos personales en general.

También es necesario hacer hincapié en la condición del titular, en cuanto sujeto publico o sujeto privado; en razón de que hay autores que señalan que el sujeto público al tener restringido su ámbito de vida privada, también tiene restringido el alcance de la protección de sus datos personales. Lucrecio Rebollo, profesor de derecho constitucional, lo fundamenta en los siguientes aspectos.

a) Es una consecuencia, negativa o positiva, implícita en el concepto de personaje público, o con relevancia social.
b) Existe en la mayoría de los casos una pretensión, una voluntariedad de salir del anonimato.
c) Por último, existe la pretensión legítima del ciudadano de conocer ámbitos de las actuaciones, o de la persona que tiene esa relevancia social.

Sin embargo, la ley señala que la reducción del ámbito de lo privado de la persona pública, no tiene una configuración ilimitada. De esta forma la línea

divisoria se encuentra en que las renuncias a la vida privada han de estar directamente relacionadas con la actividad o el cargo que le da la relevancia social, pero no pueden ir más allá. Ser un personaje público y serlo voluntariamente no implica la renuncia total a la vida privada. Sólo supone una esfera más restringida de ésta.[21] Tal como también lo señala el Tribunal Constitucional Español, en su sentencia STC 20/92 de 14 de febrero (fundamento jurídico 3°), al establecer una subdivisión del ámbito de lo privado de la persona pública en dos partes:

i) Una la constituye la intimidad relacionada o entorno a su actuación pública, en la que el sujeto está sometido a restricciones en favor de la información o libertad de expresión.
ii) La otra es propiamente la intimidad del sujeto, no expuesta a limitación y que no tiene relación con su actividad o cargo.[22]

1.3.1 Personas físicas

Existe una tendencia de reconocer como únicos titulares de los datos personales a las personas físicas, porque el régimen de tutela de los datos personales surgió inicialmente para proteger un bien jurídico en especial: la intimidad, y las personas jurídicas no gozan de tal atributo.[23]

Siguiendo esta línea es que se han pronunciado tanto la legislación española como la mexicana al señalar como único titular de los datos personales a las personas físicas. Tal como se desprende del artículo 3_o fracción 17 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, que señala como titular a *"la persona física a quien corresponden los datos."* En el mismo sentido se pronuncia la Ley Orgánica 15/1999, en su artículo 3_o inciso 5, al reconocer como afectado o interesado a *"la persona física titular de los datos que*

[21] *Cfr.* Rebollo Delgado, Lucrecio, *El derecho fundamental a la intimidad*, España, Ed. Dykinson, 2000, p.136.
[22] *Ibídem,* pp. 137-138.
[23] Gils Carbó, Alejandra M., *op. cit.,* nota 14, p. 55.

sean objeto del tratamiento….". Así como su reglamento en su artículo segundo, que la letra dice *"…este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas…."*.

Por lo que respecta a Argentina, no solamente protege el derecho de las personas físicas con vida, sino también de las personas fallecidas; así se desprende del artículo 34 de la Ley 25.326, que refiere a la legitimación activa para interponer la acción de protección de datos. Una justificación a esta extensión de la protección de datos personales, es la que señala Matilde M. Zavala de González,[24] jurista cordobesa, quien dice que algo muy distinto de afirmar la supervivencia de la intimidad de la persona fallecida es que, en virtud de la estrechez de los lazos familiares, la invasión en lo que constituye la memoria del fallecido afecte la intimidad de sus parientes; pero en tal supuesto son éstos y no aquél, los titulares del bien jurídico correspondiente y directamente ofendido por el hecho. Por lo tanto, en la medida que se vea afectada esta "intimidad familiar", cabría aceptar el hábeas data ejercido para corregir información falsa o discriminatoria sobre el causante, existente en un registro o banco de datos.

En cuanto a México el deceso del titular de los datos es causa de sobreseimiento de la solicitud de protección de datos, de acuerdo al artículo 53 fracción 1, de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Por su parte España, solamente reconoce la posibilidad de cancelar los datos de la persona fallecida; así lo señala el artículo 2_o apartado 4 del Reglamento de la Ley Orgánica 15/1999, que a la letra dice *"este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".*

[24] *Cfr.* Palazzi, Pablo, "El hábeas data en el derecho argentino", *Revista de Derecho Informático*, Argentina, núm. 4, noviembre de 1998, *http://www.robertexto.com/archivo12/data_der_argen.htm*

La Agencia Española de Protección de Datos[25] siguiendo esta idea, establece que la protección de datos al ser un derecho personalísimo se extingue con la muerte de las personas. En este sentido, si el derecho fundamental a la protección de datos ha de ser considerado como el derecho del individuo a decidir sobre la posibilidad de que un tercero pueda conocer y tratar la información que le es propia, lo que se traduce en la prestación de su consentimiento al tratamiento, en el deber de ser informado y en el ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición, es evidente que dicho derecho desaparece por la muerte de las personas, por lo que los tratamientos de datos de personas fallecidas no podrían considerarse comprendidos dentro del ámbito de aplicación de la Ley Orgánica 15/1999.

Concluye afirmando que las normas de protección de datos no son aplicables a los fallecidos porque como consecuencia del fallecimiento, la personalidad se extingue, y por tanto dejan de ser titulares de derechos; en términos del artículo 32 del Código Civil de España.

Como hemos visto, el punto de confrontación no está en este apartado, pues las tres legislaciones analizadas reconocen la titularidad de los datos personales a las personas físicas; sin embargo no ocurre lo mismo con las personas jurídicas.

1.3.2 Personas jurídicas

Sobre el tema se presentan posturas tanto a favor como en contra de que las personas jurídicas puedan ser titulares de los datos personales; primeramente nos ocuparemos de las posturas en contra.

Las posturas en contra, basan su posicionamiento en la estrecha relación entre los datos personales y el derecho a la intimidad y a la vida privada, y es por eso

[25] *Cfr.* Informe 0278/2009 de la Agencia Española de Protección de Datos Personales, *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0278_Cesi-oo-n-de-datos-de-personas-fallecidas-c--exclusi-oo-n-de-la-aplicaci-oo-n-de-la-LOPD.pdf.*

que siguiendo una concepción clásica, de corte iusnaturalista, las personas jurídicas no pueden ser titulares de derechos fundamentales, sino a lo sumo de garantías institucionales reconocidas por la ley.

Por ejemplo la Organización para la Cooperación y el Desarrollo Económico[26] no incluye a las personas jurídicas al sostener que las nociones de integridad individual y privacidad tienen características peculiares que no deben ser tratadas de la misma forma que la integridad de los grupos de personas, la seguridad y la confidencialidad empresarial. Igualmente se afirma que no sólo las necesidades para la protección de las personas físicas y jurídicas son diferentes, sino que también lo son los marcos políticos donde se deben encontrar soluciones para equilibrar los intereses existentes.

En el mismo sentido se pronuncia la Suprema Corte de Justicia de la Nación de México, en la Tesis 2a. XCIX/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, XXVIII, Julio de 2008, p. 549, que a la letra señala *"el derecho a la protección de los datos personales se refiere únicamente a las personas físicas por estar encausado al respeto de un derecho personalísimo, como es el de la intimidad, del cual derivó aquél. Esto es, en el apuntado supuesto no se actualiza una igualdad jurídica entre las personas físicas y las morales porque ambas están en situaciones de derecho dispares, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es una derivación del derecho a la intimidad, del cual únicamente goza el individuo, entendido como la persona humana".*

En palabras de Javier Plaza Penadés, profesor de derecho civil en la Universidad de Valencia, la exclusión de las personas jurídicas del ámbito de la protección de datos de carácter personal, parte de una concepción equivocada en la que se cree que todos los datos de las personas jurídicas son públicos, y en el que se desconoce tanto la existencia de datos que las personas jurídicas quieren mantener en secreto, de forma reservada y bajo su control, así como que el daño

[26] *Cfr.* Gozaini, Osvaldo Alfredo, *op. cit.,* nota 2, p. 353.

derivado del tratamiento erróneo de los datos es el mismo en las personas físicas que en las jurídicas y que, en consecuencia, deberían de gozar de los mismos derechos de acceso, rectificación y cancelación de los datos.

Por otro lado están las posturas que sostienen que las personas jurídicas pueden ser titulares de datos personales. Sin embargo estas posturas no son unánimes, puesto que por una parte se acepta la titularidad en sentido amplio de los datos personales, mientras que por la otra se acepta únicamente una titularidad restringida, es decir, solamente en lo que concierne a algunos datos.

Hay dos argumentos tradicionales a favor de extender la titularidad de los datos personales, el primero es que el reconocimiento de las personas jurídicas como titulares permitirá realizar una mejor defensa de sus miembros cuando los datos que se refieran a la composición y/o actividad de aquellas sean objeto de tratamiento informático. El otro se basa en el peligro real de que conductas prohibidas afecten a una persona jurídica y, no gozando esta de los derechos propios de un titular, ni estando amparada por los principios que los inspiran, difícilmente podrán defenderse.

Las personas jurídicas también son titulares de información personal, principalmente de índole económica, que necesita una protección adecuada, ya sea porque requiere confidencialidad o porque la circulación de datos erróneos o incompletos sobre su solvencia y situación crediticia puede traer aparejados perjuicios irreparables derivados de la frustración de negocios con base en un informe desfavorable que no estuvieron en condiciones de controlar. Por otra parte, tanto los ficheros públicos como los privados no diferencian entre personas físicas y jurídicas cuando se trata de almacenar datos en materia fiscal, inmobiliaria, bancaria, financiera, etc.

En ocasiones, el uso incorrecto de información económica hace tan vulnerable a los individuos como a las entidades jurídicas y, aunque ello no sea suficiente para afirmar la necesidad de que las personas jurídicas sean titulares de datos personales, si *“parece lógico que las entidades jurídicas puedan disfrutar de un*

derecho de acceso o de corrección sobre la información que hace referencia a esa entidad".[27] Tal como lo afirma España en su Ley Orgánica 2/1984, de 26 de marzo sobre el derecho de rectificación; en la que reconoce el derecho a toda persona natural o jurídica, a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio.[28]

Por otro lado es innegable que las personas jurídicas tienen un derecho a la identidad, que es de fácil justificación desde que las personas jurídicas son instrumentos de los que se valen los seres humanos para la consecución de ciertos fines que deben ser legítimos, por lo tanto cualquier dato relativo a una persona jurídica, lo es en cierta medida referente a cada uno de los miembros que la integran, ya sea como socios, ya sea a través de una revelación contractual de cualquier tipo, por cuanto la obtención de datos relativos a aquella pueden constituir un eslabón más en la construcción del perfil personal de estos últimos[29].

Es así que el Documento de Naciones Unidas sobre "Principios rectores aplicables a los ficheros computarizados de datos personales" ha optado por recomendar a los Estados que las leyes de protección de datos incluyan en su campo de aplicación exclusivamente a "las personas físicas", sin perjuicio de que *"deban adoptarse disposiciones especiales, cuando proceda, para extender la aplicación total o parcial de estos principios a los ficheros sobre personas jurídicas que contengan información sobre personas físicas".*

Igualmente el Tribunal Constitucional Federal alemán, mediante auto de la Sala Segunda de 8 de julio de 1992 afirmó que *"sólo cuando la formación y la actividad de una persona jurídica son expresión del libre desarrollo de los particulares, de personas naturales, cuando especialmente la mirada a los hombres que están detrás de la persona jurídica se presenta como necesaria y llena de sentido, está*

[27] Garrida Domínguez, Ana, *op. cit*., nota 9, p. 68.
[28] *Cfr.* González Murúa, Ana Rosa, "El derecho a la intimidad, el derecho a la autodeterminación informativa y la L.O. 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos personales", España, 1994, *http://ddd.uab.cat/pub/worpap/1994/hdl_2072_1371/ICPS96.pdf*
[29] Garrida Domínguez, Ana, *op. cit.,* nota 9, p. 70.

justificado considerar a las personas jurídicas como titulares de derechos fundamentales y, por ello, incluirlas también en el ámbito de protección de determinados derechos fundamentales materiales". [30]

Asimismo, la identidad o la buena imagen de las personas jurídicas se proyecta en el nombre comercial o en el valor del fondo de comercio o en la marca de sus productos y el prestigio que éstos tienen, por señalar algunos ejemplos. En la doctrina se ha dicho que frente a un ente ideal el hábeas data protege un derecho a la verdad sobre los datos sociales que se posean en un determinado registro y que hagan a la reputación fama y buen nombre del afectado.

Para Ana Rosa González Murúa, Doctora en derecho, negar el derecho a las personas jurídicas, es un acto de discriminación entre las sociedades mercantiles con personalidad jurídica y las personas físicas comerciantes, ya que éstas últimas, como personas físicas que son, entran de lleno en el campo de aplicación de las leyes de protección de datos.[31]

En cuanto a la legislación, la Comunidad Económica Europea, tanto en el Convenio 108 como en la Directiva 95/46, sólo afirma la tutela de las personas físicas. Sin embargo Austria, Dinamarca, Islandia, Luxemburgo, Noruega y Suiza admiten que las personas jurídicas tengan igual protección que los derechos humanos; criterio que mayoritariamente han aceptado las constituciones latinoamericanas.

Como caso excepcional, la Organización de las Naciones Unidas en sus directrices sobre la protección de grupos ideales, incorpora una cláusula optativa por la cual sostiene que se pueden tomar disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de los principios recogidos en el reglamento general de archivos sobre personas físicas, es decir los Estados pueden o no extender la protección de datos personales a las personas jurídicas.

---

[30] González Murúa, Ana Rosa*, op. cit.,* nota 28.

[31] *Ídem.*

A partir de estas reflexiones podemos decir que si partiéramos de la relación datos personales-intimidad, sería difícil extender a las personas jurídicas categorías como la vida privada o intimidad que fueron concebidas en función de los intereses de las personas individuales. En cambio si se considera a estas personas como titulares de un derecho autónomo y diferente del de intimidad como puede ser el derecho a la autodeterminación informativa se facilita la extensión de las mismas en el ámbito de aplicación de las leyes de protección de datos.

1.4 La protección de datos personales

La protección de datos en palabras de Davara Rodríguez, Director de los Cursos de Especialista Universitario en Protección de Datos, es "*el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad".*[32]

Por otro lado, Oscar R. Puccinelli señala que es "*la facultad conferida a las personas para actuar per se y para exigir la actuación del Estado con el fin de obtener la tutela de los diversos derechos que pudieran verse afectados en virtud de aquellas oportunidades de tratamiento de los datos de carácter personal que le conciernen".*[33]

El Tribunal Constitucional español la define como "*el derecho que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite*

[32] Davara F. de Marcos, Isabel. "Breve análisis de la reforma al artículo 6° constitucional en lo relativo a protección de datos personales", en Carbonell, Miguel y Bustillos, Jorge (coord.), *Hacia una democracia de contenidos: la reforma constitucional de transparencia,* México, Instituto de Investigaciones Jurídicas, UNAM**, 2**007, p. 73.

[33] Puccinelli, Oscar. R., *Protección de Datos De Carácter Personal*, Argentina, Editorial Astrea, 2004, pp.8-9.

al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".[34] Estos poderes de disposición y control, dice el Tribunal, sobre los datos personales que constituye parte del contenido del derecho fundamental a la protección de datos se encuentran jurídicamente en la facultad de consentir la recogida, principio de consentimiento; consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero sea el Estado o un partido.

Osvaldo A. Gozaini establece como base de este derecho, el libre consentimiento que pueda dar quien sea requerido a esos datos, y en el control que a posteriori se pueda ejercer.[35]

Esta vigilancia apunta hacia dos objetos precisos: controlar al archivo autorizado para que cumpla la finalidad oportunamente expuesta al requerir la autorización, y verificar la actualidad de los datos para que no se ofrezca información obsoleta, equivoca o inexacta.

Al analizar el tema de protección de datos, surgen cuatro preguntas a las cuales Oscar R. Puccinelli responde:[36]

¿Qué se protege? Los datos de carácter personal, pero únicamente como medio para tutelar los bienes jurídicos que el uso de esos datos puede vulnerar.

¿De qué se protege? De ciertas actividades respecto de tales datos, conocidas técnicamente como "tratamiento" y dentro de las cuales se encuentran el acceso, registración, elaboración y transferencia a terceros.

¿De quién se protege? De cualquiera que realice el tratamiento de datos de carácter personal, cuando ese tratamiento exceda o pueda razonablemente exceder el uso estrictamente privado y personal de quien lo realiza.

---

[34] Piñar Mañas, José L., *op. cit.,* nota 4, p. 21.
[35] *Cfr.* Gozaini. Osvaldo Alfredo, *op. cit*., nota 2, p. 362.
[36] *Cfr.* Puccinelli, Oscar, *op. cit*., nota 33, p. 9.

¿Cómo se protege? Isabel Davara, especialista en protección de datos personales, analiza la protección de datos a través de la estructura de un triangulo, cuyos vértices se denominarían.[37]

a) Principios: establecen los pilares en los que se basa la protección de datos.
b) Derechos: representan la concreción subjetiva del ejercicio de esos principios, es decir, cómo el titular de los datos de carácter personal puede ejercer unos derechos que concretan los principios teóricos en los que se basa toda la normativa.
c) Procedimiento: concreta la tutela estatal a la que el individuo puede recurrir cuando se ve lesionado en el ejercicio de esos derechos como consecuencia de tales principios.

A partir de la exposición de los conceptos generales sobre el tema de los datos personales podemos continuar con el siguiente capítulo, en el cual revisaremos la importancia que tiene proteger estos datos atendiendo a los distintos sectores en que se presenta el uso constante de los mismos.

[37] Davara F. de Marcos, Isabel, *op. cit*., nota 32, p. 74.

CAPITULO II Importancia de proteger los datos personales

En el primer capítulo abordamos de manera general el tema de los datos personales y al final del mismo hicimos alusión a la protección de los datos, qué significa protegerlos, de quién se protegen y cómo podemos protegerlos, si bien mencionamos que lo que protegemos son los datos de carácter personal, cabe aclarar que únicamente como medio para tutelar los bienes jurídicos que el uso inadecuado de esos datos puede vulnerar, en este apartado es necesario que precisemos de qué manera puede verse vulnerada la protección de los datos y resaltemos los principales sectores en los que a causa de un indebido manejo de la información, el titular de los datos puede verse afectado.

La protección de datos en sus inicios fue vista con un enfoque sobre todo de carácter político, pues lo que se pretendía era frenar el avance del poder político, sobre todo después de la Segunda Guerra Mundial, cuando la protección de la personalidad fue estimada insuficiente, debido a que se había generado una gran sensibilidad frente a toda clase de menosprecio por la dignidad humana. Así lo reflejan las primeras legislaciones de la materia que surgieron en Europa; por ejemplo la ley del Bundesland de Hesse dictada en 1970 en Alemania, que tenía por objeto la defensa del individuo contra un Estado que contaba con herramientas técnicas aptas para recopilar información sobre los ciudadanos.[1]

Como podemos apreciar, la preocupación de proteger los datos, no es un tema reciente, ya que desde la segunda mitad del siglo XX se vislumbraba la necesidad de proteger la dignidad humana, frente a los posibles excesos del poder político. Sin embargo, con el desarrollo de nuevas tecnologías se ha visto incrementado el riesgo de un tratamiento de datos desmesurado, tanto por parte del Gobierno como por parte de los particulares.

[1] *Cfr*. Gils Carbó, Alejandra M., *Régimen legal de las bases de datos y hábeas data*, Argentina, Ed. La Ley, 2001, p. 3.

No obstante las legislaciones se han preocupado por enfatizar la protección de datos no solamente frente al Estado, sino a los particulares, en razón de que anteriormente el Estado era quien tenía acceso a la información personal de los ciudadanos, pero con el avance tecnológico, cualquier persona tiene al alcance de la mano los medios suficientes para acceder a la información personal de terceros, así como almacenar y concatenarla entre sí, a fin de obtener un perfil detallado de una persona; lo cual agudiza la necesidad de contar con una legislación que regule esta materia.

Con los avances tecnológicos se multiplica el peligro al que se encuentran expuestos nuestros datos, en primer término porque su tratamiento puede lograrse sin que el titular de los mismos se dé cuenta, lo que genera que no pueda identificar el por qué de consecuencias negativas en la esfera de sus derechos. En segundo lugar por la facilidad y velocidad con la que puede realizarse el tratamiento y finalmente porque las barreras geográficas han prácticamente desaparecido.

Es así, como a partir de los avances de la tecnología nuestra sociedad se ha convertido en una “sociedad de la información”, en razón de que la información, como lo son nuestros datos, se ha convertido en un elemento de poder, con valor económico.

Por otro lado hay que decir que no solamente los avances tecnológicos mal utilizados constituyen un riesgo para nuestra privacidad, sino también las demandas actuales por parte de la sociedad, que por una parte reclamamos como individuos que nuestra información sea salvaguardada de las miradas públicas, por otro lado, al pertenecer a una sociedad de la información es natural que como sociedad reclamemos tener acceso a una mayor cantidad de información.

A través del uso de la tecnología hemos obtenido múltiples beneficios en diversos sectores de la sociedad, como es la disminución de costos y tiempos, facilidad en la realización de múltiples actividades, acortar distancias y agilizar los procedimientos; para lo cual se necesita del flujo de información, lo que se logra

tanto de manera directa como indirecta, es decir, sea que el titular proporcione sus datos, o sea porque estos han sido rastreados y almacenados por un tercero.

El problema comienza cuando no obstante el titular de los datos haya autorizado la utilización de sus datos, no lo ha hecho de manera ilimitada, es decir, solamente lo hizo para una determinada finalidad, lo que en la mayoría de casos no se respeta; por otro lado el rastreo de datos se hace de manera anónima, en muchas ocasiones ilícita, como es el caso de las empresas que se dedican a vender bases de datos completas, viéndose esta situación favorecida por el mundo de información que se encuentra flotando en el aire, sin que sea necesaria alguna autorización para poder acceder a ella.

Vivir en una sociedad de la información tiene además implicaciones sociales, ya que al ser la información un elemento de poder, las personas no quieren sentirse fuera de ella, por lo tanto proporcionan su información de manera voluntaria, pero en la mayoría de las veces de manera desinformada, pues al acceder a alguna página, contestar una encuesta, contratar algún servicio; no se detienen a reflexionar sobre la utilización que de sus datos se hará, ni mucho menos los riesgos que ello implica.

Así mismo, es importante subrayar que con la globalización el intercambio de información transfronterizo es un tema fundamental en las actividades cotidianas, para lo cual se requiere un sistema que garantice la protección de la información tanto del que envía como del que recibe la información.

Dentro de este tipo de sociedad puede presentarse en muchas ocasiones un conflicto de intereses, pues mientras queremos proteger nuestra información, deseamos igualmente saber más de otros, por lo que la protección de datos personales tiende a ser vista como un obstáculo para el libre ejercicio de otros derechos, como es el caso de la libertad de expresión o el derecho de información. Sin embargo, como veremos más adelante, hay algunos casos en que la ponderación de derechos beneficiará a uno u otro derecho, dependiendo de las circunstancias particulares en cada caso, pero de ninguna manera debemos

vislumbrar un derecho como obstáculo de otro. Al efecto, como menciona el filósofo argentino Garzón Valdés solamente en una sociedad en la que la intimidad está salvaguardada y la privacidad se encuentre protegida, es posible que las libertades (personal, de pensamiento, de expresión, etcétera) florezcan. Y sólo en donde existen estas libertades es posible edificar y desplegar instituciones transparentes y democráticas.[2] Por lo tanto, el reto está en encontrar el justo equilibrio entre ambos derechos, pues lo que se busca con la protección, no es censurar la información, sino mantener el control sobre la misma.

2.1.1 Importancia económica

Diversos son los nombres con los que se les empieza a calificar a los datos personales, por ejemplo el "nuevo petróleo"[3] o la "nueva divisa del siglo XXI"; dichas denominaciones les han sido asignadas en función de la amplia demanda que en el mercado existe de nuestra información, tanto por parte del Estado para llevar a cabo diversas funciones que tiene encomendadas, sean de tipo estadístico, de control, para la prestación de servicios, etcétera; como por los particulares que requieren de nuestros datos para llevar a cabo sus actividades, tal es el caso de las empresas de seguros que requieren de la obtención de datos para determinar el tipo de cliente que está contratando sus servicios, y en función de sus características saber el nivel de riesgo en que se encuentra para poder determinar las pólizas que le convienen. De igual manera las empresas de publicidad se allegan de información para conocer las preferencias de las personas y así saber qué tipo de productos estarían dispuestos a consumir.

La economía ha incorporado nuevos elementos de valor, como es la información, debido al rol esencial que juega en muchas de las actividades cotidianas ha ido

[2] *Cfr*. Garzón Valdés, Ernesto, *Lo íntimo, lo privado y lo público*, 5° ed., México, IFAI, Cuadernos de Transparencia 06, 2008, p. 8.
[3] Aradas, Anahi, "Nuestros datos personales son el nuevo petróleo", *BBC Mundo*, 16 abril 2012, *http://www.bbc.co.uk/mundo/movil/noticias/2012/04/120416_tecnologia_datos_personales_petroleo_aa.shtml*

adquiriendo un alto valor económico; luego entonces se ha convertido en un factor de poder. Algunos expertos afirman que "*la información lo es todo"*. Así pues el "chismorreo" ha dejado de ser ocupación de gente ociosa, para convertirse en una mercancía, buscada con ahínco e, incluso, con descaro.[4]

La sociedad ha dado un giro, pues mientras en la novela de George Orwell "1948",[5] el autor refería a un control estatal que vigilaba a los ciudadanos, a grado tal que violaba su vida privada; sin pensarlo dicho control ahora se ha convertido en un control mercantil, pues la intimidad se ve doblegada ante un activo en alza, es decir, la intimidad como valor mercantil.

Es justamente por este control mercantil que recobra mayor importante el tema de la protección de los datos personales, pues necesitamos buscar mecanismos jurídicos y técnicos que nos permiten contrarrestar los efectos negativos de considerar nuestra información como una mercancía.

2.1.1 Mercado de la información

Como hemos visto la información ha ido adquiriendo tal relevancia, que a la sociedad en que vivimos se le ha denominado "sociedad de la información", es decir, un modelo de organización industrial, cultural y social caracterizado por el acercamiento de las personas a la información a través de las nuevas tecnologías de la comunicación. Supone una informatización de los diversos sectores, dirigida a abrir una vida de participación de los ciudadanos en todas las facetas de la vida económica y social, así como a obtener en último término, una mejora en su calidad de vida. Se trata de conseguir que las nuevas tecnologías de la

[4] *Cfr*. Warren, Samuel y Brandeis, Louis, *El derecho a la intimidad*, España, Editorial Civitas S.A., 1995, p. 26.
[5] *Cfr.* Orwell, George, *1984*, México, Editorial Época, 2005, p. 326.

comunicación se conviertan en herramientas para la creación de una sociedad de integración en la que todos los ciudadanos tengan cabida.[6]

Para el autor Manuel Castells[7] este tipo de sociedad no es propiamente una sociedad de la información, sino una sociedad informacional, ya que para él la información es la comunicación del conocimiento, mientras que el término informacional indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de la productividad y el poder, debido a las nuevas condiciones tecnológicas que surgen en este nuevo período histórico.

La difusión y desarrollo de ese sistema tecnológico ha cambiado la base material de nuestras vidas, por tanto la vida misma, en todos sus aspectos: en cómo producimos, cómo y en qué trabajamos, cómo y qué consumimos, cómo nos educamos, cómo nos informamos-entretenemos, cómo vendemos, cómo nos arruinamos, cómo gobernamos, cómo hacemos la guerra y la paz, cómo nacemos y cómo morimos; y quién manda, quién se enriquece, quién explota, quién sufre y quién se margina. Las nuevas tecnologías de información no determinan lo que pasa en la sociedad, pero cambian tan profundamente las reglas del juego que debemos aprender de nuevo.

Dicho cambio en el comportamiento social se ve acentuado por el impacto que la sociedad de la información ha tenido en una pluralidad de modelos sociales y culturales, pues la sociedad de la información comparte algunos rasgos estructurales comunes en todo el mundo, gracias a que se fundamenta en la generación de conocimiento y procesamiento de la información con ayuda de tecnologías informacionales basadas en la microelectrónica; está organizada en redes; y sus actividades fundamentales están interconectadas en red en una

[6] *Cfr*. Campuzano Tomé, Herminia, *Vida privada y datos personales*, España, Editorial Tecnos, 2000, p. 20.
7 Cfr. Castells, Manuel. *"La era de la información", http://www.manuelcastells.info/es/obra_index_3.htm*

escala global, actuando como una unidad en tiempo real gracias a la infraestructura de las telecomunicaciones y el transporte.[8]

Para darnos una idea de la gran cantidad de información que se genera hoy en día, recurramos a la cifra que IBM nos da, 2,5 quintillones de bytes de información por día se generan en el mundo; una cantidad gigantesca sin duda, sin embargo dicha información interrelacionada entre sí, genera una cantidad aun más exorbitante.

Generar esa cantidad de información se debe inminentemente al uso de internet, el cual está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, así también nuevos riesgos para los datos personales y la intimidad.[9]

Hemos dicho la enorme cantidad de información que está ahí, disponible para aquel que tenga acceso, pero ¿cómo es se obtienen beneficios económicos a partir de ella?, pues bien desde hace tiempo los hackers dejaron de ser adolescentes con ganas de diversión para convertirse en verdaderas máquinas de hacer dinero fácil, a costa del robo de datos confidenciales de empresas y personas comunes y corrientes; nos preguntamos ahora ¿por qué pagar dinero para obtener datos que nos son propios, y que aparentemente no tienen relevancia? digamos que de manera aislada pueden no interesar a nadie, pero si se logra entrelazarlos entonces si resulta interesante, pues configuran un perfil completo de nosotros mismos, útil para los distintos sectores del comercio.

Es por eso que el negocio comienza desde aquellas empresas que se dedican a rastrear la información, para vender la base de perfiles ya identificados, como por

[8] *Cfr.* Castells, Manuel y Himanen, Pekka, *El Estado del bienestar y la sociedad de la información. El modelo finlandés*, España, Alianza Editorial, 2002, p. 18.
[9] Directiva 2002/58/CE.

ejemplo la empresa Dateas,[10] la cual es un proveedor de datos, referentes a domicilio, teléfono, familiares, estado civil, ocupación, participación en redes sociales, afiliación política, entre otros; mediante el pago de 15 euros proporciona un perfil detallado de una persona.

El otro lado del negocio se torna respecto a las empresas que solicitan determinado tipo de información, acorde a los servicios que prestan o a los productos que ofertan, por ejemplo una empresa puede necesitar datos respecto del consumo de un determinado grupo de personas, para encaminar determinado la venta de su producto; u otra puede necesitar datos respecto de los viajes realizados, por tratarse de una agencia de viajes; y es por esta razón que no importa que nosotros tengamos nuestros datos de manera dispersa, pues quienes se encargan del tratamiento facilitan a las empresas un perfil completo de cada uno de nosotros.

Vemos que la obtención de datos es útil en múltiples sectores comerciales, por lo que se ha convertido en una actividad altamente redituable, lo que provoca que mucha gente busque conseguirlos a cualquier costo, no importando emplear medios ilícitos. Por ejemplo un estudio realizado por la empresa Symantec Corporation[11] indica que los datos de una tarjeta de crédito se pueden comprar en internet por €1,50 si se compran en grandes cantidades, mientras que el precio por los datos de acceso a una cuenta bancaria en línea asciende a unos €225 euros. Los criminales también venden los datos de acceso a computadoras personales por unos €5, mientras que los datos completos de una identidad robada, con el número de la seguridad social y de la tarjeta de crédito incluidos, cuesta menos de €15.

No obstante la referencia a los hackers, hemos de señalar que la recolección de datos no solamente se hace por medios ilícitos, pues en muchas ocasiones nosotros mismos proporcionamos nuestra información a las empresas, cuando

[10] *www.dateas.com*.
[11] Una de las empresas líderes en tecnología de seguridad Internet.

adquirimos un producto o contratamos algún servicio, incluso cuando buscamos estar en comunicación con nuestros amigos y familiares, tal es el caso de las redes sociales. Un tema que de inmediato nos lleva a preguntarnos: si nosotros mismos somos quienes consentimos el tratamiento de datos, ¿cómo puede hablarse de un mercado de la información?; a dicha pregunta se puede contestar con la frase empleada por Ignacio Suárez, abogado especializado en Derecho en Internet y protección de datos, *"No hay nada gratis en internet. Mucha gente lo que no sabe es que dar sus datos en páginas web es dar dinero".*[12]

A partir de esta idea podemos decir que si las empresas online proporcionan un espacio gratuito para el disfrute de los usuarios, no sería redituable poseerlas si no se obtuviera ganancia alguna, por lo que con los datos de los usuarios se forman bases de datos que posteriormente se venden a otras empresas, especialmente de publicidad, y justo ahí es donde están las ganancias. Para darnos una idea de en cuánto están valuados nuestros datos, la empresa de seguridad Norton lanzó al mercado una herramienta llamada Norton Online Risk Calculator, que pretende arrojar el valor estimado que nuestra información distribuida en la red tiene en el mercado negro.

Hemos visto la importancia que han cobrado los datos personales actualmente a nivel mundial, y como hemos dicho esto representa un gran riesgo para la privacidad de las personas, en razón de que nuestra información puede caer en manos que hagan mal uso de ellos, o simplemente le den un tratamiento distinto al que nosotros consentimos, por lo cual es importante la regulación en materia de datos personales.

[12] Aradas, Anahi, *op. cit.,* nota 3.

2.1.2 Agencias de publicidad

Como hemos visto el mercado de la información tiene como cliente principal a las empresas de publicidad, por lo que este apartado desarrollaremos dicho sector.

El progresivo desarrollo de técnicas automatizadas de tratamiento de datos constituye una herramienta de gran utilidad para la industria de la publicidad, en la medida en que permite realizar una óptima segmentación del público destinatario de las comunicaciones comerciales. Sin embargo, para los consumidores, estas técnicas representan una potencial amenaza para su privacidad, en razón de que sus datos son tratados indiscriminadamente por las agencias de publicidad, lo que se constata con el sin número de anuncios publicitarios que son enviados sobre todo a los correos electrónicos, a pesar de que nosotros no estamos interesados en dicha propaganda ni tampoco hemos solicitado recibirla. Esto sucede porque nuestros datos como son dirección, número telefónico o dirección electrónica, que hemos proporcionado directa o indirectamente, han sido recabados por las agencias de publicidad, y como ya lo hemos mencionado, a partir del perfil que dedujeron basado en los datos personales recolectados, es que saben que dicha publicidad podría interesarnos y por lo tanto somos vistos como consumidores en potencia; por lo cual resulta necesaria la regulación de los datos personales frente a las agencias de publicidad.

Veamos en primer lugar, cómo es que las agencias de publicidad se allegan de la información para segmentar a sus consumidores.

Cada vez que se visita un sitio web, se suministra de forma rutinaria una información que puede ser archivada por el administrador o proveedor de sitio; a éste no le resulta difícil averiguar la dirección de correo electrónica del usuario, qué páginas lee y cuántas no le interesan, cuantas páginas ha visitado, así como el sistema operativo y el navegador utilizado; dando también lugar a que terceros,

por ejemplo empresas de servicios o empresas de publicidad se aprovechen de esta información y de estos datos para fines comerciales.[13]

Así mismo, las empresas de publicidad se allegan de información mediante el intercambio que pactan con los sitios web, cómo es esto, pues bien hemos de decir que los servicios aparentemente gratuitos que ofrecen algunas páginas web, como es el caso por ejemplo de las redes sociales, tienen que tener un sustento económico para que la actividad les sea redituable, y es por eso que para poder brindar sus servicios de forma gratuita pactan con las empresas de publicidad, quienes colocan anuncios publicitarios en los sitios web, a cambio de una serie de datos que otorgan los usuarios.

Con esta práctica se benefician tanto los usuarios, las agencias de publicidad y claro los sitios web. Los usuarios en el sentido de que acceden a los servicios que ofrecen diversos sitios web de manera gratuita.

Por lo que respecta a la publicidad diremos que si las agencias publicitarias tienen bien identificados a sus consumidores, incrementan su efectividad, es decir, con un nivel de información adecuada se utiliza menos publicidad y más exacta, a diferencia de una red de usuarios anónimos relativiza esa posibilidad y sería necesario incrementar la cantidad de anuncios, lo cual generaría pérdidas económicas.

Como ejemplo de lo anterior tenemos el caso de los anuncios publicados en las redes sociales, ya que publicar en estos medios multiplica por 40 la efectividad de una campaña; razón por la cual cada vez más empresas eligen a las redes sociales como canal central de sus esfuerzos publicitarios[14].

En tanto que los sitios web a cambio de la cesión de datos personales de sus usuarios reciben importantes ganancias, por cada vez que uno de sus usuarios

[13] *Cfr*. Campuzano Tomé, Herminia, *op. cit.*, nota 6, p. 68.
[14] *Cfr.* Piacente, Pablo, "Indican que publicitar en redes sociales multiplica por 40 la efectividad de una campaña", 31 agosto de 2010, *http://www.coguan.com/blog/indican-que-publicitar-en-redes-sociales-multiplica-por-40-la-efectividad-de-una-campana*

sigue la liga de algún anuncio publicitario; así lo señalan emarketer, webpronews y el blog tecnológico Techcrunch, al referir que sólo con los ingresos por publicidad Facebook habría ganado US$1.860 millones en 2010, liderando una lista seguida por YouTube con US$945 millones, Myspace con US$388, LInkendin con US$243 y los US$45 de Twitter.[15]

Como vemos los tres actores se ven beneficiados con la publicidad colocada en los sitios web, sin embargo para los usuarios la publicidad representa una amenaza para sus datos personales, pues a partir de la información que generamos es que perfiles completos de nosotros mismos se encuentran en manos de terceros que no ubicamos, en el supuesto que quisiéramos ejercer alguna acción referente a nuestra información.

Por contrarrestar lo anterior, se han generado algunas medidas para no recibir información no deseada, como es el caso de los ficheros Robinson, los cuales son definidos por Ana Garrida como "*aquéllos en los cuales deberían inscribirse los ciudadanos que deseen que su vida privada no sea contaminada por la recepción de propaganda no deseada quedando a salvo del mercado de información".*[16]

Podríamos decir que estos ficheros pretenden dar una especie de inmunidad a las personas que deciden sumarse a ellos, frente a la publicidad no solicitada. Sin embargo el catedrático español Pérez Luño refiere a estos ficheros desde otra perspectiva, al señalar que *"en el nombre dado a estos ficheros, subyace la idea de que los ciudadanos normales son aquéllos que aceptan gustosos la contaminación de su vida privada por los intereses consumistas de los mercaderes de publicidad y el ciudadano insólito y extraño es el que desea salvaguardar el*

[15] Aradas, Anahi, *op. cit.,* nota 3.
[16] Garrida Domínguez, Ana, *Tratamiento de datos personales y derechos fundamentales,* 2ª ed., España, Editorial Dykinson S.L., 2009, pp. 181-182.

derecho fundamental a la vida y se autoconfina en un aislamiento parangonable al sufrido por Robinson en su isla solitaria".[17]

Idea que no compartimos en el sentido de considerar que las personas que no se suman a los ficheros de esta naturaleza, no es porque deseen ver su privacidad invadida, sino se debe más bien a la falta de información, tanto de la existencia de estos ficheros, como del riesgo que representa que terceros conozcan y almacenen información que les concierne.

