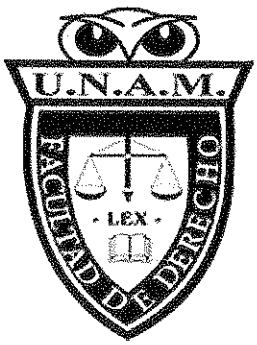
UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE DERECHO
SEMINARIO DE DERECHO CONSTITUCIONAL Y DE AMPARO

"DE LAS FACULTADES DEL CONGRESO EN MATERIA DE DATOS PERSONALES"

T E S I S
QUE PARA OBTENER EL TITULO DE
LICENCIADA EN DERECHO
P R E S E N T A :
VERONICA SEGURA CERVANTES

ASESOR: LIC. CECILIA DEL CARMEN AZUARA ARAI



CIUDAD UNIVERSITARIA 2010.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

UNIDAD DE SEMINARIOS "JOSÉ VASCONCELOS"
FACULTAD DE DERECHO
SEMINARIO DE DERECHO CONSTITUCIONAL Y DE AMPARO

Cd. Universitaria, D. F. 17 de Mayo de 2010.

DR. ISIDRO ÁVILA MARTÍNEZ.
DIRECTOR GENERAL DE LA ADMINISTRACIÓN ESCOLAR DE LA U.N.A.M.
P R E S E N T E.

Por este conducto, me permito comunicar a usted, que la pasante, **SEGURA CERVANTES VERONICA** con número de cuenta 098024159 bajo la supervisión de este Seminario, elaboró la tesis intitulada **"DE LAS FACULTADES DEL CONGRESO EN MATERIA DE DATOS PERSONALES"**, realizada con la asesoría de la profesora **Lic. Cecilia del Carmen Azuara Arai.**

Con fundamento en los artículos 8° fracción V del Reglamento de Seminarios, 19 y 20 del Reglamento General de Exámenes de la Universidad Nacional Autónoma de México, por haberse realizado conforme a las exigencias correspondientes, se aprueba la nombrada tesis, que además de las opiniones que cita, contiene las que son de exclusiva responsabilidad de su autor. En consecuencia, se autoriza su presentación al Jurado respectivo.

"La interesada deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, sabe caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente, sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad"

A T E N T A M E N T E
"POR MI RAZA HABLARÁ EL ESPÍRITU"
EL DIRECTOR DEL SEMINARIO

LIC. EDMUNDO ELÍAS MUSI

100 UNAM UNIVERSIDAD NACIONAL DE MÉXICO 1910 2010

*pcm.

Ciudad Universitaria, mayo de 2010

Lic. Edmundo Elias Musi
Director del Seminario de
Derecho Constitucional y
De Amparo
Facultad de Derecho-UNAM

Por medio del presente me permito informar a Usted, que he revisado y asesorado íntegramente el trabajo de tesis profesional de la alumna VERÓNICA SEGURA CERVANTES, con número de cuenta 09802415-9, bajo el título "DE LAS FACULTADES DEL CONGRESO EN MATERIA DE DATOS PERSONALES", mismo que se encuentra registrado en el Seminario a su digno cargo.

En razón de lo anterior otorgo mi voto aprobatorio, y someto a su superior consideración el trabajo de tesis de referencia, a efecto de que la alumna se encuentre en posibilidad de continuar con sus trámites de titulación.

Sin más por el momento, le envío un cordial saludo.

A T E N T A M E N T E

Lic. Cecilia del Carmen Azuara Arai

A Dios...

A mis padres, las personas más importantes en mi vida, a las que no tengo más que agradecer su amor, confianza y apoyo incondicional, por hacer de mí una mejor persona y alentarme en cada paso de mi vida.

A mis amigos, quienes han sido incondicionales, me han regalado momentos maravillosos y por creer en mí.

A la Lic. Cecilia Azuara, por su tiempo y disposición para llevar a buen término este trabajo, por su calidad humana y profesionalismo.

A mi abuelo Efrén, ejemplo de vida, persona que merece mi absoluta admiración y respeto y que indudablemente era un universitario de corazón.

A todos quienes forman parte de mi vida y que me han permitido crecer como persona y cumplir mis expectativas.

A la Facultad de Derecho y a mi Universidad, porque siempre será un orgullo pertenecer a la Máxima Casa de Estudios y un honor ser universitaria.

¡Gracias!

ÍNDICE

CAPÍTULO III

MARCO JURÍDICO INTERNACIONAL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

CAPÍTULO IV

RECONOCIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO.

INTRODUCCIÓN

El acceso a la información, ha sido una constante problemática dentro de nuestro sistema jurídico, es evidente que en los últimos años este tema ha tomado una gran fuerza y relevancia en aras de la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública en junio de 2002 y con ello a su vez se ha hecho referencia a otros temas como la protección de Datos Personales que sin duda alguna son de igual importancia, aunque de carente regulación.

Nuestra Carta Magna contempla el Derecho a la Información como una garantía individual desde los años 70's, también lo es que tardíamente se han tomado las riendas del mismo. Por lo que hace a la protección de datos personales, nuestra Constitución derivado de las reformas constitucionales a los artículos 16 y 73, donde se prevé la protección de datos personales y la facultad del congreso para legislar en la materia cuando los datos personales se encuentran en posesión de particulares, sin embargo no es suficiente.

La Ley Federal de Transparencia y Acceso a la Información Pública, tiene como objetivo garantizar el acceso a la información en posesión del Estado, lo que implicó necesariamente establecer la obligación de proteger los datos personales en poder de los sujetos obligados, no obstante, no basta para ello establecer medidas mínimas de protección, se necesita una normatividad específica del tema.

Es de interés general, no únicamente regular el derecho de acceso a la información, sino además la protección de datos personales, pues la información que en éstos se maneja es de vital importancia, dado que se puede llegar a manipular con ligereza por quienes la poseen. En algunos casos no se permite tener conocimiento y acceso a la misma, en otros, se ve alterada y quizá en muchos más se niega o se determina inexistente.

En nuestro país existe una regulación insuficiente por lo que hace al manejo de datos personales, toda vez que únicamente alude al sector público y no así al privado; sin embargo cabe hacer mención que encontramos diversos ordenamientos que se refieren a los mismos.

Sin duda alguna, la problemática que se desprende es en relación a cómo los individuos en su carácter de titulares de los datos personales pueden acceder a la información contenida en ellos, así como la necesidad de que se les garantice la protección de los mismos, ya en su manejo, tratamiento o divulgación; y consecuentemente se garantice el derecho a la intimidad y a la privacidad de los sujetos.

El artículo 3° de la Ley Federal de Transparencia y Acceso a la Información, señala claramente que debe entenderse por datos personales, sin embargo, como ya se ha mencionado no existe normatividad en específico. La ley menciona claramente como objetivos garantizar el derecho de acceso a la información, así como la protección de los datos personales en posesión de los sujetos obligados (sector público), pero desafortunadamente no prevé lo relativo a la información en poder de los particulares.

En el marco internacional, el tema de la protección de datos personales no es nuevo, un gran número de países cuentan con una regulación específica. Por lo que hace al tratamiento de datos personales, el derecho a la intimidad y todo lo que esto conlleva, muchos otros cuentan con reglas, normas o leyes concretas a este tema, tal es el caso de España, Polonia, Argentina, Perú, entre muchos otros países que en relación a este tema tienen ya legislación, doctrinas, jurisprudencia, entre otros instrumentos especializados.

El tema de los datos personales y derecho a la intimidad, así como el acceso a la información personal es delicado, la intención es proponer una solución a este vacío jurídico; garantizando la protección de datos personales y en consecuencia el derecho a la intimidad de los individuos.

Las recientes reformas a los artículos 16 y 73 constitucionales, obligan a que en una eventual ley se aborde el tema de la protección de los datos personales de los individuos en el sector privado, para de este modo garantizar plenamente el derecho a la intimidad y la protección de datos.

CAPITULO I

DERECHO A LA INTIMIDAD Y DERECHO A LA PRIVACIDAD COMO ANTECEDENTES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES.