Si bien los ficheros representan una alternativa al problema de la publicidad desmedida, hemos visto que con el uso de internet nos enfrentamos a problemas que no logran resolverse con esta medida, como por ejemplo el hecho de navegar entre páginas, de tal forma que con un solo "click" en un icono es posible dejar de visualizar una página ubicada en territorio nacional para pasar a ver otra página almacenada en el extranjero, lo que genera que el usuario crea estar facilitando sus datos personales a un entidad cuando en realidad es otra la que los está obteniendo, siendo muchos los casos en los que ésta última no se identifica claramente en la web.

Tal como fue posible apreciar en el presente numeral, las agencias de publicidad representan un riesgo inminente para la protección de datos personales, lo cual nos lleva a reflexionar sobre la importancia de una protección efectiva para los datos.

2.1.3 Seguridad en la realización de transacciones comerciales

La privacidad y la protección de datos personales son elementos importantes en las distintas modalidades del comercio, pero particularmente han tomado mayor relevancia al momento en que los consumidores llevan a cabo transacciones

[17] *Ídem.*

comerciales por medios electrónicos, compras en Internet o simplemente al intercambiar datos e información con otros usuarios, empresas y gobierno en la red.[18]

Por tanto es de vital importancia que se garantice la seguridad en las transacciones y se protejan los datos personales que son intercambiados en las mismas, ya que para que siga el aumento en la realización de las transacciones de manera electrónica, tanto los compradores como los vendedores necesitan estar seguros que sus pedidos y pagos tendrán lugar con un riesgo mínimo de engaño y uso indebido de la información que se proporciona.[19]

Esa seguridad se debe a la enorme cantidad de información que los consumidores tienen que proporcionar si desean realizar alguna transacción, por ejemplo antes de realizar la transacción el usuario debe registrarse en el sitio web, proporcionando datos como nombre, edad, correo electrónico, domicilio, entre otros; una vez que se hace la transacción, los siguientes datos que se le solicitan son los referentes a la forma de pago, como pueden ser los datos de cuentas bancarias.

Datos necesarios para llevar a cabo la transacción, sin embargo, se ha comprobado[20] que hay sitios web en los que no es posible identificar explícitamente al responsable del tratamiento, lo que deja de alguna forma indefenso al afectado de cara al ejercicio de sus derechos, puesto que, dicha

---

[18] *Cfr*. Velasco San Martin, Cristos, **"**Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?", *Boletín de Política Informativa*, núm. 1, 2003, *http://www.inegi.gob.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf*

[19] *Cfr***.** Knorr, Jolene Marie y otro, "La protección del consumidor en el comercio electrónico"¸ *Revista de Ciencias Jurídicas, Universidad de Costa Rica*, núm. 103, enero-abril de 2004, *http://www.iij.ucr.ac.cr/archivos/publicaciones/revista/Revista%20103.pdf*

[20] *Cfr.* Recomendaciones de la Agencia de Protección de datos al sector del comercio electrónico, para la adecuación de su funcionamiento a la ley orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal, *http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_comercio_electronico.pdf*

figura jurídica no siempre coincide con la de la entidad o persona que ha registrado el dominio en Internet.

Así mismo hemos señalado la facilidad con la que se puede navegar entre páginas, lo cual evita que el usuario tenga plena certeza de cuál es la página a la que realmente le proporcionó su información al realizar una transacción.

Aunado a lo anterior, los datos personales del usuario pasan por varias manos antes de completar la transacción, por ejemplo el que gestiona los servidores web por cuenta del comerciante, el propio comerciante, el que autoriza la transacción financiera, el que se encarga de emitir los documentos que otorgan la titularidad del producto (por ejemplo, una agencia de viajes), el que se encarga de servir el producto (logística), el que se encarga de prestar la atención al cliente, por lo que es muy importante que el usuario sepa quién de todos ellos es el que finalmente decidirá sobre el uso y finalidad de sus datos personales.

Por lo anteriormente expuesto, resalta la importancia que tiene el proteger la información personal de los actores que intervienen en las transacciones comerciales, pues se corren varios riesgos, desde que teniendo acceso legítimo a los datos haga mal uso de estos, o bien un tercero externo a la relación comercial logre infiltrarse en el flujo de información.

2.2.1 Importancia social

Un elemento a destacar de por qué debemos proteger los datos personales, es en razón de que los perfiles elaborados a partir de datos almacenados en una base, corresponden a la realidad del momento en que el dato fue recolectado, pero el dato es una referencia fija, a diferencia de la persona que es cambiante, evoluciona, corrige sus errores, modifica sus valores y, más aun, tiene derecho a ello. Por lo tanto una persona no puede ser juzgada basándose solamente en un

perfil elaborado a partir de los datos almacenados en una base, sino por los actos que realiza; evitando así, la discriminación.

Respecto al tema de la discriminación es importante aludir a que un tratamiento incorrecto de los datos personales puede provocarla contra el titular de los mismos, sobre todo si se trata de los llamados datos sensibles, lo cual atenta contra la dignidad de la persona. Esta discriminación puede ser excluir al titular de la posibilidad de acceso a un determinado bien o servicio o, también en un daño directo a su reputación, al tomar en cuenta ciertos datos de éste, por ejemplo datos referentes a la salud o a la solvencia económica.

Uno de los campos en los que mayor discriminación se ha dado debido al tratamiento incorrecto de los datos personales es el campo laboral, ya que desde de la segunda mitad del siglo XX los empresarios empezaron a seleccionar a los trabajadores sobre la base de nuevos criterios: test psicológicos, condición médica o estudios sociológicos. A la vez, el desarrollo de las tecnologías de la información aumenta exponencialmente la posibilidad del tratamiento masivo de datos, de su transmisión y uso.[21]

A partir de estos nuevos criterios de selección y basados en la libertad que tienen los patrones para elegir a su personal de trabajo, es que se han suscitado situaciones de discriminación cuando el patrón extralimita sus facultades para seleccionar al personal más apto para un determinado puesto y basa sus decisiones en criterios subjetivos o bien en información privada del trabajador obtenida de los estudios médicos que por lo regular las empresas exigen practicarse a los trabajadores.

Un ejemplo de esta situación la encontramos en el caso de FIAT, una empresa italiana que recogió en una base de datos, todos los datos posibles acerca de sus trabajadores, relacionados, además de los necesarios para llevar el control de la

[21] *Cfr*. Sánchez Urrutia, Ana Victoria, "Información genética, intimidad y discriminación", *Acta bioethica, edición online,* v.8 núm. 2, 2002, *http://www.scielo.cl/scielo.php?pid=S1726-569X2002000200007&script=sci_arttext*

gestión de la empresa, otros como la religión, afiliación sindical y política, permitiendo llevar diversas actuaciones de la empresa contra algunos trabajadores.[22]

El patrón o empleador tiene derecho a investigar no sólo los aspectos estrictamente profesionales sino, que cuando el puesto lo requiera, también puede investigar cuestiones de naturaleza psico-física, de ahí que se justifique la legalidad del interés de un patrón-empleador por evaluar la capacidad profesional de un candidato. En cualquier caso, la legalidad de solicitar tal información, debe estar relacionada con el tipo de trabajo.[23]

Para que la libertad de contratación no se vea vencida por otro derecho como el de no discriminación, el patrón deberá sustentar su decisión en criterios objetivos, es decir, en criterios estrictamente ligados a la idoneidad del puesto. Para determinar la idoneidad debe atenderse al tipo de dato que se recabe y su vinculación específica con la actividad laboral, quedando fuera del conocimiento del mismo los aspectos de la vida privada del candidato, cuya apreciación no es relevante para detectar su aptitud laboral.[24]

Al efecto, el Convenio número 111 relativo a la Discriminación en materia de empleo y ocupación adoptado el 25 de junio de 1958 por la Conferencia General de la Organización Internacional del Trabajo (OIT) en su cuadragésima segunda reunión, señala que si bien la discriminación comprende cualquier distinción, exclusión o preferencia basada en motivos de raza, color, sexo, religión, opinión política, ascendencia nacional u origen social que tenga por efecto anular o alterar la igualdad de oportunidades o de trato en el empleo y la ocupación; si dichas

[22] *Cfr*. Araujo Carranza, Ernesto, *El derecho a la información y la protección de datos personales en México*, México, Porrúa, 2009, p. 63.

[23] *Cfr.* González Martínez, Nuria, "Igualdad y discriminación genética", en Muñoz de Alba Medrano, Marcia (coord.), *Temas selectos de salud y derecho, México, Instituto de Investigaciones Jurídicas UNAM, 2002, http://biblio.juridicas.unam.mx/libros/1/357/11.pdf*

[24] *Cfr.* Corrales Castillo, Warren, "Viabilidad jurídica de la implementación del recurso de habeas data para regular la discriminación en los procesos de selección de personal en razón de bases de datos", *Instituto de Investigaciones Jurídicas, Facultad de Derecho, Universidad de Costa Rica*, 2011, *http://www.iij.ucr.ac.cr/tesis/2011?order=title_1&sort=desc*

distinciones, exclusiones o preferencias están basadas en las calificaciones exigidas para un empleo determinado no serán consideradas como discriminación.

Esta referencia que hace la OIT refuerza la idea de que a pesar de que en determinado momento se requiera preferir determinadas características en una persona para poderla elegir como candidato a ocupar una vacante laboral, si está aparente discriminación está fundamentada en los requerimiento necesarios para poder desempeñar adecuadamente la actividad para la cual se está ofertando la vacante, no se considera como un acto discriminatorio.

En igual sentido una persona puede verse discriminada en la prestación de algunos servicios, como puede ser solicitar un crédito o contratar un seguro, por ejemplo las agencias de crédito mantienen archivos detallados con información relacionada con nuestro crédito: a quién le debemos dinero y si hemos pagado a tiempo.

El proceso bajo el cual estas empresas financieras buscan, almacenan, procesan y analizan información de sus clientes se conoce en inglés como “data mining”,[25] mediante el cual las empresas pueden tomar mejores decisiones sobre qué vender y cuánto cobrar si analizan una cantidad vasta de información relacionada con sus clientes.

En el caso de la contratación de un seguro por ejemplo médico, las empresas también recurren al rastreo de información para clasificar a sus clientes, en rentables y no rentables, y en determinados casos pueden incluso negar o limitar el seguro médico a las personas que lo solicitan.

Básicamente lo que hacen es analizar qué enfermedades o condiciones médicas ocasionan altos gastos para la aseguradora. Esto lo hacen analizando millones de expedientes de sus clientes actuales y pasados. De ahí buscan ciertas “tendencias”, por ejemplo el tipo de medicamentos que una persona consume, la frecuencia con la que lo hace, cuántas veces ha sido intervenida quirúrgicamente,

[25] Técnicas para la extracción de información oculta en grandes bases de datos.

si tiene tendencia genética a alguna enfermedad, entre otras. Teniendo en cuenta estas tendencias, preparan perfiles de clientes que no son deseados, y a los que seguramente les negarán el servicio.[26]

Con los ejemplos antes mencionados se muestra cómo a partir de la elaboración de perfiles basados en la obtención de datos personales, una persona puede ser discriminada a la hora de solicitar un empleo, solicitar un crédito o querer contratar un servicio; lo cual es motivo suficiente para garantizar la adecuada protección de datos personales.

Por otro parte, dentro de la sociedad de la información en la que el tratamiento de datos es una práctica cotidiana, éste se ha llegado a convertir en un arma estratégica de manipulación de conductas individuales, debido a que las personas temen que una conducta suya quede registrada en alguna base, y al no favorecerle el derecho al olvido, pueda posteriormente afectar alguna parte de su vida.

Un caso histórico que marca el tema de la protección de los datos personales, es el de la empresa IBM con relación al holocausto. Edwin Black denuncia el uso de las máquinas tabuladoras y tarjetas perforadas por la empresa filial-Dehomag- de esa multinacional en Alemania que fue decisivo para elaborar el censo alemán de 1939 e investigar los antecedentes raciales de toda la población alemana, lo que facilitó la identificación y localización de los judíos cuya dirección se incluía en cada ficha.[27] Los nazis probaron al mundo que simples informaciones personales de conocimiento común para el círculo de amistades, reunidas en un banco de datos unificado, pueden representar la diferencia entre la inclusión y la exclusión en una sociedad fundada en mecanismos automatizados de selección estadística.[28] Esto nos lleva a insistir en que los datos personales no deben ser

[26] *Cfr.* Periu, Mike, "Influencia de las enfermedades preexistentes en el seguro de salud", *UTC*, 2 abril de 2009, *http://blog.micumbre.com/category/dinero/*

[27] *Cfr.* Piñar Mañas, José L. *IV Encuentro iberoamericano de protección de datos personales*, México, IFAI, 2005, p. 17.

[28] *Cfr.* Vianna, Túlio, "El derecho a no ser registrado", *Instituto de Investigaciones Jurídicas UNAM, http://www.juridicas.unam.mx/publica/librev/rev/dconstla/cont/2007.2/pr/pr6.pdf*

tratados de manera arbitraria, porque de hacerlo provocan daños irreparables a la sociedad, con Adolfo Hitler se demostró cómo la tecnología de procesamiento automático de registros personales tiene un gran potencial selectivo y excluyente.

Dentro de la importancia social, podemos referirnos a la importancia de que los datos personales merecen estar fuera de las miradas públicas; esto es, la dicotomía entre lo público y lo privado.

Respecto del término "privado" no encontramos múltiples variables de su acepción, porque generalmente lo asociamos con lo personal, sin embargo, el término "público" enraíza algunas variantes en cuanto a su significado, pues muchas veces llegamos a confundir lo público con lo estatal.

Por lo cual es necesario detenernos en este tema para analizar las distintas acepciones de la palabra "público". Un primer pronunciamiento lo encontramos con el jurista italiano Norberto Bobbio quien nos dice que lo público no necesariamente guarda relación con el poder público, pues en si lo podemos atribuir a la colectividad; mientras que privado refiere a lo individual.[29]

En el mismo sentido se pronuncia la Doctora Nora Rabotnikof[30] quien distingue tres significados diferentes para el término "público":

- Lo común y lo general, en contraposición con lo particular y lo privado (adjetivo).

  Lo público como lo que es de interés o de utilidad común, que atañe a lo colectivo, que concierne a la comunidad, y por ende a la autoridad de ella emanada, contra lo privado como aquello que se refiere a utilidad y al interés individual. Hablamos así de seguridad pública o salud pública. De allí que en algunas definiciones el término público aparezca como lo

[29] *Cfr.* Elizalde, Luciano H. "Lo público y lo privado como problema prepolítico. Un análisis desde la sociología de la comunicación", *Revista Doxa*, España, núm. 7, *http://www.humanidades.uspceu.es/pages/investigacion/humanidades-investigacion-revista-doxa-VII.html.*
[30] *Cfr.* Rabotnikof, Nora, *En busca de un lugar común. El espacio público en la teoría política contemporánea*, México, UNAM, Instituto de investigaciones filosóficas, 2005, pp. 18-19.

perteneciente o concerniente a todo un pueblo, lo que emana del pueblo, de donde se desprende la referencia a la autoridad colectiva, al Estado.

Contra lo privado que es particular e individual y aquello que, en su origen, pretende sustraerse a ese poder público (entendido como poder de la colectividad). Esto sirve para distinguir el derecho público del derecho privado; ley pública- contrato privado. Es en este sentido que público se vuelve progresivamente sinónimo de político, de estatal.[31]

- Visible, manifiesto u ostensible, en contraposición a lo oculto o secreto.

  Lo que es visible y se desarrolla a la luz del día, lo manifiesto y ostensible, en contraposición a lo oculto o secreto, reservado; lo que no puede verse, aquello de lo que no puede hablarse, que se sustrae a la comunicación y al examen.[32]

- Abierto en contraposición a cerrado (accesibilidad vs vedado) (sustantivo).

  Lo que es de uso común, accesible a todos, abierto, contra lo cerrado aquello que se sustrae a la disposición de otros. Lo público no es objeto de apropiación particular, se halla abierto, distribuido. El público como sustantivo (conjunto de aquellos que se benefician de esa apertura). El signo más ostensible de privacía como apropiación es la clausura[33]. (Inclusión- exclusión)

Nora Rabotnikof nos señala las distintas concepciones que enmarcan el concepto de lo "público", así mismo en su obra nos dice que las mismas han ido evolucionando históricamente y muchas veces han ido interrelacionándose.

[31] *Cfr.* Rabotnikof, Nora, *El espacio público y la democracia moderna,* México, Colección Temas de Democracia IFE, 1997, pp. 18-19.
[32] *Ibídem*, p. 19.
[33] *Ibídem,* p. 20

A partir de lo expuesto se ha podido visualizar con mayor precisión que lo público no es siempre sinónimo de estatal, pues como vimos lo público se contrapone a lo privado en razón de que atañe a la colectividad y no solamente a un individuo, sea porque es de interés o conocimiento general.

Asimismo, es de destacar que basándonos en esta dicotomía, podemos comprender que hay datos que se pueden y se deben mostrar, y por el contrario otros que no se deben mostrar o simplemente no se quieren mostrar a otros, atendiendo a la acepción de "abierto en contraposición a cerrado" de Nora Rabotnikof. Como lo señalamos anteriormente, el tratamiento de datos se ha convertido en un factor determinante en el comportamiento de las personas; por lo que deben de tener el derecho de reservarse para si los datos que en caso de hacerse públicos o dárseles un tratamiento distinto al autorizado por su titular, podrían generar consecuencias negativa; ya que *"los atributos del corazón necesitan oscuridad y protección frente a la luz pública, para poder crecer y seguir siendo lo que quieren ser, es decir, motivos interiores que no deben ser desplegados en público. No importa cuán profundamente sentido sea un motivo, una vez que se ha expuesto a la inspección pública se transforma en objeto de sospecha, a diferencia de las acciones y las labras que están destinadas a aparecer, los motivos que están detrás de esas acciones y esas palabras son destruidos en su esencia una vez que aparecen".* [34]

Decimos que es un factor determinante en el comportamiento humano, pues una persona que sabe que sus datos pueden ser utilizados de manera que puede llegar a perjudicarlo, como lo señalamos anteriormente para ser candidato a recibir algún servicio o beneficio, esta persona preferirá en primer término no manifestar sus datos de forma verídica, o incluso dejar de realizar ciertas conductas por temor a ser discriminado, por ejemplo visitar determinados lugares o comprar artículos que pueden encasillarlo en un perfil que no desea.

[34] Rabotnikof, Nora, *op. cit., nota 30,* p. 134.

Es un hecho corroborado por la antropología social y la sociología que todas las sociedades humanas, de cualquier época, dividen su vida social en dos zonas o modos de comportarse: una en la cual es legítimo y válido, normal y bueno mostrarse ante los sentidos y la percepción de otros miembros de la sociedad; otra zona, en cambio, que se usa para que las personas oculten comportamientos, ideas, objetos, etc.[35]

Ya lo mencionaba Nora Rabotnikof[36] vivir juntos en el mundo, significa, en esencia, que un mundo de cosas está entre quienes lo tienen en común, el mundo como todo lo que está en medio, que une y separa a los hombres al mismo tiempo es decir al mismo tiempo que nos une también impide que caigamos unos sobre otros.

Continuando con el tema de la dicotomía entre lo público y lo privado, resaltemos que es un tema importante ya que al concederle mayor o menor autonomía a las personas en lo individual o a los grupos sociales, es que puede hablarse de una ponderación de derechos, la cual está presente en el debate de si la protección de datos personales representa una coartada al derecho de información como algunos lo conciben; tema al que haremos referencia en los siguientes párrafos.

Para abordar el tema de un posible conflicto de intereses es necesario referirnos a las características propias del derecho a la información para estar en posibilidad de comprender el por qué este derecho puede entrar en conflicto de intereses con la protección de datos personales.

El derecho a la información enuncia el Investigador Ernesto Villanueva es *"en sentido general, el conjunto de normas jurídicas que regulan las relaciones entre el Estado, los medios y la sociedad, y en sentido estricto cuando se refiere a la*

[35] Elizalde, Luciano H, *op. cit., nota 29.*
[36] Rabotnikof, Nora, *op. cit.*, nota 30, p. 117.

prerrogativa de la persona para examinar datos, registros y todo tipo de informaciones en poder de entidades públicas y empresas privadas…".[37]

Para Juan Armagnague es *"el derecho que tiene toda persona de recibir, y como la obligación de aquel que emite mensajes por cualquier medio de comunicación de proporcionar, informaciones veraces y opiniones de relevancia pública, a fin de permitir la participación ciudadana en la vida colectiva del país mediante un debate pluralista".*[38]

El primer concepto está íntimamente relacionada con uno de los derechos que coadyuvan en garantizar la protección de datos personales, pues alude al derecho que tiene una persona de conocer la información almacenada en bancos de datos públicos y privados; por otro lado el segundo concepto refiere a una doble función del derecho a la información, como derecho de recibir información veraz, y a la vez como obligación de proporcionar la información veraz.

Sigamos con el estudio del derecho a la información, el cual es un derecho compuesto, pues se integra por varias prerrogativas a su vez:

a) Recibir información: incluye las facultades de recibir información objetiva y oportuna , la cual debe ser completa y con carácter universal, es decir que la información es para todas las personas sin exclusión alguna.
b) Investigar: incluye las libertades de expresión y de imprenta, y el de constitución de sociedades y empresas informativas
c) Difundir información: mediante la prensa o por cualquier medio de comunicación.

El derecho a la información es un derecho que incluye tres prerrogativas, la de acceder a la información, acceder a las fuentes de información y convertirse en fuente de información.

[37] Araujo Carranza, Ernesto, *op. cit*., nota 22, p. 30.
[38] Armagnague, Juan (Dir.), *Derecho a la información, habeas data e internet*. Argentina, Ediciones La Rocca, 2002, p. 87.

Respecto de las características propias de la protección de datos personales han quedado asentadas en apartados anteriores; por lo que conjuntando lo ya expuesto sobre ambos derechos señalaremos que los elementos genéricos que podemos apuntar sobre el derecho a la información y la protección de datos personales son[39]:

a) Son derechos fundamentales nuevos:

   El derecho a la información tiene su origen específico en 1948 con la Declaración Universal de los Derechos del Hombre; y el primer antecedente de la protección de datos personales lo encontramos en la Constitución de Weimar en 1919, y a nivel supranacional en la Declaración de los Derechos Humanos en 1948 de la Organización de las Naciones Unidas.

b) Son derechos de tercera generación:

   La doctrina distingue tres generaciones de derechos humanos

   i. En la primera, se configuran las libertades individuales frente a la injerencia de los poderes públicos, exigiendo sus límites y tutelados por la observancia de los derechos individuales
   ii. En la segunda, desde el Estado Social de Derecho frente al Estado Liberal de Derecho, los derechos económicos, sociales y culturales exigen una política activa que garantice su ejercicio.
   iii. En la tercera, se incluye la libertad informática como un nuevo derecho del individuo a tutelar su propia identidad informática, concentrándose en las garantías de acceso control de las informaciones procesadas.

c) Son derechos autónomos y verdaderos: autónomos por implicar características propias en cada una de ellas que las hacen independientes de otras materias, en virtud de que se les puede analizar en forma

[39] Araujo Carranza, Ernesto, *op. cit., nota 23,* pp. 53-55.

separada. Verdaderos porque el derecho a la información es evidente que los datos informativos objeto de este derecho no pueden ser equivocados, falseados o inventados. Los datos de carácter personal irremediablemente tienen que ser auténticos, de tal manera que cuando se encuentre error en ellos concurre el derecho de rectificación.

d) Son derechos objetivos y subjetivos: derecho objetivo por encontrarse positivados o reconocidos en los textos jurídicos que impone derechos y obligaciones mutuas, y como derecho subjetivo, por establecer los procedimientos o acciones legales especificas para el libre acceso a los documentos públicos. En el caso de los datos personales, subjetivos al estar señalados los procedimientos para su debida protección y rectificación.
e) Son derechos que tienden a ampliarse en el mundo: ambos derechos entrevén amplias posibilidades para que en algunos años más logren establecerse, por lo menos en la mayoría de los países del mundo.

Tanto el derecho a la información como la protección de datos personales son derechos nuevos pero que cada vez van adquiriendo mayor trascendencia en la legislación internacional; asimismo son autónomos, a pesar de que la protección de datos en un principio se trataba dentro de la protección a la intimidad y al honor, con el tiempo ha ido adquiriendo reconocimiento como derecho independiente de aquéllos; son verdaderos en cuanto que la información que protegen debe ser cierta; son objetivos por encontrarse protegidos dentro del ordenamiento normativo; subjetivos en cuanto que la normatividad establece un mecanismo que garantice su libre ejercicio.

Una vez quedadas claras las características propias del derecho a la información y las que comparte con la protección de datos, nos preguntamos ¿cómo es que se presenta la colisión entre ambos derechos?; diremos que en primer término sobre el derecho a la información predomina el interés público mientras que en la protección de los datos personales prevalece el interés privado; ahí aparece el primer conflicto interés público vs interés privado.

El problema principal es que en el ejercicio del derecho a la información en muchas ocasiones se extralimita su objetivo y perjudica la esfera protegida de los datos personales, es decir, cuando en busca de la información se deja de lado la integridad de la persona dejando al descubierto información que su titular deseaba mantener fuera del alcance de terceros.

El moderno desarrollo de los medios de comunicación lleva a quienes los manejan cada vez más a interferir en mayor medida en la vida privada para satisfacer la curiosidad del público ávido de noticias sobre intimidades de las personas sobre todo si éstas son famosas o de pública notoriedad.[40]

La colisión que se presenta no es exclusiva de estos dos derechos, pues la misma se presenta a menudo entre derechos fundamentales; dado que no se trata de derechos absolutos, sino que se encuentran limitados en atención a los derechos de los demás, por la seguridad de todos y por las justas exigencias del bien común, en una sociedad democrática, siguiendo la expresión del artículo 32 de la Convención Americana sobre Derechos Humanos.

Asimismo la colisión es inevitable atendiendo a su estructura como principios jurídicos que requieren maximización y armonización, de forma tal que es necesario acudir a un juicio de proporcionalidad o ponderación a fin de determinar en cada caso atendiendo a sus circunstancias relevantes, el alcance de un derecho frente a otros a través de los principios que estén confrontados (máxima publicidad vs privacidad).[41]

Frente a la colisión que se presenta entre ambos derechos, es necesario tomar una decisión de por cuál derecho inclinar la balanza; por una parte existe la corriente que se inclina por el derecho a la información, la que apuesta por la protección de datos personales y aquella que busca el equilibrio entre ambos.

---

[40] *Ibídem*, p. 48.

[41] *Cfr.* Nava Gomar, Salvador O., "Colisión de derechos fundamentales: acceso a la información y protección de datos personales desde la perspectiva de la jurisdicción electoral", *http://www2.scjn.gob.mx/red/IVTransparencia/Docs/Materiales/Presentaci%C3%B3n%20Magdo%20%20Nava%20Gomar.pdf*

La corriente que sostiene que la libertad de información tiene un valor preferente sobre otros derechos fundamentales, fundamenta la razón de esa prevalencia en su carácter de instrumento de formación de opinión pública en asuntos de interés general; pues conocer es estar en posibilidad de formarse un juicio exacto de la realidad de las cosas; y para ello es necesario estar informado, estar enterado de la realidad que nos circunda.[42]

En razón de la opinión pública es una institución esencial de nuestro régimen de convivencia, y por lo tanto todo lo que sirve para formarla y alimentarla ha de ser especialmente protegido.

Por otra parte la corriente que está en pro de prevalecer la protección de los datos personales sostiene que la intimidad individual y familiar, la honra, la propia imagen, la reputación, son valores que la prensa no puede comprometer amparada por la libertad de expresión y opinión,[43] es decir, la individualidad de la persona no puede verse afectada para que otra persona pueda ejercer su derecho a la información.

Asimismo al vulnerar la vida privada o la privacidad, el equilibrio se rompe y se establece una relación de dominio y de control de quien posee la información, y en consecuencia todo dominio personal restringe la libertad e impone desigualdad entre quien posee información y quien no tiene acceso a ella,[44] como habíamos mencionado en la actualidad la información se ha convertido en un factor de poder que puede generar discriminación entre quien tiene acceso a ella y quien por diversas cuestiones no accede a la misma.

[42] Armagnague, Juan, *op. cit.,* nota 38, p. 225.
[43] *Cfr.* Gozaini, Osvaldo Alfredo, *Habeas Data. Protección de datos personales,* Argentina, Rubinzal-Culzoni Editores, p. 122.
[44] *Ibídem,* pág.126

Esta corriente señala que si no hay un verdadero acontecimiento peculiar que represente un interés informativo serio, importante y útil para la sociedad, debe prevalecer el bien individual, esto es la intimidad de las personas.[45]

El fundamento de defender la prevalencia de la protección de datos no está en demeritar el derecho a la información, solamente se inclina porque el ejercicio del derecho a la libertad de buscar, recibir y difundir información sea sometido a la ley, a limitaciones razonables, con el fin de asegurar el respeto a los derechos de los otros ciudadanos; esto porque el derecho a la verdad no siempre debe invocarse para hacer públicas cosas que pertenecen a la zona íntima de la persona o de su familia.[46]

Ambas posturas basan sus argumentos en ideas concretas y ciertas, sin embargo tratándose derechos fundamentales consideramos más viable la postura neutra que busca el equilibrio entre ambos derechos, pues para poder hacer una valoración de cuál derecho debe prevalecer, es preferible tomar en consideración las características particulares de cada caso en que se presente un conflicto de intereses entre dos derechos fundamentales.

Esta postura parte de que la libertad de prensa no es un derecho absoluto, pues todos deben ser ejercidos conforme a las leyes que reglamentan su ejercicio, atendiendo su razón ideológica de ser y el interés que protegen. El ejercicio del derecho de informar no puede ser extendido en detrimento de la necesaria armonía con los restantes derechos constitucionales, entre los cuales se hallan la integridad moral y el honor de las personas.

El abogado constitucionalista Gregorio Badén afirma que de la misma manera que el reconocimiento de la intimidad no puede conducir al exceso de anular otras

---

[45] Armagnague, Juan, *op. cit.,* nota 38*,* p. 229.

[46] *Cfr*. García Plaza, Tatiana, "La aplicación del derecho a la Intimidad en la publicidad registral en la actual legislación ecuatoriana", *Revista Jurídica Online de la Facultad de Jurisprudencia y Ciencias Sociales y Políticas.* Universidad Católica de Santiago de Guayaquil, *http://www.revistajuridicaonline.com/images/stories/revistas-juridicas/derecho-publico-tomo-2/271a296_la_aplicacion.pdf*

libertades constitucionales, tampoco el ejercicio de cualquiera de estas últimas puede desembocar en el cercenamiento liso y llano de la intimidad.[47]

Esta postura como vemos no sobrepone un derecho sobre otro, es decir no establece jerarquizar los derechos, Giancarlo Rolla, destacado profesor de la Universidad de Siena, Italia, sostiene que la información, dignidad y tutela de la vida privada, aun siendo susceptibles de entrar con frecuencia en aparente colisión, representan valores directamente inherentes a la persona humana, en la que reside su matriz común, al constituir todos ellos momentos esenciales de su formación y desarrollo, agrega que encuentran todos ellos, garantía en derechos que la Constitución califica como inviolables, o incluye entre los valores superiores del ordenamiento constitucional, de ahí que no quepa jerarquizarlos en abstracto.[48]

En esta postura la ponderación retoma un valor de suma importancia al momento de optar por uno o por otro derecho; como método apropiado para formular un "enunciado de preferencia condicionada" o trazar una jerarquía axiológica móvil, útil para el caso concreto pero que no impide una respuesta distinta en otro supuesto. Todo claro está, sin perder de vista la utilidad que específicamente en la dimensión de los derechos fundamentales puede reportar como enfoque interpretativo de éstos su armonización o ajuste dentro del sistema general de derechos.[49]

El Catedrático de Filosofía del Derecho de la Universidad de Castilla-La Mancha Toledo, España, Luis Prieto Sanchís ha defendido las bondades del método ponderativo, pues identifica como rasgo característico el que con él no se logra respuesta válida para todo supuesto, sino sólo una preferencia relativa al caso concreto que no excluye una solución diferente en otro supuesto.

---

[47] Armagnague, Juan, *op. cit.,* nota 38, p. 227.
[48] Araujo Carranza, Ernesto, *op. cit.* nota 22, p. 49.
[49] *Cfr.* Bazán, Víctor, "El derecho a la vida privada y el derecho a la libertad de información en la doctrina y jurisprudencia de la Corte Suprema de Justicia Argentina", *Estudios Constitucionales*, vol. 6, núm. 001, *http://redalyc.uaemex.mx/redalyc/html/820/82060106/82060106.html*

Señala que la ponderación *"intenta ser un método para la fundamentación de ese enunciado de preferencia [condicionada] referido al caso concreto; un auxilio para resolver conflictos entre principios del mismo valor o jerarquía, cuya regla constitutiva puede formularse así: cuando mayor sea el grado de no satisfacción o de afectación de un principio, tanto mayor tiene que ser la importancia de la satisfacción de otro".*[50]

Una vez expuestas las tres posturas referentes a cómo manejar la colisión de derechos, advertimos que ni el derecho a la información ni la protección de datos personales están por encima uno del otro, pues acorde al método de la ponderación en caso de conflicto entre ellos, se va atender a las circunstancias del caso concreto para poder determinar cuál de ambos derechos debe prevalecer.

Después de haber tocado brevemente los puntos más importantes para fundamentar la protección de los datos personales desde la perspectiva social, pasemos a un estudio más a detalle de cada uno de los puntos señalados.

2.2.1 Protección al derecho a la intimidad y la privacidad

El derecho a la protección de datos personales tiene como uno de sus objetivos proteger la privacidad de la persona, por lo que este apartado lo dedicaremos al estudio del derecho a la intimidad.

Primeramente hagamos referencia a la definición literal de los conceptos intimidad y privacidad; el Diccionario de la Real Academia de la Lengua Española define la privacidad como el *"ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión",* mientras que la intimidad la define como la *"zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".*[51]

[50] *Ídem.*
[51] Diccionario de la Real Academia de la Lengua Española. *http://buscon.rae.es/draeI/*

El diccionario refiere a la vida privada, pero qué es la vida privada, Ana Isabel Herrán Ortiz profesora de la Universidad de Deusto la define como *"una esfera de retiro y aislamiento, el ámbito donde los demás dejan en paz al sujeto, con tranquilidad para actuar y donde no tienen derecho a inmiscuirse".*[52]

El Catedrático de Derecho Constitucional, Eduardo Espín Templado nos dice que la vida privada que *"podríamos entenderla como el conjunto de circunstancias y datos relativos a la vida de una persona que queda fuera del conocimiento de los demás, salvo que medie un expreso deseo de comunicarlo o de ponerlo de manifiesto por parte de la persona afectada y al margen, naturalmente, de las personas que comparten con ella aspectos más o menos amplios de su vida".*[53]

En palabras de Lucien Martin *"La vida privada es la vida familiar, personal del hombre, su vida interior, espiritual, la que lleva cuando vive detrás de su puerta cerrada".*[54]

Para el autor William F. Swuindier *"el derecho a la vida privada puede ser definido como el derecho de vivir su propia vida en soledad, sin ser sometido a una publicidad que no se ha provocado ni deseado. En resumen, es el derecho a ser dejado solo".*[55]

El profesor de la Universidad de Bucaramanga, Aberlardo Rivera Llano nos dice que *"la vida privada debe constituir una ciudadela donde estén protegidos y asegurados los cuatro estados característicos de la privacidad y la libertad: a) la soledad, cuando la persona vive sola por autodeterminación; b) la intimidad, cuando el individuo está en compañía de otro o de un pequeño grupo, familia, amigos; c) el anonimato, que consiste en el interés de no ser identificado en la*

[52] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 43, p. 77.
[53] Esteva Gallicchio, Eduardo Gregorio, "El derecho a la protección de la vida privada y el derecho a la libertad de información en la doctrina y en la jurisprudencia, en Uruguay", *Estudios Constitucionales*, Año 6, núm. 1, 2008, http://www.cecoch.cl/htm/revista/docs/estudiosconst/revistaano_6_1.htm/elderecho03.pdf
[54] García Plaza, Tatiana. *op. cit.* nota 46.
[55] *Ídem.*

rutina de cada día y d) la reserva, entendida como voluntad de no revelar ciertas cosas sobre sí mismo".[56]

A partir de estas definiciones entendemos por vida privada el ámbito de una persona en lo individual o en lo familiar que se mantiene fuera del conocimiento de terceros, por decisión propia de la persona.

La doctrina hace hincapié en diferenciar ambos conceptos, por lo cual es preciso que recurramos a la doctrina; empecemos con las definiciones de la "privacidad".

El jurista Murillo de la Cueva establece que la privacidad es el *"derecho a poder estar solo, con el alcance que cada uno desee, incluso completamente solo, sin sufrir injerencias no deseadas y sin interferir en el derecho de los demás".*[57]

Por su parte el autor Louis Lusky amplia el concepto de privacidad de forma, que ya no tiene únicamente un sentido estático de defensa de la vida privada del conocimiento ajeno, sino que tiene una función dinámica, *"la posibilidad de controlar la circulación de informaciones relevantes para cada sujeto".*[58] Ciertamente la esencia de la privacidad es el derecho del individuo a ejercer el control de aquella información de sí mismo que desee compartir con otros, de la cantidad que de la misma facilite a otros y del momento en que desee hacerlo.

Lusky a diferencia del primer autor define la privacidad de manera extensiva, pues no solamente se queda con la concepción propuesta por Brandeis y Warren de "*the right to be alone*", ya que refiere más al sentido de autodeterminación informativa, temas que más adelante analizaremos.

---

[56] *Ídem.*

[57] Murillo de la Cueva, Pablo Lucas, *El derecho a la autodeterminación informativa*, España, Fundación Coloquio Jurídico Europeo, 2009, p. 83.

[58] Rebollo Delgado, Lucrecio, *El derecho fundamental a la intimidad*, España, Ed. Dykinson. 2000, p. 83.

Para la Maestra Marcia Muñoz de Alba Medrano dentro del derecho a la privacidad, se comprenden dos aspectos:[59]

1. Derecho de reserva o confidencialidad: que tiene por finalidad la protección de la difusión y revelación de los datos pertenecientes a la vida privada.
2. El respeto a la vida privada: que tiene como objeto la protección contra intromisiones ilegítimas en ese espacio. Frente a este derecho se generan las siguientes obligaciones:[60]

    - Recrear la doctrina del derecho a estar a solas, evitando que la persona humana sea invadida por intromisiones de cualquier naturaleza que afecten su vida privada.
    - Auspiciar una defensa efectiva del individuo contra la publicidad de actos personales que se ponen a disposición del público interesado sin conocimiento ni permiso del afectado.
    - Propiciar un régimen de control sobre el almacenamiento de datos personales y el destino que a ellos se asigne.
    - Formular un criterio economicista respecto a la vida privada, a cuyo fin se la puede analizar como resultado de la difusión y retención de la información en el contexto comercial y personal.
    - Dar un sentido amplio al derecho a tener una vida privada para evitar el egoísmo de considerar únicamente el problema del tratamiento de datos, sin relacionar otras situaciones tan o más importantes que ella, como son las intercepciones telefónicas, la penetración de los correos electrónicos, la invasión domiciliaria de publicidad, etcétera.

A partir de lo expuesto notamos que la privacidad no atañe únicamente el derecho a estar solo, sino al derecho que tiene una persona de mantener fuera de las miradas públicas algunos aspectos que le son propios y que no desea que sean conocidos por terceros.

[59] *Cfr*. Muñoz de Alba Medrano, Marcia y Cano Valle, Alberto, *Derechos de las personas con síndrome de inmunodeficiencia adquirida*, México, Cámara de diputados-UNAM, 2002, p. 38.
[60] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 43, p. 78.

En cuanto al siguiente término que es la "intimidad", Ana Garrida la define como *"la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario-según las pautas de nuestra cultura-para mantener una mínima calidad de la vida humana*", que se extiende, además, *"no solo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con la que se guarde una especial y estrecha vinculación, como es la familia, aspectos que por la relación o vinculo existente con ellas, inciden en la propia esfera de la personalidad del individuo y que se configuran como un ámbito o reducto en el que se veda que otros penetren".* [61]

En tanto que el autor argentino Juan Armagnague define el derecho a la intimidad como "*el que garantiza a su titular el desenvolvimiento de su vida y su conducta dentro de aquel ámbito privado, sin injerencias ni intromisiones que puedan provenir de la autoridad o de terceros, y en tanto dicha conducta no ofenda al orden público, la moral y las buenas costumbres, ni perjudique los derechos de los demás".* [62]

Para Lucrecio Rebollo, el derecho a la intimidad *"es la protección de la autorrealización del individuo. Es el derecho que toda persona tiene a que permanezcan desconocidos determinados ámbitos de su vida, así como a controlar el conocimiento que terceros tienen de él. La intimidad es el elemento de desconexión social. El concepto de derecho a la intimidad como estricto derecho de defensa tiene incardinación directa en la dignidad humana y en el libre desarrollo de la personalidad. La potestad de control de lo que afecta al individuo en su ámbito de intimidad tiene una correlación también directa con la libertad".* [63]

[61] Garrida., Ana, *op. cit.,* nota 16, p. 23.
[62] Armagnague, Juan, *op. cit.,* nota 38, p. 238.
[63] Rebollo Delgado, Lucrecio, *op. cit.,* nota 58, p. 94.

En palabras de la Columnista Tatiana García Plaza, *"La intimidad es la esfera secreta de la vida del individuo en la que tiene el poder legal de evitar a los demás".* [64]

Nizer, en 1939 escribió: *"El derecho a la intimidad es el derecho del individuo a una vida retirada y anónima".*[65]

Los autores antes mencionados relacionan el concepto intimidad con la parte interna de la persona, aspectos de su vida que no deben ser conocidos por terceros, porque evitaría que la persona se desenvolviera de una forma libre, lejos de las miradas de terceros.

La concepción que tenemos de la "intimidad" ha ido evolucionando. En la concepción liberal el derecho a la intimidad era una libertad negativa, un *status libertatis*, de no injerencia del Estado o individuos en la subjetividad, configurada como un haz de derechos y deberes.

En la sociedad postindustrial el derecho a la intimidad no sólo se visualiza solamente como una libertad negativa, sino también como una libertad positiva; puesto que se trata de tutelar la subjetividad de la injerencia ajena (estatal o privada), y de preservar la identidad y libertad frente al intenso e invisible poder informático.[66]

De esta manera el derecho a la intimidad ya no es sólo la potestad que tenemos de que un tercero conozca o no nuestra vida privada, sino también, implica la posibilidad de controlar lo que otros conocen de nosotros mismos. Por lo tanto podemos establecer que el derecho a la intimidad tiene dos aspectos, uno negativo que es "la exclusión del conocimiento ajeno de cuanto hace referencia a

[64] García Plaza, Tatiana, *op. cit.* nota 46.
[65] *Ídem.*
[66] *Cfr.* Puccinelli, Oscar. R., *Protección de datos de carácter personal*, Argentina, Editorial Astrea, 2004, pp. 14, 15.

la propia persona", y otro positivo de "control por su titular de los datos e información relativos a la propia persona".[67]

Esta última apreciación que se hace la intimidad guarda estrecha relación con la acepción de privacidad, que antes mencionamos, propuesta por Lusky.

Para continuar el estudio del concepto de intimidad, es necesario recurrir a las teorías que han abordado el tema desde distintas perspectivas, entre las que destacan las siguientes:

a) Teoría de las esferas

   Se refiere al derecho de la intimidad representado en círculos concéntricos donde el anillo central es la esfera de la máxima reserva y las demás, dirigidos hacia el exterior, van hilando sucesivamente las esferas del secreto, de la confidencialidad, de la confianza, hasta llegar a las cercanías de lo público que constituye las relaciones del hombre con los demás, persiguiendo crear una imagen de sí mismo.

b) Teoría del mosaico

   Formulada por Madrid Conesa, recibe este nombre por la comparación que hace entre las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado. Es una configuración doctrinal[68] muy reciente y que surge como explicación a la necesidad de protección de la intimidad del individuo frente a las amenazas que de forma genérica los nuevos ingenios tecnológicos y en concreto la informática suponen; pues la sola navegación en internet implica la posibilidad de que sea violada nuestra intimidad, porque vamos dejando rastros de nuestro perfil, costumbres, etc., que pueden ser

[67] Garrida, Ana, *op. cit*., nota 16, p. 22.
[68] Rebollo Delgado, Lucrecio, *op. cit.,* nota 58, p. 92.

observados, seguidos y utilizados, mediante las herramientas llamadas cookies.

Estas teorías nos dan dos aspectos muy importantes para comprender el concepto de intimidad, a partir de la primera vemos como la información referente a una persona puede ser conocida por un determinado grupo dependiendo de la esfera en la que se encuentre, es decir que tan íntima sea; por lo que respecta a la teoría del mosaico, nos aclare un elemento esencial de los datos personales, que si bien en lo particular pueden no ser representativos de una persona, cuando estos son entrelazados permiten vislumbrar un perfil completo de su titular.

Una vez que hemos comprendido el concepto de "intimidad", es necesario mencionar los aspectos que lo integran; el Profesor Jean Carbonnier señala los siguientes:

a) La tranquilidad: es el derecho que tiene todo ser humano a disponer de momentos de soledad, recogimiento y quietud que le permiten replegarse sobre sí mismo.
b) La autonomía: es la libertad de tomar decisiones relacionadas con las áreas fundamentales de nuestras vidas; es entonces, la libertad que tiene cada individuo para elegir entre las múltiples opciones que se le plantean en todas las instancias de su existencia. Es elegir por sí mismo, sin intromisiones indeseadas que dirijan la elección en forma directa o indirecta.
c) El control de la Información: es el medio más adecuado para proteger la reserva de la vida privada de las personas, en cualquiera de sus formas de manifestación. Esta se manifiesta en dos direcciones: por un lado, la posibilidad de mantener ocultos o reservados ciertos aspectos de la vida de las personas, y por otro, la posibilidad que corresponde a cada individuo controlar el manejo y circulación que sobre su persona ha sido confiada a un tercero.

La intimidad como vemos no se limita únicamente a ser dejado a solas, Carbonnier ya introduce el tema del control de la información es decir asocia el tema de la intimidad con la protección de los datos personales; pero ¿por qué es necesario controlar la información propia en posesión de terceros a efecto de proteger la intimidad?, diremos que porque con el uso inadecuado de nuestros datos se puede caer en alguno de los cuatro supuestos que la doctrina establece como maneras de vulnerar el derecho a la intimidad, a saber éstos son:

a) La intromisión en la soledad física que cada persona reserva para sí misma,
b) La divulgación pública de hechos privados,
c) La presentación al público de circunstancias personales bajo falsa apariencia; y,
d) La apropiación, no autorizada, de lo que pertenece a nuestro círculo personal, como la imagen o la fotografía.[69]

Una vez estudiados los conceptos de intimidad y de privacidad de manera diferenciada, veamos que las particularidades de cada uno de los conceptos son meramente doctrinarias pues la legislación no hace distinción alguna, al manejar ambos términos de manera indistinta.

Por ejemplo en el caso de Argentina, su Corte Suprema no hace diferencia entre ambos conceptos, pues como fundamento de ambos toma lo prescrito por el artículo 19 de la Constitución Nacional, es decir la protección jurídica de un ámbito de autonomía individual constituido por sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física, y en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad, están reservados al propio

[69] García Plaza, Tatiana, *op. cit.,* nota 46.

individuo, y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial a la intimidad.[70]

Por lo que respecta a España, no existe una distinción legislativa ni jurisprudencial entre los conceptos de privacidad e intimidad. Ambos se identifican y acogen el significado de una esfera en la que sólo cada persona tiene potestad para decidir lo que le afecta, evitar las intromisiones no deseadas, y en definitiva, tener control al respecto de lo que no se quiere que otros conozcan, o de lo que se quiere dar a conocer. Ambos conceptos se identifican con soberanía interna, son el todo y la parte.[71]

Finalmente la Suprema Corte de Justicia de la Nación de México tampoco distingue entre intimidad y privacidad, pues en la tesis con número de registro 169700 dictada por la Segunda Sala, alude a que la protección de estos derechos se encuentra consagrada en el artículo 16 constitucional.

Una vez hecha la alusión a lo prescrito por la legislación en el presente trabajo manejaremos de manera indistinta el término de intimidad y privacidad, entendiendo por ambos el derecho de una persona de conservar para sí aspectos que le conciernen fuera de las miradas públicas.

Una vez que hemos visto las características del derecho a la intimidad, podríamos pensar que se trata de un símil del derecho a la protección de datos, si bien encontramos ciertas similitudes, es preciso aclarar que no se trata del mismo derecho, para lo cual presentamos el siguiente cuadro comparativo:

Derecho a la intimidad	**Derecho a la protección de datos**
Objeto: vida privada personal y familiar	**Objeto:** cualquier tipo de dato personal, sea o no intimo, cuyo conocimiento o

[70] Armagnague, Juan, *op. cit.,* nota 38, p.238.
[71] Rebollo Delgado, Lucrecio, *op. cit.,* nota 58, p. 224.

	empleo por terceros pueda afectar a sus derechos.
Bien Jurídico tutelado: intimidad	**Bien Jurídico tutelado:** bienes de la personalidad que pertenecen al ámbito de la vida privada, como el derecho al honor y al pleno ejercicio de los derechos de la persona. Es decir, amplia la garantía aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado.
Finalidad: Proteger a la persona de cualquier intromisión en el ámbito de la vida personal y familiar que se desea excluir del conocimiento de terceros.	**Función:** Garantizar un poder de control sobre nuestros datos personales, sobre su uso y destino, a fin de impedir su tráfico ilícito y lesivo para nuestra dignidad y derechos.

Como vemos reflejado en el cuadro anterior, tanto el objeto, el bien jurídico tutelado y la finalidad del derecho a la intimidad como del derecho a la protección de los datos personales son distintos; especialmente consideramos que la diferencia principal radica en que el derecho a la intimidad protege cierta parte de nuestra vida del conocimiento de terceros, mientras que el derecho a la protección de los datos personales busca que el titular de los datos tenga el control de la

información relativa a sí mismo, es decir sepa quién la posee, con qué finalidad, los medios a través de los cuales se obtuvo, y en caso de alguna irregularidad estar en posibilidad de corregirla o suprimirla.

El tema de intimidad/privacidad no podría quedar estudiado si no hiciéramos alusión a un case leading rector en el tema; es decir el famoso artículo de Samuel Warren y Louis Brandeis titulado “The right to privacy”, el cual será materia de estudio del siguiente apartado.

2.2.1.1 The right to privacy de Samuel Warren y Louis Brandeis

El artículo titulado “The right to privacy” fue publicado por Samuel Warren y Louis Brandeis en Harvard Law Review, vol. IV, núm. 5, el 15 diciembre de 1890.

Warren y Brandeis basaron su artículo en la obra del Juez Thomas McIntyre Cooley, llamada “The elements of torts” de 1873, en la cual definió la privacidad como el “derecho a ser dejado a solas” (The right to be alone) el cual comprende dos ámbitos, la soledad y la tranquilidad; pero no solamente en el campo de la religión, la moral o la filosofía sino por el Estado, para asegurar la determinación autónoma de su conciencia cuando toma las decisiones requeridas para la formación de su plan de vida.

Pero ¿cuál fue el motivo que llevo a Warren y Brandeis a escribir dicho artículo?, no era simplemente realizar una aportación doctrinal, sino que su verdadera pretensión estribaba en poner de manifiesto la necesidad del reconocimiento de un nuevo derecho, el derecho a la “privacy”;[72] atendiendo a la necesidad de la época, pues con la mecanización de la imprenta y la consecuente capacidad de difundir rápidamente la información a gran cantidad de público, había que describir la necesidad de la protección del ámbito de lo privado y exigir la capacidad de

[72] *Ibídem,* p. 94.

reaccionar ante el daño emocional que la invasión de este ámbito vedado suponía. Sobre todo porque los derechos que tradicionalmente, servían como límite a la libertad de imprenta, el derecho al honor, en cuanto capacidad de reacción frente al menoscabo de la reputación, y el derecho a la propiedad intelectual, en cuanto derecho de las personas a que sus creaciones literarias y científicas no fueran difundidas sin su consentimiento, no eran suficientes para garantizar la protección frente a la invasión del ámbito de lo privado.[73]

Antes de analizar los argumentos vertidos en el artículo, haremos alusión a la situación particular que llevo a Warren a pedir el apoyo de Brandeis.

La señora Warren hija del senador Bayard, casada con un joven y adinerado empresario del papel, acostumbraba a ofrecer en su residencia de Boston frecuentes fiestas sociales y los periódicos locales cubrían cada detalle de estas reuniones; sin embargo en la ocasión de la boda de una de sus hijas, el periódico Saturday Evening Gazzette, especializado en asuntos de alta sociedad, realizó la crónica del evento de una manera sumamente detallista, con la intención de crear en el lector la idea de una fiesta muy costosa, en la que no solamente se derrocharon grandes cantidades de dinero, sino además se caracterizó por una relajación de la moral entre sus asistentes.

Ante esta situación Warren se molestó seriamente por lo que acudió con un antiguo compañero de clases, Louis D. Brandeis, quien ejercía como abogado; es a raíz de dicha situación que deciden escribir el famoso artículo, para manifestarse en pro del reconocimiento de un nuevo derecho, es decir el derecho a la privacidad.

Una vez puesta la situación en contexto pasemos a revisar el artículo, en el cual Warren y Brandeis[74] señalan que los cambios políticos, sociales y económicos

[73] Sánchez Urrutia, Ana Victoria, *op. cit.* nota 21.
[74] *Cfr.* Warren and Brandeis. "The Right of Privacy". *Harvard Law Review*, Vol. IV, 15 diciembre 1890, Núm. 5, http://www.dataprotection.it/the_right_to_privacy.htm

entrañan la necesidad del reconocimiento de nuevos derechos, como es la privacidad.

Hasta antes de la publicación de este artículo la privacidad solo se conceptualizaba dentro del derecho a la propiedad , lo cual de acuerdo a Warren y Brandeis no es admisible, pues la privacidad no se ve afectada únicamente por una inferencia física, sino también si sus sentimientos, pensamientos y sensaciones no permanecen fuera del alcance de las miradas públicas; por ejemplo un manuscrito, que a pesar de ser transferible, tener un valor, no puede encuadrarse dentro de los bienes tutelados por el derecho de propiedad; pues el valor que tiene no está en las ganancias que se obtengan de su publicación, sino en la paz de la mente, y el alivio de saber que no será publicada, es decir la existencia del derecho no depende de la naturaleza o el valor del pensamiento o la emoción, ni de la excelencia de los medios de expresión,[75] pues la protección otorgada a los pensamiento, sentimientos y emociones manifestados por escrito o en forma artística, en tanto en cuanto consista en impedir la publicación, no es más que un ejemplo de la aplicación del derecho más general del individuo a no ser molestado.[76]

Y es a partir de este ejemplo que demuestran que no todos los bienes pueden protegerse con el derecho de propiedad, sino que es necesario avanzar en la protección de la persona a través de reconocer la privacidad.

Este ejemplo muestra como el principio que protege los textos personales y todas las otras producciones personales, no contra el robo o la apropiación física, sino contra cualquier forma de publicación, es, en realidad, no el principio de la propiedad sea esta material (como en la inviolabilidad de domicilio) o inmaterial (como en la protección de derechos de autor), sino de la inviolabilidad personal, es decir, la privacidad.[77]

[75] Vianna, Túlio, *op. cit.,* nota 28.
[76] Warren, Samuel y Brandeis, Louis, *op. cit.,* nota 4, p. 44.
[77] Vianna, Túlio, *op. cit.,* nota 28.

No obstante los motivos expuestos por Warren y Brandeis para defender el reconocimiento del derecho a la privacidad, también reconocen ciertas limitaciones a éste y establecen algunas reglas generales para limitarlo, entre las que encontramos:

1) El derecho a la privacidad no prohíbe la publicación de lo que es público o se caracteriza por ser de interés general. Los temas que no deben publicarse son los que conciernen a la vida privada, hábitos, conductas y relaciones de un individuo, y no tengan relación con ningún cargo público.
2) No está prohibida la publicación de todo lo que, en principio, es privado, pues no habría lesión de la intimidad cuando la revelación se hace ante un Tribunal de Justicia, una asamblea legislativa o municipal, ni en general cuando tiene lugar en el cumplimiento de un deber público o privado, o en la dirección de los asuntos propios cuando nuestros mismos intereses se ven concernidos.
3) Probablemente, la ley no amparará la exigencia de reparación cuando la intromisión originada por una revelación verbal no haya causado especiales daños.
4) El consentimiento del afectado excluye la violación del derecho.
5) La excepción de verdad no es admisible como defensa del agresor.
6) La ausencia de dolo en el editor tampoco puede ser aducida como defensa.

A partir de estas reglas queda establecido que no toda la información privada es motivo de protección si esta es de interés general o necesaria para el cumplimiento de una obligación, así como si fue consentida su publicación por el titular, sin embargo cuando no estamos en presencia de ninguno de dichos supuestos, la verdad en la información o la ausencia de dolo no excluye la responsabilidad de quien la difunde.

El mérito del estudio hecho por Warren y Brandeis fue que impulsó la tutela legal de bienes inmateriales, como el pensamiento, las creencias y las sensaciones,

cuando hasta entonces la protección del common law sólo alcanzaba a los bienes materiales.[78]

2.2.2 Derecho a la autodeterminación informativa

Durante el desarrollo de este capítulo hemos hecho alusión al control que una persona debe tener sobre información que le es propia y que en ocasiones está en posesión de terceros; nos referimos precisamente al derecho a la autodeterminación informativa.

Este derecho tiene su antecedente en la ley alemana del Censo de Población, Profesión y Lugares de trabajo de 25 de marzo 1982; a través de la cual el Estado buscaba la obtención de información sobre los ciudadanos mediante un censo de población, se pretendía requerirles sus nombres, apellidos, dirección, teléfono, sexo, fecha de nacimiento, ideología política, religión, nacionalidad, el tipo relación con otras personas, domicilio, clase de trabajo, ingresos, profesión, duración del período de estudios, dirección del trabajo, los medios de transporte utilizados para ir al trabajo, tiempo promedio utilizado para ese recorrido, duración de la jornada laboral, clase, extensión y usos de la vivienda, número y uso de las habitaciones, cuantía de la renta mensual; y en caso de negarse a proporcionarla se aplicaban severas sanciones.[79]

Si bien dicha ley no tenía aparentes intenciones de violentar la intimidad de las personas, la misma fue recurrida por un ciudadano quien interpuso un amparo por considerar que violaba el derecho al libre desenvolvimiento de la personalidad, la dignidad humana, la libertad de expresión y las garantías procesales, derechos consagrados en la Ley Fundamental de Bonn.[80]

---

[78] Gils Carbó, Alejandra M, *op. cit.,* nota 1, p. 29.
[79] *Ibídem,* p. 13.
[80] *Cfr.* Davara F. de Marcos, Isabel. "Breve análisis de la reforma al artículo 6° constitucional en lo relativo a protección de datos personales", en Carbonell, Miguel y Bustillos, Jorge (coord.), *Hacia una democracia de*

La sentencia que recayó sobre dicho planteamiento, es relevante en el sentido que reconoció los efectos producidos por los avances tecnólogos en el ámbito de la intimidad; señaló que gracias a la tecnología es posible producir *"una imagen total y pormenorizada de la persona respectiva -un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en "hombre de cristal".*[81] Lo relevante de reconocer estos efectos es que el Tribunal Constitucional Alemán trata de garantizar la capacidad del individuo para determinar la transmisión y empleo de sus datos personales; sobre todo porque el libre desarrollo de la personalidad presupone la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos.

Así mismo en esta sentencia el Tribunal configuró a partir del derecho general de la personalidad *"la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuando y dentro de que limites procede revelar situaciones referentes a la propia vida".* El tribunal extrae del derecho al libre desarrollo de la personalidad la facultad de cada individuo de disponer sobre la revelación y el uso de sus datos, entendiendo el derecho a la autodeterminación informativa como la facultad general de disponer de los datos propios.[82]

Es por esta determinación del Tribunal, que la doctrina reconoce en aquella sentencia el origen del derecho a la autodeterminación informativa; el cual en palabras del Doctor Murillo de la Cueva es el *"bien jurídico tutelado consistente en asegurar a las personas el control de la información-de los datos- que les es propia para ponerles en resguardo, o al menos, permitirles protegerse de los perjuicios derivados del uso por terceros, público privados, de ese material. Las ilimitadas posibilidades que ofrece la tecnología de captar, acopiar, asociar, recuperar en tiempo real y conservar indefinidamente datos personales, así como*

---

contenidos: la reforma constitucional de transparencia, México, Instituto de Investigaciones Jurídicas, UNAM**, 2**007, p. 75.

[81] Fernández Delpech, Horacio et al, "Privacidad y Autorregulación en la era digital", *Universidad del Salvador,* http://www.hfernandezdelpech.com.ar/PDF-PubliTrabPrivaAutoEraDigital.pdf.

[82] Garrida, Ana, *op. cit.,* nota 16, p. 32.

de obtener ulterior información personal mediante su tratamiento, junto a la necesidad creciente de los mimos en todo tipo de relaciones, han hecho imprescindible garantizar a los individuos instrumentos jurídicos que hagan posible ese control.[83]

Este derecho consiste esencialmente en controlar la información que nos es propio, sea que no queremos que esté expuesta a miradas de terceros, o sea porque queremos asegurarnos quién posee nuestros datos, de qué manera se obtuvieron y con qué finalidad; por lo que generalmente se ejerce a través de los derechos de acceso, rectificación, cancelación y oposición, mismos que serán estudiados a profundidad en el siguiente capítulo.

Es importante resaltar que la protección del derecho a la autodeterminación se extiende a cualquier tipo de dato personal, sea intimo o no, cuyo conocimiento o empleo por terceros pueda afectar los derechos del titular, así como a los datos públicos que, aun siendo accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.

Entre las características que le son propias a este derecho destacan las siguientes:[84]

a) Es un derecho individual, previsto para atacar las intromisiones en la intimidad concretadas con un fin específico.
b) Es un derecho de acceso irrestricto, a excepción de fuentes de información que puedan mantener su secreto por razones de seguridad justificadas.
c) Es un derecho de requerir la verdad del registro (principio de exactitud y actualidad del dato archivado), o de promover su rectificación o supresión.
d) Un derecho de exigencia por el cual se pretende que el titular de la base de datos utilice la información compilada con la finalidad concreta para la que fue autorizado el archivo.

[83] Murillo de la Cueva, Pablo Lucas, *op cit.,* nota 57, p. 18.
[84] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 43, pp. 107 y 108.

Estas características provocan que el derecho a la autodeterminación le permita a una persona poder identificar si información que le es propia está siendo objeto de algún tratamiento y con qué finalidad y en caso de oponerse al mismo, estar en posibilidad de exigir la culminación del tratamiento, o en el caso de no oponerse pero detectar que existe alguna incongruencia o imprecisión en la información que se está manejando, poder corregirla o actualizarla.

2.2.3 El impacto tecnológico

Durante el desarrollo de este capítulo hemos hecho hincapié en los efectos que los avances tecnológicos han tenido sobre nuestro modo de vivir, por lo que en este apartado haremos una breve exposición de las principales formas en que estos avances han impactado en la seguridad de nuestra información.

Si bien es cierto, la tecnología brinda múltiples beneficios a la sociedad, no podemos negar que debido a la inmensa cantidad de información personal que está en circulación, el desvanecimiento de las fronteras estatales que provoca una difícil aplicación de normas jurídicas; así como los mecanismos que permiten rastrear la navegación de los usuarios, es que puede verse vulnerada la protección de datos personales.

Como dice el autor Red Whitaker[85] las nuevas tecnologías de la información son un arma de doble filo, porque por un lado aumentan nuestras capacidades y nuestro poder, y por el otro hacen a sus usuarios más vulnerables a la vigilancia y a la manipulación; así pues navegar por la red nos permite comunicarnos con personas de todo el mundo, pero también puede significar que todas nuestras comunicaciones puedan ser interceptadas por terceros que al mismo tiempo, nos localicen e identifiquen. Esto quiere decir que otras personas o grupos están construyendo un perfil en red de nosotros mismos, a través de los sitios web que visitamos, los anuncios que nos interesan, los productos que compramos, los

[85] *Ibídem,* pp. 9 y 10.

periódicos a los que nos suscribimos o los destinatarios de nuestra mensajería electrónica; así mismo significa que personas totalmente desconocidas accedan al disco duro de nuestro ordenador personal, observen lo que guardamos en él y quizás, decidan cambiar o borrar ciertos archivos, o transmitirle un virus a nuestro equipo de cómputo; y aunado a estas circunstancias encontramos que todas ellas pueden llevarse a cabo desde el anonimato.

Un medio por el cual estas conductas pueden realizarse es mediante el fenómeno conocido como "*spam*", el cual ha sido definido por la Agencia Española de Protección de Datos como *"cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa"*.[86] Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico; para lo cual se necesita conocer la dirección de correo electrónico del receptor del mensaje, lo que se logra a través la venta, alquiler o intercambio de direcciones de correo por parte de los proveedores de acceso, captura de direcciones en directorios de correo electrónico, o mediante el *hoax,* el cual es "un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, cuya finalidad es captar direcciones de correo";[87] algunos hoax informan sobre virus, otros invocan a la solidaridad, o contienen fórmulas para ganar millones o crean cadenas de la suerte.

No obstante que el spam puede llegar a molestar o incomodar a los usuarios, lo realmente grave de esta práctica es que con la obtención de las direcciones de correo electrónico, están obteniendo además información personal asociada a estas, como lo es la organización donde trabaja o a la que pertenece una persona, lo que puede ser de gran interés para una empresa que se dedique a la publicidad directa. Un ejemplo respecto al spam, es el caso de la firma America On Line (AOL) sobre la firma CN Productions, En 1998 la firma fue demandada por haber

[86] "Guía para la lucha contra el Spam", *Agencia Española de Protección de Datos,* http://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM--ap-V.-30-mayo-cp-.pdf.
[87] *Ídem.*

remitido casi mil millones de mails de publicidad de cibersitios para adultos, por lo que fue sancionada por la Corte del Distrito Oriental de Virginia, por el envío masivo de mensajes no solicitados, a sus suscriptores, condenado al pago de U$7, 000,000.

Otra manera en la que pude verse vulnerada la protección de datos personales es la técnica conocida como "*Phising",*[88] mediante la cual se duplican páginas web para hacer creer al visitante que se encuentra en determinada página cuando en realidad se encuentra navegando en alguna otra con fines ilícitos; esto se logra mediando el envío indiscriminado de correos solicitando que se acceda a una página con el fin de actualizar los datos de acceso al sitio, como son contraseñas, fechas de caducidad, etc.

Así mismo, también nos enfrentamos a los programas espía, mejor conocidos como Spyware, las cookies, o programas rastreadores o sniffers, los cuales permiten seguir al usuario a medida que navega por determinados sitios web, vigilando sus acciones, acumulando información personal, desde saber cuál es el lugar desde el que accede el usuario, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo que utiliza, los sitios más visitados en una página web, el número de clics realizados, e infinidad de datos relacionados con el desarrollo de la vida del usuario dentro de la red, con lo cual se han convertido en una herramienta que vulnera el derecho a la intimidad y la privacidad de los usuarios.

Los ejemplos que hemos mencionado son sólo una pequeña muestra de las múltiples situaciones que se presentan a diario, en torno a los datos personales; pero hemos de preguntarnos qué es lo que conduce a realizarlas, a lo podemos responder de la siguiente manera.

- Para obtener ganancias económicas.

[88] *Ídem.*

- Por el Síndrome de “Robín Hood”; el cual es una visión construida alrededor de la figura del “hacker” a comienzos de la década de los ochenta. Mostrándolo como el que ataca o roba a la organización rica titular del sistema (aunque después no reparta el botín entre los pobres).
- Por una cuestión de ocio y diversión.
- Como venganza, ya sea de un trabajador despedido, de un novio traicionado, en fin de cuestiones de rencor hacia los demás.

Si bien existen muchas razones por las cuales se cometen acciones que vulneran la seguridad de nuestra información, lo importante es saber contraatacarlas, sea con normatividad jurídica o bien complementándola con soluciones técnicas.

La medida técnica que en la actualidad es la que mejores resultados está dado es la técnica del cifrado, en razón de que aporta mayor confidencialidad, al evitar la intercepción de terceros que no comprenderán el mensaje a pesar de que puedan tener acceso al mismo; autenticidad y fiabilidad para el contenido del mensaje.

Esta técnica consiste en un proceso de protección de datos mediante un cifrado de los mismos que evita una manipulación no deseada; de un texto claro (plaintext) se pasa a un criptograma (ciphertext)[89]; esto es, la información que se envía mediante el cifrado es descompuesta en miles de pequeñas partes que provoca que aunque un tercero tenga acceso a dicho envío, no podrá comprender la información que el mismo porta, en razón de que solamente tendrá en su poder esas pequeñas partes en desorden y sin ninguna relación entre ellas.

La técnica del Cifrado puede ser de dos tipos:

a) Privada o de clave simétrica: se utiliza una misma clave tanto para encriptar como para desencriptar un documento, siendo necesario para que el sistema funcione que tal clave se mantenga en secreto.

[89] Fernández Rodríguez, José Julio*, Lo público y lo privado en internet. Intimidad y libertad de expresión en la Red*, México, Instituto de Investigaciones Jurídicas, UNAM, 2004, p. 111.

b) Pública o de clave asimétrica: se utiliza una clave para encriptar el texto y otra diferente de la primera para desencriptar el texto cifrado y recuperar así el original. En este sistema una de las claves es pública (de allí el nombre), mientras que la otra se mantiene en secreto. Es en la actualidad el que brinda mayor seguridad ya que elimina la necesidad de que remitente y receptor compartan la misma clave.

Estos dos tipos difieren esencialmente en el número de claves que se utilizan para enviar y para recibir un mensaje, en el de clave simétrica es la misma clave que se utiliza para enviar que para recibir el mensaje, mientras que en el de clave asimétrica se utiliza una clave diferente para cada acción.

Sin duda podríamos seguir citando ejemplos de técnicas y acciones que ponen en peligro la salvaguarda de los datos personales, sin embargo consideramos que con los que hemos señalado, ha quedada ilustrada la manera en que los avances tecnológicos repercuten en el derecho a la protección de los datos personales.

Conforme hemos avanzado en el desarrollo del presente capítulo hemos hecho alusión a aquellos supuestos que justifican la procedencia de la protección de los datos personales, que como vimos son variados y de distinta naturaleza, pero que como característica principal buscan la obtención de la mayor cantidad de datos posible para estar en posibilidad de formular un perfil completo de una persona que sea de utilidad para distintos sectores en el mercado.

Ante esta situación es urgente tomar ciertas medidas que hagan frente a la posible vulneración del derecho a la protección de datos personales, como lo es el ejercicio de los derechos ARCO, tema que es materia del siguiente capítulo.

CAPITULO III Derechos ARCO

3.1 ¿Qué son los derechos ARCO?

En el capítulo anterior estudiamos los múltiples supuestos que pueden presentarse en el haber diario, y que en muchas ocasiones llegan a vulnerar la protección de los datos personales, y mencionamos que es necesario hacer frente a los mismos; por lo cual este capítulo lo dedicaremos al estudio de los cuatro derechos básicos que garantizan la protección de los datos personales, es decir los denominados derechos "ARCO".

El primer paso para comprender el alcance de estos derechos, es hacer referencia a su significado como acrónimo y posteriormente de manera particular; en conjunto se definen como *"el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales".*[1]

Esta definición es limitada en cuanto a su alcance, pues solamente refiere a las personas físicas como titulares de datos personales, y como quedó establecido en el primer capítulo la titularidad de los datos personales engloba tanto a personas físicas como jurídicas, dependiendo de la legislación a la que aludamos, tal es el caso de la legislación argentina.

Otra definición en el mismo sentido, pero sin limitar el control de los datos a las personas jurídicas, a pesar de que el derecho español no reconoce dicha titularidad, es la contenida en la sentencia 292/2000 pronunciada por el Tribunal Constitucional Español, que los define como aquellos derechos que "*constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos... y garantizan a la persona un poder de control sobre sus datos personales…"* [2]

[1] *Cfr.* Pérez Serna, Jesús Mayo, "Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)", *Ayuda ley protección de datos*, 12 mayo de 2010, *http://www.ayudaleyprotecciondatos.es/2010/05/12/los-derechos-arco-acceso-rectificacion-cancelacion-y-oposicion/*

[2] *http://www.cuidatusdatos.com/infoderechosarco.html*

Ambas definiciones dejan claro que la finalidad fundamental de los Derechos ARCO es garantizar un control sobre los datos personales, sin embargo, no especifican de qué manera se ejerce dicho control, por lo que es necesario recurrir a las definiciones que nos proporcionan los órganos de control.

Por ejemplo en la guía para el Ciudadano emitida por la Agencia Española de Protección de Datos Personales (AEPD), se establece que a través de los derechos ARCO, podemos saber qué información personal está siendo objeto de tratamiento, de quién o de dónde se obtuvieron los datos y a quién se les ha cedido; asimismo, modificar o rectificar errores, cancelar datos que no se deberían estar tratando u oponernos a tratamientos de datos personales realizados sin nuestro consentimiento.[3]

Por lo que respecta al Instituto Federal de Acceso a la Información y Protección de Datos de México (IFAI),[4] emitió una Guía Práctica para Ejercer el Derecho a la Protección de Datos Personales, en la cual afirma que los derechos ARCO garantizan al titular el poder de decisión y control que tiene sobre la información que le concierne y en consecuencia, su derecho a la protección de sus datos personales; asimismo estos derechos actúan como complemento del deber del responsable de cumplir con las obligaciones que le son impuestas en la Ley, permitiéndole identificar aquellos casos en los que el tratamiento pudiera no resultar adecuado.

Encontramos mayor explicativa la propuesta española, en el sentido de que especifican en qué consiste el control sobre los datos, al señalar que a través de los derechos ARCO podemos estar ciertos que determinada información que nos es propia está siendo objeto de algún tratamiento, así como saber las condiciones

[3] *Cfr.* "El derecho fundamental a la protección de datos: Guía para el Ciudadano". *Agencia Española de Protección de Datos,*
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf#

[4] *Cfr.* "Guía Práctica para ejercer el Derecho a la Protección de Datos Personales", *Instituto Federal de Acceso a la Información y Protección de Datos,*
http://www.ifai.org.mx/

en que se está llevando a cabo dicho tratamiento y en caso de no estar de acuerdo con la manera en que se está tratando nuestra información poder corregirla o cancelar su tratamiento; en cambio la propuesta del IFAI al igual que las definiciones anteriormente vistas, solamente alude al control sobre los datos pero no señala de qué manera se ejecuta el mismo; no obstante, esta propuesta aporta un elemento importante al señalar que los derechos ARCO implican una duplicidad de funciones porque por un lado representan prerrogativas para el ciudadano, y por el otro son un mecanismo para controlar que los responsables del tratamiento cumplan sus obligaciones que la ley les impone.

Recapitulando las definiciones antes mencionadas podemos puntualizar que los derechos ARCO representan un poder de control que el titular ejerce sobre sus datos, en razón de que en todo momento puede acceder a información que le es propia, así como saber el origen, fin y medio por el cual se obtuvo; a efecto de estar en posibilidad de corregir la información que pudiera resultar incorrecta o desactualizada, cancelarla en caso de que se haya cumplido la finalidad o la temporalidad para la cual se autorizo su tratamiento, o en dado caso oponerse a su tratamiento.

Habiendo ya definido los derechos ARCO como acrónimo, observamos con toda claridad que cada una de las siglas que conforma la palabra, representa los controles que el titular de los datos posee respecto a su información, es decir:

- Acceso
- Rectificación
- Cancelación
- Oposición

Para continuar con el estudio de los derechos ARCO, es momento de pasar al siguiente apartado, destinado a las características de los mismos.

3.1.1 Características de los derechos ARCO

Respecto a las características del acrónimo de derechos ARCO, encontramos que hay algunas que podríamos denominar generales para cada uno de los derechos, las que a continuación se enlistan:

a) Se trata de derechos personalísimos, es decir, que sólo pueden ser ejercidos por el titular de los datos, salvo los casos en que la ley admite una persona distinta a éste, como puede ser el representante legal.
b) Se ejercen directamente ante el responsable del tratamiento de los datos.
c) Son derechos independientes, pues el ejercicio de cualquiera de ellos no excluye la posibilidad de ejercer alguno de los otros, ni puede constituir requisito previo para el ejercicio de cualquiera de los otros.
d) El ejercicio de estos derechos debe ser sencillo, gratuito, no puede suponer ingreso adicional alguno para el responsable.
e) Son derechos limitados, pues la legislación de cada país establece supuestos generales y particulares sobre la improcedencia del ejercicio de los derechos.

Los derechos ARCO se caracterizan principalmente por ser derechos que únicamente pueden ser ejercidos por quien tenga interés jurídico, es decir, el titular de los datos; se ejercen directamente ante el responsable del tratamiento, no son excluyentes entre sí; su ejercicio no representa ni una ganancia para el responsable ni una afectación en el patrimonio del titular y no se trata de derechos absolutos.

A pesar de que los derechos ARCO como vimos buscan garantizar al titular el control de sus datos personales, éstos no son absolutos, pues la legislación establece algunos supuestos en los que se restringe su ejercicio, a continuación mencionamos los supuestos que establecen cada una de las legislaciones materia del presente trabajo.

En cuanto a Argentina, encontramos los siguientes supuestos que restringen el ejercicio de los derechos ARCO:

i. En función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.
ii. Cuando 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 la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas.

Por lo que respecta a la legislación de España, en ella se establecen las siguientes limitantes:

i. En función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.
ii. Cuando se obstaculicen las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Finalmente en el caso de México, la legislación en la materia enumera los siguientes supuestos:

i. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello.
ii. Cuando en su base de datos, no se encuentren los datos personales del solicitante.
iii. Cuando se lesionen los derechos de un tercero.
iv. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos.

v. Cuando la rectificación, cancelación u oposición haya sido previamente realizada.
vi. Disposiciones de orden público, seguridad y salud pública.

Una vez enlistados los supuestos que limitan el ejercicio de los derechos ARCO, notamos que las tres legislaciones son uniformes en cuanto que justifican dicha limitación en función de salvaguardar el orden y la seguridad pública, los derechos de terceros, así como el mandato normativo.

Habiendo señalado las características principales de los derechos ARCO de forma conjunta es momento de enfocarnos en las características particulares de cada uno de los derechos.

3.2 Derecho de Acceso

Este apartado lo dedicamos al estudio de las características principales del primero de los derechos ARCO, es decir el derecho de Acceso. En primer lugar haremos alusión a la acepción que la doctrina nos da para este derecho.