1. DERECHO A LA INTIMIDAD.

1.1. CONCEPTO DE INTIMIDAD.

En su origen etimológico, Intimidad proviene del termino Intus (dentro), superlativo de interior. Es decir, refiere no solo a lo que está adentro, sino a lo que esta "más" adentro.

El diccionario de la Real Academia de la Lengua la define como: "zona espiritual intima y reservada de una persona o un grupo, especialmente de una familia".

El diccionario Larousse dice: "Interior y profundo. Que forma parte e la esencia de una cosa... Que existe en lo más profundo de nosotros mismos".

El Black's Law Dictionary define Right of Privacy como "The right to be let alone (el derecho a ser dejado solo), the right of a person to be free from unwarranted publicity. (el derecho de una persona a quedar libre de publicidad no justificada).

De diversos autores u obras consultadas se desprenden las siguientes definiciones, mismas que se transcriben con una mención rápida de autores y sin mayores datos de identificación pues estos únicamente se utilizarán a manera de referencia:

- Derecho a una vida retirada y anónima (Nizer).

- Derecho a vivir su propia vida en soledad sin estar sometido a una publicidad que no se ha provocado ni deseado (Swindle).

- Derecho del individuo de decidir por si mismo en que medida compartirá con otros sus pensamientos y los hechos de su vida privada. (Office of science and technology).

- Control que podemos ejercer sobre nuestra propia información personal. (Fried).

- Derecho a ser dejado en paz. (Nizer).

- Sector personal reservado, a fin de hacer inaccesible al público, sin la voluntad del interesado lo que constituye lo esencial de su personalidad. (Nerson).

- Vida familiar, personal del hombre, su vida interior, espiritual, la que lleva cuando vive detrás de su vida privada. (Martin)

- Derecho a ser dejado en paz para vivir su propia vida con el mínimo de injerencias exteriores. (congreso de Juristas Nórdicos).

- Determinar por sí mismos, cuándo, cómo y hasta dónde puede comunicarse a otros información sobre ellos. (Westin)

- Esfera secreta de la vida del individuo en la que tiene el poder legal de evitar a los demás. (Carbonnier)

De lo anterior se concluye, que la intimidad es el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con la libertad de decidir a quién se le da

acceso al mismo, según la finalidad que persiga, que impone a todos los demás la obligación de respectar y que solo puede ser obligado a develar en casos justificados cuando la finalidad perseguida por la develación sea licita.[1]

1.2. DOCTRINAS O TENDENCIAS RESPECTO DEL CONCEPTO DE INTIMIDAD.[2]

Aunado a los intentos de definición del concepto, se han elaborado diversas doctrinas que desarrollan el concepto. Básicamente se puede decir que existen dos grandes grupos de doctrinas o tendencias en la explicación del concepto de intimidad: Las teorías de las "esferas" y las del "mosaico".

Conforme el primer grupo de planteamientos doctrinales el ser humano es un centro de actividad alrededor del cual se desarrollan varios círculos concéntricos. Los más unidos al individuo son los más íntimos y los más externos son los menos privados.

El número de círculos varía según los autores, la exposición más amplia nos habla de:

Una esfera *secreta,* en la cual absolutamente nadie tiene acceso incluso el mismo individuo mantiene a veces en el subconsciente.

Una esfera *íntima,* en la cual el hombre se cuida de no dar entrada a prácticamente nadie.

Una esfera de *confianza* en la cual acceden algunos cuantos cercanos.

Una esfera *individual,* más restringida que la siguiente:

---

[1] Meján, Luis Manuel, *"El Derecho a la Intimidad y la Informática,* Porrúa, México, 1994, p. 87
[2] Ibídem, 73-75.

Una esfera *propia.*

Una esfera *privada,* que contiene relaciones con otras personas pero en un margen de relación personal, es el caso de clientes, familiares, etc.

Una esfera *social,* en la que el individuo es consciente de que es conocido y observado por una colectividad.

Por último, una esfera *pública,* en donde, al contrario que la primera, el propósito específico del individuo es lo contrario a la intimidad, busca darse a conocer, relacionarse, crear una imagen y no sólo permite sino que provoca que los demás se introduzcan ahí.

En cambio las teorías del "mosaico" hacen más énfasis en los roles que sociológicamente desempeñan el individuo cuya privacía se afecta y la entidad que pretende penetrar la misma. El término "mosaico" deviene de la afirmación de que un individuo no es solo una información, sino un complejo de ellas y, relacionadas unas con otras el resultado puede variar.

Es decir, un dato en sí puede no ser agresivo al derecho a la intimidad, reunido con otros varios sí puede serlo. Un dato dado a una persona, o conocido por ella puede no suponer invasión de la vida privada, pero sí si quien accede es otra persona distinta.

Por ejemplo, el que un individuo consuma servicios en un restaurante y los pague con tarjeta de crédito parece ser inocuo en sí, lo está haciendo a vistas de los comensales del restaurante y de sus invitados, pero si se toman todos los estados de cuenta de la tarjeta de crédito de ese sujeto durante un año y se observa con qué frecuencia asiste a ese restaurante, a qué otros sitios va, dónde compra, cuánto gasta en promedio, etcétera, tomaremos conocimiento de otras realidades del sujeto, estaremos penetrando a la vida privada de él.

Asimismo, no constituye ninguna agresión el que un juez penal investigue y recabe información sobre los antecedentes y vida pasada de un indiciado, pero si quien lo hace es una fuerza policíaca o un grupo de inteligencia sin ninguna base o fundamento derivados de una sospecha de un proceso legal abierto, estaremos en presencia de un atentado a la privacía.

1.3. EL DERECHO A LA INTIMIDAD

El nombre que se le asigna a este derecho puede variar, el consenso entre los países de habla latina gira alrededor de la palabra "Intimidad" aunque en otros países se usa el término "Privacía" que también llena los extremos de la realidad que se desea regular.

Al buscar el concepto de Intimidad, la selección del nombre "Intimidad" o "Privacía" o "Vida Privada", obedece no sólo a la selección de sinónimos, sino de un esfuerzo por conocer la naturaleza exacta de la realidad sobre la que se regula.

Quienes se inclinan por "Privacía" o "Vida Privada" consideran esta la manifestación externa de la "Intimidad" que pueden ser reguladas por el derecho, ya que "Intimidad" es un concepto filosófico que escapa al ámbito de lo jurídico. Quienes se inclinan, por el concepto de "Intimidad" lo hacen basados en que esta es un concepto global que comprende tanto realidades como raíces profundas en la naturaleza del ser humano.

Del Derecho a la Intimidad habrá que decir en primer término que es un derecho de los que deben catalogarse entre los *Derechos Fundamentales* del ser humano, la propia naturaleza del hombre, la propia conciencia que todos los individuos tenemos de ello, así como la experiencia y el consenso histórico y universal así lo demuestran.

El contenido del derecho deberá conllevar una enumeración objetiva de las áreas en las que se considera que son materia de intimidad o privacía y deberá tomar en cuenta que para que un concepto, circunstancia, información o situación se considere intimo o privado, es menester que el titular del mismo desee mantenerlo así. Es decir, en el contenido del derecho a la intimidad debe estar presente no sólo el catalogo objetivo referido sino también el control que el titular ejerce sobre él.

Otro elemento a tomar en cuenta en el contenido del Derecho es el fin perseguido al recabar la información. Un criterio para determinar cuándo es ilícito usar una información agrediendo a la intimidad es el *destino para el cual fueron recogidos.* Utilizarlo para otra cosa es agresión a la intimidad.

1.4. TITULARES DEL DERECHO A LA INTIMIDAD.

El sujeto activo del derecho, es decir, el protegido o titular, será el individuo en cuanto a tal como ser humano, sin que se requieran circunstancias de mayoría de edad, domicilio, nacionalidad, será un típico derecho de goce que asista al ser humano por el hecho de serlo.