En palabras de Osvaldo Gozaini es "*el derecho a solicitar y obtener información de un archivo o registro, para saber si el mismo contiene o no información personal que a alguien concierne; contribuye el fundamento esencial del habeas data. Es el derecho de entrada a los bancos de datos y la garantía principal que tiene la persona para conocer qué información existe sobre ella".*[5]

Por otra parte la abogada Iciar López-Vidriero y el abogado Efrén Santos, se refieren al derecho de acceso como *"aquél que deberá ser ejercitado cuando el afectado quiera conocer con exactitud los datos personales de que un tercero -responsable del fichero- dispone, dónde fueron recabados -de una tercera*

[5] Gozaini, Osvaldo Alfredo, *Habeas data. Protección de datos personales*, Argentina, Rubinzal-Culzoni Editores, 2001, pp. 357-359.

empresa, del propio afectado, etc.- y si dichos datos personales o parte de ellos han sido comunicados o van a ser comunicados a un tercero". [6]

Finalmente la profesora de la Universidad de Montpellier Rocío Ovilla señala que es el *"derecho de poder procurarse la comunicación de los datos que le conciernen. Es un derecho a obtener, previa solicitud y con una frecuencia razonable, la confirmación de la existencia o inexistencia de los datos que le conciernen, la comunicación de dichos datos en forma inteligible, así como información acerca de su origen y en general, su utilización".* [7]

A efecto de reforzar el concepto del derecho de Acceso, hagamos hincapié en uno de los pronunciamientos emitidos por el Director de la Agencia Española de Protección de Datos, esto es, la Resolución Nº. R/01490/20 de fecha 12 de julio de 2011, en la cual define este derecho como "*aquél que concede al interesado la posibilidad de comprobar si se dispone información sobre sí mismo y conocer el origen del que procede, la existencia y finalidad con la que se conserva".* [8]

Basándonos en las ideas expuestas por los autores antes mencionados, el derecho de acceso se perfila como un derecho que permite a una persona saber si sus datos personales están siendo objeto de algún tipo de tratamiento, así como las condiciones en que dicha información fue obtenida; los fines para los cuales se almacenó y en dado caso saber si los datos han sido transferidos a otro archivo.

En razón de que uno de los objetivos del derecho de Acceso es dar certeza a las personas de saber si información que les es propia es objeto de algún tipo de tratamiento convendría hacer un paréntesis, a efecto de hacer breves pronunciamientos en torno al tema del tratamiento de datos personales.

Como lo hemos venido haciendo durante el estudio de un tema, empezaremos por la definición del concepto "tratamiento"; en primer lugar recurriremos a la

[6] López-Vidriero Tejedor, Iciar y Santos Pascual, Efrén, *Protección de datos personales. manual práctico para empresas*, España, Editorial Fundación Confemetal 2005, p. 91.
[7] Ovilla Bueno, Rocío, *La protección de los datos personales en México*, México, Porrúa, 2005, p. 36.
[8] *www.agpd.es*

acepción que nos proporciona el Diccionario de la Real Academia de la Lengua Española, al definir el tratamiento de datos como la *"aplicación sistemática de uno o varios programas sobre un conjunto de datos para utilizar la información que contienen".*[9]

Si bien esta definición nos es de mucha utilidad para comprender el tratamiento de datos, se pronuncia únicamente sobre el tratamiento automatizado dejando de lado el manual, por lo cual debemos recurrir a otras definiciones, como lo son las proporcionadas por la legislación.

En primer término la ley 25.326 de Argentina define al tratamiento como las *"operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias".*

Por lo que hace a la Ley Orgánica 15/1999 de España, establece que el tratamiento de datos comprende las *"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".*

México por su parte, a través de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, define el tratamiento de datos como *"la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales".*

Tanto la legislación argentina como la española son prácticamente idénticas en cuanto su concepción del tratamiento de datos, sin embargo en el caso de la legislación mexicana si bien la idea que expone va en esencia en el mismo

[9] Diccionario de la Real Academia de la Lengua Española. 22 ed. *http://buscon.rae.es/draeI/.*

sentido, difiere en cuanto que no retoma la manera en que los datos son obtenidos, usados o almacenados, es decir parece que se mezcla la finalidad del tratamiento con su manera de operar, porque en las primeras dos legislaciones refieren al tratamiento como el mecanismo para obtener, almacenar y transferir los datos, mientras que esta última equipara el tratamiento con el hecho mismo de la obtención, almacenamiento y transferencia.

Podemos concluir que el tratamiento de datos es el mecanismo sea automatizado o manual, mediante el cual los datos son obtenidos sea de manera directa (cuando se toma la información directamente de su titular) o indirecta (cuando se toman de diversas fuentes de información distintas del titular); almacenados en una base de datos, manipulados, utilizados y en su caso transferidos a una tercera persona, distinta a la que los recolecto.

Uno de los supuestos que puede presentarse durante el tratamiento de datos es el relativo a la cesión de los mismos, la cual representa un factor importante en materia del derecho de Acceso, toda vez que no sería posible ejercer dicho derecho si los datos hubieran sido cedidos a una persona distinta al responsable del tratamiento y no se conociera al cesionario; por tanto es preciso dedicar unas líneas a este tema antes de concluir este apartado.

Retomando el estudio del derecho de Acceso sigamos con las características particulares de dicho derecho, entre las que encontramos:[10]

- ✪ El contenido del derecho de Acceso comprende los datos del afectado y los resultantes de cualquier elaboración o proceso informático, así como los cesionarios de los mismos y la especificación de los usos concretos y finalidades para los que se almacenaron los datos.
- ✪ El derecho de Acceso nos permite obtener gratuitamente información sobre nuestros datos de carácter personal sometidos a tratamiento, con la salvedad que el derecho sea ejercido en intervalos menores de 6 y 12

[10] "El derecho fundamental a la protección de datos: Guía para el Ciudadano", *op. cit.*, nota 3.

meses, para el caso de Argentina y México respectivamente. Cabe señalar que la legislación de España no establece ninguna temporalidad para ejercer el derecho de manera gratuita, sin embargo, establece el plazo de 12 meses para estar en posibilidad de volver a ejercer el derecho.

- ✪ Para ejercer el derecho de Acceso no se requiere que el titular alegue la existencia de un gravamen o perjuicio, ya que la verdad integra el mundo jurídico y por tanto el peticionario puede promoverlo en resguardo de la simple verdad.[11]

El derecho de Acceso es una facultad que al ejercerla nos da la pauta para saber qué datos están siendo tratados, los usos y finalidad así como en su caso el cesionario de los mismos; es asimismo un derecho gratuito en razón de que su ejercicio no implica un detrimento en el patrimonio de quien lo ejercer ni una retribución para el responsable del tratamiento, y para su ejercicio no se requiere la existencia de ningún gravamen.

Como vemos para ejercer el derecho de Acceso no se requieren muchos requisitos, sin embargo podría facilitarse si el titular de los datos pudiese conocer los ficheros existentes que puedan contener sus datos personales; para lo cual es de gran utilidad que los ficheros se encuentren inscritos en algún Registro, tal como lo prescribe la ley 25.326 de Argentina, al establecer que para que una base de datos sea licita, debe inscribirse en el Registro Nacional de Bases de Datos; en igual sentido se pronuncia la legislación española, al crear el Registro General de Protección de Datos, sin embargo, por lo que respecta a México la ley no prevé la creación de algún Registro en donde haya que inscribir los archivos que almacenan datos de carácter personal; esta decisión se tomó en la Cámara de Senadores al considerar que no se requería un Registro de las bases de datos porque conllevaría un proceso burocrático que no añadiría bondades significativas a la protección de los datos de los titulares.

[11] *Cfr.* Gozaini, Osvaldo Alfredo, *op. cit.,* nota 5, p. 432.

Sin embargo consideramos que la existencia de un Registro de bases de datos si facilitaría el ejercicio del derecho de Acceso, porque si bien solamente se necesita presentar una solicitud ante el responsable del tratamiento, lo verdaderamente engorroso podría resultar el estar investigando quiénes podrían ser los responsables de algún tipo de tratamiento que esté versando sobre nuestros datos.

Sabiendo en qué consiste este derecho y cuáles son sus características, es momento de aludir a la finalidad del derecho de acceso, en los siguientes términos:[12]

1) El titular pueda conocer la efectiva existencia del tratamiento a que son sometidos sus datos personales.
2) El titular tenga acceso a sus datos personales que están en posesión del responsable.
3) El titular conozca las fuentes y los medios a través de los cuales se obtuvieron los datos.
4) El titular conozca las circunstancias esenciales del tratamiento, lo cual se traduce en el deber que tiene el responsable de informar al titular sobre el tipo de datos personales tratados; todas y cada una de las finalidades que justifican el tratamiento; las personas que intervienen en el tratamiento (encargados); en caso de transferencias, los destinatarios, las finalidades de las mismas, la información personal transferida, entre otra información que el titular esté interesado en conocer.
5) El titular sepa si el archivo se encuentra registrado en el Registro de Bases de Datos (para el caso particular de Argentina y España).

Al ejercer el derecho de Acceso el titular tiene que obtener la información listada, es decir mediante el Acceso se conoce la existencia real de algún tipo de tratamiento sobre nuestros datos, así como las condiciones generales del tratamiento y saber si la base de datos está lícitamente constituida.

[12] "Guía Práctica para ejercer el Derecho a la Protección de Datos Personales, *op. Cit,* nota 4.

Ahora bien, ¿para qué sirve tener garantizado este derecho?, para Ana Isabel Herrán Ortiz lo trascendente es que el afectado tenga constancia de la información relativa a sus datos, de un modo claro, completo y exacto, de suerte que se procure al afectado el conocimiento de aquellos aspectos fundamentales del tratamiento automatizado, para poder ejercer una defensa de sus derechos con ciertas garantías jurídicas.[13]

Luego entonces, es importante porque al enterarnos de la manera en que nuestros datos fueron recolectados, podemos advertir si la recolección fue lícita o no, así como para establecer la responsabilidad de los sujetos que intervinieron en el tratamiento. Así mismo, podemos decir que el derecho de acceso constituye una premisa para asegurar que los datos personales que se incorporan a un archivo responden a los deberes y principios que los bancos de datos deben asegurar. Los cuales, Osvaldo Alfredo Gozaini[14] los explica de la siguiente manera:

1. P. de legalidad: la formación de archivos es licita cuando se encuentran debidamente inscritos; esto supone que se tiene una presunción de legalidad por el sólo hecho de encontrarse inscrito en el Registro. Mediante este principio se establecen algunas reglas básicas.

    a) Licitud en la recolección de datos: supone que las acciones emprendidas para la obtención de informaciones personales han dado cumplimiento a una pauta general de buena fe y lealtad hacia las personas interesadas.
    b) Buena fe en la búsqueda de información, como en las etapas sucesivas de almacenamiento, tratamiento, cesión y transferencia
    c) Lealtad hacia la persona que resulta concernida: significa que cuando se piden datos es necesario informar para qué se solicitan, dónde se archivarán y el destino pensado para ellos.
    d) Participación del individuo en la incorporación al banco de datos.

[13] *Cfr.* Gils Carbó, Alejandra M. *Régimen legal de las bases de datos y hábeas data*. Argentina. Editorial La Ley. 2001, p. 168.
[14] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 5, pp. 192-194,196, 198.

e) Exclusión inmediata de los datos sensibles.

2. Principio de finalidad: colectar datos que estén vinculados con el fin que persigue su objeto. Asimismo, la permanencia del dato en la base debe estar relacionada con los motivos del registro, y mantenerlo en él hasta que el mismo se alcance.
3. Principio de congruencia: todo dato debe ser congruente con las finalidades que se buscan al archivarlo. Los datos no deben ser más de los necesarios para la información que persiguen.

De lo anterior podemos advertir que una vez que el titular de los datos tiene resuelto el problema del acceso, podrá resolver conductas posteriores. En este sentido, validará la información contenida, podrá ratificar la autorización prestada si ella se hubiere requerido, tendrá la facultad de exigir la actualización o rectificación de los datos, planteará la supresión del dato sensible, y en cada caso queda de manifiesto el poder de control de la persona sobre los archivos de datos personales.[15]

No obstante todos los beneficios que representa el ejercicio del derecho de acceso, es de hacer notar que éste no es absoluto, pues la ley establece algunas restricciones particulares para este derecho:

Por lo que toca a España, la ley establece que el responsable del tratamiento de datos podría denegar el acceso a los datos cuando:[16]

1. El derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

2. Así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

[15] *Ibídem,* pp. 357-359.
[16] Artículo 30 del Reglamento de la Ley 15/1999.

México por su parte, señala las siguientes restricciones:

1. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
2. Cuando en su base de datos, no se encuentren los datos personales del solicitante;
3. Cuando se lesionen los derechos de un tercero;
4. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales.

En tanto que Argentina no establece restricciones específicas para cada unos de los derechos, se desprende del artículo 14 de la Ley 25.326 que la única limitante para ejercer este derecho es que el solicitante no acredite su carácter de titular de los derechos.

Podemos resaltar que no hay criterios uniformes ya que cada legislación determina sus propios supuestos de improcedencia para el ejercicio del derecho de acceso, salvo por lo que respecta a que la solicitud no sea presentada por el titular de los datos, para el caso de México y Argentina.

Para culminar con el estudio de este derecho, pasemos a analizar cómo es que éste queda satisfecho. La legislación nos ofrece una amplia gama de medios por los cuales el titular puede optar para que la información solicitada le sea proporcionada.

La legislación argentina establece que el titular de los datos podrá elegir entre los siguientes medios, para que el responsable del tratamiento le entregue la información respecto a sus datos:

i. Visualización en pantalla,
ii. Informe escrito entregado en el domicilio del requerido,
iii. Informe escrito remitido al domicilio denunciado por el requirente,

iv. Transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información, o
v. Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario del mismo.

En el caso de España la ley de la materia[17] señala que el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla,
b) Escrito, copia o fotocopia remitida por correo, certificado o no,
c) Telecopia,
d) Correo electrónico u otros sistemas de comunicaciones electrónicas, o
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

Por lo que respecta a México, el responsable del tratamiento para dar cumplimiento al derecho de acceso ejercido por el titular de los datos, debe poner a disposición de éste, de manera gratuita, los datos personales; siendo factible que el responsable y el titular acuerden la modalidad de entrega o reproducción de los datos personales solicitados, cuando así lo considere conveniente el responsable[18]. Las modalidades que sugiere son:

1. En sitio,
2. Expedición de copias simples,
3. Medios magnéticos, ópticos, sonoros, visuales u holográficos, o
4. Cualquier otro medio señalado en el aviso de privacidad.

[17] Ley 15/1999.
[18] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Como podemos ver la legislación no limita los medios en que puede quedar satisfecho el derecho de acceso, en función de no constituir una barrera en el cumplimiento de la obligación por parte del responsable del tratamiento.

No podemos concluir este apartado sin antes dedicar las líneas que habíamos anunciado previamente respecto al tema de cesión de datos.

Primeramente señalaremos la definición de la cesión de datos, para lo cual nos basaremos en la doctrina; Ana Garrida define la cesión de datos como *"toda revelación de datos personales realizada a una persona distinta del interesado".*[19]

En igual sentido se pronuncia el autor argentino Luis R. Carranza al definir la cesión como el *"contrato en virtud del cual una de las partes (cedente) transmite a otra (cesionario), a título gratuito u oneroso, determinados datos personales que posee en sus registros, y el derecho de hacer uso de los mismo en lo sucesivo".*[20]

La cesión la entenderemos como la transmisión de datos por parte del cedente, quien es la persona que ha recogido y almacenado datos personales, al cesionario quien es una persona tercera a la relación original entre el responsable del tratamiento de datos y el titular de los mismos, debiendo quedar establecido que la cesión solamente puede realizarse previo consentimiento del titular de los datos.

Únicamente referiremos a lo estipulado por la legislación para decir que existe unanimidad en cuanto al alcance de la cesión, ya que los tres países en cuestión establecen que la cesión solamente podrá hacerse para el cumplimiento de fines directamente relacionados con el interés legítimo del cedente y cesionario, previo consentimiento del titular de los datos.

Hecha la aclaración de que uno de los requisitos primordiales para efectuar la cesión de datos, es haberse obtenido primeramente el consentimiento del titular,

---

[19] Garrida Domínguez, Ana*, Tratamiento de datos personales y derechos fundamentales*, 2ª ed., España, Editorial Dykinson S.L. 2009, p. 76.

[20] Carranza Torres, Luis R., *Hábeas data. La protección jurídica de los datos personales,* Argentina, Editorial Alveroni, 2001, p. 79.

viene a colación que el titular de los datos, puede ejercer su derecho de acceso, aun cuando sus datos hayan sido cedidos, dado que para ello se requirió de su consentimiento y por tanto conoce la existencia del cesionario; aunque cabe decir que quien debe dar aviso en caso de que se ejerza alguno de los derechos ARCO, es el cedente al cesionario.

3.3 Derecho de Rectificación

Una vez revisada la posibilidad que tiene el titular de los datos de acceder a información que le es propia, podemos avanzar con el siguiente derecho de los llamados derechos ARCO es decir el derecho de Rectificación.

Tal como lo hicimos con el primero de los derechos ARCO, comenzaremos este apartado definiendo el derecho de Rectificación. El Diccionario de la Real Academia de la Lengua Española hace alusión al derecho de rectificación, y señala que es *"el que concede o reconoce la ley de imprenta a la persona aludida expresamente en un periódico para contestar desde este a las alusiones que se le hayan dirigido".*[21]

Esta definición no consideramos que sea aplicable a la materia de protección de datos, pues refiere más al derecho de réplica; no obstante el Diccionario nos proporciona una definición de lo que debemos entender por la palabra "rectificar", la cual proviene del latín *rectificāre*; de *rectus*, recto, y *facĕre*, hacer; y entre las múltiples connotaciones que la palabra recibe, la que más se adecúa a nuestro tema, es la siguiente. *"corregir las imperfecciones, errores o defectos de algo ya hecho".*[22]

Si bien esta definición nos da una idea más clara de en qué consiste el término "rectificar" al señalar que es corregir algo incorrecto, necesitamos recurrir a la

[21] Diccionario de la Real Academia de la Lengua Española, op. cit., nota 9.
[22] *Ídem.*

doctrina para tener una definición precisa no del verbo rectificar sino del derecho de Rectificación.

Carranza Torres nos dice que *"es la facultad legal que posee toda persona a la cual no se le han mantenido actualizados los datos o no han sido sometidos a la confidencialidad que les corresponde, siendo los mismos en consecuencia inexactos, erróneos o incompletos o indebidos en su difusión, de adecuarlos a la situación actual o al marco legal que les correspondiere".*[23]

Agrega este mismo autor que constituye la acción constitucional o legal de toda persona física a acceder de manera permanente a las bases de datos de su propia información para verificar su debida integración, y en su caso, de ser necesario, completarla o rectificarla.[24]

Rocío Ovilla por su parte señala que "*este derecho se aplica a las informaciones inexactas, incompletas, equivocas o caducas. El responsable o usuario de la base de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias. Es decir, este derecho de rectificación se convierte en una obligación de rectificación para el responsable de los archivos personales".*[25]

Recapitulando las definiciones previamente enunciadas, podemos concluir que el derecho de Rectificación es entonces aquél mediante el cual el titular de los datos puede solicitar al responsable del tratamiento la corrección de los datos que conciernen a su persona, sea porque éstos son incorrectos, por encontrarse incompletos o por estar desactualizados; se convierte así mismo en una obligación para el responsable del tratamiento de hacer las adecuaciones que pertinentes que le solicite el titular de los datos.

[23] Carranza Torres, Luis R, *op. cit.,* nota 11, pp.94-95.
[24] *Ibídem,* p. 66.
[25] Ovilla Bueno, Rocío, *op. cit*., nota 7, p. 37.

Compartiendo esta misma base la legislación española se pronuncia en el mismo sentido al definir este derecho como "*el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos".* [26]

Una vez que ha quedado definido el derecho de rectificación, debemos referir a los supuestos en que es procedente su ejercicio; así tenemos que procede cuando los datos que están siendo objeto de tratamiento sean:

- Datos erróneos: aquéllos que no corresponden con la realidad presente o pasada de las cosas.
- Datos incompletos: en el caso de información incompleta que dibuja un perfil insuficiente por lo que se debe incorporar al archivo la información parcialmente omitida.
- Datos desactualizados:[27] aquéllos que en un momento pasado fueron correctos, pero que con el transcurso del tiempo han devenido en incorrectos por no reflejar la situación existente al presente. No es información real para el tiempo donde se produce y por eso la finalidad es actualizar el registro.

De estos supuestos enlistados se desprende que el derecho de Rectificación procede en aquellos casos en que los datos que han sido almacenados y que son objeto de algún tipo de tratamiento son erróneos por no coincidir con información verdadera respecto al titular, incompletos por solamente reflejar una parte de la información concerniente al titular y al no ser la totalidad de la misma puede provocar alguna confusión, o desactualizados es decir que en un momento fueron correctos sin embargo con el devenir del tiempo han cambiado y por tanto se han convertido en erróneos.

En cuanto a los efectos que produce el ejercicio del derecho de rectificación encontramos no solamente la corrección de la información errónea o desactualizada, sino además que se notifique al cesionario la rectificación que de

[26] Reglamento de la Ley 15/1999.
[27] Carranza Torres, Luis R, *op. cit.,* nota 11, pp. 94-95.

los datos deba efectuar; así mismo aparece la figura del bloqueo, sólo respecto de la legislación Argentina, pues tanto España como México prevén esta figura en el caso del derecho de cancelación, por lo que consideramos prudente reservar su estudio para el siguiente apartado.

Como hemos mencionado anteriormente el ejercicio de ninguno de los derechos ARCO es absoluto, pues la legislación plantea algunos supuestos en los que no procede su ejercicio.

La legislación de España dispone como único supuesto de improcedencia, que lo prevea una ley o una norma de derecho comunitario de aplicación directa, o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

Por lo que respecta a México podemos deducir a contrario sensu de la propia ley, que no será procedente si el titular no señala a qué datos se refiere y/o no acompaña la documentación que justifique su dicho.

Argentina, como ya lo mencionamos no establece situaciones particulares para negar el ejercicio de cada derecho ARCO.

El derecho de Rectificación ve limitado su ejercicio por mandato de ley en el caso de España; y por lo que respecta a México.cuando el titular no precise sobre qué datos debe versar la corrección o no aporte pruebas de que los datos que pretende corregir son erróneos, incompletos o desactualizados.

1.4 Derecho de Cancelación

Hemos visto cómo acceder a los datos personales objeto de tratamiento, cómo corregirlos en caso de ser erróneos, incompletos o desactualizados; toca ahora analizar cómo podemos cancelar dicho tratamiento.

Partamos de nueva cuenta de la definición del Diccionario de la Real Academia de la Lengua Española, que nos dice que la cancelación "*es la acción y efecto de cancelar"*, y por cancelar debemos entender *"anular, hacer ineficaz un instrumento público, una inscripción en registro, una nota o una obligación que tenía autoridad o fuerza".* Así también nos proporciona una definición de cancelación en materia jurídica, esto es *"asiento en los libros de los registros públicos, que anula total o parcialmente los efectos de una inscripción o de una anotación preventiva".*

Esta última definición guarda estrecha relación con el derecho de Cancelación de datos, pues aunque la definición sólo refiere a registros públicos, podemos equiparlos con los archivos particulares.

Pero para tener una idea más clara de este derecho, es preferible recurrir a la doctrina; en primer término Osvaldo A. Gozaini menciona que la Cancelación "*exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas".*[28] El derecho se fundamenta en la potestad de reclamar la eliminación de toda información que violente la esfera de la privacidad personal cuyo almacenamiento no fuera autorizado. También el poder de exclusión o supresión permite demandar la cancelación del dato que se ha tornado impertinente o ha devenido en innecesario.[29]

Ana Garrida define el derecho de Cancelación como *"la facultad de eliminar de un fichero aquellos datos de carácter personal que no deban figurar en él, ya sea porque nunca debieron ser registrados, ya sea porque habiéndose recogido legalmente, diversas causas exigen su supresión".*[30] Solo la desaparición de los datos permite al interesado tener la completa seguridad de que no van a poder ser recuperados de nuevo y ejercer así un completo control y seguimiento de los mismos.

[28] Gozaini. Osvaldo Alfredo, *op. cit.,* nota 5, p. 373.
[29] *Ibídem,* p. 365.
[30] Garrida Domínguez, Ana, *op. cit.,* nota 10, p. 133.

En el mismo sentido se pronuncia Juan Armagnague, quien define este derecho como *"el derecho de todo titular de exigir al responsable del tratamiento la cancelación de sus datos personales almacenados en forma inexacta y, asimismo, de los datos incompletos que nunca debieron ser registrados".* [31]

La primera definición dada por Gozaini hace hincapié en que la cancelación debe implicar el borrado físico y no basta simplemente con cesar en el tratamiento, así mismo al igual que por lo que respecta a las siguientes definiciones agregan los supuestos en que el derecho de cancelación es procedente, los cuales enlistaremos en párrafos posteriores.

Con las ideas expuestas nos queda una noción más clara de en qué consiste el derecho de Cancelación, sin embargo como complemento a la doctrina daremos paso a lo expuesto por la legislación.

El Instituto Federal de Acceso a la Información y Protección de datos alude a que el derecho de cancelación *"consiste en que los titulares de los datos personales pueden solicitar que se eliminen sus datos personales cuando consideren que no están siendo utilizados o tratados conforme a las obligaciones y deberes que tiene el responsable y que se encuentran contenidos tanto en la Ley como en su Reglamento".*[32] Esto partiendo del contenido del Reglamento de la Ley de Protección de Datos Personales en posesión de particulares, que a la letra dice *"la cancelación implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de los mismos y su posterior supresión".*

El Reglamento de la Ley española 15/1999 aclara que este derecho "es *el procedimiento en virtud del cual el responsable del tratamiento cesa en el uso de los datos; la cancelación implicara el bloqueo de datos, consistente en la*

[31] Armagnague, Juan (Dir.), *Derecho a la información, habeas data e internet*, Argentina, Ediciones La Rocca, 2002, p. 389.
[32] "Guía Práctica para ejercer el Derecho a la Protección de Datos Personales". *op. cit.*, nota 3.

identificación y reserva de los datos con el objetivo de impedir su tratamiento y, cesión de datos".[33]

A diferencia de la doctrina, la legislación prevé un paso antes de la supresión de los datos almacenados en un archivo, esto es el bloqueo de datos, tema que en el apartado del derecho de rectificación dejamos pendiente, sin embargo es necesario retomar su estudio en este punto; no sin antes culminar definiendo el derecho de cancelación como la facultad que tiene el titular para solicitar al responsable del tratamiento el cese del tratamiento de sus datos, y su posterior eliminación del archivo en que se encuentren almacenados.

Por lo que respecta a la figura del "bloqueo de datos"; primeramente definiremos el término "bloquear" siguiendo al Diccionario de la Real Academia de la Lengua Española como *"Interceptar, obstruir, cerrar el paso".*[34]

Esta definición nos ilustra en cuanto que en efecto el bloqueo de datos implica como un primer paso obstruir el normal desarrollo del tratamiento de datos, no obstante es muy abierta la posibilidad de obstruir el tratamiento, por lo que para precisar más sobre el tema recurriremos a la legislación; la normatividad argentina establece que durante el proceso de 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 se encuentra sometida a revisión.

El Reglamento de la Ley 15/1999 alude que el bloqueo consiste *"en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades".*

[33] Garrida Domínguez, Ana, *op. cit*., nota 10, pp. 74-75.
[34] Diccionario de la Real Academia de la Lengua Española, *op. cit.,* nota 9.

La Ley Federal de Protección de Datos Personales en Posesión de Particulares define el bloqueo como *"la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde".* Esta definición se complementa con el Reglamento de la propia ley, que dice que el bloqueo tiene como propósito impedir el tratamiento, a excepción del almacenamiento o posible acceso por persona alguna, salvo disposición en contrario.

Cada una de las legislaciones destaca puntos importantes respecto al bloqueo de datos, por lo que toca a la argentina, no impide continuar con el tratamiento de datos pues basta con que se advierta que los datos en cuestión están en proceso de rectificación; en tanto que la española identifica y reserva la información a efecto de impedir el tratamiento salvo disposición de autoridades administrativas o jurisdiccionales, y finalmente México limita el bloqueo de datos a aquéllos que ya han cumplido con la finalidad para la cual fueron almacenados.

Recapitulando estas definiciones diremos que el bloqueo es la etapa previa a la eliminación de los datos personales del archivo en que fueron almacenados, con el fin de resguardar los datos por un tiempo razonable en el que podrían surgir responsabilidades relacionadas con el tratamiento, esto es, responsabilidades que para poder ser verificadas requieran de los datos. Durante este periodo, los datos no podrán ser tratados para otra finalidad.

Una vez revisado el concepto del derecho de Cancelación, y visto el efecto que produce su ejercicio, es decir el bloqueo, continuemos con el estudio de los supuestos en que es procedente este derecho, siguiendo lo estipulado en cada una de las legislaciones en comento.

La Ley Orgánica 15/1999 señala que procede en aquellos casos en que el tratamiento de los datos no se ajuste a lo prescrito por la ley, los datos sean

inexactos o incompletos, así como cuando hayan dejado de ser pertinentes o necesarios para la finalidad para la cual se recabaron; su Reglamento complementa los supuestos, al extenderlos a los datos que resulten ser excesivos.

El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares otorga el derecho de cancelación en el supuesto en que el titular de los datos considere que éstos no están siendo tratados conforme a los principios y deberes que establece la ley y su reglamento.

Por lo que respecta a la legislación argentina, ésta no define los supuestos en los que el ejercicio de este derecho es procedente.

El derecho de Cancelación podríamos decir que su ejercicio procede cuando los datos personales no estén siendo tratados conforme a lo estipulado por la legislación de la materia, así como cuando hayan cumplido con la finalidad para la cual se recopilaron.

Como lo hemos venido desarrollando en los anteriores derechos, es momento de enlistar los supuestos en que no es procedente el ejercicio del derecho de Cancelación.

La legislación de Argentina refiere que la cancelación de los datos no procede en los siguientes supuestos:

I. Cause perjuicio a derechos o intereses legítimos de terceros.
II. Exista obligación legal de conservar los datos.

Por su parte la legislación española enumera los siguientes supuestos:

I. Los datos de carácter personal deban 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 que justificaron el tratamiento de los datos.

II. Lo prevea una ley o una norma de derecho comunitario de aplicación directa.

En el caso de México, la legislación apunta a los siguientes supuestos:

I. Los datos se refieran a las partes en un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento.
II. Los datos deban ser tratados por disposición legal.
III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular.
V. Sean necesarios para realizar una acción en función del interés público.
VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular.
VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

El ejercicio del derecho de Cancelación puede verse limitado porque así lo prevea una disposición legal, o cuando la supresión de los datos pueda generar el incumplimiento de alguna obligación contraída, o pueda entorpecer alguna actuación judicial o administrativa, así mismo se limita su ejercicio para salvaguardar los derechos de terceros o algún beneficio para el titular de los datos o en pro del interés público.

Antes de concluir con este apartado, dedicaremos unas líneas a revisar un derecho que entraña el ejercicio del derecho de cancelación en sí mismo, es decir, el derecho al olvido.

El derecho al olvido recobra relevancia en el uso de internet, ya que se ha convertido en una práctica más común entre las personas, que soliciten el borrado

de sus datos contenidos en sitios, portales, blogs y motores de búsqueda; sin embargo para algunos expertos esta práctica es un mera extensión de los derechos ARCO; mientras que otros argumentan que se trata de un nuevo derecho que debería estar explícitamente previsto en las disposiciones reglamentarias respectivas para ser ejercido como tal.[35]

Uno de los pronunciamientos más recientes sobre el tema es el de la Sección Primera de la Sala Contencioso Administrativo de la Audiencia Nacional Española, el 2 de marzo de 2012, quien solicitó al Tribunal de Justicia de la Unión Europea aclarar cuestiones sobre jurisdicción y derecho aplicables en casos relacionados con denuncias individuales sobre privacidad de la información en contra de Google y motores de búsqueda en general.

De acuerdo con la Audiencia Nacional Española, no está claro quién debe tomar una decisión judicial respecto a quejas relacionadas con la privacidad de los individuos que no desean que su información y datos aparezcan en portales de Internet.

Sin embargo ante la falta de un criterio fijo sobre el tema, la Audiencia Nacional se ha pronunciado al respecto citando que al *"sostener que la indexación de datos procedentes de páginas web situadas en España, en relación con una información publicada en España, con base en una norma legal española, que afecta a datos de un ciudadano español y que fundamentalmente puede tener una repercusión negativa, a juicio del afectado, en su entorno personal y social situado en España (centro de intereses), tenga que defender la tutela de su derecho a la protección de datos en EEUU, por ser el lugar que el gestor del buscador ha elegido para ubicar los medios técnicos, colocaría a los afectados en una situación de especial vulnerabilidad e impediría o dificultaría enormemente la tutela eficaz de este derecho que podría resultar incompatible con el espíritu y finalidad que inspira la*

[35] *Cfr.* Rosen, Jeffrey , "The Right to Be Forgotten", *Stanford Law Review*, núm. 64, 13 febrero de 2012, *http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten*

Directiva y, sobre todo, con una tutela eficaz de un derecho fundamental contenido en la Carta Europea de Derechos Fundamentales".[36]

La Audiencia destaca la vulnerabilidad en que se situarían los usuarios de internet si tuvieran que someterse a la jurisdicción aplicable al Estado en que se sitúan los medios técnicos del sitio web a pesar de que el tratamiento y el afectado se encuentren en un territorio distinto.

Esta decisión fue muy oportuna en virtud de las múltiples reclamaciones que se han instaurado en contra de Google, a efecto de que elimine de su base datos personales por considerar que se violan derechos del titular.

Entre los principales argumentos de defensa de Google es que las actividades se realizan desde los Estados Unidos, y por tanto no le aplica la legislación española; sin embargo la Agencia Española ha basado sus pronunciamientos en el documento WP 148 de 4 abril de 2008 elaborado por el Grupo de Trabajo "G 29" relativo a buscadores; en el cual se establece que un Estado miembro aplicará su derecho nacional a un buscador establecido fuera de la Comunidad Europea si recurre a medios situados en su territorio, sin que su utilización sea únicamente con fines de tránsito; y por lo que respecta a Google Spain, resulta imprescindible que GOOGLE haya visitado con anterioridad las páginas ubicadas en servidores web españoles y registrado esta circunstancia durante la labor de rastreo realizada por sus "arañas web", para estar en posibilidad de dar respuesta a las búsquedas de los usuarios españoles. Por tanto para la prestación del servicio de búsqueda a los usuarios españoles, es requisito ineludible que se utilicen medios técnicos ubicados en territorio español. Así mismo es importante especificar que la legislación española incluye a los buscadores dentro de la definición de "servicios de la sociedad de la información".

[36] Nota de la AEPD sobre el auto de la AN en el que plantea al TJUE diversas cuestiones prejudiciales sobre el ejercicio de derechos frente a buscadores de internet, 2 de marzo 2012, *http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/marzo/120302_Nota_cuestion_prejudicial.pdf*

Siguiendo el documento del Grupo de Trabajo “G 29”, el sitio web debe someterse a la legislación en que se efectúa el tratamiento de datos y donde se encuentra el usuario que ve vulnerado su derecho al olvido, debido a que si bien los medios técnicos del sitio web se encuentran en otro Estado, la información en que basa los servicios que ofrece fueron obtenidos dentro del Estado Español respecto de un ciudadano español, no dándole participación al estado en cuyo territorio se encuentren las oficinas centrales del sitio web. Esta decisión lejos de parecer arbitraria es razonable en cuestión de que busca salvaguardar el derecho al olvido del usuario a través de una protección jurisdiccional accesible.

Como se desprende de los párrafos anteriores, el ejercicio del derecho al olvido se encuentra respaldado mediante la aplicación extraterritorial de la norma española, que expresamente establece la Ley Orgánica 15/1999. Dicha aplicación es importante para no dejar desprotegidas a las personas por cuestiones de territorio, sobre todo en la actualidad que el intercambio de datos personales se da principalmente a nivel internacional.

Prácticamente en el mismo sentido que la legislación española, se pronuncia el Reglamente de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, sin embargo aún no tenemos resoluciones por parte del Instituto Federal de Acceso a la Información y Protección de Datos en esta materia.

Desafortunadamente en la legislación argentina, no se encuentra delimitada la aplicación territorial de la norma protectora de datos personales; no obstante entre las resoluciones que ha emitido la Dirección Nacional encontramos que si hay pronunciamientos respecto de responsables extranjeros que cuentan con establecimientos en territorio argentino, siguiendo la línea establecida por la Agencia Española.

1.5 Derecho de Oposición

Toca el turno de estudiar el último de los derechos ARCO, es decir, el derecho de Oposición que al igual que los tres anteriores comenzaremos por definirlo en términos del Diccionario de la Real Academia de la Lengua Española que define la palabra oposición como "*la acción y efecto de oponer"*, y oponer como *"poner algo contra otra cosa para entorpecer o impedir su efecto".*

La definición literal siempre nos da un panorama general para aproximarnos a comprender el significado de una palabra, como en este caso que alude con el término oposición a la acción mediante la cual se impide que algo surta efectos, por lo que nos da la visión para entender que el derecho de Oposición está relacionado con la acción de impedir que el tratamiento siga surtiendo efectos, pero para no tener dudas al respecto recurramos a la doctrina para dilucidar con mayor claridad el concepto de derecho de Oposición.

En palabras de Pérez Serna el derecho de oposición es *"el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que se trate de ficheros de giro comercial o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos".*[37]

Isabel Davara nos dice que el derecho de oposición *"consiste en que el titular, en aquellos casos en los que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una ley no disponga lo contrario, podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos".*[38]

---

[37] Pérez Serna, Jesús Mayo, *op. cit., .* nota 1.

[38] Davara F. de Marcos, Isabel. "Breve análisis de la reforma al artículo 6° constitucional en lo relativo a protección de datos personales", en Carbonell, Miguel y Bustillos, Jorge (coord.), *Hacia una democracia de contenidos: la reforma constitucional de transparencia,* México, Instituto de Investigaciones Jurídicas, UNAM**. 2**007, p. 85.

Por su parte Iciar López-Vidrieto y Efrén Santos señalan que *"el derecho de oposición reconoce al afectado la posibilidad de negarse al tratamiento de sus datos de carácter personal por un tercero, siempre y cuando no exista una base legal que obligue al tratamiento de dichos datos como relación contractual, administrativa, etc. Así, cuando no existan motivos legales y legítimos, el afectado podrá oponerse al tratamiento de sus datos".*[39]

Partiendo de estas definiciones queda claro que el derecho de Oposición consiste en la facultad que tiene el titular de rechazar que sus datos personales sean objeto de algún tipo de tratamiento, siempre y cuando no hubiese prestado su consentimiento o alguna disposición normativa exija el tratamiento.

Durante el desarrollo del estudio de los anteriores derechos ARCO una vez satisfecha la mención a la doctrina damos pié a lo dispuesto en la legislación con dos objetivos fundamentales, el primero como complemento y el segundo para verificar que no exista alguna contradicción en lo establecido por la doctrina; por lo tanto es momento de hacer una revisión de lo estipulado en la legislación.

En cuanto a la legislación argentina encontramos que no reconoce expresamente el derecho de Oposición, pues lo único que menciona es lo consagrado en el artículo 27 inciso 3, al señalar que el titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos con fines de publicidad.

Por lo que respecta a la española el derecho de Oposición nos dice que es *"el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo".*

El derecho de Oposición en México es *"aquel derecho que tiene el titular de los datos en todo momento y por causa legítima a oponerse al tratamiento de sus datos, a efecto de que el responsable no pueda tratar los datos relativos al titular".*

[39] López-Vidriero Tejedor, Iciar y Santos Pascual, Efrén, *op. cit.,* nota 6, pp. 91-93.

Si bien la legislación argentina no refiere expresamente al derecho de Oposición si refiere a uno de los sectores en que se puede presentar este derecho, como es el del campo de la publicidad; por lo que toca a las otras dos legislaciones al igual que la doctrina retoman el derecho de Oposición como una posibilidad para el titular de rechazar el tratamiento de sus datos por razones fundadas, las cuales enlistamos a continuación:

En lo que respecta a México, los supuestos en que es procedente el derecho de oposición son:[40]

- ✓ Cuando el tratamiento de datos personales ha sido llevado a cabo con pleno respeto a los principios básicos de protección de datos personales, sin embargo el titular cuenta con una razón legítima derivada de su propia situación personal para oponerse a que sus datos personales sigan siendo tratados para fines específicos, a fin de evitar un perjuicio al titular derivado de la persistencia en el tratamiento de la información que le concierne.
- ✓ Cuando el titular requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos. Es de resaltar que si bien el titular puede oponerse a que sus datos sean tratados para una determinada finalidad, como puede ser de mercadotecnia, publicitarios o de estudios comerciales, entre otros; el derecho de oposición, mantiene a salvo otros fines del tratamientos que el responsable, de conformidad con su aviso de privacidad, puede llevar a cabo y con los que el titular está de acuerdo.

Para el caso de España, la ley señala los siguientes casos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

[40] Guía Práctica para la atención de las solicitudes de Ejercicio de los Derechos ARCO*, op. cit*., nota 4.

Es decir:

- Que exista un motivo legítimo y fundado.
- Que dicho motivo se refiera a su concreta situación personal.
- Que el motivo alegado justifique el derecho de oposición solicitado.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.
c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

La legislación en este tema deja muy abierta la posibilidad de ejercer este derecho, pues refiere de manera general a cuestiones de la situación personal del titular, sin delimitar algún tipo en particular, sin embargo consideramos que se debe a que en el campo principal en que podría ejercerse este derecho es el de la publicidad, en el cual no están inmersas situaciones trascendentales que requieran el tratamiento de datos personales como parte vital para su funcionamiento.

Como vimos en España, uno de los supuestos de procedencia del ejercicio del derecho de Oposición es que para efectuar el tratamiento de los datos no haya sido requisito el consentimiento del titular; por lo que debemos detenernos a revisar los supuestos en que la ley española marca que no es necesario el consentimiento.

Primeramente es necesario puntualizar en qué consiste el consentimiento, el cual la legislación española lo define como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen."* Así podemos decir que el consentimiento se constituye como un derecho inherente al afectado, y conjuntamente como deber del responsable del tratamiento el recabarlo previo a iniciar el tratamiento de los datos.

El consentimiento del titular reviste determinadas características para que pueda considerarse que satisfizo el requisito primordial en materia de tratamiento de datos las cuales a saber son:[41]

I. Libre: que haya sido obtenido sin la intervención de vicio alguno del consentimiento, que no esté viciado.
II. Especifico: debe ser referido a una determinada operación de tratamiento y para una finalidad determinada, explicita y legitima del responsable del tratamiento.
III. Informado: el titular conoce con anterioridad al tratamiento de sus datos la existencia del mismo y las finalidades para las que el mismo se produce; así como quién va a ser el responsable del fichero, dónde poder ejercer sus derechos, entre otros.
IV. Inequívoco: ha de existir alguna acción que permita conocer o demostrar que, verdaderamente, se ha prestado el consentimiento no siendo válido un consentimiento presunto.

El consentimiento para que cubra dichas características ha de ser libre, es decir sin ninguna presión o maquinación que provoque tomar dicha determinación; especifico esto es, enfatizar la información sobre la cual consiente el tratamiento y para qué finalidad; informado para lo cual el responsable del tratamiento debe haber previamente proporcionado la información correspondiente a las características generales del tratamiento; así como inequívoco en razón de que no pueda presentarse algún elemento que provoque poner en duda la determinación del titular de haber consentido el tratamiento de sus datos.

Para cumplir con el elemento de informado, la legislación prevé que el consentimiento debe ser recabado mediante una solicitud que deberá referirse a un tratamiento concreto, con delimitación de la finalidad para la que se recaba, así como de las restantes condiciones que concurran en el tratamiento.

[41] Davara F. de Marcos, Isabel, *op. cit*., nota 39, p. 79.

Si bien una de las características del consentimiento es que sea inequívoco, la ley no fija como requisito que el consentimiento sea expreso, salvo en los casos así previstos, pues el Reglamento de la Ley 15/1999 establece que el responsable concederá un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

Visto en qué consiste el consentimiento y cuáles son las características que debe cubrir para ser válido, sigamos con los supuestos en los cuales no es necesario recabarlo para llevar el cabo el tratamiento de los datos personales.

- Cuando se refieran a las partes de un contrato o precontrato de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento
- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado.
- Cuando los datos figuren en fuentes accesibles al público[42] 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.

Es decir, el tratamiento de datos puede llevarse a cabo sin el consentimiento del interesado siempre que sea necesario para cumplir con alguna obligación contractual, sea porque se busca el beneficio para el titular o bien cuando los datos se encuentren en fuentes accesibles al público.

[42] 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.

Para concluir con el tema del derecho de Oposición nos resta señalar que los casos en que no es procedente el ejercicio del derecho de oposición para ambas legislaciones, es cuando la ley disponga que el tratamiento de datos deba continuar, así como en los casos en que no haya un motivo legítimo y fundado para oponerse al tratamiento.

Mediante el estudio de los derechos ARCO en lo general y en lo particular hemos podido ver de qué manera contribuyen a tener un control sobre información que nos es propia y que está siendo objeto de algún tipo de tratamiento; desde saber en si existe un tratamiento, en qué base se está almacenando, las finalidades para las cuales se recabaron, quién es el responsable, la manera en que se obtuvieron, si han sido cedidos a un tercero; así como en caso de error o desactualización poder solicitar que se hagan las correcciones correspondientes; inclusive poder pedir la cancelación del tratamiento o más aún oponerse a que nuestros datos sean objeto de tratamiento.

En el siguiente capítulo veremos los dos procedimientos establecidos en la ley que permiten el ejercicio de los derechos ARCO, es decir directamente frente al responsable del tratamiento o bien con la intervención de la autoridad sea administrativa o judicial.

CAPITULO IV La protección de los Derechos ARCO.

En los capítulos precedentes hemos estudiado los aspectos generales de los datos personales, la importancia de protegerlos, así como los derechos que tiene el titular para mantener un control sobre su uso y destino; por lo que es este capítulo veremos la manera de hacer efectivo ese control, mediante el ejercicio de los derechos ARCO.

Antes de comenzar con el estudio de los procedimientos mediante los cuales podemos ejercer los derechos ARCO, haremos un breve recorrido histórico a través de la legislación tanto internacional como nacional, para estar en posibilidades de tener un panorama amplío que nos permita comprender el sentido de las disposiciones que norman el ejercicio de los derechos ARCO.

4.1 Antecedentes de la protección de datos

El primer antecedente lo encontramos en la Constitución de Weimar en 1919, la cual reconoció en su artículo 127, a los empleados administrativos el derecho de acceder y controlar su legajo personal, derecho que adquiere relevancia al ser reconocido años posteriores como derecho autónomo en la sentencia del Tribunal alemán sobre la Ley del Censo de Población de Alemania.

Posteriormente a nivel supranacional se proclamó la Declaración de los Derechos Humanos en 1948 por la Organización de las Naciones Unidas, en la cual se estableció que nadie podrá ser sujeto de injerencias arbitrarias en su vida, familia, domicilio o correspondencia. Si bien esta disposición remite directamente a la protección de la vida privada, nos sirve de antecedente en razón de que a partir de ella se creó la Sociedad de Naciones, quien inició los acuerdos para la protección de datos personales, y en su artículo 12 señaló que “nadie será objeto de injerencias arbitrarias en su vida privada, familia, su domicilio o su

correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".[1]

Como se deprende de este párrafo, podemos constatar que la protección de datos personales encuentra su antecedente más remoto en el reconocimiento del derecho a la intimidad; no obstante en el presente trabajo nos enfocaremos a revisar únicamente las disposiciones que refieren a la protección de datos personales como derecho autónomo.

En este sentido de reconocer la protección de datos personales como derecho autónomo, es decir en cuanto a separarlo del derecho a la intimidad, los primeros antecedentes se desarrollan en Europa, pues es en 1967 cuando se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a la intimidad. Como fruto de la Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre los derechos humanos y nuevos logros científicos y técnicos.

Un año más tarde se llevó a cabo la Conferencia Internacional de Derechos Humanos, en Teherán, el 22 de abril, en la cual se destacó el riesgo que implican los avances tecnológicos y científicos que pudieran afectar a derechos humanos básicos.

Es a partir de esta preocupación que como en Alemania en el Bundesland de Hesse se adopta en el año 1970 la Ley sobre Tratamiento de Datos Personales; con el propósito de regular el funcionamiento de las bases de datos de la administración pública.

[1] "Proceso legislativo de la Ley Federal de Protección de Datos Personales en Posesión de Particulares", *Suprema Corte de Justicia de la Nación, http://www2.scjn.gob.mx/AccesoInformacion/UnProcLeg.asp?nIdLey=75562&nIdRef=1&nIdPL=1&cTitulo=LEY FEDERAL DE PROTECCION DE DATOS PERSONALES EN POSESION DE LOS PARTICULARES&cFechaPub=05/07/2010&cCateg=LEY&cDescPL=EXPOSICION DE MOTIVOS*

Tres años después, siguiendo la misma línea de protección, el Parlamento Sueco emitió su primera ley nacional "Data Act", que también surgió como una forma de proporcionar a los ciudadanos algunas garantías ante el almacenamiento de datos en forma global por el Estado, que se venían utilizando con fines de vigilancia y prevención del delito;[2] es así que se considera la primera ley realmente orgánica y completa sobre protección de la intimidad frente a la informática y sobre el control de los bancos de datos.[3]

No solamente Europa se ocupó de la protección de datos ya que el primer antecedente en el continente americano lo encontramos en Estados Unidos, al aprobarse en 1974 la Privacy Act, la cual estableció normas para la protección de los datos en poder del Estado, su objetivo era prevenir el robo de identidad y fraudes. Existieron intentos de extender la protección al sector privado, sin embargo el Congreso no lo permitió.

Regresando a Europa, en 1976 el Comité de Ministros del Consejo Europeo, motivado por la investigación de la normatividad que existía en materia de protección de la privacidad y derechos conexos en relación con los avances tecnológicos, elaboró el texto de la Convención para la Protección de los Individuos con Relación al Procesamiento Automático de Datos Personales, conocida como la Convención de Estrasburgo, la cual fue suscrita por 21 Estados europeos.

Siguiendo esta Convención, surge la primera consagración constitucional del derecho a la protección de las personas frente a la informática en la Constitución de Portugal de1976, específicamente en su artículo 35 consagró una restricción al poder del Estado en la utilización de la informática y garantizó expresamente el acceso de los ciudadanos a las informaciones que, respecto de ellos, constasen en órganos o entidades estatales o privados, pudiendo exigir la rectificación o actualización de aquéllas; asimismo prohibió, además, el acceso de terceros a

[2] Gils Carbó, Alejandra M., *Régimen legal de las bases de datos y hábeas data*, Argentina, Ed. La Ley, 2001, p. 4.
[3] Rebollo Delgado, Lucrecio, *El derecho fundamental a la intimidad*, España, Ed. Dykinson, 2000, p. 189.

ficheros con datos personales y su respectiva interconexión, así como también los flujos de datos transfronterizos, salvo en los casos excepcionales previstos por la ley. Por último, proscribió la utilización de la informática en el tratamiento de datos referentes a convicciones filosóficas o políticas, filiación partidaria o sindical, fe religiosa o vida privada, excepto cuando se trate del procesamiento de datos estadísticos no identificables individualmente.

No obstante haber sido la primera Constitución en haber reconocido expresamente la necesidad de proteger a las personas frente a los riesgos informáticos, el desarrollo legislativo del precepto constitucional se prolongó 15 años, dictándose en abril de 1991 la Ley número 10 sobre "protección de datos personales frente a la informática".[4]

El primer gran consenso internacional en materia de protección de datos personales se dio en el Simposio de Viena en 1977, organizado a instancias del Grupo de Expertos sobre Bancos de Datos de la Organización para la Cooperación y el Desarrollo Económico (OCDE). El Simposio de Viena recogió un conjunto de principios básicos que, en términos generales, han permanecido y continúan vigentes hasta la fecha, con ligeras variantes.

Estos principios reconocen (a) la necesidad de que la información fluya de forma regulada entre los países; (b) que es legítimo que los países impongan regulaciones para el flujo de información que pueda resultar contraria al orden público, o que atente contra la seguridad nacional; (c) que el flujo de información tiene un valor económico intrínseco importante para las economías de los países; (d) que los países deben adoptar medidas de seguridad mínimas para la protección de la información, así como regular sobre la protección de dicha información, para evitar su uso o aprovechamiento ilegítimos; y (e) que los países

[4] Bazán, Víctor, "El Habeas Data, el Derecho a la Autodeterminación Informativa y la Superación del Concepto Preinformático de la Intimidad", *Boletín Mexicano de Derecho Comparado*, México, núm. 94, enero-abril 1999, *http://www.juridicas.unam.mx/publica/rev/boletin/cont/94/art/art1.htm*

(particularmente los países miembros de la OCDE) deben asumir un compromiso de adopción de principios generales para la protección de datos personales.

Posteriormente aparece la Ley Nacional Alemana en 1977, a partir de la cual el fenómeno protector se fue difundiendo por el resto del continente europeo; como fue el caso de Francia que dictó igualmente una ley sobre informática y libertades, la Ley 78/17 de Informática, Ficheros y Libertades, del 6 de enero de 1978.

Siguiendo el ejemplo legislativo, otros países europeos emitieron regulación en la materia, tales como Dinamarca, con las leyes sobre ficheros públicos y privados (1978); Austria, con la Ley de Protección de Datos (1978); y Luxemburgo, con la Ley sobre la utilización de datos en tratamientos informáticos (1979).[5]

A nivel supranacional, la Organización para la Cooperación y el Desarrollo Económico (OCDE) en virtud de la preocupación que el surgimiento de la tecnología de la información, como internet, representaba para el avance del surgimiento de una sociedad global de la información, crea el primer instrumento a este nivel, que analiza a profundidad el derecho a la protección de datos de carácter persona, esto es las "Directrices Relativas a la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales (Guidelines)", adoptada el 23 de septiembre de 1980.

Su adopción se funda en la constatación, por parte del Consejo de la OCDE, de la inexistencia de uniformidad en la regulación de esta materia en los distintos Estados miembros, lo que dificultaba el flujo de los datos personales entre los mismos.

Dichas Directrices tuvieron el carácter de recomendaciones que los Estados adherentes fueron incorporando a sus legislaciones, promoviendo también su adopción por el sector privado. Este modelo sirvió de base para que el 29 de

[5] Ornelas Núñez, Lina y López Ayllón Sergio, "La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo", *http://www.seminariodatospersonales.ifai.org.mx/index.php/materia-del-seminario*

enero de 1981 la Subcomisión para la Prevención de la Discriminación de las Naciones Unidas (ONU), aprobara sus propias directrices sobre ficheros de datos personales tratados informáticamente.[6]

Posteriormente la ONU emite la Resolución 45/95 de 14 de diciembre de 1990, conteniendo fundamentalmente una lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial, entre otros, los de licitud, exactitud, finalidad, acceso y no discriminación.

Son igual de importantes, los principios emitidos por el Foro de Cooperación Económica Asia Pacífico (APEC). Uno de los grupos formados en este organismo, es el Grupo de Manejo del Comercio Electrónico (ECSG) establecido en febrero de 1999, y que dentro de sus principales actividades está el desarrollo de legislaciones y políticas compatibles entre las economías en el campo de la Privacidad, para lo cual ha desarrollado los lineamientos generales en la materia con el fin de que los mismos sean contemplados y establecidos en los cuerpos legales correspondientes y con esto lograr un flujo de datos seguro y sin obstáculos.

Los principios desarrollados para el Marco de Privacidad de APEC se basan en las Recomendaciones de la OCDE. Estos principios tienen como fin los siguientes aspectos: proteger la Privacidad de información personal; prevenir la creación de barreras innecesarias al flujo transfronterizo de datos; fomentar la uniformidad por parte de empresas multinacionales en los métodos utilizados para la recolección, uso y procesamiento de datos personales; fomentar los esfuerzos nacionales e internacionales para promover y hacer cumplir las disposiciones legales de protección de datos personales.

Las normas a las que hemos referido en este apartado si bien no son todas las que en materia de datos se han promulgado, si las consideramos como las más destacadas para comprender la evolución de este derecho. Como pudimos

[6]Gils Carbó, Alejandra, *op. cit*., nota 2, p. 34.

observar el principal objetivo de la protección de datos en un inicio, fue protegerlos frente a las arbitrariedades del Estado, para posteriormente hacer énfasis en las posibles vulneraciones a que puede dar lugar el uso de las nuevas tecnologías.

Estas normas son objeto de una clasificación doctrinaria propuesta por Fappiano, quien las divide en generaciones atendiendo a los diversos objetivos que pretendían alcanzar:[7]

a) Primera Generación: las normas pertenecientes a esta generación tienen como objetivo garantizar los derechos individuales estableciendo determinados límites al empleo de la informática. Se interpretó que la eficacia de la protección reposaba en la autorización previa del banco de datos y en el posterior control de su gestión mediante órganos específicos de vigilancia. Era la época de las computadores escasas y de hardwares voluminosos, y, por consiguiente, localizables con facilidad. Por ejemplo:

   - ✓ Datenschultz, del Land de Hesse de 1973
   - ✓ Landesdatenschutgesetz, de Rumania-Palatinado de 1977.
   - ✓ Data sueca de 1973.

b) Segunda Generación: las normas de la segunda generación centran su inquietud en asegurar el derecho de acceso de las personas a las informaciones que les conciernen, mostrando especial atención por la calidad de los datos y no del hardware que los memoriza, mediante cláusulas especificas de protección de las informaciones consideradas sensibles por su directa incidencia sobre la vida privada o sobre el ejercicio de las libertades. Por ejemplo:

   - Privacy act de 1974
   - Informatique aux fichiers et aux libertés francesa de 1978
   - Constituciones de Portugal de 1976 artículo 35

[7] Gozaini, Osvaldo Alfredo, Habeas Data. Protección de datos personales, Argentina, Rubinzal-Culzoni Editores, 2000, pp. 119-120.

- Constitución de España de 1978 artículo 18.4

c) Tercera Generación: las normas de la última generación se hacen cargo de los cambios en la tecnología provocados por la revolución microinformática y, también de la necesidad de conciliar la defensa de los datos personales con las exigencias de una sociedad en la que la trasmisión de informaciones constituye un compromiso social, económico, político y cultural ineludible; es la época de las computadoras personales. Por ejemplo:

   - Convenio Europeo de 1981
   - Data Protection Act Inglesa de 1984

Vista la clasificación, observamos que los objetivos que persiguen las normas están condicionados al desarrollo tecnológico, pues en la primera generación en que la informática se encontraba en sus inicios, lo que se buscaba era limitar el uso de la misma en beneficio de derechos individuales; en tanto que la segunda generación busca que la información que sea objeto de tratamiento pueda ser controlada por su titular a efecto de asegurar que sean datos de calidad, así como garantizar una mayor protección a aquellos que se consideran como sensible. Por último la tercera generación no se preocupa solo por limitar el uso de la informática o por proteger a la información de las personas, sino que intenta lograr un equilibrio entre el potencial desarrollo de la informática frente a la efectiva protección de los datos personales, un objetivo que en muchas ocasiones resulta polémico al enfrentarse a un conflicto de intereses.

Como dijimos al principio del capítulo, con la revisión histórica lo buscábamos era tener una visión global de la protección de datos personales, hagamos el mismo ejercicio pero en cada uno de los Estados materia del presente trabajo, en lo particular.

4.2 Derecho Español

El derecho español ha previsto desde su Constitución la protección de los datos personales, sin embargo por los compromisos que ha adquirido frente a la Comunidad Europea, es que ha tenido que adecuar su legislación no solamente a lo estipulado en su texto constitucional, sino a la normativa europea.

En este apartado haremos primeramente referencia a lo previsto por la Constitución de 1978, para posteriormente ver cómo ha sido desarrollado el precepto constitucional en la legislación española. Y para concluir con el apartado de España una vez vistos los antecedentes, haremos alusión a los procedimientos previstos para ejercer los derechos ARCO en España.

4.2.1 La Constitución Española de 1978

En este apartado dedicado a la protección de datos personales prevista en la Constitución de 1978, haremos alusión en primer lugar a las características generales de la misma, y posteriormente al precepto que prevé el tema en cuestión.

La Constitución de España fue aprobada por Las Cortes en sesiones plenarias del Congreso de los Diputados y del Senado celebradas el 31 de octubre de 1978; ratificada por el pueblo español en referéndum de 6 de diciembre de 1978 y sancionada por S. M. el Rey ante Las Cortes el 27 de diciembre de 1978.

La Constitución de 1978 se singulariza en primer término por ser la primera Constitución en España obra del pueblo español en su conjunto y no de una facción de él frente al resto, fruto entonces del consenso y no de la imposición, toda vez que es promulgada hacia finales del período histórico de autoritarismo, carente de libertades.

En segundo lugar, la Constitución se caracteriza por conceptualizarse como una norma jurídica suprema, es decir, la que prevalece sobre todas las demás, la que domina a todas, las articula, les da su sentido, dirige su interpretación, las sitúa en su lugar propio en el seno del ordenamiento: una norma *normarum.*[8]

Podría pensarse que esta no es ninguna peculiaridad tratándose de un texto constitucional, sin embargo, en el tiempo en que fue promulgada si lo era, ya que en el periodo de autoritarismo en el que se vivía, la Constitución no tenía dicho reconocimiento en el ordenamiento normativo.

Al ser una norma que culmina con un período de imposición, el constituyente buscaba que el nuevo texto constitucional estableciera la justicia, la libertad y la seguridad y el bien de cuantos integraban la nación española, objetivos que, sólo si ella misma funcionaba efectivamente como una norma, podrían lograrse. Asimismo consolidar un Estado de derecho, proteger a todos los españoles y pueblos de España en el ejercicio de los derechos humanos, sus culturas y tradiciones, lenguas e instituciones.[9]

Es bajo estas premisas del constituyente y del movimiento popular que animaron la transición política hacia la democracia en los años 1975-1978; que la Constitución de España se comprende a sí misma como una Constitución de derechos; pues a la par de la tarea de reconciliación nacional y de la restitución del autogobierno a las nacionalidades y regiones, los derechos fundamentales figuraron como una de las aspiraciones básicas para el nuevo texto normativo.

No obstante la visión garantista de esta Constitución es una de sus principales particularidades, en la historia del constitucionalismo español hubo varios intentos de consolidar esta visión, tales como la Constitución de 1869 la cual representa el primer intento de una monarquía democrática parlamentaria, así como en la Constitución republicana de 1931; la Constitución de 1876 la de más larga

[8] García de Enterría, Eduardo, "La Constitución Española de 1978 como pacto social y como norma jurídica", *Boletín Mexicano de Derecho Comparado*, México, núm. Conmemorativo, 2008, *http://www.juridicas.unam.mx/publica/rev/boletin/cont/123.5/cnt/cnt16.htm*
[9] *Ídem.*

duración en la historia constitucional de España, y que posibilitó una cierta cultura de determinados derechos, en particular de las libertades públicas de expresión y asociación, si bien con unos instrumentos jurídicos bastante más sencillos.[10]

Estos intentos demuestran el interés del constituyente español por garantizar los derechos actualmente denominados fundamentales, lo cuales en la nueva Constitución representan el pilar del orden jurídico español vigente.

Continuando con el aspecto garante, la Constitución de 1978 es uno de los primeros textos constitucionales que introduce la protección de los datos frente al uso de la informática, como respuesta a los crecientes peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos; tomando como ejemplo la Constitución portuguesa.

El artículo específicamente que consagra la protección de datos personales es el 18 en su apartado cuarto; en el cual se emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Cabe aclarar que tal limitación no era en el sentido de prohibir el uso de la informática, sino lograr el justo equilibrio entre su uso y la protección de la intimidad de los españoles.

Se hace preciso delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas.

[10] Clavero, B., Manual en Cruz Villalón, Pedro y Pardo Falcón, Javier, "Los Derechos Fundamentales en la Constitución Española de 1978", *Boletín Mexicano de Derecho Comparado*, México, núm. 97, enero-abril de 2000, *http://juridicas.unam.mx/publica/rev/boletin/cont/97/art/art2.htm#N1*

Una vez visto cómo la Constitución vigente en España ha acogido el reconocimiento a la protección de datos personales, veamos en el siguiente apartado la manera en que el legislador ha plasmado el sentido constitucional en la norma secundaria.

4.2.2 Antecedentes legislativos en materia de protección de datos personales

Respecto a los antecedentes legislativos, veremos en este capítulo que son dos las normas que el legislador ha promulgado obedeciendo al mandato constitucional del artículo 18.4 y a lo estipulado por la Comunidad Europea; a fin de coadyuvar con el desarrollo y progreso de la implementación del derecho a la protección de datos personales en España.

En España a pesar de contar con un precepto constitucional que protege los datos personales, el legislador no promulgó ninguna legislación respecto al tema, sino hasta después del Convenio 108, que enseguida veremos.

Es en 1967 cuando se constituyó en el seno del Consejo de Europa, una Comisión Consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a no sufrir injerencias en la vida privada, derecho que se había ya recogido en la Declaración Universal de Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos del año 1966.

De tal Comisión Consultiva surgió la resolución 506 de la Asamblea del Consejo de Europa, referente a los derechos humanos y los nuevos logros científicos y técnicos; la cual respondía a una inquietud existente en todo el Continente. En tal resolución se encuentra el verdadero origen del movimiento legislativo que desde

entonces recorrerá Europa y el mundo entero, en materia de protección de datos.[11]

Continuando con el movimiento legislativo, en la década de los años ochenta cuando surgen los instrumentos normativos en los que se plasma un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como las medidas de seguridad a observar por parte de los responsables de los ficheros. Es precisamente en esta década cuando el Consejo de Europa promulgó el Convenio 108 de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal; con el propósito de garantizar a los ciudadanos de los estados contratantes, el respeto de sus derechos y libertades, en particular, el derecho a la vida privada frente a los tratamientos de datos personales, conciliando el respeto a ese derecho y la libre circulación de la información entre los estados.

De esta forma, el Convenio 108 constituye el primer instrumento de carácter vinculante para los Estados en el que se plasman los principios de protección de los datos de carácter personal, sin embargo dichos principios constituyen el piso mínimo, que posteriormente sería desarrollado por los Estados miembros.

Entre los postulados más importantes contenidos en este Convenio encontramos los siguientes:[12]

1. La obtención de las informaciones deben tratarse según un principio de lealtad entre las partes y de manera lícita.
2. Debe asegurarse la exactitud de las informaciones que se archiven.
3. El propósito de la obtención de estos datos debe darse a conocer a los individuos (el principio de finalidad).
4. La prohibición del registro de informaciones sensibles.
5. Un derecho de acceso y rectificación de los datos.

[11] Basterrra, Marcela I., *Protección de datos personales. Ley 25.326 y Dto. 1558/01 comentados Derecho Constitucional Provincial Iberoamericana y México,* Argentina, Ed. Ediar, 2008, p 13.
[12] Ovilla Bueno, Rocío, *La protección de los datos personales en México*, México, Porrúa, 2005, p. 16.

6. Los Estados deben garantizar la seguridad de las bases de datos.

A partir de estos principios se desprende que el Convenio busca armonizar los valores fundamentales del respeto a la vida privada y la libre circulación de la información entre los pueblos. Asimismo, el Convenio pretende compatibilizar en todo momento la protección del derecho a la intimidad personal con la liberación de los flujos de datos entre Estados partes, siendo así que la libre circulación de los datos de carácter personal entre los Estados signatarios sólo decaerá en dos supuestos:

a. Cuando la protección de los datos de carácter personal no sea equivalente en la otra parte.
b. Cuando la transmisión de los mismos se realice a un tercer Estado que no sea parte en el Convenio.

Siguiendo la línea trazada por este Convenio, en 1990 eran ya quince Estados miembros de la Comunidad Europea que habían adoptado sus propias leyes sobre la materia. Esta expansión resultó potenciada por la necesidad de los países europeos de eliminar barreras comerciales que pudieran generarse por incompatibilidades legislativas; además de otras razones de naturaleza política vinculadas a los acuerdos de Schengen, que establecieron un régimen de cooperación policial a través de un sistema informático llamado SIS; aduanera y en materia de inmigración, para compensar la supresión de los controles en las fronteras interiores, lo cual exigía una ley uniforme, a fin de llevar a cabo el objetivo común de constituir un mercado interior con una frontera europea única.[13]

El eje marcado por el Convenio 108, ratificado el 31 de enero de 1984 por España, así como los acuerdos de Schengen sirvieron de base para la promulgación el 29 de octubre de 1992 de la Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Sin olvidar el influjo de la Carta de Derechos Fundamentales de la Unión Europea, con la cual la

[13] Gils Carbó, Alejandra, *op. cit.,* nota 2, p. 35.

protección de los datos de carácter personal se configuró como un derecho fundamental y como un derecho autónomo del derecho a la intimidad de las personas.

Dicha ley Orgánica además tuvo como precedente la sentencia STC 254/1993[14] de 20 de julio de 1993, dictada por el Tribunal Constitucional Español; a la cual dedicaremos los siguientes párrafo a efecto de comprender el por qué sirvió de antecedente a la LORTAD.

Haciendo un esbozo sobre los planteamientos del caso, en primer lugar diremos que el acto impugnado es la denegación por parte del Gobernador Civil de Guipúzcoa y del Ministro del Interior, respecto de la solicitud de información relativa a los datos de carácter personal existentes en fichero automatizados de la Administración del Estado, presentada por Francisco Javier Olaverri Zazpe.

El caso comienza con la solicitud de Olaverri en febrero de 1986, dirigida al Gobernador Civil para solicitar lo siguiente:

1) Que se le comunicara si la administración del Estado o cualquier organismo de ella dependiente dispone de ficheros automatizados donde figuraran sus datos de carácter personal.
2) Que en caso afirmativo se le indicara la finalidad principal de dichos ficheros, la autoridad que los controla y su resistencia habitual.
3) Que se le comunicaran los datos existentes en dichos ficheros referidos a su persona, de forma inteligente y sin demora.

Dichas pretensiones del actor encuadran dentro de lo dispuesto en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, suscrito en Estrasburgo el 28 de enero de 1981; mismo que sirvió de fundamento a la solicitud del actor.

[14] "STC 254/1993 de 20 de julio de 1993" , Congreso de los Diputados de España, *http://www.congreso.es/constitucion/ficheros/sentencias/stc_254_1993.pdf*

Sin embargo el Gobernador no se pronunció sobre la solicitud; por lo cual Olaverri recurrió a las siguientes instancias, es decir ante la Audiencia Territorial de Pamplona y ante el Tribunal Supremo; obteniendo de ambas una respuesta no favorable a su pretensión.

Ambas instancias coincidieron en su respectivo pronunciamiento sobre el tema, al considerar que no podía ser aplicado directamente al caso lo estipulado por una norma supranacional, en virtud de que para su aplicación práctica se requería de una actividad interna legislativa y reglamentaria que el Estado aun no había desarrollado.

Una vez que el recurrente había agotado todas las posibilidades ordinarias, interpuso el recurso de amparo ante el Tribunal Constitucional en julio de 1990, dando así lugar a la primera decisión del Tribunal Constitucional sobre la materia: la STC 254/1993, de 20 de julio.

El pronunciamiento del Tribunal en dicha sentencia toma como punto de partida lo citado en el artículo 8 del Convenio 108, así como lo prescrito en el artículo 10.2 de la Constitución de España, en el cual se establece la prevalencia de los tratados a la hora de interpretar las normas respecto a los derechos fundamentales.

Así también alude al artículo 18.4 de la Constitución de España, en el cual el Tribunal reconoce una doble función del contenido de este, por un lado representa una garantía del derecho a la intimidad, y por otro lado un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la “informática”. Esta libertad se garantiza mediante el control del uso de los datos personales insertos en un programa informático (habeas data).[15]

[15] Aguado Renedo, César, “La protección de los datos personales ante el Tribunal Constitucional Español”, *Revista Mexicana de Derecho Constitucional*, México, núm. 23, julio-diciembre de 2010,

Tal como se desprende de lo sustentado por el Tribunal, éste lo sigue considerando como una extensión del derecho a la intimidad, con la salvedad de que lo concibe como un aspecto positivo y no solamente como negativo o de exclusión, es decir un derecho de control sobre los datos a la propia persona.

Sustentada la resolución del Tribunal en los argumentos señalados, concluye diciendo que *"es suficiente con constatar que, al negarse a comunicarle la existencia e identificación de los ficheros automatizados que mantiene con datos de carácter personal, así como los datos que le conciernen a él personalmente, la administración demandada en este proceso vulneró el contenido esencial del derecho a la intimidad del actor, al despojarlo de su necesaria protección".*

Finalmente en la sentencia STC 254/1993 aprobada por la mayoría de los miembros de la Sala sentenciadora del Tribunal Constitucional, se concede el amparo al recurrente e impone la obligación de aportarle la información solicitada.

Esta determinación es tomada no importando que no se haya desarrollado legislativamente el contenido del artículo 18.4 de la Constitución, toda vez que las facultades de información forman parte del derecho a la intimidad, y por lo tanto merece ser salvaguardado por el Tribunal Constitucional.

Pocos meses antes de dictarse la SCT 254/93, el legislador español dio cumplimiento al mandato constitucional referido en el artículo 18.4 de la Constitución de España mediante la promulgación de la citada Ley Orgánica reguladora del Tratamiento Automatizado de Datos LO 5/ 1992.

Esta ley supuso innovar el ordenamiento español en relación con la protección de datos mediante el establecimiento por primera vez de un régimen jurídico sobre tal materia, régimen que estableció los dos elementos fundamentales en los que se basa el sistema de protección:[16]

---

http://biblio.juridicas.unam.mx/revista/pdf/CuestionesConstitucionales/23/ard/ard1.pdf

[16] *Ídem.*

1) Una agencia de protección de datos, caracterizada como ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las administraciones públicas en el ejercicio de sus funciones.
2) Un registro general de protección de datos integrado en ella, en el cual han de figurar todos los ficheros informáticos que se generen y al que pueden acceder individuos.

A pesar de ser considerados los dos argumentos citados como pilares de la protección de datos, hemos dicho que en México se consideró poco necesaria la creación de un registro, por representar un incremento burocrático.

Esta primera Ley Reguladora de la Protección de Datos en España tuvo asimismo importancia de forma indirecta, en cuanto fue recurrida por su supuesta inconstitucionalidad fundada en la invasión de competencias autonómicas,[17] recurso que dio lugar a la importante sentencia SCT 290/2000, del 30 de noviembre de 2000 del Tribunal Constitucional. Recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal.[18]

Los recursos de inconstitucionalidad fueron promovidos por Diputados del Partido Popular, el Defensor del Pueblo, el Consejo Ejecutivo de la Generalidad de Cataluña y el Parlamento catalán.

Los dos primeros centran sus argumentos en motivos sustantivos, es decir, parten de la idea de que el apartado 4 del artículo 18 de la Constitución de España garantiza un nuevo derecho fundamental autónomo, la autodeterminación informativa.

[17] Interpusieron conflicto competencial el Parlamento y el Gobierno de Cataluña

[18] "Sentencia 290/2000, de 30 de noviembre de 2000 del Tribunal Constitucional", *Agencia Española de Protección de Datos, http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/Sentencia2901.PDF*

En tanto que el Consejo y el Parlamento tachan algunos preceptos de la Constitución por haber infringido el orden constitucional de reparto de competencias.

Los argumentos particulares del Defensor del Pueblo, se refieren a que la ley era inconstitucional por permitir la cesión de datos sin el consentimiento del titular, previendo regular dichos supuestos mediante normas reglamentarias. Así como por imponer excepciones al ejercicio de los derechos de acceso, rectificación y cancelación escasamente delimitadas y distintas a las fijadas en el Convenio de Estrasburgo de 1981.

Por lo que respecta a los Diputados del Partido Popular al igual que el Defensor del Pueblo veían en el derecho a la intimidad una doble vertiente, por un lado como una función negativa por parte del Estado, y por el otro una positiva que permitía controlar la información referida a uno mismo.

En el recurso de inconstitucionalidad que los Diputados interpusieron argumentaban que había artículos de la Ley Orgánica que vaciaban de contenido los límites que debían imponerse a la informática; por el empleo de conceptos jurídicos indeterminados en las excepciones al ejercicio de derecho a la autodeterminación informativa. Así mismo los diputados refiriendo a los datos sensibles, consideraban inconstitucional la posibilidad de su tratamiento por parte de las Fuerzas y Cuerpos de Seguridad el Estado.

Particularmente el Consejo tachó de inconstitucional el hecho de que la Ley reservaba a la Agencia de Protección de Datos las potestades de ejecución de la Ley respecto a los ficheros; la inscripción para cualquier fichero de titularidad pública, sin hacer distingo alguno, en el Registro General dependiente de la Agencia de Protección de Datos; así como por la exclusión de la Comunidad Autónoma en las funciones inspectoras que la Ley Orgánica atribuía en exclusiva a la Agencia de Protección de Datos. Con estas facultades exclusivas de la Agencia, el Consejo considera que se vulnera la distribución de competencias señalada en la Constitución, pues impedía que la Comunidad Autónoma pudiera

crear un ente donde se inscribieran los ficheros creados por la Administración Local catalana; asimismo que las facultades de inspección pudiesen ser efectuadas por un órgano local.

El Consejo estimaba que era procedente la distribución de competencias entre el Estado y las Comunidades Autónomas siempre que la misma se hiciera atendiendo a la naturaleza y utilidad de la información objeto de tratamiento.

En tanto que el Parlamento de Cataluña, centró sus argumentos prácticamente en el mismo sentido que el Consejo, al considerar inconstitucional la distribución de competencias propuesta por la ley, al quebrantar el principio de autonomía de las comunidades autónomas.[19]

Los argumentos sostenidos por el Abogado del Estado en defensa de la Constitucionalidad de la Ley, versan en el sentido de no considerar que el artículo 18.4 de la Constitución española consagre algún derecho fundamental, pues simplemente lo ve como un mandato para limitar el uso de la informática, garantizando los derechos al honor y a la intimidad. Igualmente a los derechos de información, acceso, rectificación, cancelación y cesión los concibe como instrumentos que coadyuvan en la efectividad del precepto constitucional, sin considerarlos como derechos fundamentales, sino como derechos legales. Razón por la que argumenta que no gozan ni de la protección del amparo judicial ni del constitucional.

El Tribunal Constitucional español declaró que los recursos promovidos por los Diputados y por el Defensor del Pueblo habían quedado sin materia al haber sido derogada la ley presuntamente inconstitucional; en tanto que desestimó los recursos interpuestos por el Consejo y el Parlamento, por considerar que los preceptos recurridos eran constitucionales. Tomando en cuenta que la Constitución ha atribuido a los derechos fundamentales la necesidad de que sean protegidos, incluso en el ámbito del reparto competencial; asimismo las funciones

[19] Aguado Renedo, César, *op. cit.,* nota 15.

y potestades que la Ley había atribuido a la Agencia de Protección de Datos, se hizo con el propósito de asegurar su respeto en todo el territorio nacional mediante el establecimiento de condiciones básicas que hagan posible que el disfrute de tales derechos sea igual para todos los españoles; imponiendo así un límite a las potestades de las Comunidades Autónomas. Así también específicamente tal distribución se justifica en el sentido de que fueran respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada.