El derecho que deviene al sujeto activo no es sólo un derecho de goce, sino que debe tener la posibilidad de ser un derecho de ejercicio, pues la regulación del mismo debe permitir al sujeto tutelado el tener medios contra pretensiones de invasión o invasiones a su intimidad o privacía, así como acciones para restañar o corregir los daños causados por tales invasiones. Recuérdese que este derecho es más que un derecho sobre cosas, un derecho a guardar cosas en forma discreta, es decir un derecho a tomar una decisión y a desplegar una conducta, activa u omisiva, respecto del contenido.

El sujeto pasivo del derecho es, en principio, un sujeto universal, esto es, la generalidad de seres humanos que deberán respetar el que el sujeto activo no desee intromisiones en sus zonas o esferas de intimidad.

El sujeto pasivo universal se tornará en individualizado y preciso al surgir una situación específica en la que una persona, sujeto activo, se vea involucrada en una intromisión; por ejemplo, cuando una persona da una serie de datos e información a un laboratorio médico, éste se convierte en un sujeto pasivo del derecho al tener la obligación de recabar solo los datos que son relevantes, de conservarlos solo por el tiempo y para los efectos que sean necesarios, no usarlos para otros propósitos que aquellos para los cuales se obtuvieron y no comunicarlos a nadie sin la autorización de la persona interesada. El sujeto pasivo universal se ha materializado en un sujeto específico (laboratorio médico).

1.5. LIMITES AL DERECHO A LA INTIMIDAD.

El derecho debe conllevar, en la regulación de su ejercicio, la regulación de cuando la intimidad puede, o debe, ser *develada*, en atención a la existencia de otro derecho con el que entra en conflicto y que debe tener un rango superior.

Esta revelación debe darse en casos de derechos de terceros (tal sería el caso de un auto judicial que ordene a un patrón informar cuánto gana un empleado a fin de asegurar una pensión alimenticia.

El conflicto entre develar información o guardarla discreta es añejo como la humanidad, desde que el hombre ha vivido en comunidades, ha visto la generación de una dicotomía axiológica: por un lado los valores inherentes al individuo y, por otro, los valores propios de la colectividad.

En todas las épocas, en todas las doctrinas, se han aceptado dos principios básicos:

1. El hombre tiene valores individuales que no pueden ser sacrificados jamás en aras de ningún otro valor.

2. Existen casos y circunstancias en que el valor comunitario, el bien general (común), debe prevalecer sobre los intereses particulares.

Lo difícil es determinar cuáles valores están en la lista de cada uno de esos dos principios básicos. Eso es lo que ha venido pasando con el Derecho a la Intimidad. La humanidad ha reconocido siempre que el ser humano tiene derecho a su intimidad, a una zona reservada, en donde nadie debe incursionar, ese es un valor estable, perenne. Lo que ha cambiado es la determinación de cuáles son los contenidos de ese derecho, que cosas es válido que estén dentro de esa esfera de intimidad.

La humanidad ha reconocido siempre que la colectividad tiene derecho a imponer un sacrificio a los bienestares individuales para proteger el bienestar común, ese es otro valor estable. Lo que ha cambiado son los elementos que pueden conformar el bien común.

El derecho a la intimidad o privacidad es un derecho fundamental que asiste a los sujetos de derecho consistente en la facultad de mantener reserva sobre diversas situaciones relacionadas con la vida privada, que debe ser reconocido y regulado por el sistema jurídico y que es oponible a todos los demás salvo en los casos en que puede ser develado por existir un derecho superior de terceros o para el bienestar común.[3]

Dentro del derecho a la intimidad debe comprenderse el tratamiento de la información que compilan tanto los particulares, ya sea en actividades cotidianas, como en los casos de empresas que, por su objeto, realizan actividades de acumulación y uso de información, como, y muy especialmente, el Estado, a fin de

[3] Idem, p. 105.

que se realice el concepto de un Estado de Derecho en donde el papel de gobernantes y gobernados, recopiladores de información y sujetos de ella tengan bien claros sus derechos y obligaciones.

2. EL DERECHO A LA VIDA PRIVADA.[4]

Es el derecho fundamental de la personalidad consistente en la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público. El bien jurídicamente protegido de este derecho está constituido por la necesidad social de asegurar la tranquilidad y la dignidad de las personas para el libre desarrollo de la personalidad humana, con miras a que cada uno pueda llevar a cabo su proyecto vital.

El derecho a la vida privada se materializa al momento de proteger del conocimiento ajeno el hogar, la oficina o ámbito laboral, los expediente médicos, legales y personales, las conversaciones o reuniones privadas, la correspondencia por cualquier medio, la intimidad sexual, la convivencia familiar o afectiva y todas aquellas conductas que se llevan a efecto en lugares no abiertos al público.

El derecho a la privacidad contiene algunas peculiaridades que es conveniente puntualizar:

a) Es un *derecho esencial del individuo*. Se trata de un derecho inherente a la persona con independencia del sistema jurídico particular o contenido normativo bajo el cual está tutelado por el derecho positivo.

b) Es un *derecho extrapatrimonial*. Se trata de un derecho que no se puede comercial o intercambiar como los derechos de crédito, habida cuenta que

[4] Villanueva, Ernesto, *"Temas selectos de derecho de la información"*, Serie Estudios Jurídicos número 67, Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, México, 2004, p.p. 37-38.

forma parte de la personalidad del individuo, razón por la cual es *intransmisible e irrenunciable*, y

c) Es un derecho *imprescriptible e inembargable*. El derecho a la privacidad a dejado de ser sólo un asunto doctrinal para convertirse en contenido de derecho positivo en virtud del desarrollo científico y tecnológico que ha experimentado el mundo moderno con el uso masivo de la informática, que permite el acceso casi ilimitado a información personal por parte de instituciones públicas y privadas.

2.1. EL ÁMBITO DE LO PRIVADO, SU RELACIÓN CON LO ÍNTIMO.

Frecuentemente se ha considerado que lo privado debe vincularse con una realidad que afecta a la persona en sus relaciones con los demás, se perfila así un concepto que ha de ponerse en relación con la publicidad que invade la actuación humana. Por tanto, los comportamientos son públicos o privados no en sí mismos, sino en atención al espacio en que se desenvuelven. Conviene advertir, que la publicidad sobre determinado comportamiento no siempre procede de una intromisión ajena, sino del propio sujeto quien con su actitud transforma en públicas conductas o sentimientos que podrían ser privados.

De lo expuesto se concluye que las actuaciones privadas y públicas se caracterizan respectivamente, bien porque son necesariamente observables, o bien porque son posiblemente observadas, mientras que las actuaciones, sentimientos o pensamientos referidos a la intimidad no pueden contemplarse sin más, sino a través del propio sujeto, de su actitud o de sus palabras. Lo íntimo se corresponde con la libertad interior de la persona, con su capacidad para la reflexión o para el autoanálisis, se trata, en definitiva, de actividades que la persona realiza en su interioridad, aislada del mundo exterior, que no tiene acceso a las mismas.

Privado se define, por tanto, como contrapuesto a público; representa lo apartado, lo retirado, exclusivo de la persona. Se identifica con comportamientos, actitudes o comunicaciones que no se exponen a los demás, si bien una decisión del sujeto los podría fácilmente transformar en públicos. Es sencillo imaginar qué situaciones se corresponden con la idea de privado, que no de íntimo, que se ha acogido, y cuándo esas mismas realidades se pueden calificar como públicas. Una declaración de matrimonio, pudiera pensarse que representa una manifestación de la intimidad de la persona; por el contrario, si se acepta la definición de privado e íntimo que se viene suscribiendo, se tratará de una situación privada del individuo si se desarrolla lejos de las miradas ajenas de terceros; pero, esa misma realidad será pública si se efectúa en una plaza pública o a voz en grito en un centro comercial. Así, la naturaleza privada de las realidades humanas tiene un carácter relativo, depende de la decisión de la persona que en cada momento realice la actividad privada de que se trate.

Siguiendo a GONZÁLEZ GAITANO debe considerarse que intimidad y vida privada constituyen dos realidades diferentes. La intimidad afecta a lo más interno e indisponible del ser humano lo propio de la intimidad no es la ausencia de conocimiento de lo que al individuo le acontece, sino la *esencialidad* en relación a la persona[5]. Si con el derecho a la intimidad se ampara el modo de ser y actuar de cada sujeto, lo que le es más próximo y que tan sólo él conoce, con la *vida privada* se salvaguarda de modo voluntario aquello que el individuo considera que no tiene obligación de publicar y poner al alcance del conocimiento de los demás. Si lo propio de la vida privada es su carácter de secreto o reservado, lo que caracteriza a la intimidad es que incide en lo más interno y personal de cada individuo.

No todo aquello que sea considerado privado goza además de la naturaleza de íntimo por que la intimidad es ajena en esencia a lo público o lo privado, se caracteriza por afectar a la esfera más propia e interna del individuo. Ciertamente,

[5] GONZÁLEZ GAITANO, Norberto, *"La trascendencia jurídica de la intimidad"*, Revista de fundamentación de las instituciones jurídicas y de derechos humanos. Suplemento Humana Iura, núm. 1, 1991, pág. 275.

vida privada e intimidad no son términos sinónimos en su acepción exacta por que lo íntimo es un núcleo más interno que lo meramente privado, es el corazón del corazón de cada persona[6].

En resumen, "vida privada" hace referencia a una esfera de retiro y aislamiento, al ámbito donde los demás dejan en paz al sujeto, con tranquilidad para actuar y, donde no tienen derecho a inmiscuirse. En tanto que la intimidad se refiere al interior del individuo, a un "mundo propio", fuera de los ojos de los demás, se trata de la esfera más sagrada de la persona. A este respecto, para la delimitación de ambos derechos antes debe aceptarse la consideración del derecho a la vida privada como garantía de desarrollo de determinados aspectos de la existencia individual, alejada de la observación indiscreta de terceros, y vedada al acceso de éstos. El derecho a la intimidad tutela la zona espiritual reservada de la persona que permanece en su interior, referida a la conciencia de sí mismo como ser humano libre en su ámbito moral e intelectual. Así, el derecho a la vida privada se manifiesta a través de la realización de actividades y comportamientos en un ámbito estrictamente personal, de amistad o familiar en que el sujeto decide desarrollar su existir, preservando esa esfera de su existencia del conocimiento general.

2.2. DERECHO A LA PRIVACIDAD EN EL MARCO JURÍDICO MEXICANO.

En México el derecho a la privacidad está regulado por el artículo 7° constitucional al prescribir como límite a la libertad de prensa el respeto a la vida privada. También es aplicable el artículo 16 de la Constitución primer párrafo, que a la letra dice: *"Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de un mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento".*

---

[6] URABAYEN, Miguel, *Vida privada e información: un conflicto permanente*, Pamplona, EUNSA, 1977, pág. 347.

Esta garantía de seguridad jurídica es, sin duda, amplia y suficiente para garantizar el derecho a la privacidad de los individuos, pues regula con precisión los requisitos que debe reunir el mandamiento escrito por el cual se pueda afectar o molestar a la persona, es decir, por el que la autoridad puede invadir la esfera de privacidad del individuo.

El artículo 16 de nuestra Constitución es uno de los preceptos que imparten mayor protección a cualquier gobernado, sobre todo a través de la garantía de *legalidad* que consagra, la cual, dada su extensión y efectividad jurídicas, pone a la persona a salvo de todo acto de mera afectación a su esfera de derecho que no sólo sea arbitrario, es decir, que no esté basado en norma legal alguna, sino contrario a cualquier precepto, independientemente de la jerarquía o naturaleza del ordenamiento a que éste pertenezca.

La primera parte del artículo 16 constitucional, ordena textualmente:

"Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento."

- ***Titularidad de las garantías consagradas en la primera parte del artículo 16 constitucional.***

El término "nadie", que es el que demarca desde el punto de vista subjetivo la extensión de tales garantías individuales, es equivalente a "ninguna persona", "ningún gobernado". Por ende, interpretando *a contrario sensu* la disposición constitucional en que se contienen las garantías involucradas en el artículo 16, el titular de las mismas es *todo gobernado,* es decir, todo sujeto cuya esfera jurídica sea susceptible de ser objeto de algún acto de autoridad.[7]

[7] Burgoa O. Ignacio, *"Las Garantías Individuales"*, Porrúa, México, 2005, p. 590.

- ***Bienes jurídicos preservados por las garantías consignadas en la primera parte del artículo 16 constitucional.***

El acto de molestia, puede afectar a alguno o algunos de los siguientes bienes jurídicos comprendidos dentro de la esfera subjetiva del gobernado: a su misma *persona,* a su *familia,* a su *domicilio,* a sus *papeles* o a sus *posesiones.*

a) A través del elemento *persona,* el acto de molestia puede afectar no solamente la *individualidad Psico-física* del sujeto con todas la potestades naturales inherentes, sino a su *personalidad jurídica propiamente dicha.* En efecto, el concepto de "persona" desde el punto de vista jurídico, se establece en atención a la capacidad imputable al individuo, consistente en adquirir derechos y contraer obligaciones; por lo que concierne a personas morales esta afectación se materializa cuando por un acto de autoridad, se le reduzcan las potestades inherentes a su ser jurídico, impidiéndole el ejercicio de las facultades correspondientes.

En conclusión, el gobernado, a través de su "persona" es susceptible de afectarse por un acto de molestia en sentido lato, en los siguientes casos:

1. Cuando se le restringe o perturba su actividad o individualidad psicofísica propiamente dicha e inclusive su libertad personal;

2. Cuando tal restricción o perturbación concierne a su capacidad jurídica de adquirir derechos y contraer obligaciones (libertad de contratación);

3. Tratándose de personas morales, al reducirse o disminuirse las facultades inherentes a su entidad jurídica, impidiendo o limitando el ejercicio de su actividad social.

4. Cuando se vulnere cualquier cualidad de la persona humana, como es su honor, su nombre, su familia, su actividad y, en general todo elemento, atributo, situación o derecho humano.[8]

b) La afectación por un acto de molestia en perjuicio del gobernado a través de su *familia,* no implica que la perturbación consiguiente se realice precisamente en alguno o algunos de los miembros pertenecientes a dicho grupo, sino que opera en los *derechos familiares* del individuo o del gobernado, entendiéndose por tales todos lo que conciernan a su estado civil, así como a su situación de padre, de hijo, etc.,etc.[9]

c) El *domicilio* del gobernado equivale a su propio *hogar,* es decir, a su casa o habitación particular donde convive con su familia.

Sin embargo, se puede decir que la connotación de dicho bien jurídico se refiere igualmente a los diversos lugares, a que aluden los artículos 29 y 33 del Código Civil para el Distrito Federal, por lo que la afectación que a través de dicho elemento puede experimentar el gobernado, es factible que se realice en las distintas hipótesis que a continuación mencionamos:

1. *En el sitio o lugar en que la persona tenga establecido su hogar, esto es, su casa-habitación donde conviva con sus familiares, comprendiéndose en él todos los bienes que se encuentren dentro de ella, los cuales, por tal motivo, pueden constituir la materia del acto de molestia;*

2. *En cuanto a las personas morales, el sitio o lugar donde se halle establecida su administración, conforme a lo dispuesto por el artículo 33 del Código Civil.*

[8] Ibídem, p. 592-593.
[9] Ídem.

Es evidente que para que el domicilio de un sujeto pueda reputarse afectable por un acto de molestia en los términos del artículo 16 constitucional, no debe traducirse en el *domicilio legal* propiamente dicho, que es el lugar donde el individuo deba ejercer sus derechos y cumplir sus obligaciones (art. 31 del ordenamiento indicado), sino en el *domicilio efectivo,* o sea, en el sitio donde la persona resida realmente, es decir, donde tenga establecida su casa-habitación, en cuyo caso la perturbación necesariamente debe recaer en los bienes u objetos que dentro de ella se encuentren.[10]

d) Bajo la denominación de *papeles* a que se refiere el artículo 16 constitucional, se comprenden todos los documentos de una persona, es decir, todas las constancias escritas de algún hecho o acto jurídico.