De esta sentencia es importante el pronunciamiento del Tribunal Constitucional al reconocer la protección de datos como un derecho fundamental que debe ser garantizado a todos los españoles, superponiéndolo a la *vacatio legis* del texto constitucional, al no preverlo expresamente. Como lo señala el Magistrado Manuel Jiménez de Parga y Cabrera en su voto particular, la última clase de derechos (los creados por la jurisprudencia) tiene especial relieve. Los derechos no-escritos han de ser tutelados por la jurisprudencia, ya que las Constituciones proporcionan al intérprete un punto de apoyo, unas palabras (escasas a veces, lapidarias), sobre los que hay que efectuar, mediante una actividad creadora, la construcción del derecho fundamental.

Y es bajo esta perspectiva de los derechos fundamentales que el Tribunal Constitucional en la presente sentencia, consagra el derecho a la protección de datos personales como un derecho fundamental que puede desprenderse de la interpretación del artículo 18.4 de la Constitución de España.

Para concluir con el estudio de esta ley, cabe decir que tardó siete años en disponer de su desarrollo reglamentario, que llegó con el Real Decreto 994/1999, de 11 de junio: Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal (RMS). Sin embargo la vigencia de la ley sólo duró siete años, pues fue derogada por la Ley 15/1999, 13 de diciembre, de Protección de Datos.

Es importante señalar que esta ley no fue derogada por resultar inadecuada, sino por la obligada transposición[20] de la directiva europea 1995/46/CE, de 24 de octubre, sobre protección de las personas físicas en lo referido al tratamiento y libre circulación de sus datos personales; a la que haremos alusión en los párrafos siguientes.

Es debido a esta transposición que en 1990 el Parlamento Europeo y el Consejo de la Unión Europea convocaron a una comisión de expertos que debatieron durante 5 años para elaborar un texto referido exclusivamente a la protección de datos de carácter personal. Finalmente se aprobó la Directiva[21] 95/46 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.

El proyecto de Directiva 95/46 se inspiró esencialmente en la doctrina constitucional alemana y en la ley francesa de 1978; teniendo dos objetivos para su promulgación, por un lado ampliar los principios ya recogidos en otras normas internacionales, otorgando un mayor nivel de protección dentro de la Comunidad, sin disminuir el ya existente; y por el otro adoptar un marco comunitario que garantizara la libre circulación de los datos de carácter personal, no pudiendo los estados miembros de la Unión Europea invocar el derecho a la protección de datos como justificación para impedir dicha libre circulación; esto es, se pretendía conciliar la libre circulación de información como instrumento necesario para el

[20] En los ordenamientos de los países miembros de la Comunidad Europea, es obligatorio transponer las directivas que ésta acuerde, esto es, proceder a regular en el ámbito interno la materia objeto de la directiva, siguiendo las indicaciones señaladas en ellas, con el fin de lograr los objetivos que se han acordado al respecto.

[21] Directiva: es una norma legislativa europea destinada a los Estados miembros, que una vez adoptada a escala europea, cada Estado miembro debe garantizar su aplicación efectiva en su sistema jurídico, la cual dispone el resultado final, y la forma y los métodos de aplicación corren a cargo de cada Estado miembro. En principio, una directiva entra en vigor mediante las medidas nacionales de aplicación. Sin embargo, cuando un Estado miembro no haya aplicado una directiva, parte de lo dispuesto en ella puede tener efectos directos. Esto significa que si una directiva confiere derechos directos a las personas físicas, estas podrán alegar ante un juez tal directiva sin tener que esperar a su aplicación en la legislación nacional. Además, si las personas físicas opinan que se han visto perjudicadas por una incorrecta aplicación de la directiva por parte de las autoridades nacionales, tendrán derecho a denunciarlas por daños y perjuicios, ante tribunales nacionales. Carranza Torres, Luis R. *Hábeas data. La protección jurídica de los datos personales.* Argentina, Editorial Alveroni, 2001, pp. 96-97.

progreso de las actividades económicas, políticas y sociales; con la necesaria tutela de los derechos y libertades de los ciudadanos, pero sin que el recurso a estos derechos pudiera constituir nunca por sí sólo una traba u obstáculo al progreso informático.

Para la elaboración del texto de la Directiva en comento, el Parlamento Europeo y el Consejo de la Unión Europea tomaron como elementos el objetivo de la Comunidad definido en el Tratado constitutivo de la Unión Europea, es decir busca lograr la unión estrecha de los pueblos europeos, a fin de eliminar las barreras para asegurar el progreso económico y social. Mediante la regulación homogénea en la materia se busca proteger los derechos fundamentales de las personas físicas sin limitarlos en función de su nacionalidad o residencia; así como asegurar la libre circulación de los datos dentro del mercado interno, protegiendo los derechos fundamentales; así como para facilitar la cooperación científica y técnica.

Es así como la Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales; al crear un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. Con ese objetivo, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.[22]

La Directiva previó un plazo de tres años a partir de su entrada en vigor, para que los Estados miembros pudieran aplicar de manera progresiva las nuevas disposiciones nacionales mencionadas a todos los tratamientos de datos ya existentes; se concedió a los Estados miembros un período suplementario que expiraría a los doce años de la fecha en que se adopte la presente Directiva, para

[22] Instituto de Acceso a la Información Pública y protección de datos del DF, "Manual de autoformación sobre la ley de protección de datos personales para el Distrito Federal" *Colección Capacitación a Distancia* México, núm. 05, 2009, *http://www.infodf.org.mx/capacitacion/publicacionesDCCT/manual5lpdpdf/manualdatospersonales.pdf*

garantizar que los ficheros manuales existentes en dicha fecha se ajustaran a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese período transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento.

A efecto de compeler a los Estados miembros a dictar sus propias legislaciones, y a los que ya las tuvieran a adecuarlas, vencido el plazo señalado en el párrafo anterior, estaría prohibida la transferencia internacional de datos a países de la Comunidad Europea que no tuvieran una protección equivalente.

Con la finalidad de asegurarse del cumplimiento por parte de los Estados miembro, la Directiva previó la creación de un Grupo de Trabajo[23], para que continuara con la elaboración y actualización de las reglas contenidas en la Directiva; el Grupo tiene asignada la tarea de informar a sobre las divergencias de las legislaciones y prácticas de los Estados miembros a fin de evaluar el nivel de protección de terceras naciones. Cumple la función de buscar soluciones prácticas a los problemas planteados en el seno comunitario y facilita la labor de la Comisión para negociar diferencias con los países que no han instituido un régimen de protección.

La Directiva 95/46/CE, del Parlamento europeo y del Consejo de 24 de octubre de 1995, sobre protección de datos y libre circulación de esos datos dio lugar a la redacción de una nueva ley, la L.O.15/1999, de 13 de diciembre, de protección de datos de carácter personal, la cual entró en vigor el 14 de enero del año 2000, y a diferencia de su predecesora no solamente se circunscribe a los ficheros de carácter personal que se tratan en soportes automatizados, ya que su el ámbito de aplicación se extiende a todo tipo de ficheros, independientemente del soporte en el cual sean tratados, con el fin de proteger los derechos fundamentales y libertades públicas de los ciudadanos.

[23] Gils Carbó, Alejandra M., *op. cit*., nota 2, p. 37.

La mayoría de los preceptos de la Ley Orgánica 15/1999 son exactos a los de la Ley de 1992, sin embargo lo importante con esta ley no es limitar la informática, sino garantizar de forma efectiva los derechos fundamentales de las personas. La finalidad de la ley no es proteger los datos personales de los ciudadanos, sino la protección de estos en relación con el tratamiento de los mismos, para salvaguardar en último término la libertad de la persona y posibilitar su desarrollo sin interferencias.[24]

El contenido de esta Ley se consolida mediante el Reglamento de de desarrollo de la Ley Orgánica 15/1999 de 13 diciembre, de protección de datos de carácter personal, aprobado mediante el Real Decreto 1720/2007.

No obstante la norma antes referida es la vigente en España, en Europa los trabajos legislativos no han concluido con el estudio de la protección de los datos personales, y es así como en el año 2000 aparece la Carta de Derechos Fundamentales de la Unión Europea, aprobada por la cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza el 7 de diciembre de 2000, reconociendo entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8, cuestión que se retoma en el Tratado de Lisboa del año 2007.

Al igual que sucedió con la ley anterior, la ley 15/99 fue recurrida ante el Tribunal Constitucional por el Defensor del Pueblo. Los argumentos del Defensor fueron prácticamente en el mismo sentido que su recurso de inconstitucionalidad contra la ley 5/1992, pues estimó inconstitucional la posibilidad prevista en la ley de ceder los datos personales sin el previo consentimiento del titular; así como las excepciones fijadas al ejercicio de los derechos de acceso, rectificación y cancelación.

Por su parte el Abogado del Estado, considera que la cesión de datos entre administraciones públicas, sin el previo consentimiento del interesado, se justifica

[24] Garrida Domínguez, Ana*, Tratamiento de datos personales y derechos fundamentales*, 2ª ed., España, Editorial Dykinson S.L., 2009, p. 52.

por el principio de lealtad institucional y las reglas de acción y cooperación interadministrativa que imponen en ciertos casos el suministro de datos entre Administraciones Públicas para el ejercicio de las respectivas competencias.

El Tribunal Constitucional resuelve estimar el recurso de inconstitucionalidad y, en consecuencia declara inconstitucional apartado 1 del artículo 21 y el apartado 1 del artículo 24; en razón de considerar el derecho a la protección de datos como un derecho autónomo diferente en cuanto a función, objeto y contenido del derecho a la intimidad. El Tribunal señala la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado; siendo así que el consentimiento en la cesión de datos constituye uno de los derechos para hacer efectivo dicho control.

Es en este sentido que el Tribunal declara inconstitucional el primer precepto señalado porque la ley no ha fijado por sí misma, como le impone la Constitución en el artículo 53.1, los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas, sino que se ha limitado a identificar la norma que puede hacerlo en su lugar.

Así también se declara inconstitucional la utilización de términos imprecisos para formular las excepciones al ejercicio de derechos fundamentales; ya que a falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental, es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica.

Como puede apreciarse de la resolución del Tribunal Constitucional, lo relevante es el reconocimiento del derecho a la protección de datos personales como un derecho autónomo frente al derecho a la intimidad.

4.2.3 Ejercicio de los derechos ARCO

Visto el desarrollo legislativo de la protección de datos personales, hace falta aludir a la aplicación práctica mediante la cual se hace efectiva la protección de los derechos ARCO; es decir, los procedimientos previstos en la norma para ejercer estos derechos. Primeramente haremos algunas acotaciones referentes a lo plasmado en la ley 15/99 y desarrollados por su reglamento, respecto al procedimiento administrativo que debe efectuarse directamente frente al responsable del tratamiento; lo cual sigue la misma lógica que la ley pues el agotamiento de este procedimiento es presupuesto para poder instaurar el procedimiento de tutela de derechos.

4.2.3.1 Frente al responsable del tratamiento

La norma en la materia establece la posibilidad de acudir ante el responsable a efecto de solicitar el acceso a la información que pudiese estar siendo tratada por aquél, o bien como lo vimos en el capítulo anterior cuando la información sea incorrecta, incompleta, desactualizada poder solicitar la rectificación o en su caso cancelación de la información; o en el caso de no consentir el tratamiento de la información oponerse al mismo.

Para efectuar la solicitud, la ley no fija un formato único pero si señala los requisitos mínimos que el escrito debe satisfacer, los cuales son:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y,

en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

b) Petición en que se concreta la solicitud.
c) Dirección a efectos de notificaciones, fecha y firma del solicitante.
d) Documentos acreditativos de la petición que formula, en su caso, como en las solicitudes de rectificación y cancelación.
e) Para el caso particular de las solicitudes de rectificación, el titular deberá indicar a qué datos se refiere y la corrección que haya de realizarse.
f) En las solicitudes de cancelación se deberá indicar los datos que se pretende cancelar.
g) Tratándose de solicitudes de oposición, cuando no haya sido necesario el consentimiento del titular para el tratamiento, en la solicitud se deberán expresar los motivos fundados y legítimos que justifiquen el ejercicio de tal derecho.

En el supuesto que la solicitud no cumpla con estos requisitos, el responsable podrá solicitar que el titular subsane tal omisión.

Del inciso a) se desprende que la solicitud puede efectuarse directamente por el titular de los datos, o en su caso por un representante ya sea legal o .voluntario. Esta posibilidad podría parecer contraria a la finalidad de la protección de datos, pues se trata de un derecho personalísimo que evitar intromisiones indeseadas en la vida privada de las personas, por lo que la delegación hacia otros para conocer la información concernida podría resultar en si misma contradictoria, al habilitar un acceso más a lo que se pretende conservar secreto o confidencialidad; sin embargo en palabras de Osvaldo Gozaini el primer reclamo debe ser hecho por la persona afectada o que ostente un interés legitimo para ingresar al registro informativo, pudiendo discernir, en situaciones excepcionales -caso de incapacidad física o legal, impedimentos manifiestos, minoría de edad-, la

representación de un tercero. Éste a su vez, consigue legitimación por mandato, pero el acceso sólo podrá acordarse cuando actúe en interés y beneficio del afectado, y no para la satisfacción de intereses de terceros.[25]

Presentada la solicitud en comento, el responsable dispone de un mes para dar respuesta a la pretensión de acceso, mientras que para el caso de rectificación y cancelación dispone de diez días determinar la procedencia de la solicitud, y siendo procedente tendrá diez días más para hacer las adecuaciones correspondientes.

Finalmente si el responsable no diera respuesta a la solicitud o bien no se efectuaran las adecuaciones solicitadas sea total o parcialmente, el titular podrá interponer la reclamación ante la Agencia Española de Protección de Datos.

4.2.3.2 Procedimiento de tutela de los derechos ARCO

Agotada la vía administrativa frente a la responsable del tratamiento, el titular puede acudir al órgano de control; el cual de acuerdo a la legislación española en materia de protección de datos tiene una triple función, una jurídica que abarca todo lo relativo a la defensa y protección de los derechos de los afectados; otra administrativa regulando los aspectos de gestión de la Agencia, recibiendo reclamaciones, proporcionando informaciones, publicaciones periódicas y una tercera, estrictamente de contralor imponiendo sanciones, ejerciendo la supervisión de los movimientos internacionales de datos y cooperando internacionalmente en materia de protección de datos.[26]

En este apartado rescataremos la función jurídica de la Agencia, pues el órgano que dará trámite al procedimiento de tutela de derechos; sin olvidar que en cada

[25] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 7, p. 412.
[26] Armagnague, Juan (Dir.), *Derecho a la información, habeas data e internet*, Argentina, Ediciones La Rocca, 2002, p. 400.

Comunidad Autónoma existe un órgano equivalente que se encargara de los procedimientos que encuadren dentro de su competencia.

El procedimiento es muy breve, pues comienza a instancia de parte con la presentación de la reclamación; una vez recibida ésta la Agencia correrá traslado al responsable del fichero para que en un plazo de quince días de respuesta a la misma.

Vencido el plazo señalado en el párrafo anterior, y previos los informes, pruebas y celebrada la audiencia, la Agencia resolverá la reclamación formulada, en un plazo no mayor a seis meses. Ante la falta de pronunciamiento de la Agencia se considerara que la pretensión resultó procedente; y en tal caso se requerirá al responsable para que en un plazo de diez días haga efectivo el ejercicio de los derechos, debiendo dar cuenta a la Agencia sobre el cumplimiento de la resolución dentro de los siguientes diez días.

Contra las resoluciones de la Agencia Española de Protección de datos procederá el recurso contencioso-administrativo.

De este procedimiento resalta que la redacción no prevea un plazo límite para interponer el escrito ante la Agencia, una vez finalizado el procedimiento frente al responsable, lo cual resulta benéfico para no obstaculizar el ejercicio de los derechos ARCO imponiendo un plazo, sin embargo consideramos que si lo que se busca es resolver una situación que nos está afectando, debe actuarse de inmediato.

4.3 Derecho Argentino

Sin lugar a dudas lo anteriormente expuesto respecto a los antecedentes en España nos servirán en este apartado, pues recobra importancia el artículo 18 apartado 4 de la Constitución española al haber sido una de las fuentes de derecho extranjero más utilizadas en el ciclo constituyente provincial que se abre

en Argentina a partir de 1985, y que precedió y sirvió de fuente a la reforma constitucional nacional de 1994.[27]

4.3.1 Reforma Constitucional de 1994

El tema en Argentina de una reforma constitucional cobra vigor con la reinstalación democrática en 1983. La idea reformista tuvo sus antecedentes durante el Gobierno del Presidente Alfonsín, quien constituyó el Consejo de Consolidación de la Democracia, integrado por figuras políticas e intelectuales de vastos espectros, a fin de que se fueran realizando estudios, debates y seminarios, para reunir los elementos de juicio necesarios para una posible Reforma Constitucional. Pero a pesar de todo, la crisis del gobierno radical fue opacando este proceso reformador, hasta que quedó prácticamente paralizado.[28]

Asimismo durante los primeros años del primer Gobierno justicialista (1989 – 1993), el partido gobernante elaboró a través de su Comisión de juristas, tres documentos que justificaban la necesidad y la oportunidad de la reforma y que se identificaron con la dirección y el sentido reformista del proyecto de reforma radical de 1986 y las reformas de las constituciones provinciales.

Durante el gobierno del Presidente Menem, a partir de 1989 el proceso reformador tomó nuevos impulsos motivados fundamentalmente por el tema de la reelección presidencial.

En 1993 aparece el primer Acuerdo de Menem y Alfonsín del 14 de Noviembre, mejor conocido como Pacto de Olivos (por la ciudad vecina a la Capital Federal donde, además de tener su sede la residencia presidencial, se habían entrevistado

[27] Carranza Torres, Luis R., *op. cit.,* nota 21, p. 27.
[28] Haro, Ricardo, "Perfiles Fundamentales de la Reforma Constitucional Argentina De 1994", Argentina, 21 diciembre de 1998, *http://www.catedrajuansola.com.ar/wp-content/uploads/2010/06/Ricardo-Haro.pdf*

los dos líderes); en sus respectivos caracteres de presidente de los Partidos Justicialista y Radical.

Dicho pacto explica el porqué y para qué de la reforma; ambos líderes coinciden en impulsar un proyecto de reforma constitucional sin introducir modificación alguna a las declaraciones, derechos y garantías de la primera parte de la constitución; la atenuación del poder del presidente mediante instituciones que lo limitaran y la modernización de ciertos contenidos que la hicieran más funcional.

A este pacto le sigue el Acuerdo de las comisiones asesoras de ambos partidos del 1º de Diciembre, y luego el segundo Acuerdo entre Menem y Alfonsín del 13 de Diciembre, conocido como Pacto de la Rosada, el cual detalla las materias a reformar y los procedimientos a seguir formando un núcleo de coincidencias básicas y mecanismos jurídico-político para garantizar la concreción de los acuerdos.

Este pacto luego toma forma legislativa mediante la Ley 24.309 sancionada por el Congreso de la Nación el 31 el mismo mes y año,[29] mediante al cual se declara formalmente la necesidad de reformar la Constitución Nacional de 1853 con sus respectivas reformas de 1860. 1866, 1898 y 1857.

Esta ley contenía tres partes fundamentales a saber:[30]

a. Cláusulas pétreas, es decir la parte de la Constitución que no puede ser modificada por la Convención, constituida por la parte dogmática de la constitución que comprende los artículos 1 al 35 contenidos en el primer capítulo de la Constitución, denominado “Declaraciones, derechos y garantías”
b. Núcleo de Coincidencias Básicas, que contiene los acuerdos alcanzados entre Menem y Alfonsín. Entre los temas incorporados

[29] *Ídem.*
[30] Montbrun, Alberto et al, “Apuntes Sobre la Reforma Constitucional de 1994”, *Material de estudio de los Cursos de Equivalencia del Instituto Universitario de Seguridad Pública, http://www.albertomontbrun.com.ar/archivos/reforma_constitucional_de_1994.pdf*

están: la reelección inmediata del presidente por un período, en forma directa pero con doble vuelta; la creación de la figura del jefe de gabinete; la incorporación del tercer senador por la minoría con elección directa por provincia; la creación del Consejo de la Magistratura y un nuevo procedimiento de remoción de magistrados; la regulación de los decretos de necesidad y urgencia y el ministerio público, entre otros. El Núcleo de Coincidencias Básicas tiene la particular característica de que debe votarse en conjunto y sin modificaciones por los convencionales constituyentes, por lo que se lo llamó "cláusula cerrojo" o "paquete".

c. Por último están los temas habilitados o autorizados para el libre debate por la convención constituyente, es decir, temas sobre los cuales los constituyentes podían expresarse con libertad y formular propuestas de reforma. Entre ellos se encuentra la posibilidad de incorporar nuevos derechos y garantías, el fortalecimiento del federalismo y otros.

La Ley 24.309 habilitaba el libre debate de ciertos temas por la Convención Constituyente federal, la cual sesionó de mayo a agosto de ese año en las ciudades de Paraná y Santa Fe. Estaba integrada por 305 miembros (un número igual al de los miembros de ambas Cámaras del Congreso Nacional) correspondiendo 136 al Partido Justicialista; 76 a la Unión Cívica Radical; 29 al Frente Grande; 18 al MODIN y el resto a más de quince agrupaciones.

En el artículo 3º la ley preveía la consagración expresa del hábeas corpus y del amparo, lo que se haría mediante la incorporación de un artículo nuevo en el capítulo segundo de la primera parte de la Constitución nacional, aunque ninguna referencia hacia a la figura del hábeas data.[31]

[31]Puccinelli, Oscar. R., *Protección de Datos De Carácter Personal*, Argentina, Editorial Astrea, 2004, p. 42.

Dado que el tema no estaba previsto en la ley 24.309, podría pensarse en su inconstitucionalidad tal como pasó en el caso Fayt.[32] Sin embargo, pese a la falta de alusión concreta, esta nueva acción fue intensamente tratada a partir de la presentación de 27 proyectos en la Convención.

De los 27 proyectos presentados, ninguno constituyó la base única del texto definitivo que insertó el habeas data en el artículo 43 párrafo 3º, de la Constitución y que, a partir de las 27 iniciativas presentadas, la Comisión de Nuevos Derechos y Garantías elaboró un proyecto que fue girado a la Comisión de Redacción, y que, reformulado por ésta, quedó de la siguiente manera *"Asimismo toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos que consten en registros públicos o privados y del fin de éstos, y en su caso para exigir la supresión, rectificación o actualización de aquellos".*[33]

A partir de la reforma de 1994, la Constitución Nacional ha instituido al hábeas data como una acción de amparo especial, que permite a toda persona tomar conocimiento de los datos o informaciones a ella referidos, o que lo afectan o puedan afectarla, alterando o restringiendo indebidamente sus derechos, especialmente el de intimidad y a la veracidad de su imagen, y una vez comprobada la inexactitud, falsedad, carácter discriminatorio o lo indebido de la difusión a terceros de los mimos, otorga al afectado la potestad de exigir su supresión, rectificación, modificación, actualización o confidencialidad, según fuere el caso.[34]

Además de el pronunciamiento sobre el tema que nos ocupa, con la reforma constitucional de 1994, se sancionaron 20 nuevas normas constitucionales, 24 se reformaron y 17 disposiciones transitorias.

---

[32] En dicho caso la Corte declaró la inconstitucionalidad parcial del artículo 99 de la Constitución, debido a que el tratamiento del tema de la edad límite para jueces federales no se encontraba habilitada por la ley 24.309.

[33] Puccinelli, Oscar, *op. cit*., nota 31, p. 43.

[34] Carranza Torres, Luis R., *op. cit*., nota 21, p.28.

Entre los avances en materia de derechos fundamentales con la reforma se reconoce la defensa de la democracia, los derechos políticos, formas de participación semidirectas como el plebiscito y el referéndum; así también establece la posibilidad de la iniciativa popular para presentar leyes, la consulta popular respecto a proyectos de ley; además institucionalizar e incorporar al texto constitucional la figura del Defensor del Pueblo.[35]

Es importante también la inclusión en la Constitución del amparo bajo la forma de una garantía tutelar de naturaleza constitucional, que habilita el acceso inmediato, rápido y efectivo del justiciable a la jurisdicción judicial, para demandar el cese de todo acto u omisión que en forma actual o inminente, lesione o amenace, con arbitrariedad o ilegitimidad manifiesta cualquiera de los derechos fundamentales reconocidos en la Constitución, en un Tratado o en una Ley, excepto de aquellos derechos protegidos por la garantía del hábeas corpus o hábeas data.

Así también se protege a los derechos de incidencia colectiva o intereses difusos, mediante la llamada acción popular, a fin de defender aquello objetivos. Habilita al afectado, al defensor del pueblo y a las asociaciones intermedias registradas conforme a la ley, a ejercer la acción para protección de intereses difusos. Por último otorga a los magistrados del Poder Judicial la atribución de llevar a cabo el examen y control de constitucionalidad de todo material infraconstitucional que pugne con la carta magna en el marco del juicio de amparo.[36]

Un tema de suma importancia fue el reconocimiento constitucional de los tratados, es decir el nuevo artículo 75, que estableció las atribuciones del Congreso, después de ratificar la potestad de celebrar tratados, estableció que éstos y los concordatos con la Santa Sede “tienen jerarquía superior a las leyes”, zanjando constitucionalmente la discusión en torno a que una ley pudiera dejar sin efecto compromisos resultantes de un tratado.

[35] Es una institución que recibe quejas de ciudadanos agredidos o no adecuadamente atendidos por la administración pública y que tiene el poder para investigar y recomendar acciones correctivas.
[36] Montbrun, Alberto et al*, op. cit*., nota 30.

Asimismo estableció que diez tratados internacionales sobre derechos humanos (incluyendo declaraciones universales y americanas sobre derechos humanos, económicos y sociales, genocidio, discriminación racial, discriminación contra la mujer, torturas, derechos del niño) tenían jerarquía constitucional. También brindó flexibilidad a la Constitución al admitir que otros tratados internacionales pudiesen incorporarse posteriormente a este rango supremo con el voto favorable de dos tercios de la totalidad de los miembros de cada Cámara.[37]

En función de la inclusión en la reforma de la Constitución Federal de 1994, del habeas data, surge la necesidad de crear legislación ordinaria, materia del siguiente apartado.

4.3.2 Antecedentes legislativos en materia de protección de datos personales

A partir de la reforma constitucional de 1994, que incluyó al habeas data como una acción para permitir el acceso a bancos de datos personales y para corregir información falsa o discriminatoria, surgió la necesidad de regularlo mediante una ley especialmente enfocada a la materia.

No obstante esta necesidad por mandato constitucional, el congreso argentino sintió la necesidad de una norma en función del pronunciamiento de la Comisión Europea, la cual advirtió que sería ineficaz que un país dictara su propia regulación sobre datos personales, mientras su tratamiento sin controles ni restricciones pudiera realizarse en otros países, burlando sus sistemas legales instituidos para la defensa de sus ciudadanos.[38] Razón que justifica lo previsto en la Directiva 95/46, sobre la prohibición de la transferencia internacional de datos a los Estados Miembros de la Unión Europea que no tuvieran un nivel de protección

[37] "Reforma Constitucional 1994. Convencional Nacional Constituyente", *Blog jurídico dedicado al derecho constitucional argentino*, *http://federacionuniversitaria52.blogspot.mx/2009/04/reforma-constitucional-1994.html*

[38] Gils Carbó, Alejandra M., *op. cit.,* nota 2, p. 46.

de datos personales equivalente al establecido en sus respectivas legislaciones. Siendo igualmente aplicable a los países ajenos a esa comunidad que no tuvieran un nivel de protección adecuada. Por lo tanto resultaba trascendente para su inserción en el mercado internacional que Argentina dictara una ley de protección de datos.

Tal como sucedió en España, en Argentina se promovieron juicios fundamentándose en lo prescrito por la Constitución a pesar no contar con legislación secundaria; tal fue el caso "Urteaga, Facundo R. c/ Estado Mayor Conjunto de las Fuerzas Armadas" de 15 de octubre de 1998.

El planteamiento en este caso surge a partir de la promoción de una acción por Facundo Urteaga, basándose en el artículo 43 de la Constitución nacional contra el Estado nacional (Fuerzas Armadas y Organismo de Inteligencia) y contra el Estado de la Provincia de Buenos Aires, para obtener la última información que sobre su hermano Benito Urteaga, obraba en los bancos o registros de datos de dichos organismos requeridos, quien había sido supuestamente abatido en un enfrentamiento en Villa Martelli en el año 1976.

No obstante estar sustentada la pretensión del actor en un precepto constitucional, tanto en Primera Instancia, como en la Cámara de Apelaciones, se rechazó la acción intentada con fundamento en la falta de legitimación del actor, y al considerar improcedente la vía procesal elegida, razonando que la vía correcta era la del habeas corpus.

Ante esta negativa a su pretensión, Urteaga acudió a la Corte Suprema de Justicia de la Nación; la cual emite un pronunciamiento de gran trascendencia para el desarrollo de la protección de datos personales. El primero de los argumentos sostenidos por la Corte deja claro que la vigencia de ciertos derechos y garantías individuales protegen a los individuos por el solo hecho de estar consagradas en la Constitución, independientemente de las leyes reglamentarias, de forma tal que la ausencia de las mismas no es óbice para su ejercicio. En tal sentido, entendió que dentro del marco constitucional no reglamentado, en ese

momento, por el órgano competente, correspondía a la Corte delinear los alcances de la garantía mencionada con razonable flexibilidad.

La Corte para resolver tomó como referencia el planteamiento de la Suprema Corte de Estados Unidos en el fallo Mc Culloch vs. Maryland cuando dice "*no nos olvidemos que lo que estamos interpretando es una Constitución".*[39] Esta flexibilidad de la Corte en su interpretación ha sido fundamental en relación a la legitimación del actor, puesto que hubiera sido lamentable que el Máximo Tribunal se limitara a hacer una interpretación literal.

Así, el Alto Tribunal expuso *debe admitirse la legitimación invocada por el apelante en su calidad de hermano de quien se supone fallecido, toda vez que la habilitación para accionar de un familiar directo con sustento en el derecho a que se proporcione información, aparece en las circunstancias del caso, como una de las alternativas de reglamentación posibles en el marco de una discreta interpretación del texto constitucional*. *Proteger el derecho a conocer todo lo relativo a la muerte de un familiar cercano ocurrida en las circunstancias referidas significa en última instancia, reconocer el derecho a la identidad y a reconstruir la propia historia, los cuales se encuentran estrechamente ligados a la dignidad del hombre.*[40]

Por lo que respecta al segundo argumento por el cual la Cámara de Apelaciones había desestimado la acción, en cuanto a la procedencia de la vía, la Corte rechazó que procediera el hábeas corpus atendiendo al hecho de que habían transcurrido 22 años de la desaparición del hermano. Por lo tanto era el hermano del fallecido quien poseía el derecho de esclarecer las circunstancias en que se produjo la muerte de su hermano, que integraba su estado de familia y constituía un atributo de su personalidad cuya tutela se desprendía del artículo 33 de la Constitución Nacional y, en su caso, el destino dado a su cadáver.

[39] Basterrra, Marcela I., *op. cit.,* nota 11, pp. 65-66.
[40] *Ídem.*

A partir de esta resolución la Corte Suprema de Justicia de la Nación dejó establecido que el habeas data ampara la identidad personal y permite ampliar la cobertura sobre el sentido personalísimo de ese derecho; siendo el habeas data un instrumento destinado a evitar injerencias extrañas en la vida privada, y en la medida de sus posibilidades, responde también para reparar el honor agraviado, la imagen perturbada o la identidad igualmente afectada.

Sin duda alguna el caso Urteaga deja asentado que el habeas data se orienta a garantizar que sea el titular de los datos el que pueda obtener el desarme informativo del Estado, o de quien fuere, para poder decidir acerca del destino y contenido de dichos datos. Pero además, en tanto el texto constitucional permite ejercer un control activo sobre los datos, a fin de supervisar no sólo el contenido de la información en sí, sino también aquello que atañe a su finalidad, es evidente que se trata, a la vez, de un instrumento de control.[41]

Una vez revisado el caso Urteaga, notamos que al igual que el Tribunal Constitucional Español también la Corte Suprema de Argentina, concedió la protección de los datos personales, no obstante se careciera de una disposición que desarrollara el precepto constitucional que lo previera.

Armado de esta manera escenario es que se presentan varios proyectos de ley ante la Legislatura que en su mayoría no se limitaban a regular el trámite procesal de la acción sino a establecer un régimen global del tratamiento de datos, recogiendo principios básicos aceptados por otras legislaciones. Entre los proyectos presentados cabe destacar los de los diputados Hernández en 1194, Arias en 1995 y el del senador Menem en 1996.

A partir de estos proyectos ambas Cámaras tanto la de Senadores como la de Diputados, sancionaron el 27 de noviembre de 1996, el proyecto de ley 24.745. Sin embargo la norma nunca entró en vigencia, pues el Poder Ejecutivo la vetó totalmente mediante decreto 1616/96.

[41] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 7, p. 98.

La decisión de vetarla se debe a que el Ejecutivo consideró que la ley era muy estricta en cuanto a la obtención del consentimiento para la recolección y transmisión de datos a terceros; lo que motivó la reacción de las corporaciones bancarias, financieras y publicitarias, porque conducía virtualmente a suprimir la utilización de registros automatizados para proveer informes sobre la solvencia y la publicidad por marketing directo. Además, el Poder Ejecutivo objetó el texto legal porque instituía como autoridad de control del nuevo régimen a una Comisión Bicameral de Seguimiento de Protección Legislativa de Datos, que tenía tan amplias atribuciones (incluso jurisdiccionales) que vulneraban la distribución constitucional de incumbencias estatales. También consideró inaceptable la prohibición de transferencia internacional de datos a países que no tuvieran una protección adecuada, porque afectaría las relaciones y el comercio internacional, ya que ni siquiera se preveían excepciones en aras de la cooperación con otros Estados. Por otra parte, tuvo en cuenta que la ley confería al Defensor del Pueblo funciones jurisdiccionales en exceso de sus atribuciones y que la acción de hábeas data regulada era insuficiente para una adecuada tutela del justiciable porque no era de aplicación contra entes públicos.[42]

Después de este intento por legislar en materia de protección de datos personales, el Senador Menem junto con otros senadores presentó al Senado una propuesta que culminó, en noviembre de 1998, con la aprobación de un proyecto de Ley de Habeas Data y Protección de Datos Personales. El l4 de septiembre de 2000, la Cámara de Diputados aprobó su versión de la Ley de Protección de Datos Personales y finalmente la Ley fue aprobada y promulgada en noviembre del 2000 (ley 25.326).

Los antecedentes *stricto sensu* del proyecto iniciado en el senado en 1998 fueron los proyectos de de los senadores López, Menem, Branda, Berhongaray, Romero Feris, Villaverde y Del Piero.[43]

[42] Gils Carbó, Alejandra, *op. cit.,* nota 2, p. 46.
[43] Puccinelli, Oscar, *op. cit.,* nota 31, p. 46.

Con estas aportaciones y sobre la base del proyecto del senador Menem (que ya había sido presentado en 1995), el 29 de septiembre de 1998 se emite un dictamen con despacho por la mayoría y que sería la base de la ley finalmente aprobada.

Expuesto el dictamen por el senador Menem, se aprobó el texto final por la Cámara de Senadores por dos tercios de los miembros presentes, cumpliendo así con lo previsto en el artículo 81 constitucional.

En la Cámara revisora, es decir la Cámara de Diputados, las comisiones de Asuntos Constitucionales; de Justicia; de Legislación General; de Legislación Penal, y de Presupuesto y Hacienda consideraron el proyecto aprobado por el Senado; emitieron un dictamen el 28 de agosto del 2000 por el que se introdujeron importantes reformas.[44]

Luego de un intenso debate el 14 de septiembre del 2000 la Cámara de Diputados aprobó la norma enviada por el Senado, sin embargo sólo algunas de las modificaciones propuestas por la Cámara revisora fueron aceptadas por la Cámara de Origen.[45]

El iter legislativo de la ley 25.326 concluiría el 30 de octubre del 2000 con un veto parcial del Poder Ejecutivo (decreto 995/00) de los artículos 29 apartados 2 y 3, referentes a la autoridad de control, y 47 relativo al blanqueo de ciertos datos negativos de carácter financiero para quienes hubieran cancelado sus

[44] Al informar el proyecto , la diputada Carrió sintetizó las reformas que proponían del texto aprobado por el Senado, indicando que eran "en materia de de datos sensibles, por ejemplo la sanción del Senado habilitaba el registro de datos sensibles referidos a la identidad sexual, hábitos personales, ideología política, raza y religión, mientras que el presente dictamen prohíbe el registro de todo dato sensible, es decir, prohíbe todo criterio de comercialización sobre estos datos en el entendimiento de que el consentimiento puede ser forzado, ya que según la sanción original, cuando alguien quería entrar en un banco de datos para conseguir empleo se le podía poner como condición consentir el registro de este tipo de información a cambio de figurar en ese banco. Las otras modificaciones introducidas a la sanción del Honorable Senado están referidas a las informaciones crediticias; básicamente se disminuye el tiempo por el cual la información puede estar en el banco de datos, ya que la sanción del Senado establecía un plazo de 5 años para todos y el dictamen en consideración lo disminuye en los casos en que el deudor haya cancelado su deuda. (Debate legislativo respecto a la ley 25.326, *http://www.protecciondedatos.com.ar/debatedip.htm*)

[45] Puccinelli, Oscar, *op. cit.*, nota 31, p. 47.

obligaciones al momento de entrada en vigencia de la ley. Fue publicada en el Boletín Oficial el 2 de noviembre del 2000, pero no se le dio el trámite parlamentario ulterior debido a la falta de creación de la Comisión Bicameral Permanente.

En general tanto la Cámara de origen como la Cámara revisora votaron a favor del proyecto de creación de una norma en materia de protección de datos, sin embargo hubo un voto disidente formulado por el Senador Rodríguez Saá, quien votó en contra del proyecto de ley toda vez que consideró que el contenido de la misma, no se enfocaba mayoritariamente al hábeas data como garantía procesal; lo que para el senador representaba un retroceso sobre la Constitución, así como el hecho de que el procedimiento planteado en la ley fuera un juicio sumarísimo, lo que significaba que los plazos se prolonguen meses incluso años.[46]

En efecto la ley no se aboca únicamente al hábeas data, pues como lo mencionamos en párrafos anteriores lo que el legislador buscaba era una protección integral a los datos personales, y no únicamente establecer una acción en caso de violación a los mismos.

Esta ley a diferencia de la legislación mexicana, se es compatible con la legislación provincial, pues al respecto nos dice Carranza Torres que en relación con las provincias, la parte de la ley referente a datos es de aplicación obligatoria, y esto no puede ser de otro modo, pues esta normativa reglamenta derechos contenidos en la Constitución Nacional, pero nada obsta a que, respetando ese piso mínimo y obligatorio de protección, y de consonancia con lo establecido en sus constitucionales provinciales, las mismas dicten leyes respecto de datos de archivos, bancos o similares que actúen en sus territorios o creen organismos de control de los mismos.

Respecto del habeas data, por ser éste un instituto de naturaleza procesal, y por tanto una facultad reservada de las provincias, la normativa de la ley alcanza

[46] "Antecedentes Parlamentarios de la Ley de Protección de los Datos Personales", *http://www.protecciondedatos.com.ar/debatedip.htm*

únicamente a los procesos que se instauren ante la justicia federal o nacional ordinaria.