Debe tenerse en cuenta que el acto de molestia que afecte a la documentación del gobernado, únicamente debe consistir en la requisición o apoderamiento de las diversas y variadas constancias escritas que la integren, más nunca extenderse a los actos o derechos que en las mismas se consignen, pues la perturbación a estos últimos opera a través de otros bienes jurídicos preservados por el artículo 16 constitucional.[11]

Cabe hacer mención que recientemente debido a la adición de un segundo párrafo al artículo 16 constitucional, se desprende un nuevo derecho con rango de garantía constitucional "el derecho de protección de datos", el cual quedó plasmado en los siguientes términos:

(...)

[10] Ibídem, p.p. 593-594.
[11] Ibídem, p. 595.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

(...)

En este mismo sentido es importante destacar la reforma al artículo 73 constitucional, a través de la cual se faculta al Congreso de la Unión para legislar en materia de protección de datos, lo que viene a fortalecer la nueva garantía constitucional del derecho a la protección de datos.

Artículo 73. El Congreso tiene facultad:

I. a XXIX-N. ...

XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.

XXX. ...

Por lo que concierne a la vida privada, a manera de referencia se enunciarán diversos ordenamientos que tutelan la protección prevista en la Constitución.

La Ley de Imprenta establece las hipótesis normativas que actualizan un ataque a este derecho fundamental en el artículo 1° que dispone:

"Artículo 1º .Constituyen ataques a la vida privada:

I. *Toda manifestación o expresión maliciosa hecha verbalmente o por señales en presencia de una o más personas, o por medio de manuscrito, o de la imprenta, del dibujo, litografía, fotografía o de cualquier otra manera que expuesta o circulando en público, o transmitida por correo, telégrafo, teléfono, radiotelegrafía o por mensaje, o de cualquier otro modo, exponga a una persona al odio, desprecio o ridículo, o pueda causarle demérito en su reputación o en sus intereses;*

II. *Toda manifestación o expresión maliciosa hecha en los términos y por cualquiera de los medios indicados en la fracción anterior, contra la memoria de un difunto con el propósito o intención de lastimar el honor o la pública estimación de los herederos o descendientes de aquel, que aún vivieren;*

III. *Todo informe, reporte o relación de las audiencias de los jurados o tribunales, en asuntos civiles o penales, cuando refieran hechos falsos, o se alteren los verdaderos con el propósito de causar daño a alguna persona, o se hagan, con el mismo objeto, apreciaciones que no estén ameritadas racionalmente por los hechos, siendo éstos verdaderos;*

IV. *Cuando con una publicación prohibida expresamente por la Ley se compromete la estimación de una persona, exponiéndola al odio, desprecio o ridículo, o a sufrir daño en su reputación o en sus intereses ya sean personales o pecuniarios".*

La noción de vida privada ha sido también preocupación de la Suprema Corte de Justicia de la Nación, que en tesis jurisprudencial ha sostenido que: "La ley no da un concepto de vida privada de una manera explícita, pero sí puede decirse que lo contiene implícito, toda vez que en los artículos siguientes se refiere a los ataques a la nación mexicana, a las entidades políticas que la forman, a las entidades del país y a la sociedad. Para determinar lo que es vida privada puede acudirse al

método de la exclusión y sostener que vida privada es aquella que no constituye vida pública. Precisando dicho concepto, puede afirmarse que la vida que observan los funcionarios con este carácter, es decir, en el desempeño de su cargo y que es lo que interesa a la sociedad, se opone a las actividades del individuo como particular, a sus actividades en el hogar y en la familia esto da la tónica para considerar cuales fueron los ataques que la ley de imprenta quiso reprimir en la fracción I y en la IV del artículo 1° de la ley de imprenta. Allí se contiene una limitación a las garantías de los artículo 6 y 7 constitucionales, pero se refiere a la vida privada, no a la que observan los funcionarios en el desempeño de su cargo..."[12]

Cabe hacer mención en este apartado de la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal, la cual fue inspirada en base a la protección de los derechos de la personalidad a nivel internacional y cuya finalidad es regular el daño al patrimonio moral, derivado del abuso del derecho de la información y de la libertad de expresión, así como garantizar el derecho a la vida privada, al honor y la propia imagen de las personas en el Distrito Federal.

Esta ley define a la vida privada como *"aquella que no está dedicada a una actividad pública y, por ende, es intrascendente y sin impacto en la sociedad de manera directa; y en donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia ni les afecta".*[13]

Además señala que *"el derecho a la vida privada se materializa al momento que se protege del conocimiento ajeno a la familia, domicilio, papeles o posesiones y todas aquellas conductas que se llevan a efecto en lugares no abiertos al público, cuando no son de interés público o no se han difundido por el titular del*

[12] Semanario Judicial de la Federación. Sexta época. Tomo VII, p. 10.
[13] Artículo 9° de la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal

derecho"[14], que para efectos de la propia ley considera como titulares de los mismos tanto a personas físicas como a personas morales.

En términos generales la referida ley en su contenido de 44 artículos, contempla a la Vida Privada, el Honor y la Propia Imagen, como derechos de la personalidad, además de prever medios de defensa, responsabilidades y sanciones respecto de los mismos, aunando a ella que sin duda alguna toma como base la garantía constitucional consagrada en el artículo 16 de este ordenamiento.

En este mismo sentido haremos una breve reseña de algunos de los ordenamientos del orden jurídico nacional que prevén en alguno de sus artículos lo referente al manejo de la información personal o su protección, únicamente de manera enunciativa.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[15] señala en diversos artículos la protección a la información de carácter personal, mismos que se transcriben a continuación:

Artículo 4. *Son objetivos de esta Ley:*

...

III. *Garantizar la protección de los datos personales en posesión de los sujetos obligados;*

...

Artículo 18. *Como información confidencial se considerará:*

...

[14] Artículo 10 de la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal

[15] Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, tomado de http://www.ifai.org.mx/transparencia/LFTAIPG.pdf

II. *Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.*

...

En cuanto al ordenamiento Constitucional, el artículo 6° señala que:

Artículo 6°*.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.*

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. *Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.*

II. *La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*

III. *Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.*

IV. *Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.*

V. *Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.*

VI. *Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.*

VII. *La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.*

Por lo que hace a la Ley Federal Del Derecho De Autor[16], esta dispone que:

Artículo 165.- El registro de una obra literaria o artística no podrá negarse ni suspenderse bajo el supuesto de ser contraria a la moral, al respeto a la vida privada o al orden público, salvo por sentencia judicial.

La Ley General de Población[17] establece que:

Artículo 78.- Las personas que pretendan emigrar del país, están obligadas a satisfacer, además de los requisitos generales de migración, los siguientes:

---

[16] Artículo 165 de la Ley Federal Del Derecho De Autor.
[17] Articulo 78 de la Ley General de Población.

I. *Identificarse y presentar a la autoridad de Migración correspondiente, las informaciones personales o para fines estadísticos que les requieran;*

La Ley General de Salud[18] señala:

Artículo 77 bis 37.- Los beneficiarios del Sistema de Protección Social en Salud tendrán además de los derechos establecidos en el artículo anterior, los siguientes:

...

X. Ser tratado con confidencialidad;

...

La Ley Federal de Procedimiento Administrativo[19] señala:

Artículo 33.- Los interesados en un procedimiento administrativo tendrán derecho de conocer, en cualquier momento, el estado de su tramitación, recabando la oportuna información en las oficinas correspondientes, salvo cuando contengan información sobre la defensa y seguridad nacional, sean relativos a materias protegidas por el secreto comercial o industrial, en los que el interesado no sea titular o causahabiente, o se trate de asuntos en que exista disposición legal que lo prohíba.

La Ley Federal de Procedimiento Contencioso Administrativo[20] establece:

Artículo 7o.- Los miembros del Tribunal incurren en responsabilidad si:

...

IV. Dan a conocer información confidencial o comercial reservada.

...

[18] Artículo 77 bis 37 de la Ley General de Salud.
[19] Articulo 33 de la Ley Federal de Procedimiento Administrativo.
[20] Articulo 7° de la Ley Federal de Procedimiento Contencioso Administrativo.

La Ley Federal de Protección al Consumidor[21] señala:

Artículo 89.- La Procuraduría, en la tramitación del registro de modelos de contratos de adhesión, podrá requerir al proveedor la aportación de información de carácter comercial necesaria para conocer la naturaleza del acto objeto del contrato, siempre y cuando no se trate de información confidencial o sea parte de secretos industriales o comerciales.

La Ley para regular las Sociedades de Información Crediticia[22] en diversos numerales establece:

Artículo 33.- La Sociedad deberá contar con sistemas y procesos para verificar la identidad del Usuario o del Cliente mediante el proceso de autenticación que ésta determine, el cual deberá ser aprobado previamente por el propio consejo de administración de la Sociedad, a fin de salvaguardar la confidencialidad de la información en los términos de las disposiciones legales aplicables.

Artículo 38.- Con excepción de la información que las Sociedades proporcionen en los términos de esta ley y de las disposiciones generales que se deriven de ella, serán aplicables a las Sociedades, a sus funcionarios y a sus empleados las disposiciones legales relativas al Secreto Financiero, aun cuando los mencionados funcionarios o empleados dejen de prestar sus servicios en dichas Sociedades.

Los Usuarios de los servicios proporcionados por las Sociedades y cualquier otra persona distinta del Cliente que tenga acceso a sus Reportes de Crédito o Reportes de Crédito Especiales, así como los funcionarios, empleados y prestadores de servicios de dichos Usuarios y personas, deberán guardar confidencialidad sobre la información contenida en los referidos reportes y no utilizarla en forma diferente a la autorizada.

---

[21] Articulo 89 de la Ley Federal de Protección al Consumidor.
[22] Artículos 33, 38 y 52 de la Ley para Regular las Sociedades de Información Crediticia.

Artículo 52.- Aquellos Usuarios que obtengan información de una Sociedad sin contar con la autorización a que se refiere el artículo 28 de esta Ley o que de cualquier otra forma cometan alguna violación al Secreto Financiero, así como las personas que violando el deber de confidencialidad a que hace referencia el artículo 38 de la presente Ley hagan uso de la información respectiva de manera distinta a la autorizada por el Cliente, estarán obligados a reparar los daños que se causen. Lo anterior sin menoscabo de las demás sanciones, incluyendo las penales, que procedan por la revelación del secreto que se establece.

Respecto de las Empresas Comerciales y Sofomes E.N.R., que no obtengan la autorización a que se refieren los artículos 28, 29 y 30 de la presente ley, la Profeco o la Condusef, según corresponda, previo derecho de audiencia y considerando para tal efecto la gravedad y reincidencia del caso, podrán ordenar a todas las Sociedades que se abstengan de prestar servicios al infractor de manera temporal.

Por su parte la Ley de Instituciones de Crédito[23] establece:

Artículo 117.- La información y documentación relativa a las operaciones y servicios a que se refiere el artículo 46 de la presente Ley, tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios que en este artículo se establece, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios, incluyendo los previstos en la fracción XV del citado artículo 46, sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio.

Como excepción a lo dispuesto por el párrafo anterior, las instituciones de crédito estarán obligadas a dar las noticias o información a que se refiere dicho párrafo,

[23] Artículos 117 y 117 bis de la Ley de Instituciones de Crédito.

cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el titular o, en su caso, el fideicomitente, fideicomisario, fiduciario, comitente, comisionista, mandante o mandatario sea parte o acusado. Para los efectos del presente párrafo, la autoridad judicial podrá formular su solicitud directamente a la institución de crédito, o a través de la Comisión Nacional Bancaria y de Valores.

Las instituciones de crédito también estarán exceptuadas de la prohibición prevista en el primer párrafo de este artículo y, por tanto, obligadas a dar las noticias o información mencionadas, en los casos en que sean solicitadas por las siguientes autoridades:

I. El Procurador General de la República o el servidor público en quien delegue facultades para requerir información, para la comprobación del cuerpo del delito y de la probable responsabilidad del indiciado;

II. Los procuradores generales de justicia de los Estados de la Federación y del Distrito Federal o subprocuradores, para la comprobación del cuerpo del delito y de la probable responsabilidad del indiciado;

III. El Procurador General de Justicia Militar, para la comprobación del cuerpo del delito y de la probable responsabilidad del indiciado;

IV. Las autoridades hacendarias federales, para fines fiscales;

V. La Secretaría de Hacienda y Crédito Público, para efectos de lo dispuesto por el artículo 115 de la presente ley;

VI. El Tesorero de la Federación, cuando el acto de vigilancia lo amerite, para solicitar los estados de cuenta y cualquier otra información relativa a las cuentas

personales de los servidores públicos, auxiliares y, en su caso, particulares relacionados con la investigación de que se trate;

VII. La Auditoría Superior de la Federación, en ejercicio de sus facultades de revisión y fiscalización de la Cuenta Pública Federal y respecto a cuentas o contratos a través de los cuáles se administren o ejerzan recursos públicos federales;

VIII. El titular y los subsecretarios de la Secretaría de la Función Pública, en ejercicio de sus facultades de investigación o auditoría para verificar la evolución del patrimonio de los servidores públicos federales.

La solicitud de información y documentación a que se refiere el párrafo anterior, deberá formularse en todo caso, dentro del procedimiento de verificación a que se refieren los artículos 41 y 42 de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, y

IX. El Instituto Federal Electoral.

Las autoridades mencionadas en las fracciones anteriores solicitarán las noticias o información a que se refiere este artículo en el ejercicio de sus facultades y de conformidad con las disposiciones legales que les resulten aplicables.

Las solicitudes a que se refiere el tercer párrafo de este artículo deberán formularse con la debida fundamentación y motivación, por conducto de la Comisión Nacional Bancaria y de Valores. Los servidores públicos y las instituciones señalados en las fracciones I, VII y IX, podrán optar por solicitar a la autoridad judicial que expida la orden correspondiente, a efecto de que la institución de crédito entregue la información requerida, siempre que dichos servidores especifiquen la denominación de la institución, el número de cuenta,

nombre del cuentahabiente o usuario y demás datos y elementos que permitan su identificación plena, de acuerdo con la operación de que se trate.

Los empleados y funcionarios de las instituciones de crédito serán responsables, en los términos de las disposiciones aplicables, por violación del secreto que se establece y las instituciones estarán obligadas en caso de revelación indebida del secreto, a reparar los daños y perjuicios que se causen.

Lo anterior, en forma alguna afecta la obligación que tienen las instituciones de crédito de proporcionar a la Comisión Nacional Bancaria y de Valores, toda clase de información y documentos que, en ejercicio de sus funciones de inspección y vigilancia, les solicite en relación con las operaciones que celebren y los servicios que presten, así como tampoco la obligación de proporcionar la información que les sea solicitada por el Banco de México, el Instituto para la Protección al Ahorro Bancario y la Comisión para la Protección y Defensa de los Usuarios de Servicios Financieros, en los términos de las disposiciones legales aplicables.

Se entenderá que no existe violación al secreto propio de las operaciones a que se refiere la fracción XV del artículo 46 de esta Ley, en los casos en que la Auditoría Superior de la Federación, con fundamento en la ley que norma su gestión, requiera la información a que se refiere el presente artículo.

Los documentos y los datos que proporcionen las instituciones de crédito como consecuencia de las excepciones al primer párrafo del presente artículo, sólo podrán ser utilizados en las actuaciones que correspondan en términos de ley y, respecto de aquéllos, se deberá observar la más estricta confidencialidad, aún cuando el servidor público de que se trate se separe del servicio. Al servidor público que indebidamente quebrante la reserva de las actuaciones, proporcione copia de las mismas o de los documentos con ellas relacionados, o que de cualquier otra forma revele información en ellos contenida, quedará sujeto a las responsabilidades administrativas, civiles o penales correspondientes.

Las instituciones de crédito deberán dar contestación a los requerimientos que la Comisión Nacional Bancaria y de Valores les formule en virtud de las peticiones de las autoridades indicadas en este artículo, dentro de los plazos que la misma determine. La propia Comisión podrá sancionar a las instituciones de crédito que no cumplan con los plazos y condiciones que se establezca, de conformidad con lo dispuesto por los artículos 108 al 110 de la presente Ley.