La ley deja abierta en forma expresa la posibilidad de que los gobiernos provinciales adhieran a la misma, pero ello, desde luego, no obsta a que regules la figura de modo autónomo, respetando lo dispuesto en la Constitución Nacional.

De no tener una regulación propia deberá estarse a lo que digan los textos constitucionales locales. De no contener éstos la regulación de la figura, o pauta alguna respecto de la faz procesal de la misma, cabrá la aplicación de lo preceptuado para el amparo, o la figura de protección de derechos constitucionales que sea más eficaz frente al caso en concreto.[47]

El Poder Ejecutivo reglamentó esta ley por decreto 1558/01, y por resoluciones 17/02, 98/02 y 325/02 del Ministerio de Justicia, Seguridad y Derechos Humanos; por decreto 1892/02 se designó y puso en funciones al titular del organismo de control, cuyas decisiones amplían el plexo normativo aplicable.[48]

4.3.3 Ejercicio de los derechos de acceso, rectificación y cancelación

Del mismo modo que la legislación española prevé dos procedimientos para efectuar el ejercicio de los derechos de acceso, rectificación y cancelación, la legislación argentina lo retoma, sin embargo la ley 25.326 se diferencia de la norma española, en razón de que prevé un procedimiento administrativo frente al titular y un proceso jurisdiccional frente a un juez.

[47] Carranza Torres, Luis R., *op. cit.,* nota 21, pp. 29-30.
[48] Puccinelli, Oscar, *op. cit.,* nota 31, pp.45-46.

4.3.3.1 Frente al responsable del tratamiento

Este procedimiento es muy parecido al previsto por la legislación española, solamente reduce los plazos. Primeramente debe presentarse una solicitud que podrá formular el titular o su representante, y en el caso de personas fallecidas sus herederos previa presentación de la declaratoria de herederos.

Una vez recibida la solicitud, el responsable tiene un plazo de diez días para dar respuesta, únicamente cuando se trate del derecho de acceso, pues por lo que respecta al derecho de rectificación y cancelación el responsable deberá efectuar la misma en un plazo de cinco días.

La obligatoriedad de agotar este procedimiento antes de accionar el habeas data ha sido motivo de un intento debate, no solamente doctrinal sino jurisprudencial. Lo cual deviene de la confusión respecto a la naturaleza del habeas data, pues por un lado se le considera como un tipo de amparo especial y por el otro se le configura como una figura procesal autónoma.

Esta confusión se genera en torno al lugar donde el habeas data se sitúa dentro del texto constitucional, pues quienes afirman que es una especie de amparo lo derivan de que se encuentra previsto en el mismo artículo que prevé el amparo y no se denomina de ninguna forma específica como sucede con el habeas corpus. Por el contrario quienes lo consideran como una figura independiente sostienen que su naturaleza no se puede desprender únicamente a partir de su ubicación en la ley fundamental.

La consecuencia de considerarlo como una especie de amparo, sería que para ejercer el habeas data sería indispensable satisfacer los presupuestos de admisibilidad del amparo común: acreditar la existencia de ilegalidad o arbitrariedad manifiesta y el agotamiento de vías administrativas.

La corriente doctrinaria que supone que dichos presupuestos no deben ser condición para ejercer el habeas data, debido a que el habeas data debería servir

para evitar el daño antes de que se produzca; lo que legitima el accionante para conocer los datos es, que están referidos a una persona y sólo le basta que tiene un interés legitimo para conocerlos;[49] es decir no tendría que acreditar la existencia de ilegalidad o arbitrariedad manifiesta. En tanto que el tránsito previo por la instancia administrativa, si bien recomendable y adecuado no puede surtir las veces de un obstáculo para acceder a la justicia, de modo tal que si el interesado prefiere recurrir a la acción de habeas data, el archivo podrá alegar que no ha tenido posibilidad de ser oído, y en tal caso la instancia jurisdiccional podrá ser de encuentro y de conciliación antes que de controversia pura.[50]

Compartimos los argumentos de esta postura, debido a que la ley no exige la existencia de un perjuicio o daño directo, pues como lo indica Gozaini la verdad integra el mundo jurídico y por tanto el peticionario puede promover en resguardo de la simple verdad.[51] En tanto que el agotamiento de la vía administrativa ha generado mayor polémica no solo en la doctrina, sino a nivel jurisdiccional.

Así por ejemplo la Cámara Nacional de Apelaciones en lo Comercial, específicamente en los casos "Figueroa Hnos"[52] y "Faiman"[53] resolvió que el promovente debía acreditar que realizó las gestiones administrativas frente al responsable, a efecto de poder incoar la acción de hábeas data.

Por el contrario, la Cámara Nacional de Apelaciones en lo Civil se ha pronunció en contra la resolución anterior; pues en el caso "Warksberg",[54] sostuvo que de la lectura del artículo 43 constitucional no se desprende la obligación de agotar las gestiones administrativas para estar en posibilidad de recurrir al habeas data.

No obstante este debate ha quedado dilucidado mediante lo dispuesto en el artículo 14 inciso 2 de la ley 25.326, que exige la obligación de agotar las

[49] Gils Carbó, Alejandra, *op. cit.,* nota 2, p. P. 249.
[50] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 7, p. 451.
[51] Gozaini, Osvaldo Alfredo, *op. cit.,* nota 7, p. 432.
[52] CN Com, Sala D. *"Figueroa Hnos. v. Banco de la Provincia de Santiago del Estero"*, del 13/5/96.
[53] CN Com, Sala E, "Faiman, Enrique v. Organización Veraz SA", del 15/7/99.
[54] CN Civ, Sala B. "Warksberg, Herman", del 11/7/96.

gestiones frente al responsable para acudir al habeas data; presupuesto que se puede considerar una verdadera vía administrativo, o simplemente una solicitud que no requieres mayores gestiones. Disposición que en palabras de la profesora de derecho constitucional de la Universidad de Buenos aires, María Luisa Peluffo, si la ley ofrece un remedio rápido, idóneo y eficaz, como lo es el poder acceder en forma directa, sin necesidad de intervención judicial, éste debe ser un requisito obligatorio para la procedencia de la acción de habeas data, a efecto de evitar litigios innecesarios y hace que el principio de economía procesal sea aplicado de un modo práctico.[55]

4.3.3.2 Hábeas data

Agotadas las gestiones administrativas frente al responsable del tratamiento, se da paso al ejercicio de la acción de habeas data. Una vez vencido el plazo para contestar la solicitud de acceso o para efectuar la correspondiente rectificación o cancelación, el titular (su curador o tutor, sus sucesores, por sí o por representante y en el caso de las personas jurídicas, su representante legal) podrá ejercer la acción de hábeas data y denunciar el hecho ante la Dirección Nacional de Protección de Datos.

Los supuestos que la ley establece para la procedencia del hábeas data son los siguientes:

a) Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
b) En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se

[55] Peluffo, Maria Laura, "La acción de habeas data. ¿Es necesario agotar la vía prejudicial para interponer esta acción? Criterios a favor y en contra", *Universidad del Salvador, http://www.salvador.edu.ar/juri/jadpc/Maria%20L.%20Peluffo.pdf*

encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo y, en su caso, el nombre del responsable o usuario del mismo. Pudiéndose presentar ante el Juez del domicilio del actor, el del responsable o bien el del lugar en que el hecho se cometió o pudiera tener efecto, a elección del actor.[56]

Cabe aclarar que el ejercicio de la acción se regula supletoriamente por lo dispuesto en el código procesal civil, tratándose del caso particular de que la acción se ejerza frente a archivos privados, debido a que dicha situación presentada entre particulares corresponde a la jurisdicción ordinaria. Salvo en el caso de que el registro demandado se dedique comercialmente a difundir información del contenido de su banco privado de datos, ello lo instala en la calidad de comerciante y, como tal, debe intervenir ante la justicia del fuero federal.[57]

El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.

[56] No obstante el hábeas data es un procedimiento constitucional, en Argentina se aplica el criterio de control de constitucional difuso, es decir, en Argentina todo amparo es constitucional, porque la jurisdicción constitucional está diseminada entre todos los jueces, y ello sin perjuicio de la instancia supraestatal interamericana. Carnota, Walter F., "Dos visiones constitucionales divergentes sobre el amparo: los casos Argentino y Español", *Cuestiones Constitucionales,* México, núm., 9, julio-diciembre de 2003, *http://www.ejournal.unam.mx/cuc/cconst09/CUC00902.pdf*

[57] Gozaini, Osvaldo Alfredo, "El proceso de habeas data en la nueva ley de protección de datos personales", *Revista Jurídica*, Argentina, 21 abril de 2006, http://dspace.uces.edu.ar:8180/dspace/bitstream/123456789/412/1/El_proceso_de_habeas_data_parte01.pdf

Presentada la demanda el Juez deberá resolver sobre la procedencia de la vía en la que fue presentada, la cual se confronta con el objeto solicitado y con los medios procesales obtenidos.

Cabe destacar que la ley prevé la aplicación de medidas cautelares durante el hábeas data, es decir aquellas medidas de carácter precautorio que cumplen la función de significar un anticipo asegurativo de la garantía jurisdiccional, para impedir que el derecho, cuyo reconocimiento se pretende obtener por medio del proceso, pierda su virtualidad o eficacia hasta el pronunciamiento de la sentencia definitiva.[58]

La ley prevé dos tipos de cautelares específicas en el proceso de hábeas data :

a) Anotación de dato litigioso: ésta puede ser pedida por el propio interesado en su escrito de demanda.
b) Bloqueo de la difusión de datos: resulta una especie dentro del género de las medidas de no innovar, que la norma adjudica como deber del juez cuando está frente a datos manifiestamente falsos, inexactos o discriminatorios. Deber ser de oficio. Supone la indisponibilidad del dato o datos en cuestión, para su difusión a terceros, en tanto se sustancia el proceso. En caso de información sensible.

Una vez admitida la demanda, el Juez requerirá al responsable para que remita la información con la que cuenta respecto al actor¸ así como informes que puedan servir para resolver el asunto; el responsable tendrá cinco días para rendir los informes, plazo que podrá ser ampliado. En la contestación a dichos informes, el responsable deberá decir al Juzgador los motivos por los cuales almacenó la información del actor y los motivos para no haber procedido favorablemente a la solicitud de los derechos de acceso, rectificación o cancelación.

Contestados los informes, la ley otorga un plazo de tres días a objeto de que el actor amplíe los términos de su demanda y ofrezca pruebas, corriendo traslado al

[58] Carranza Torres, Luis R, *op. cit.*, nota 21, pp. 164-166.

responsable para que en el plazo de tres días conteste lo que a su derecho convenga.

Al vencimiento de los plazos señalados, el Juez dictara sentencia; en la cual constará:[59]

a) La individualización concreta de la información sobre la que se falla y respecto de la cual debe realzarse algún tipo de acto.
b) La determinación precisa de la conducta a cumplir por el demandado, con las necesarias especificaciones para su debida ejecución, es decir, todas aquellas instrucciones, limites o similares que el juzgador dictará a fin de asegurar la realización del acto ordenado, de acuerdo a la intensión y voluntad que el tribunal expresa en la sentencia. Daños y perjuicios a cargo del Estado, delitos, se tienen que plantear por otra vía distinta al amparo.
c) La fijación de un plazo para el cumplimiento de lo resuelto, que deberá ser de la mayor brevedad posible, atenta al carácter de urgencia que caracteriza al amparo.

La sentencia que sobre el caso se pronuncie deberá ser comunicada a la Dirección Nacional de Protección de Datos, quien se encargará de llevar un registro de las sentencias pronunciadas.

Contra la sentencia dictada procede el recurso de apelación, el cual debe ser interpuesto 48 horas computables a partir de la hora en que se realizó el acto de notificación, siéndole de aplicación las normas referentes a los plazos por horas, salvo que en tal diligencia se hubiera omitido tal dato, en cuyo caso el término será computable desde la medianoche del día en que la parte recibió la notificación del acto susceptible de ser recurrido.

En lo que respecta a la vía extraordinaria recursiva federal, es doctrina de la Corte Suprema que la sentencia definitiva dictada sobre una cuestión de habeas data,

[59] *Ibídem,* pp. 174-175.

ya fuere admitiendo o desestimando la pretensión aducida, en la cual se ponga en juicio la inteligencia del art. 43 de la Constitución Nacional, es susceptible de ser revisada merced al uso del recurso extraordinario, previsto en el artículo 14 de la ley nacional 48 ante la Corte Suprema.[60]

Tal como vimos en el desarrollo de este apartado dedicado al derecho argentino, a partir de la instauración del habeas data en la Constitución y posteriormente desarrollado por la legislación secundaria se amplía la protección de los datos personales, al ser previsto como un remedio con jerarquía constitucional, para que los individuos puedan ejercer sus derechos por vía judicial ante un tratamiento de datos personales, sin embargo el profesor Chirino Sánchez dice que el hábeas data fracasa al conceder una garantía procedimental, que en la mayoría de los casos funcionará siempre después de que sucedió la transmisión de los datos, a velocidades infinitesimales, y el daño para la personalidad ya ha sido verificado. Y pone como ejemplo de una mejor protección el camino seguido por Europa en donde se hizo mayor énfasis en la prevención mediante la actuación de autoridades administrativas, asignándoles a los Comisionados de Datos un papel estelar ya que estos funcionarios cuentan con amplías facultades de investigación y de acceso a la ley, a cuyo fin pueden aplicar sanciones pecuniarias a los responsables y disponer la clausura de archivos.

La postura del profesor parecería correcta tomando en cuenta que en España la Agencia de Protección de Datos es quien ejerce las facultades administrativas tanto de resolver el procedimiento de tutela de los datos así como de imponer las medidas correctivas en función del desacato a lo dispuesto en la normatividad; mientras que en Argentina el juez civil carece de jurisdicción para ordenar la supresión de datos de terceros ajenos al juicio ni clausurar la base de datos o sancionar a los responsables por esa actividad ilícita, en virtud del principio de congruencia que le veda pronunciarse sobre cuestiones que vayan más allá de lo planteado por las partes. Sin embargo no debemos perder de vista que si bien es cierto el juez civil carece de facultades administrativas, la ley de protección de

[60] *Ibídem,* pp. 176-178.

datos prevé un órgano de control que se encargue de ellas, es decir, tanto el juez como los particulares tienen la posibilidad de denunciar cualquier situación contraria a la norma a la Dirección Nacional de Datos Personales para que ejerza sus facultades disciplinarias, complementando de esta forma el régimen de protección. Tal como lo señala Alejandra Gils, el habeas data es en realidad una mínima porción en el universo de la protección de los datos personales, es solo una herramienta para ejercer los derechos del titular.[61]

4.4 Derecho Mexicano

En México en materia de protección de datos, se ha tenido que reformar desde el ámbito constitucional hasta la legislación secundaria, para estar en posibilidad de garantizar el derecho a la protección de datos.

4.4.1 Reformas constitucionales

Las reformas a la Constitución fueron una respuesta a la necesidad de homogeneizar las leyes estatales que preveían en primer lugar el derecho de acceso a la información y en seguida la protección de datos personales, a efecto de evitar la disparidad legislativa que podría resultar perjudicial para la práctica de un derecho fundamental.

4.4.1.1 Artículo 6º

Antes de presentarse la iniciativa formal de reforma constitucional al artículo 6°, surgieron diversos proyectos que buscaban una reforma que permitiera

[61] Gils Carbó¸ Alejandra M., *op. cit*., nota 2, p. 261.

homogeneizar la regulación del derecho de acceso a la información en todo el país.

El primer proyecto, es la denominada "Declaración de Guadalajara", firmada el 22 de noviembre del año 2005 al concluir el Primer Foro Nacional de Transparencia Local, celebrado en la capital del Estado de Jalisco, por tres Gobernadores Amalia García Medina de Zacatecas, Luis Armando Reynoso Femat de Aguascalientes y José Reyes Baeza Terrazas de Chihuahua. En dicha declaración después de un diagnóstico completo sobre las leyes locales y de las reglamentaciones municipales, se propuso una reforma constitucional que incorporara al texto fundamental el derecho de acceso a la información pública y los requisitos mínimos a cumplir en toda la República.

A partir de esta Declaración, el tema de la reforma se retomó en la XXVII Reunión ordinaria de la Conferencia Nacional de Gobernadores (CONAGO), celebrada en Guanajuato durante el mes de marzo de 2006; y los miembros presentes decidieron inscribirla en la agenda de trabajo de 2006 de la CONAGO.

Posteriormente el 10 de noviembre de 2006 se presentó la Iniciativa de Chihuahua, en el marco del Segundo Congreso de Transparencia Local, que tuvo lugar en aquella entidad. El documento fue firmado por los Gobernadores de Aguascalientes, Chihuahua y Zacatecas y se sumaron el Gobernador del Estado de Veracruz, Fidel Herrera, y el entonces Jefe de Gobierno del Distrito Federal, Alejandro Encinas. La misma fue presentada por el Gobernador de Chihuahua José Reyes Baeza Terrazas, el 13 de diciembre de 2006 ante los integrantes de la Junta de Coordinación Política.

Siguiendo el interés mostrado por las Entidades Federativas, el 16 de noviembre de 2006, la Junta de Coordinación Política de la LX Legislatura tomó un acuerdo para su presentación ante el Pleno de la Cámara de Diputados, en el sentido de fortalecer el derecho fundamental de acceso a la información y la transparencia. Dicho acuerdo reconoció el hecho de que Gobernadores habían elaborado un diagnóstico y una propuesta para llevar a cabo reformas tendientes a elevar a

rango constitucional, obligaciones básicas e iguales en materia de transparencia y acceso a la información. Así también en dicho acuerdo se argumentó la necesidad de la reforma al artículo sexto de la Constitución, en atención al problema de la heterogeneidad en las leyes de transparencia en México. El mismo fue aprobado el 28 de noviembre de 2006 por el Pleno de la Cámara.

Es a partir de la Iniciativa de Chihuahua, que surge la iniciativa formal de reforma al artículo 6° constitucional, presentada el 19 de diciembre de 2006 en la sesión Plenaria de la Cámara de Diputados firmada por los Coordinadores de las fracciones parlamentarias de los ocho partidos políticos, en cumplimiento del compromiso que establecieron los mismos durante la referida Iniciativa.

El Pleno de la Cámara envío la iniciativa a la Comisión de Puntos Constitucionales para su dictamen; la cual decidió incluir en el mismo estudio la iniciativa presentada el 16 de noviembre del año 2006 por la Diputada Erika Larregui Ángel, del Partido Verde Ecologista de México, en la parte concerniente al artículo 6°.El tema del derecho de acceso a la información fue incluido como una prioridad de la agenda legislativa, al ser considerado como un derecho fundamental al proteger un bien jurídico valioso en sí mismo (que los ciudadanos puedan saber y acceder a información relevante para sus vidas) y porque sobre él se erige la viabilidad de un sistema democrático, porque cumple una función vital para la república, que los ciudadanos conozcan el quehacer, las decisiones y los recursos que erogan sus autoridades elegidas mediante el voto.

La finalidad primordial de la reforma al artículo 6° era otorgar protección constitucional al derecho de acceso a la información pública gubernamental, en cualquier punto del territorio nacional y en los tres niveles de gobierno, a su vez, prevé el derecho a la protección de los datos personales.

Entre los objetivos esenciales que se buscaban con la reforma era convertir en derecho fundamental al derecho de acceso a la información en México, contando con mecanismos jurisdiccionales de control de constitucionalidad; a través de criterios mínimos obligatorios para todos los Estados; así como favoreciendo en

todo momento la publicidad de la información, lo que obligaba a la rendición de cuentas; previendo como excepción el respeto a la vida privada. Para lograrlo se planteaba la creación de órganos especializados en la materia. Específicamente respecto al tema que nos ocupa, la reforma buscaba que se expidiera una legislación en materia de protección de datos personales que precisara los límites entre la información pública y la información que se refiera a las personas físicas, identificadas o identificables, relativa a sus características físicas, morales, emocionales, a su vida afectiva y familiar, creencias o convicciones, estado de salud, preferencias sexuales u otras análogas que atañan a su intimidad.

Finalmente la reforma fue publicada en el Diario Oficial de la Federación el 20 de julio de 2007, en los artículos transitorios se estableció que a partir de esta fecha, todos los Estados y el Distrito Federal tendrían un año para aprobar o modificar sus leyes de acceso a la información, de tal manera que incluyeran los nuevos conceptos constitucionales, tales como la protección a los datos de la vida privada y personales de los individuos, la creación de procedimientos de acceso a la información, y el establecimiento de órganos especializados con autonomía operativa para manejar este tema.[62]

Esta reforma constitucional es importante dentro de la evolución constitucional de la protección de datos personales en nuestro país, pues si bien está enfocada a garantizar el derecho de acceso a la información, vislumbra como un derecho fundamental la protección de datos imponiéndola como un límite al ejercicio del derecho de acceso a la información.

4.4.1.2 Artículo 16

El siguiente eslabón en la cadena constitucional para garantizar la protección de datos personales, y sin lugar a dudas el más importante respecto al tema, es la reforma al artículo 16 constitucional.

[62] Carranza Torres, Luis R., *op. cit.,* p.178.

En ese sentido, la reforma del artículo 16 constitucional permitiría continuar con lo alcanzado con la reforma al artículo 6°; porque si bien en ella se hizo alusión a la protección de datos personales, con esta otra reforma se estaría dotando finalmente de contenido a este derecho fundamental.

El proceso de reforma comienza con la presentación de la iniciativa de adición al artículo 16 constitucional, presentada por el Senador Antonio García Torres el 5 de abril de 2006; la cual fue dictaminada y aprobada en el Senado el 18 de abril del mismo año. El 19 de abril de 2006 la minuta fue recibida en la Cámara de Diputados y el dictamen respectivo fue aprobado por el Pleno el 20 de septiembre de 2007, en el que se introdujo el derecho de oposición que no estaba contemplado en el texto original[63].

Si bien esta iniciativa en cuanto a contenido la aprobaron ambas Cámaras, por cuestiones sistémicas, lingüísticas y de técnica legislativa, y con el ánimo de enriquecer la reforma; la Cámara de diputados propuso una nueva redacción respetando la esencia de la iniciativa de García Torres.

Es por este motivo que se presenta una nueva iniciativa con proyecto de decreto por el que adiciona un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Presentada por los Senadores Santiago Creel Miranda y Alejandro González Alcocer (PAN), Pablo Gómez Álvarez (PRD) y Pedro Joaquín Coldwell (PRI); el 25 de noviembre de 2008. Finalmente publicada en el Diario Oficial de la Federación el 1 de junio de 2009.

El objetivo central de la reforma era desarrollar en el máximo nivel de nuestra normatividad la protección de datos personales, mediante el reconocimiento de un nuevo derecho fundamental y sus correlativos derechos al acceso, rectificación, cancelación u oposición en torno al manejo de nuestra información por parte de cualquier entidad o persona, pública o privada, que tuviera acceso o dispusiera de los datos personales de los individuos. Asimismo, contempla que dicha legislación

[63] Cámara de Diputados, *http://www.diputados.gob.mx/LeyesBiblio/legis/reflx.htm*

establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, pues como el legislador lo señala al adquirir el derecho a la protección de datos personales el carácter de un derecho fundamental, resulta indispensable que las excepciones a la aplicación de los principios que rigen la materia sean establecidas al mismo nivel jerárquico; supuesto que también reconoció el Tribunal Constitucional español en la sentencia 292/2000.

El profesor Marcos del Rosario nos dice que si bien, el reconocimiento expreso a nivel constitucional conlleva un incremento en la vigencia de este derecho, es un hecho que aún no se configura del todo un esquema de defensa óptimo, es decir un auténtico hábeas data, como medio de control constitucional de tipo jurisdiccional, a fin de proteger de forma directa e inmediata la intangibilidad de los datos personales y demás derechos fundamentales vinculados a la esfera íntima de la persona.[64]

No obstante la visión del profesor, podemos considerar que si bien el legislador no instauró la figura del habeas data, si es a partir de esta reforma constitucional que se reconoce y se da contenido al derecho a la protección de datos personales en la Constitución de los Estados Unidos Mexicanos. En ese sentido, que en la reforma se plasman los derechos con los que cuentan los titulares de los datos personales como lo son los de acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO). Aunado a este reconocimiento, el otro merito logrado a partir de esta reforma es la posibilidad de ejercer este derecho frente a particulares, es decir en sentido horizontal.

[64] Rosario Rodríguez, Marcos Francisco Del, "La protección de datos personales entre particulares: esbozos de un esquema de regulación y protección en México", *Revista Derecho Comparado de la Información*, Nueva serie, México, núm. 20, julio-diciembre 2012, *http://biblio.juridicas.unam.mx/revista/pdf/DerechoInformacion/20/art/art4.pdf*

4.4.1.3 Artículo 73

Una vez reconocida la protección de datos personales como un derecho fundamental, era preciso que se facultara al legislador para estar en posibilidad de dictar la legislación que desarrollara el mandato constitucional, es por eso que toma relevancia reformar el artículo 73 constitucional.

Se presenta el 27 de marzo de 2007 la iniciativa con proyecto de decreto que adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos; por los diputados del grupo parlamentario del Partido Acción Nacional, Luis Gustavo Parra Noriega, María del Pilar Ortega Martínez, Rogelio Carbajal Tejada, Dora Alicia Martínez Valero, Esmeralda Cárdenas Sánchez y Jesús de León Tello.

Dentro de la iniciativa se destaca que si bien las Entidades Federativas habían promulgado diversas leyes en matera de protección de datos en posesión de particulares, este esfuerzo en vez de haber resultado benéfico, por el contrario había generado restricciones comerciales entre las propias entidades derivadas de las disparidades entre sus respectivas leyes; motivo suficiente para pretender dotar al Congreso de facultades expresas para legislar en la materia.

Es en este sentido que derivado de la relación existente entre la utilización de los datos personales en la realización de transacciones comerciales, el legislador estima que al ser el comercio una materia exclusiva del ámbito federal en toda la República. Por esta misma razón es que el legislador justifica que la protección a los datos en posesión de la administración pública, puedan ser competencia de las legislaturas locales, toda vez que son utilizados con fines comerciales.

Aunado a lo anterior, el legislador estima conveniente otorgarle facultades al Congreso a fin de que el derecho a la protección de datos pueda ser ejercido en todo el territorio nacional del mismo modo y bajo las mismas condiciones para cualquier interesado, no importando el estado o municipio del país donde se encuentre el titular de los datos personales; esto es, tratándose de un derecho

fundamental debe tener el mismo piso para todos los mexicanos sin importar en la entidad federativa que residan o que se encuentren.

Concluye el legislador que se requiere una protección a nivel federal para poder hacer frente a los riesgos derivados de las tecnologías de la información a nivel internacional. Es así que la reforma al artículo 73 se publica en el Diario Oficial de la Federación el 30 de abril de 2009.

No obstante uno de los objetivos de esta reforma era garantizar la protección de los datos personales en posesión de particulares de manera igualitaria en todo el territorio nacional, no debemos perder de vista que el principal móvil de esta reforma al igual que como aconteció en Argentina, era eliminar los obstáculos que pudieran interferir en las transacciones comerciales.

4.4.2 Antecedentes legislativos

En México la protección de datos personales tuvo su primer antecedente con la presentación del proyecto de la Ley Federal de Protección de Datos Personales, presentado por el Senador Antonio García Torres el 14 de febrero de 2001.

El objetivo central de este proyecto era tener una adecuada regulación en materia de protección de datos a fin de evitar que se prohibieran las transferencias de datos por parte de los Estados europeos hacia México. Además de consolidar una protección integral de los datos personales, inclusive respecto de personas jurídicas, asentados en archivos u otros medios técnicos de tratamiento de datos, fueran públicos o privados destinados a dar informes; así como la creación tanto del Instituto Federal de Protección de Datos Personales, como de un Registro de bases de datos. Inclusive proponía reformar el artículo 16 constitucional a efecto de adicionar la garantía de habeas data.

Meses después a la presentación de esta iniciativa, el Diputado Miguel Barbosa Huerta presentó el proyecto de la Ley Federal de Protección de Datos Personales

el 6 de septiembre de 2001.[65] Este proyecto busca instrumentar una nueva protección al derecho a la intimidad, pues el Diputado considera que los límites naturales que lo protegían, es decir el tiempo y el espacio, han desaparecido con el avance tecnológico. Por lo cual estima regular el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos para salvaguardar el derecho a la intimidad de las personas.

Entre los aspectos relevantes de esta iniciativa, cabe destacar que prevé la creación de un órgano de control, el Registro Nacional de Protección de Datos, sin embargo, lo ubica dentro como un ente integrado al Instituto Nacional de Estadística, Geografía e Informática; lo cual consideramos no es pertinente pues limitaría sus funciones al no ser un organismo autónomo o por lo menos descentralizado.

Esta iniciativa siguiendo la línea europea, limita la transferencia internacional de datos a países que no contaran con una adecuada regulación; y en concordancia con la argentina, extendía la protección de los datos tanto a personas físicas como jurídicas.

En cuanto a la parte procedimiento, la iniciativa contemplaba como norma supletoria lo referente a los juicios ordinarios civiles previstos en la legislaciones locales.

Continuando con los antecedente legislativos, el siguiente lo encontramos en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada el 11 de julio de 2002 y cuyo objetivo es regular el derecho de acceso a la información; se establecen una serie de disposiciones dirigidas a garantizar el derecho a la protección de datos personales, tales como principios, derechos de los titulares de los datos, la existencia de un registro de protección de datos, así como algunas reglas en torno a los procedimientos de acceso y corrección de datos personales. Es de resaltar que dentro del glosario de la ley se definen los

[65]Gaceta Parlamentaria, año IV, número 832, viernes 7 de septiembre de 2001, *http://gaceta.diputados.gob.mx/*

datos personales tanto en sentido amplío como en sentido estricto, pues la definición incluye dentro del mismo concepto a los datos sensibles.

A nivel local encontramos un antecedente específicamente abocado a la protección de los datos personales, esto es la Ley de Protección de datos Personales de Colima, aprobada por el Congreso Local y puesta en vigor el 22 de junio del 2003.

Mientras las reformas constitucionales en materia de protección de datos estaban gestionándose, en el año 2007 el presidente Felipe Calderón Hinojosa, en el Plan Nacional de Desarrollo 2007-2012, estableció la necesidad de desarrollar una Ley Federal de protección de datos personales, que regulara la información en poder de los particulares.

Como resultado del mandato constitucional de legislar una ley especializada en materia de datos personales, se presentaron ante el Congreso diversos proyectos de iniciativa de ley; a los cuales aludiremos en los siguientes párrafos; haciendo la aclaración pertinente de que solamente resaltaremos el objetivo de la iniciativa y algunos elementos destacados de la misma y que difieren de la ley vigente.

Comencemos con la iniciativa presentada por el Diputado Jesús Emilio Martínez Álvarez el 1° de diciembre de 2005, la Ley Federal de Protección de Datos Personales.[66]

Distintamente a otras iniciativas que buscan legislar en esta materia a fin de asegurar las relaciones comerciales, esta iniciativa vislumbra en la protección de datos un presupuesto para consolidar la estructura democrática del país. Teniendo como objetivo garantizar la protección de los datos personales que se encontraran contenidos en documentos, archivos, registros, bancos de datos, o bien, en otros medios tecnológicos de procesamiento de datos, fueran de carácter públicos o privados, a efecto de proteger los derechos de las personas a la vida privada y a la

[66] Gaceta Parlamentaria, Cámara de Diputados, número 1895-I, jueves 1 de diciembre de 2005, *http://gaceta.diputados.gob.mx/*

intimidad, así como el acceso a la información que sobre las mismas se registre. Al igual que otras de las iniciativas presentadas, ésta estipula la creación de un Registro de bases de datos. Un elemento característico de esta iniciativa es que tal como lo hace la ley argentina 25.326, amplía la protección de datos personales a las personas jurídicas.

La siguiente iniciativa se presentó el 23 de febrero de 2006, por el Diputado David Hernández Pérez;[67] con la cual se pretendía regular las conductas de terceros en relación con los datos personales de los individuos, permitiendo a éstos, el derecho inalienable de decidir como proveer y controlar el acceso y uso de su información personal.

Es una iniciativa que prevé la protección de datos frente a particulares; alude al aviso de privacidad que sólo deberá ser dado en los casos que sea necesario, contrariando de esta manera el principio de consentimiento. Otro aspecto negativo de esta iniciativa es que no contempla el derecho de oposición.

Un mes después, el 22 de marzo del mismo año, la Diputada Sheila Aragón presentó su iniciativa de la Ley Federal de Protección de Datos Personales.[68] Para la Diputada lo relevante de tener una ley que garantizara la protección de datos personales, específicamente en posesión de particulares, radicaba en tratar de evitar el entorpecimiento del comercio, particularmente el comercio detonado por el dinamismo de las tecnologías de información actuales, debido a éstas presentan un gran potencial para los beneficios personales y de negocios en los países, para sus gobiernos, así como para la expansión de mercados, la productividad, la educación, la salud pública o la innovación tecnológica y científica. Así también busca que México cumpla los compromisos internacionales asumidos, tales como los lineamientos de la OCDE y el Marco de Privacidad de APEC. Esta iniciativa no solo buscaba la protección de derechos humanos y

[67] Gaceta Parlamentaria, Cámara de Diputados, número 1953-I, jueves 23 de febrero de 2006, *http://gaceta.diputados.gob.mx/*

[68] Gaceta Parlamentaria, Cámara de Diputados, número 1972-I, miércoles 22 de marzo de 2006, *http://gaceta.diputados.gob.mx/*

libertades fundamentales, sino también de la economía nacional y el aseguramiento del comercio irrestricto entre las entidades federativas, y con otros Estados extranjeros. Como propuesta de la iniciativa, se alude a la creación de un Registro de bases de datos; sobre el procedimiento de protección de datos no refiere nada, dejando el tema a reserva de lo previsto en el Reglamento correspondiente. Un aspecto que consideramos erróneo en esta ley es que prevé un costo respecto de las solicitudes de información; lo cual podría convertirse en un obstáculo para el pleno ejercicio de este derecho.

Dos años más tarde vuelve a presentarse una iniciativa, esta vez por parte del diputado Luis Gustavo Parra Noriega, el 7 de octubre de 2008, la Ley de Protección de Datos Personales en Posesión de Particulares.[69]

Al igual que el Senador García Torres, el Diputado Parra consideró la necesidad de esta ley en razón de que México no cumplía con los requisitos mínimos en materia de protección de datos personales, lo cual desincentivaba el comercio con países de la Unión Europea que exigen cierto grado de protección en la materia. Esta iniciativa propuso una ley federal atendiendo a lograr la efectividad de la protección de datos en todo el país, a fin de no entorpecer el buen desarrollo del comercio. Se prevé la creación de un órgano especializado en protección de datos, la Comisión Nacional de Protección de Datos Personales. El Diputado Parra además de pretender la promulgación de una ley especializada en la materia, propone una reforma al artículo 73 de la Constitución para facultar al Congreso a legislar en materia de datos personales. Un dato curioso que esta iniciativa es que denomine al Procedimiento de protección de derechos ante el IFAI como Procedimientos de declaración administrativa de infracción; con lo cual pudiera confundirse el objetivo del procedimiento que es garantizar el control sobre nuestra información, y no así sancionar infracciones, pues para ello se debería referir a un procedimiento sancionatorio específicamente.

[69] Gaceta Parlamentaria, Cámara de Diputados, número 2607-III, martes 7 de octubre de 2008, *http://gaceta.diputados.gob.mx/*

El mismo año el 11 de diciembre, el Diputado Adolfo Mota Hernández presenta su iniciativa de la Ley Federal de Protección de Datos Personales[70]. El Diputado consideró que los principales sectores que manejan una gran cantidad de datos personales y por ende necesitan ser objeto de regulación, son el comercio, la publicidad y el ámbito laboral. En los cuales los datos personales adquieren un valor económico importante dentro de la economía nacional.

Al ser los datos un insumo necesario para estos ámbitos, el Diputado pretendía instaurar una legislación que encontrara un balance entre la protección efectiva de los datos, y por tanto de los derechos de los particulares, y la necesidad de dichos datos para la generación de productos y servicios que generen valor económico, empleo y desarrollo en el país. Además de que permitiera cumplir con los compromisos internacionales adquiridos por el Estado mexicano, tales como lo establecido por la APEC y OCDE.

Para cumplir con este objetivo, el Diputado propone no solamente sancionar el mal uso de los datos, sino de proveer a los individuos de mecanismos para ejercer efectivamente los derechos ARCO. Es decir, busca regular el derecho a la autodeterminación informativa de las personas que permita, por una parte, la transferencia legítima, controlada e informada de los datos personales y por otra, la protección a la privacidad cuando se trate de datos sensibles, así como regular el tratamiento de los datos personales por parte de los sujetos responsables conforme a este ordenamiento.

Es relevante destacar que esta iniciativa no ve en las nuevas tecnologías de información solo un riesgo para los datos personales, sino como un mecanismo que puede proveer medidas de protección adecuadas y positivas que permitan a los individuos ejercer su derecho a elegir quienes manejan, y como deben ser manejados sus datos personales.

[70] Gaceta Parlamentaria, Cámara de Diputados, número 2653-VII, jueves 11 de diciembre de 2008, *http://gaceta.diputados.gob.mx/*

Un aspecto negativo de esta iniciativa es que no establece la responsabilidad de consentimiento ante la transferencia por encontrar que ello no es ni práctico, ni establece un nivel efectivo de protección para el titular de los datos; lo cual vulnera el principio del consentimiento. Así también consideramos una contradicción que por un lado se prevea el Instituto de Protección de Datos Personales como un organismo descentralizado, pero al mismo tiempo disponga que dependa de la Secretaría de Economía.

Por su parte el 2 de febrero de 2010, la Diputada Norma Leticia Orozco Torres presentó su iniciativa de la Ley General de Protección de Datos Personales;[71] con la finalidad proteger a la ciudadanía de las grandes corporaciones, que pueden hacer un uso indebido de la información que poseen de sus clientes, motivo por el cual esta iniciativa se enfoca al sector privado.

Sin dejar desprotegido el mercado, dicho de otra manera, la Diputada pretende una ley flexible para que las empresas puedan crear libremente bases de información dentro de las exigencias del mundo globalizado a fin de atraer inversiones extranjeras dando certidumbre jurídica tanto a empresas como a ciudadanos. Así como dar cumplimiento al mandato constitucional del artículo 16; a fin de establecer los principios, derechos y obligaciones que regulan la protección y tratamiento de los datos personales en posesión de los sectores públicos y privados.

Como aspecto característico de esta iniciativa, es que no prevé la creación de un nuevo organismo especializado en protección de datos, sino que otorga facultades al Instituto Federal de Acceso a la Información Pública (IFAI) para vigilar y sancionar el correcto cumplimiento del ordenamiento, amén de la seguridad de los datos de las personas.

[71] Gaceta Parlamentaria, Cámara de Diputados, número 2940-III, martes 2 de febrero de 2010, *http://gaceta.diputados.gob.mx/*

Al proponerse una ley general, la legisladora buscaba que la misma se aplicara en lo no dispuesto por las leyes locales ya existentes en la República, tal como la Ley de Colima.

Finalmente para concluir con las iniciativas presentadas, toca el turno al Senador José Guillermo Anaya Llamas, quien presento la Ley de Protección de Datos Personales, el 1° de diciembre de 2009.[72]

La prioridad de esta ley, el Senador la encuentra en el volumen de servicios que necesitamos contratar, y para los cuales es necesario proporcionar nuestros datos, tales como obtener un crédito, realizar comprar, inscribirse a alguna organización o institución.