La Comisión emitirá disposiciones de carácter general en las que establezca los requisitos que deberán reunir las solicitudes o requerimientos de información que formulen las autoridades a que se refieren las fracciones I a IX de este artículo, a efecto de que las instituciones de crédito requeridas estén en aptitud de identificar, localizar y aportar las noticias o información solicitadas.

Artículo 117 Bis.- La Comisión Nacional Bancaria y de Valores estará facultada para proporcionar a autoridades financieras del exterior, información sobre las operaciones y servicios previstos en el artículo 117, así como en la fracción XV del artículo 46 de esta Ley, que reciba de las instituciones de crédito, siempre que tenga suscritos con dichas autoridades acuerdos de intercambio de información en los que se contemple el principio de reciprocidad, debiendo en todo caso abstenerse de proporcionar la información cuando a su juicio ésta pueda ser usada para fines distintos a los de la supervisión financiera, o bien, por causas de orden público, seguridad nacional o por cualquier otra causa prevista en los acuerdos respectivos.

CAPITULO II

DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

1. ANTECEDENTES

En el marco normativo internacional, encontramos el reconocimiento de los derechos personalísimos, entre los que destacan los siguientes instrumentos:

1.1. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS 1948.

La *Declaración Universal de los Derechos Humanos* (DUDH), adoptada por la Asamblea General de la ONU en 1948[24], es generalmente considerada la declaración por excelencia sobre derechos humanos internacionales. De observancia obligatoria para todos los Estados por el derecho internacional público consuetudinario, garantiza una serie de derechos fundamentales, inalienables y esenciales al ser humano en los siguientes términos:

Artículo 6

Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica.

Artículo 12

Nadie será objeto de injerencias arbitrarias en su vida privada, su 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.

[24] Resolución 257 A (III), 10 de Diciembre de 1948.

1.2. CONVENCIÓN EUROPEA PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES 1950.

La Convención Europea de Derechos Humanos fue adoptada por el Consejo de Europa en 1950 y entró en vigor en 1953. El nombre oficial de la Convención es *Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.*

Dicha convención se celebró tomando en consideración la Declaración Universal de Derechos Humanos, proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948; la cual tiende a asegurar el reconocimiento y la aplicación universales y efectivos de los derechos en ella enunciados.

La finalidad del Consejo Europeo era realizar una unión más estrecha entre sus miembros y considerando que uno de los medios para alcanzar dicho fin es la protección y el desarrollo de los derechos humanos y de las libertades fundamentales, las cuales constituyen las bases mismas de la justicia y la paz en el mundo, cuyo mantenimiento reposa esencialmente por un lado en un régimen político verdaderamente democrático y por otra parte en una concepción y un respeto comunes de los derechos humanos; los gobiernos de los Estados Europeos animados de un mismo espíritu y en posesión de un patrimonio común de ideales y de tradiciones políticas, de respeto a la libertad y de preeminencia del derecho, acordaron celebrar dicho convenio con el objeto de asegurar la garantía colectiva de los derechos enunciados en la Declaración Universal.

Artículo 8. Derecho al respeto a la vida privada y familiar.

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

1.3. PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS 1969.

Los Estados parte en este Pacto[25] toman en consideración los principios enunciados en la Carta de las Naciones Unidas, la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables, y que éstos derechos se derivan de la dignidad inherente a la persona humana, busca como se establece en la Declaración Universal promover el respeto universal y efectivo de los derechos y libertades humanos. Sus artículos 16 y 17, garantizan el derecho en los siguientes *términos:*

Artículo 16

Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica.

Artículo 17

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

---

[25] Pacto Internacional de Derechos Civiles y Políticos de fecha 16 de Diciembre de 1966.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

1.4. DECLARACIÓN AMERICANA DE LOS DERECHOS Y DEBERES DEL HOMBRE.[26]

Derecho a la protección a la honra, la reputación personal y la vida privada y familiar.

Artículo V: Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

Derecho a la inviolabilidad del domicilio.

Artículo IX: Toda persona tiene el derecho a la inviolabilidad de su domicilio.

Derecho a la inviolabilidad y circulación de la correspondencia.

Artículo X: Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia.

Derecho de reconocimiento de la personalidad jurídica y de los derechos civiles.

Artículo XVII: Toda persona tiene derecho a que se le reconozca en cualquier parte como sujeto de derechos y obligaciones, y a gozar de los derechos civiles fundamentales.

---

[26] Declaración Americana de los Derechos y Deberes del Hombre, tomado de http://www.jusneuquen.gov.ar/share/legislacion/leyes/tratados/derechos_deberes_hombre.htm

1.5. CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS.

Dicha convención se llevó a cabo en la Ciudad de San José, Costa Rica el 22 de noviembre de 1969 y se denominó ***"PACTO DE SAN JOSÉ DE COSTA RICA"***[27], los Estados signatarios de ésta Convención tienen como propósito consolidar en este continente, dentro del cuadro de las instituciones democráticas un régimen de libertad personal y de justicia social, instituido en el respeto de los derechos esenciales del hombre que tienen como fundamento los atributos de la persona humana, razón por la cual justifican una protección internacional, de naturaleza convencional coadyuvante o complementaria de la que ofrece el derecho interno de los Estados Americanos y tomando en consideración que estos principios han sido consagrados en la Carta de la Organización de los Estados Americanos, en la Declaración Americana de los Derechos y Deberes del Hombre y en la Declaración Universal de los Derechos Humanos, han convenido proteger los derechos sociales, económicos, culturales, civiles y políticos de todo individuo.

Artículo 3. Derecho al Reconocimiento de la Personalidad Jurídica

Toda persona tiene derecho al reconocimiento de su personalidad jurídica.

Artículo 11. Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

---

[27] Convención Americana sobre Derechos Humanos suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos en la Ciudad de San José Costa Rica el 22 de Noviembre de 1969. (Pacto de San José).

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Artículo 14. Derecho de Rectificación o Respuesta

1. Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.

3. Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.

1.6. DECLARACIÓN SOBRE LA LIBERTAD DE EXPRESIÓN.[28]

3. Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.

Del numeral 3 de la declaración sobre la libertad de expresión, se infiere que hay ya un reconocimiento de otro derecho personalísimo, el derecho a la protección de los datos personales, el que al estar incluido en dicho instrumento, parecería estar ubicado más como una limitante de la libertad de expresión, o bien como parte del

[28] Aprobada por la Comisión interamericana de Derechos Humanos en el año 2000, tomado de http://www.cidh.oas.org/Basicos/Basicos13.htm

denominado derecho a la información, que como un derecho autónomo y de carácter personalísimo.

No obstante lo anterior, y aún cuando el derecho a la protección de los datos personales surge como un derecho que tutela otros derechos personalísimos, como el derecho a la intimidad, al honor o a la imagen, tanto la doctrina como algunas legislaciones nacionales han reconocido ya su naturaleza como derecho personalísimo y autónomo respecto de aquellos que garantiza.

Oscar Puccinelli afirma que el derecho a la protección de datos contiene reglas de fondo propias y es tutelable mediante ciertas garantías específicamente creadas para ello, por lo que es un derecho autónomo por su contenido y esencia, que aunque se nutre en aspectos parciales con los de otros derechos que coadyuvan a su integración, es exclusivo de él. La defensa de la autonomía de este derecho, radica en la propia evolución del derecho a la intimidad, dado el carácter dinámico de los derechos fundamentales.[29]

En este sentido, Puccinelli afirma que puede argumentarse como fundamento de este derecho a otros preexistentes, pero el contenido del derecho a la protección de datos difiere de aquellos, con lo cual se justifica su autonomía, y requiere de garantías específicas para su tutela.

El derecho a la protección de datos personales[30] como hoy se encuentra perfilado en la doctrina más calificada es de reciente acuñación, encontrando su germen en el derecho a la intimidad personal y familiar, reconocido en diversos textos de carácter internacional en la época de la posguerra.

---

[29] PUCCINELI, Oscar, *"El Habeas Data en Indoiberoamerica"*, Editorial temis, Bogotá, Colombia 1999, p.p. 70 y 71.