Esta iniciativa al igual que la propuesta por la Diputada Orozco, está en pro de ampliar las facultades al IFAI para que sea el órgano garante de la protección de datos personales, a fin de compatibilizar el derecho a la información sin vulnerar el derecho a la vida privada y a la intimidad, a la vez de que administrativamente se aprovechará una estructura existente que impida un mayor gasto en el erario público.

Una particularidad de esta iniciativa es que en vez de un procedimiento administrativo ante el IFAI, establece un recurso de reclamación, y contra la resolución sobre este recurso, establece otro recurso, el de revisión.

Como pudimos constatar en este apartado, las iniciativas que se presentaron en materia de protección de datos personales, tienen como objetivo en su mayoría salvaguardar los intereses del comercio a la par de garantizar un control sobre su información a las personas. Encontramos algunas disparidades entre cada una de ellas, pues por un lado algunas iniciativas amplían su protección a las personas jurídicas, otras las restringen; así también algunas buscan regular tanto los ficheros de titularidad pública como privada, o simplemente se avocan a las relaciones entre particulares. Inclusive en el alcance de la norma hay

[72] Gaceta del Senado, *http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=23424*

disparidades, pues no todas las iniciativas responden al precepto constitucional contenido en el artículo 73, pues algunas tratan de darle cabida a las legislaciones locales.

Estas iniciativas forman parte del antecedente la actual Ley de Protección de Datos Personales en Posesión de Particulares; misma que será motivo de estudio en los siguientes párrafos.

De las iniciativas que hemos visto en los párrafos anteriores, debemos advertir que sin bien constituyen todas ellas un antecedente legislativo en materia de protección de datos, no todas fueron consideradas para elaborar la ley actual de protección de datos personales en posesión de particulares, ninguna de las presentadas por los Diputados Barbosa Huerta, Martínez Álvarez y Orozco Torres.

Respecto a la ley actual cabe decir que el legislador optó por federalizar la ley que regulara los datos personales, debido a la necesidad de unificar la tutela de un derecho fundamental en todo el país, en cuanto a derechos, principios y procedimientos de protección, evitando de esta manera su respeto asimétrico al expedirse tantas leyes como entidades federativas tiene la República mexicana; por otro lado, atendiendo al comercio internacional, en virtud de que el Estado Mexicano hacia el exterior es uno y como tal debe contar con una legislación uniforme en sus relaciones internacionales, independientemente del área del territorio nacional donde materialmente se estén tratando los datos personales; y por la otra, dado la naturaleza federal de la materia de comercio.

En cuanto a las iniciativas que preveían la creación de un órgano especializado en datos personales, el legislador compartió el punto de vista planteado por Orozco Torres, y en vez de crear un nuevo organismo, decidió dotar de nuevas facultades al Instituto Federal de Acceso a la Información (IFAI); atendiendo a evitar costos; lograr una unicidad de criterios a fin de evitar conflictos potenciales entre los criterios de apertura de información y la protección de datos personales; para aprovechar el conocimiento y especialización en materia de datos personales

adquirido por este instituto, y finalmente debido al posicionamiento con que éste contaba dentro de la sociedad.[73]

Otro aspecto que la ley actual no tomó en cuenta de las propuestas presentadas en las diferentes iniciativas, es lo referente al Registro de bases de datos, pues de acuerdo al dictamen emitido por el Senado, esto conllevaría un proceso burocrático que no añade bondades significativas a la protección de los datos de los titulares.

Finalmente el 5 de julio de 2010 es publicada en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en posesión de Particulares; no es hasta el 21 de diciembre de 2011 que se publica el reglamento que desarrolla el contenido de esta ley; no obstante en los transitorios de la ley se había previsto que el reglamento debía formularse un año después de la entrada en vigor de la ley.

En la jurisprudencia emitida por los Tribunales Federales, el avance es precario y todo conlleva al desarrollo de criterios interpretativos que giran en torno a la protección del domicilio o de las comunicaciones privadas, claros ejemplos de regulación que va encaminada la protección de la intimidad.

4.4.3 Ejercicio de los derechos ARCO

Una vez que hemos revisado el proceso constitucional y legislativo del tema de protección de datos personales en nuestro país, podemos comprender de mejor manera el sentido de la Ley Federal de Protección de Datos Personales en Posesión en Particulares; la cual establece dos procedimientos para ejercer los

[73] "Proceso legislativo de la Ley Federal de Protección de Datos Personales en Posesión de Particulares", *http://www2.scjn.gob.mx/AccesoInformacion/ProcsLegs.asp?nIdLey=75562&nIdRef=1&cFechaPub=05/07/2010&cCateg=LEY&cTitulo=LEY%20FEDERAL%20DE%20PROTECCION%20DE%20DATOS%20PERSONALES%20EN%20POSESION%20DE%20LOS%20PARTICULARES*

derechos ARCO, a fin de garantizar la protección de los datos personales; los cuales son:

a) Procedimiento de solicitud para el acceso, rectificación, cancelación y oposición a los datos personales, ante el responsable del tratamiento de los datos personales.
b) Procedimiento de solicitud de protección de derechos, ante el Instituto de Acceso a la Información y Protección de Datos.

4.4.3.1 Frente al responsable del tratamiento

El primer paso para ejercer los derechos ARCO se realiza ante el responsable del tratamiento, mediante la presentación de una solicitud por parte del titular de los datos o bien de su representante legal, para lo cual no se fija ningún plazo. Dicha solicitud debe contener como requisitos generales los siguientes:

i. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
ii. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;
iii. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y
iv. Cualquier otro elemento o documento que facilite la localización de los datos personales.

Además de estos requisitos, para ejercer el derecho de rectificación es necesario que el solicitante indique cuáles son las modificaciones a su información que solicita, así como presentar la documentación que sustente su petición. El responsable podrá requerir dentro de los cinco días siguientes a recibida la solicitud, información adicional; para lo cual el titular dispondrá de diez días para satisfacer el requerimiento.

Presentada la solicitud, el responsable deberá dar respuesta dentro de los siguientes veinte días, y en caso de ser procedente deberá proceder a ejecutar la solicitud dentro de los quince días siguientes; en el supuesto de ser improcedente el solicitante podrá acudir ante el Instituto Federal de Acceso a la Información y Protección de Datos Personales para continuar con el procedimiento de protección de derechos.

Los plazos por la ley fijados, pueden ampliarse por una sola vez por un período igual, siempre que el responsable justifique las circunstancias del caso, previa notificación al solicitante.

4.4.3.2 Procedimiento de protección de derechos

Una vez que el titular haya agotado la vía frente al responsable del tratamiento y no siendo favorable la respuesta de aquél, en razón de no haberse pronunciado sobre la solicitud, la haya estimado improcedente, o habiendo dado contestación ésta sea incompleta, incomprensible o no se refiera al asunto planteado en la solicitud; el titular podrá iniciar el procedimiento de protección de derechos.

El procedimiento inicia con la presentación de una solicitud de protección de datos ante el Instituto Federal de Acceso a la Información y Protección de Datos Personales, la cual puede ser presentada por derecho propio o en representación de otro dentro de los quince días siguientes a que haya recibido contestación a su solicitud o habiendo vencido el plazo para ello; siendo validos tanto los medios físicos como electrónicos, siempre y cuando contenga los siguientes requisitos:

I. El nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay;
II. El nombre del responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales;

III. El domicilio para oír y recibir notificaciones;
IV. La fecha en que se le dio a conocer la respuesta del responsable, salvo que no hubiera dado respuesta;
V. Los actos que motivan su solicitud de protección de datos, y
VI. Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

Además de proporcionar estos datos, el titular deberá acompañar a su solicitud la respuesta que hubiese recibido por parte del responsable, en el supuesto de haberla recibido. En caso de que el titular haya optado por presentar la solicitud físicamente, deberá anexar las copias de traslado.

Una vez recibida la solicitud el Instituto deberá acordar sobre su admisión, o en el supuesto de que no cumpla con alguno de los requisitos, dentro de los siguientes veinte días a presentada la solicitud, prevendrá al solicitante, para que en un plazo de cinco días subsane las omisiones.

Admitida la petición el Instituto correrá traslado al responsable para que en un plazo de quince días dé respuesta a la misma y ofrezca pruebas. En el supuesto que el responsable no de respuesta, el Instituto le dará vista para que en el plazo de diez días acredite haber respondido en tiempo o bien responda en ese plazo.

Cuando el responsable haya dado contestación, el Instituto procederá a la admisión de pruebas, pudiendo solicitar pruebas para mejor proveer, las cuales de atendiendo a su naturaleza podrán ser desahogadas en audiencia. Después de haberse desahogado el Instituto fijará un plazo de cinco días para que las partes expongan sus alegatos.

Finalmente el Instituto deberá dictar su resolución dentro de los cincuenta días siguiente a la presentación de alegatos, plazo que puede ser prorrogado por un período igual por una sola vez y mediante causa justificada. Los efectos de la resolución serán el sobreseimiento, desechamiento, confirmación, revocación o modificación de la respuesta dada por el responsable. Contra las resoluciones que

emita el Instituto procederá el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

La solicitud será desechada por improcedente cuando el Instituto no sea competente; por haber una resolución firme contra el mismo hecho; porque se encuentre en trámite ante otra instancia; se trate de una solicitud ofensiva o irracional, o se haya presentado de forma extemporánea.

Los casos previstos por la ley en que las solicitudes serán sobreseídas; son cuando el titular fallezca, por desistimiento del titular; sobrevenga una causal de improcedencia; o bien la solicitud quede sin materia.

En caso de que sea procedente la solicitud, el responsable contará con un plazo de diez días para dar cumplimiento a la resolución del Instituto; debiendo dar cuenta del cumplimiento al mismo en un plazo de diez días.

Es importante resaltar que la ley prevé la posibilidad de un procedimiento de conciliación entre las partes, el cual será a voluntad de ellas; la cual deberá ser manifestada en un plazo no mayor a diez días siguientes a la admisión de la solicitud o bien en cualquier momento del procedimiento. Al efecto el Instituto señalara lugar y fecha para la celebración de la audiencia de conciliación; misma que deberá celebrarse dentro de los siguientes veinte días a que se hubiese expresado la voluntad de las partes de conciliar. La audiencia podrá suspenderse hasta en dos ocasiones. En el caso de que alguna de las partes no asista a la audiencia por causa injustificada o no se llegue a ningún acuerdo se continuara con el procedimiento de protección de derechos. Si ambas partes logran conciliar se establecerá el acuerdo mediante escrito que tendrá efectos vinculantes; y con el cumplimiento de éste se terminara el procedimiento de protección de derechos.

Visto el procedimiento de protección de derechos, resaltaremos que de las resoluciones publicadas por el IFAI, la mayoría de solicitudes se ha desechado por improcedente al haberse presentado fuera de los plazos establecidos en la ley; lo cual nos lleva a reflexionar sobre la falta de divulgación que sobre el tema persiste

entre la ciudadanía; no obstante haber sido la popularidad y experiencia del Instituto entre la sociedad, el móvil para facultarlo como órgano especializado en materia de protección de datos.

Al termino de este capítulo tenemos una idea somera del proceso legislativo que ha recorrido la protección de datos personales en los tres países objeto de estudio; así como también que en cada uno de ellos el procedimiento establecido para el ejercicio de los derechos ARCO toma una vía distinta, pues mientras en España y Argentina se ha optado por la vía administrativa en Argentina se recurre a la vía ordinaria civil.

CONCLUSIONES

PRIMERA: La protección de datos personales ha sido materia de regulación normativa desde hace tiempo, sin embargo ha cobrado trascendencia retomar su estudio, en virtud de que dicha legislación se ha visto rebasada por la utilización de las nuevas tecnologías.

SEGUNDA: Actualmente vivimos en una sociedad conocida como de la información, debido a la gran cantidad de información que diariamente fluye entre los diversos sectores. La sociedad de la información conlleva a que se garantice una mayor protección de datos personales; en razón de que nuestra información es requerida en casi todas las actividades que realizamos de manera cotidiana, como lo son acceder a un servicio o realizar una compra.

TERCERA: El derecho de acceso a la información, que en algunos casos puede encontrarse en conflicto con la protección de datos personales, sin embargo tendrá que encontrar el justo equilibrio entre ambos derechos mediante la ponderación de derechos; pues lo que se busca con la protección, no es censurar la información, sino mantener el control sobre la misma.

CUARTA: La protección de datos personales no busca proteger propiamente a los datos, sino la repercusión que su inadecuada utilización podría provocar, vulnerando otros bienes jurídicamente tutelados.

QUINTA: Los datos personales no deben minimizarse a los datos íntimos, en virtud de que aquéllos son una especie del género, pues lo esencial de estos datos no es que refieran a la vida íntima de la persona, sino que mediante su entrelazamiento se logra configurar un perfil del titular.

SEXTA: La protección de datos en su origen representó una modalidad positiva del derecho a la intimidad, sin embargo actualmente mantiene un reconocimiento a nivel constitucional como derecho autónomo e independiente, y más aun como un derecho fundamental.

SÉPTIMA: Reconocer la autonomía del derecho a la protección de datos, nos permite sostener que las personas jurídicas al igual que las físicas pueden ser consideradas como titulares de datos personales, sin dejar de tomar en cuenta que esta extensión no sería aplicable para el caso especifico de los datos sensibles.

OCTAVA: Las legislaciones en materia de protección de datos se han visto influenciadas de tintes meramente mercantiles, pues el objetivo principal antes que proteger la esfera jurídica de la persona, ha sido salvaguardar el normal desarrollo de las transacciones comerciales, impidiendo que obstáculos como el no contar con una adecuada legislación en materia de protección de datos pueda impactar negativamente en las relaciones comerciales que se tienen tanto al interior como al exterior de cada país.

NOVENA: Los derechos ARCO representan un medio de control que permite garantizar la protección de datos mediante un control de los datos personales objeto de tratamiento.

DÉCIMA: El derecho de Acceso constituye en la mayoría de los casos el primer paso para ejercer los derechos de rectificación, cancelación y oposición; por lo tanto es importante garantizar el ejercicio de este derecho mediante la creación de un registro de bases privadas de datos, que lejos de ser innecesario, constituye una útil herramienta que permitiría no solamente dar certeza a los titulares de a dónde acudir para conocer las bases existentes que posiblemente contengan información que les es propia; sino también, ejercer un control sobre la creación y operación de las bases encargadas del tratamiento de los datos personales, a fin de que se encuentren apegadas a los principios establecidos.

DÉCIMA PRIMERA: A partir de las resoluciones publicadas por el IFAI, en las cuales la constante en las mismas, es el desechamiento por extemporaneidad en la presentación de las solicitudes de protección de datos, lo cual nos lleva a la reflexión de que hace falta una mayor difusión de la cultura de los datos personales y sus correlativos derechos ARCO.

DÉCIMA SEGUNDA: Es necesario que la sociedad tome conciencia de la problemática en torno a la inadecuada protección de datos personales, para que además de las medidas normativas que se han emprendido, se complementen con acciones técnicas que los propios particulares pueden emplear.

BIBLIOGRAFÍA

ARAUJO CARRANZA, Ernesto, *El derecho a la información y la protección de datos personales en México*, México, Editorial Porrúa, 2009.

ARMAGNAGUE, Juan (Dir.), *Derecho a la información, habeas data e internet,* Argentina, Ediciones La Rocca, 2002.

BASTERRRA, Marcela I., *Protección de datos personales. Ley 25.326 y Dto. 1558/01 comentados Derecho Constitucional Provincial Iberoamericana y México, Argentina*. Argentina. Editorial Ediar. 2008.

BASTIDA, Francisco J. et al, *Teoría general de los derechos fundamentales en la Constitución española de 1978*, España, Ed. Tecnos, 2004,

BOBBIO, Norberto, *Estado, gobierno y sociedad. Por una teoría general de la política*, México, Fondo de Cultura Económica, 2006.

CAMPUZANO TOMÉ, Herminia, *Vida privada y datos personales*, España, Editorial Tecnos, 2000.

CARBONELL, Miguel, *Los derechos fundamentales en México*, México, Editorial Porrúa, 2004.

CARRANZA TORRES, Luis R. Hábeas data. *La protección jurídica de los datos personales. Argentina*, Editorial Alveroni, 2001.

CASTELLS, Manuel y HIMANEN, Pekka, *El Estado del bienestar y la sociedad de la información. El modelo finlandés*, España, Alianza Editorial, 2002.

CELIS QUINTAL, Marcos Alejandro. “La protección como derecho fundamental de los mexicanos” en CIENFUEGOS SALGADO, David y MACÍAS VÁZQUEZ, María Carmen (Coods.), *Estudios en homenaje a Marcia Muñoz De Alba Medrano. Protección de la persona y derechos fundamentales,* México, UNAM, 2006.

CORRALES CASTILLO, Warren, Tesis: “Viabilidad jurídica de la implementación del recurso de habeas data para regular la discriminación en los procesos de selección de personal en razón de bases de datos”, Instituto de Investigaciones Jurídicas, Facultad de Derecho, Universidad de Costa Rica, 2011.

DAVARA F. DE MARCOS, Isabel. “Breve análisis de la reforma al artículo 6° constitucional en lo relativo a protección de datos personales”, en CARBONELL, Miguel y BUSTILLOS, Jorge (Coords.), *Hacia una democracia de contenidos: la reforma constitucional de transparencia*, México, Instituto de Investigaciones Jurídicas, UNAM, 2007.

FERNÁNDEZ RODRÍGUEZ, José Julio, *Lo público y lo privado en internet. Intimidad y libertad de expresión en la Red*, México, Instituto de Investigaciones Jurídicas, UNAM, 2004.

ECO, Humberto, *Como se hace una tesis: técnicas y procedimientos de estudio, investigación y escritura*, España, Gedisa, 2001.

GARRIDA DOMÍNGUEZ, Ana, *Tratamiento de datos personales y derechos fundamentales,* 2ª ed., España. Editorial Dykinson S.L., 2009.

GARZÓN VALDÉS, Ernesto, *Lo íntimo, lo privado y lo público*, 5° ed., México, IFAI, Cuadernos de Transparencia 06, 2008.

GILS CARBÓ, Alejandra M., *Régimen legal de las bases de datos y hábeas data*, Argentina, Editorial La Ley, 2001.

GONZÁLEZ MARTÍNEZ, Nuria, “Igualdad y discriminación genética”, en MUÑOZ DE ALBA MEDRANO, Marcia (coord.), *Temas selectos de salud y derecho*, México, Instituto de Investigaciones Jurídicas UNAM, 2002.

GÓMEZ-ROBLEDO, Alonso y ÓRNELAS NÚÑEZ, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, Instituto de Investigaciones Jurídicas, UNAM, 2006.

GOZAINI, Osvaldo Alfredo, *Habeas data. Protección de datos personales*, Argentina, Rubinzal-Culzoni Editores, 2001.

GÜITRON FUENTEVILLA, Julián, *Tesis*, México, Promociones Jurídicas y Culturales, 1991.

LÓPEZ-VIDRIERO TEJEDOR, Iciar y SANTOS PASCUAL, Efrén, *Protección de datos personales. Manual práctico para empresas*, España, Editorial Fundación Confemetal 2005.

MALDONADO OTERO, Claudia, "La Ley Federal de Protección de Datos Personales en posesión de los particulares en México", en IBARRA SÁNCHEZ, Ernesto y ROMERO FLORES, Rodolfo, (coords), *Jurismática. El derecho y las Nuevas Tecnologías. Estudios en homenaje a Julio Téllez Valdés por sus 30 años de labor académica en el derecho informático*, México, Universidad Autónoma de Nuevo León, 2010.

MÁRQUEZ ROMERO, Raúl, *Lineamientos y criterios del proceso editorial*, México, Instituto de Investigaciones Jurídicas UNAM, 2008.

MONTBRUN, Alberto et al, "Apuntes Sobre la Reforma Constitucional de 1994", *Material de estudio de los Cursos de Equivalencia del Instituto Universitario de Seguridad Pública.*

MUÑOZ DE ALBA MEDRANO, Marcia y CANO VALLE, Alberto, *Derechos de las personas con síndrome de inmunodeficiencia adquirida*, México, Cámara de diputados-UNAM, 2002.

MURILLO DE LA CUEVA, Pablo Lucas, *El derecho a la autodeterminación informativa,* España, Fundación Coloquio Jurídico Europeo, 2009.

OVILLA BUENO, Rocío, *La protección de los datos personales en México*, México, Editorial Porrúa, 2005.

ORWELL, George, *1984,* México, Editorial Época, 2005.

PIÑAR MAÑAS, José L*., IV Encuentro iberoamericano de protección de datos personales*, México, IFAI, 2005.

----------, *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de datos, La Antigua-Guatemala, 2-6 de junio de 2003),* España, Editorial Tirant lo blanch, 2005.

PUCCINELLI, Oscar. R., *Protección de Datos De Carácter Personal*, Argentina, Editorial Astrea, 2004.

RABOTNIKOF, Nora, *En busca de un lugar común. El espacio público en la teoría política contemporánea,* México, UNAM, Instituto de investigaciones filosóficas, 2005.

----------, *El espacio público y la democracia moderna*, México, Colección Temas de Democracia IFE, 1997.

REBOLLO DELGADO, Lucrecio, *El derecho fundamental a la intimidad*, España, Ed. Dykinson, 2000.

----------, "Vida Privada y protección de datos: Un acercamiento a la regulación internacional Europea y Española" en MAQUEDA ABREU, Consuelo y MARTÍNEZ BULLÉ GOYRI, Víctor M. (Coords.), *Derechos humanos: temas y problemas*, México, Instituto de Investigaciones Jurídicas UNAM, 2010.

RIQUERT, Marcelo Alfredo, *Protección Penal de la Intimidad en el Espacio Virtual,* Argentina, Editora Ediar, 2003.

RUIZ MIGUEL, Carlos, *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, España Editorial Civitas, 1994.

SERRANO PÉREZ, Ma. Mercedes, “El derecho fundamental a la protección de datos. Su contenido esencial”, *Nuevas políticas públicas. Anuario multidisciplinar para la modernización de las administraciones públicas.*

SCHWABE, Jürgen, *Cincuenta Años de Jurisprudencia del Tribunal constitucional Federal Alemán*, Colombia, Ediciones jurídicas Gustavo Ibañez, 2003.

UICICH, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad*, Argentina, Ad-Hoc, 1999.

VIANNA, Túlio, “El derecho a no ser registrado”, en *Anuario de derecho constitucional latinoamericano*, Tomo II, Konrad Adenauer Stiftung, Uruguay, 2007.

WARREN, Samuel y BRANDEIS, Louis, *El derecho a la intimidad*, España, Editorial Civitas S.A., 1995.

Hemerografía

AGUADO RENEDO, César, “La protección de los datos personales ante el Tribunal Constitucional Español”, *Revista Mexicana de Derecho Constitucional*, México, núm. 23, julio-diciembre de 2010, *http://biblio.juridicas.unam.mx/revista/pdf/CuestionesConstitucionales/23/ard/ard1.pdf*

ARADAS, Anahi, “Nuestros datos personales son el nuevo petróleo”, *BBC Mundo*, Reino Unido, 16 abril de 2012, *http://www.bbc.co.uk/mundo/movil/noticias/2012/04/120416_tecnologia_datos_personales_petroleo_aa.shtml*

AVELEYRA, Antonio M. “El derecho de acceso a la información pública vs el derecho de libertad informática (¿conflicto entre el derecho a la información y el derecho a la intimidad de los datos personales?). Aportaciones desde la teoría del derecho”, *Jurídica. Anuario del Departamento de Derecho de la*

Universidad Iberoamericana, México, núm., 32, 2002, *http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/32/pr/pr24.pdf*

BAZÁN, Víctor, "El derecho a la vida privada y el derecho a la libertad de información en la doctrina y jurisprudencia de la Corte Suprema de Justicia Argentina", *Estudios Constitucionales*, Chile, vol. 6, núm. 001, 2008, *http://redalyc.uaemex.mx/redalyc/html/820/82060106/82060106.html*

----------, "El Habeas Data, el Derecho a la Autodeterminación Informativa y la Superación del Concepto Preinformático de la Intimidad", *Boletín Mexicano de Derecho Comparado,* México, núm. 94, enero-abril 1999*, http://www.juridicas.unam.mx/publica/rev/boletin/cont/94/art/art1.htm*

CARBONELL, Miguel (coord.), *Derechos fundamentales y Estado. Memoria del VII Congreso Iberoamericano de Derecho Constitucional*, México, Instituto de Investigaciones Jurídicas UNAM, 2002. *http://www.ejournal.unam.mx/cuc/cconst09/CUC00902.pdf*

CARNOTA, Walter F., "Dos visiones constitucionales divergentes sobre el amparo: los casos Argentino y Español", *Cuestiones Constitucionales*, México, núm., 9, julio-diciembre de 2003,

CLAVERO, B., Manuel en CRUZ VILLALÓN, Pedro y PARDO FALCÓN, Javier, "Los Derechos Fundamentales en la Constitución Española de 1978", *Boletín Mexicano de Derecho Comparado*, México, núm. 97, enero-abril 2000, *http://juridicas.unam.mx/publica/rev/boletin/cont/97/art/art2.htm#N1*

ELIZALDE, Luciano H. "Lo público y lo privado como problema prepolítico. Un análisis desde la sociología de la comunicación", *Revista Doxa*, España, núm., 7,
http://www.humanidades.uspceu.es/pages/investigacion/humanidades-investigacion-revista-doxa-VII.html.

ESTEVA GALLICCHIO, Eduardo Gregorio, “El derecho a la protección de la vida privada y el derecho a la libertad de información en la doctrina y en la jurisprudencia, en Uruguay”, *Estudios Constitucionales*, Chile, Año 6, núm. 1, 2008, *http://www.cecoch.cl/htm/revista/docs/estudiosconst/revistaano_6_1.htm/elderecho03.pdf*

FERNANDO MAGARZO, María del Rosario, “La protección de datos personales en el ámbito de la publicidad en la legislación española, Revista Chilena de derecho informático, núm. 7, Chile, 2005, *http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10764/1102*

GARCÍA DE ENTERRÍA, Eduardo, “La Constitución Española de 1978 como pacto social y como norma jurídica”, *Boletín Mexicano de Derecho Comparado*, México, núm. Conmemorativo, 2008, *http://www.juridicas.unam.mx/publica/rev/boletin/cont/123.5/cnt/cnt16.htm*

GARCÍA PLAZA, Tatiana, “La aplicación del derecho a la Intimidad en la publicidad registral en la actual legislación ecuatoriana”, *Revista Jurídica Online de la Facultad de Jurisprudencia y Ciencias Sociales y Políticas. Universidad Católica de Santiago de Guayaquil*, Ecuador, *http://www.revistajuridicaonline.com/images/stories/revistasjuridicas/derecho-publico-tomo-2/271a296_la_aplicacion.pdf*

GERON, Tomio , “Path Apologizes For Contact Uploads, Deletes Data”, *Forbes Review*, 2 agosto de 2012, *http://www.forbes.com/sites/tomiogeron/2012/02/08/path-apologizes-for-contact-uploads-deletes-data/*

GOZAINI, Osvaldo Alfredo, “El proceso de habeas data en la nueva ley de protección de datos personales”, Revista Jurídica, Argentina, 21 abril de 2006,

http://dspace.uces.edu.ar:8180/dspace/bitstream/123456789/412/1/El_proceso_de_habeas_data_parte01.pdf

KNORR, Jolene Marie et al, "La protección del consumidor en el comercio electrónico", *Revista de Ciencias Jurídicas*, Universidad de Costa Rica, Costa Rica, núm. 103, enero-abril de 2004, *http://www.iij.ucr.ac.cr/archivos/publicaciones/revista/Revista%20103.pdf*

LÓPEZ-BELLO MORENO, Alfonso I., "Protección de datos de carácter personal", *El mundo del abogado*, 1 diciembre de 2011, *http://elmundodelabogado.com/2011/proteccion-de-datos-de-caracter-personal/*

NÁJERA, Javier, "El aspecto axiológico de los datos personales en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental", *Revista de Derecho Comparado de la Información*, México, núm. 11, enero-junio de 2008,
http://www.juridicas.unam.mx/publica/rev/decoin/cont/11/art/art5.htm

PALAZZI, Pablo, "El hábeas data en el derecho argentino", *Revista de Derecho Informático*, Argentina, núm. 4, noviembre de 1998, *http://www.robertexto.com/archivo12/data_der_argen.htm*

PERALTA, Leonardo, "En México tienes derecho al olvido digital, pero, ¿qué es eso? De acuerdo con la ley, los internautas pueden pedir que sus datos personales sean borrados de la red con fines de seguridad", *CNN,* México, 14 marzo 2012, *http://mexico.cnn.com/tecnologia/2012/03/14/en-mexico-tienes-derecho-al-olvido-digital-pero-que-es-eso*

ROSARIO RODRÍGUEZ, Marcos Francisco del, "La protección de datos personales entre particulares: esbozos de un esquema de regulación y protección en México", *Revista Derecho Comparado de la Información*, México, Nueva serie, núm. 20, julio-diciembre 2012, *http://biblio.juridicas.unam.mx/revista/pdf/DerechoInformacion/20/art/art4.pdf*

ROSEN, JEFFREY, “The Right to Be Forgotten”, *Stanford Law Review,* núm., 64, 13 febrero de 2012, *http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten*

SÁNCHEZ PÉREZ, Gabriel y ROJAS GONZÁLEZ, Isai, “Leyes de protección de datos personales en el mundo y la protección de datos biométricos”, Parte I, *Revista Seguridad defensa digital*, México, núm., 13, 5 junio de 2012, *http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93*

SÁNCHEZ URRUTIA, Ana Victoria, “Información genética, intimidad y discriminación”, Acta bioethica, edición online, vol. 8 núm. 2, 2002, http://www.scielo.cl/scielo.php?pid=S1726569X2002000200007&script=sci_arttext

VELASCO SAN MARTIN, Cristos, “Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?”, *Boletín de Política Informativa*, núm. 1, 2003, *http://www.inegi.gob.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf*

WARREN, Samuel y BRANDEIS, Louis, “The Right of Privacy”. *Harvard Law Review,* Vol. IV, Estados Unidos, Núm. 5, 15 diciembre de 1890, *http://www.dataprotection.it/the_right_to_privacy.htm*

Diccionarios

Diccionario de la Real Academia de la Lengua Española. 22 ed. *http://buscon.rae.es/draeI/.*

Documentos de Internet

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía para la lucha contra el Spam", *http://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM--ap-V.-30-mayo-cp-.pdf.*

----------,"El derecho fundamental a la protección de datos: Guía para el Ciudadano". *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf#*

----------, "Recomendaciones al sector del comercio electrónico, para la adecuación de su funcionamiento a la ley orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal", *http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_comercio_electronico.pdf*

----------, Informe 0278/2009, *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0278_Cesi-oo-n-de-datos-de-personas-fallecidas-c--exclusi-oo-n-de-la-aplicaci-oo-n-de-la-LOPD.pdf*.

----------, Nota sobre el auto de la Audiencia Nacional en el que plantea al Tribunal de Justicia de la Unión Europea diversas cuestiones prejudiciales sobre el ejercicio de derechos frente a buscadores de internet", 2 marzo de 2012, *http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/marzo/120302_Nota_cuestion_prejudicial.pdf*

AUDIENCIA NACIONAL ESPAÑOLA, "Solicitud al Tribunal Europeo de Justicia respecto a Denuncias relacionadas con el Derecho al Olvido", *http://www.protecciondedatos.org.mx/2012/03/solicitud-audiencia-nacional-*

espaola-tribunal-europeo-justicia-respecto-denuncias-relacionadas-derecho-olvido/

BLOG JURÍDICO DEDICADO AL DERECHO CONSTITUCIONAL ARGENTINO, "Reforma Constitucional 1994. Convencional Nacional Constituyente", *http://federacionuniversitaria52.blogspot.mx/2009/04/reforma-constitucional-1994.html*

CÁMARA DE DIPUTADOS DEL CONGRESO DE LA NACIÓN DE LA REPÚBLICA ARGENTINA, "Antecedentes Parlamentarios de la Ley de Protección de los Datos Personales", *http://www.protecciondedatos.com.ar/debatedip.htm*

CÁMARA DE DIPUTADOS DEL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, Gaceta parlamentaria, año IV, número 832, viernes 7 de septiembre de 2001, *http://gaceta.diputados.gob.mx/*

----------, número 1895-I, jueves 1 de diciembre de 2005, *http://gaceta.diputados.gob.mx/*

----------, número 1953-I, jueves 23 de febrero de 2006, *http://gaceta.diputados.gob.mx/*

----------, número 1972-I, miércoles 22 de marzo de 2006, *http://gaceta.diputados.gob.mx/*

----------, número 2607-III, martes 7 de octubre de 2008, *http://gaceta.diputados.gob.mx/*

----------, número 2653-VII, jueves 11 de diciembre de 2008, *http://gaceta.diputados.gob.mx/*

----------, número 2940-III, martes 2 de febrero de 2010, *http://gaceta.diputados.gob.mx/*

CÁMARA DE SENADORES DEL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, Gaceta del Senado, número 66, 08 diciembre de 2009,*http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=23424*

CASTELLS, Manuel. "La era de la información", *http://www.manuelcastells.info/es/obra_index_3.htm*

CONVENCIÓN NACIONAL CONSTITUYENTE DE 1994, "Diario de sesiones", http://www1.hcdn.gov.ar/dependencias/dip/Debate-constituyente.htm

FERNÁNDEZ DELPECH, Horacio et al, "Privacidad y Autorregulación en la era digital", Universidad del Salvador, Argentina, *http://www.hfernandezdelpech.com.ar/PDFPubliTrabPrivaAutoEraDigital.pdf*

GONZÁLEZ MURÚA, Ana Rosa, "El derecho a la intimidad, el derecho a la autodeterminación informativa y la L.O. 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos personales", España, 1994, *http://ddd.uab.cat/pub/worpap/1994/hdl_2072_1371/ICPS96.pdf*

HARO, Ricardo, "Perfiles Fundamentales de la Reforma Constitucional Argentina De 1994", Argentina, 21 diciembre de 1998, *http://www.catedrajuansola.com.ar/wp-content/uploads/2010/06/Ricardo-Haro.pdf*

INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS, "Guía Práctica para ejercer el Derecho a la Protección de Datos Personales", *http://www.ifai.org.mx/*

INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS DEL DF, "Manual de autoformación sobre la ley de protección de datos personales para el Distrito Federal" Colección Capacitación a Distancia, México, núm. 05, 2009, *http://www.infodf.org.mx/capacitacion/publicacionesDCCT/manual5lpdpdf/manualdatospersonales.pdf*

Morachimo, Miguel, “Regulación sobre datos personales y publicidad basada en la identidad”, *Blog Blawyer*, Perú, 12 julio de 2010, *http://www.blawyer.org/2010/07/12/privacidad-datos-mercado-publicidad/*

NAVA GOMAR, Salvador O., “Colisión de derechos fundamentales: acceso a la información y protección de datos personales desde la perspectiva de la jurisdicción electoral”, Suprema Corte de Justicia de la Nación, México, *http://www2.scjn.gob.mx/red/IVTransparencia/Docs/Materiales/Presentaci%C3%B3n%20Magdo%20%20Nava%20Gomar.pdf*

ORNELAS NÚÑEZ, Lina y López Ayllón Sergio, “La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo”, *http://www.seminariodatospersonales.ifai.org.mx/index.php/materia-del-seminario*

PELUFFO, Maria Laura, “La acción de habeas data. ¿Es necesario agotar la vía prejudicial para interponer esta acción? Criterios a favor y en contra”, *Universidad del Salvador,* Argentina, *http://www.salvador.edu.ar/juri/jadpc/Maria%20L.%20Peluffo.pdf*

PÉREZ SERNA, Jesús Mayo, “Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición*)”, Ayuda ley protección de datos*, 12 mayo de 2010, *http://www.ayudaleyprotecciondatos.es/2010/05/12/los-derechos-arco-acceso-rectificacion-cancelacion-y-oposicion/*

PERIU, Mike, “Influencia de las enfermedades preexistentes en el seguro de salud”, *UTC*, 2 abril de 2009, *http://blog.micumbre.com/category/dinero/*

PIACENTE, Pablo, “Indican que publicitar en redes sociales multiplica por 40 la efectividad de una campaña”, 31 agosto de 2010, *http://www.coguan.com/blog/indican-que-publicitar-en-redes-sociales-multiplica-por-40-la-efectividad-de-una-campana*

PLAZA PENADÉS, Javier, Protección de datos de las personas jurídicas, 11 marzo de 2012, *http://www.legaltoday.com/practicajuridica/publico/proteccion_de_datos/proteccion-de-datos-de-las-personas-juridicas*

SALAZAR SANTANA, Bernardo Alfredo, Tratamiento y protección de los datos personales en los expedientes judiciales en La Cuarta Edición del Seminario Internacional de Acceso a la Información Judicial, encaminado a "los beneficios para la Sociedad", 25 al 27 octubre de 2011.

SALGADO SEGUÍN, Víctor Alberto, "Protección jurídica de los datos personales: Aproximación a la LORTAD", La Coruña, 1968, http://www.ua.es/oia/es/legisla/articulo.htm#DES012

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, "Proceso legislativo de la Ley Federal de Protección de Datos Personales en Posesión de Particulares", *http://www2.scjn.gob.mx/AccesoInformacion/UnProcLeg.asp?nIdLey=75562&nIdRef=1&nIdPL=1&cTitulo=LEY FEDERAL DE PROTECCION DE DATOS PERSONALES EN POSESION DE LOS PARTICULARES&cFechaPub=05/07/2010&cCateg=LEY&cDescPL=EXPOSICION DE MOTIVOS*

----------, "Versión Estenográfica del Segundo Día de Trabajos del IV Seminario Internacional de Acceso a la Información Judicial y los Beneficios para la Sociedad", 26 Octubre de 2011, http://www2.scjn.gob.mx/red/IVTransparencia/Docs/VEstenograficas/2%C2%B0d%C3%ADa%20IV%20Seminario%20Acceso%20Informaci%C3%B3n.pdf

OFICINA INTERNACIONAL DEL TRABAJO*, "*Protección de los datos personales de los Trabajadores OIT Organización Internacional del Trabajo 1997"*, Repertorio de recomendaciones prácticas de la OIT,* Ginebra, *http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf*

Páginas de Internet

http://www.diputados.gob.mx/LeyesBiblio/legis/reflx.htm

http://www.ifai.gob.mx/InformacionGeneral/informacion

http://www.congreso.es/portal/page/portal/Congreso/Congreso

http://www.congreso.gov.ar/

http://www.cuidatusdatos.com/infoderechosarco.html.

www.dateas.com

http://www.tuguialegal.com/protecciondatos.htm

http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

http://www.jus.gov.ar/

http://www.cuidatusdatos.com/infoderechosarco.html

Sentencias y Jurisprudencia

Sentencia 254/1993 de 20 de julio de 1993 del Tribunal Constitucional de España Recurso de Amparo núm. 1827/1990.

Sentencia 290/2000, de 30 de noviembre de 2000 del Tribunal Constitucional de España, Recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal.

Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley

Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Tesis 2a. XCIX/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, XXVIII, Julio de 2008, p. 549.

Legislación

Constitución española de 1978.

Constitución de la Nación Argentina.

Constitución Política de los Estados Unidos Mexicanos.

Convenio 108 del Consejo de Europa de 28 enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Convenio número 111 relativo a la Discriminación en materia de empleo y ocupación adoptado el 25 de junio de 1958 por la Conferencia General de la Organización Internacional del Trabajo (OIT).

Decreto 1558/2001. Reglamentación de la Ley Nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.

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

Directiva 95/46/CE 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.

Ley 25.326 Protección de los Datos Personales.

Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.