[30] La expresión protección de datos hace alusión al amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte en su entorno personal, social o profesional. *Veáse*. DAVARA RODRÍGUEZ, Miguel Ángel, *"Manual de Protección de Datos para Abogados"* Aranzadi, Navarra, 2006.

Cabe señalar que la Carta de Derechos Fundamentales de la Unión Europea fue aprobada por la cumbre de Jefes de Estado y de Gobierno celebrada en la Ciudad de Niza el 07 de diciembre de 2000, reconociendo entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8.

De este modo, a partir de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y como un derecho autónomo del derecho a la intimidad y a la privacidad de las personas.

La Carta de Derechos Fundamentales de la Unión Europea[31] señala que:

Artículo 8 Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Este mismo ordenamiento en su artículo 7 contempla lo relativo al Respeto de la vida privada y familiar que a la letra dice:

---

[31] Carta de Derechos Fundamentales de la Unión Europea, tomado de http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

2. EL DERECHO A LA PROTECCIÒN DE DATOS PERSONALES.

2.1. LA SOCIEDAD DE LA INFORMACIÓN.

Resulta indiscutible la evolución que en los últimos años está experimentando el sector de las telecomunicaciones.[32]

La informática, unida a las comunicaciones, ofrece un potencial ilimitado de acceso inmediato a la información. Ésta se ha convertido en nuestro recurso más valioso. Nuestra forma de comunicación –ya sea entre particulares, ya frente a la administración-, de utilización del ocio, de adquisición de nuevos conocimientos y, en general, nuestra forma de vida está cambiando. Consecuentemente las instituciones sociales, las reglas de conducta, los modelos de enseñanza y nuestro estilo de vida deben adaptarse a esos cambios con el fin de extraer el máximo beneficio posible de la que ya con carácter general se viene denominando *"sociedad de la información"*.

En nuestro entorno, tanto personal como profesional, continuamente estamos recibiendo mensajes acerca del potencial que para nuestras vidas van a suponer las nuevas tecnologías de la información y de las comunicaciones. La aparición de conceptos tales como *aldea global* y *sociedad de la información*, tan familiares para algunos y tan ajenos para otros, ha propiciado un amplio debate político y jurídico en el ámbito nacional, internacional y fundamentalmente, comunitario, dirigido a examinar las incidencias que de ellos se derivan y sobre todo a buscar el material legislativo adecuado para hacer frente a los cambios que comportan las nuevas formas de comunicación y de transmisión de datos.

---

[32] Las tecnologías de la información y de las comunicaciones (TIC) son el sector de actividad que más rápidamente está creciendo en el mundo, registrando una tasa de crecimiento anual de 7 al 8 por 100.

Pero ¿Qué es en realidad la sociedad de la información? Como punto de partida para el análisis de este fenómeno, debe destacarse el hecho de que el desarrollo y la universalización de las nuevas tecnologías de la información y las comunicaciones, si bien provocan una revolución técnica en el estado de la ciencia, no agotan ahí sus efectos. Su impacto es también cultural, económico, legal y social.

Actos básicos del ser humano –como el empleo, la educación, la sanidad- o necesidades derivadas de su carácter de ser social –como el comercio- se van a ver influidos por ellas. El carácter universal y más accesible que en los últimos años han adquirido los recursos informáticos, unido al desarrollo de las nuevas tecnologías, ha propiciado el que la informatización de la sociedad, anunciada desde finales de los años setenta, se haya convertido en una realidad que se concreta en una nueva forma de organización social. Este fenómeno engendra una revolución que, a decir de algunos, tendrá una incidencia equivalente a la que tuvo la revolución industrial hace un siglo.[33]

Las nuevas tecnologías configuran la información como uno de los valores fundamentales de nuestra sociedad. Estamos cambiando desde una forma de vida asentada en los bienes físicos hacia una centrada en el "conocimiento y la información". Como afirma FERNÁNDEZ ESTEBAN[34] *las nuevas tecnologías y entre ellas Internet, han creado una nueva mercancía que es el intercambio de datos.*

---

[33] En este sentido se dirigen las palabras pronunciadas por el Sr. MODOL PIFARRE ante la comisión de Internet creada en el Senado al manifestar que: "*El nuevo fenómeno de la información representará en poco tiempo un impacto similar al que supuso la Revolución Industrial inglesa en el siglo XIX*". Como decía Manuel Castell en una reciente entrevista, no todo mundo se hizo británico en el XIX, pero sí cambiaron en todo el planeta los parámetros de la economía y de la sociedad. Debemos ser conscientes de que no toda la sociedad va a entender, por lo menos desde el principio, de que estamos hablando: debemos ser conscientes de que no todo el mundo va a entender que estamos ante un cambio igual o más importante al vivido en la revolución industrial. *Comisión especial sobre redes informáticas celebrada el lunes 18 de mayo de 1998, Cortes Generales, Diario de Sesiones del Senado, año 1998, Comisiones, 290.*

[34] En estos términos se pronunció en su comparecencia ante la Comisión especial sobre redes informáticas celebrada el 16 de junio de 1998. *Cortes Generales, Diario de Sesiones del Senado, año 1998, Comisiones, 308.*

Así, podemos definir *la sociedad de la información* como un nuevo 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 vía 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 comunicación se conviertan en herramientas para la creación de una sociedad de integración en la que todos los ciudadanos tengan cabida.[35]

Las actividades que pueden verse afectados por el fenómeno de la sociedad de la información son muy amplios y afectan prácticamente a todos los aspectos de nuestra vida: al hogar, a la enseñanza, al trabajo, a la actividad empresarial, a la sanidad, a las relaciones con las administraciones públicas e incluso a nuestra forma de participación en la vida política.

2.2. NECESIDAD DE TUTELAR DE MANERA ESPECÍFICA LOS DATOS DE CARÁCTER PERSONAL.

Las dos últimas décadas del segundo milenio marcaron un desarrollo incontenible del poder de la información (incluido el informático) en todos los sectores y estratos sociales, en especial por la multiplicación y el abaratamiento de los medios tecnológicos de almacenamiento y transmisión. Además de popularizarse la casetera, la televisión satelital y el fax, las computadoras disminuyeron de

[35] El advenimiento de la sociedad de la información en el tercer milenio fue precedido por G. ORWELL a finales de los años cuarenta en su obra 1984, donde se retrata una sociedad futura basada en la electrónica. Más tarde, en los sesenta, MARSHAL MMCLUHAN, en la *galaxia gutenberg,* va más allá que Orwell y acuña el término *aldea global* que encierra toda una visión de futuro de lo que sería el planeta a finales del presente siglo: una sociedad basada en la tecnología de la información y la comunicación. Pero quizás haya sido A. TOFFLER, en los años setenta, quien alcanzó una mayor repercusión y difusión de sus teorías. Este autor sitúa en el final del milenio la mayor y más rápida revolución en la historia de la humanidad, aventurando una nueva civilización desconocida hasta el momento, que se caracteriza por el saber, el conocimiento y la información (*datos extraídos de la Guía de recursos: Trabajar en Internet, Consejería de Cultura, Principado de Asturias).*

tamaño y se introdujo la Internet, creando lo que hoy se conoce como "ciberespacio", un marco virtual en permanente e incontenible expansión, donde todos pueden participar, aportando y recibiendo información, lo que implica en su faz positiva, que resulte un inagotable dínamo de la libertad, aunque en su faz negativa, es capaz de producir lesiones difícilmente conjurables sobre los derechos.

Comentando este proceso expansivo de nuevas tecnologías y libertades KINSLEY explica que, en los años ochenta, además de la aparición de la computadora personal, hubo otro avance que resultó aún más importante para la libertad política: el fax, que "hizo imposible el monopolio estatal y el control de tráfico interno y externo de la información.

En los años noventa surgió la Internet, y la posibilidad de que cualquier gobierno controlara la información quedó cancelada para siempre. Además esta red de comunicación electrónica dio a los individuos más poder que la computadora personal en relación con las grandes empresas... cualquier poseedor de una computadora y un módem puede publicar en la red. Lo único que necesita para tener acceso a Internet son ciertos programas y un pago mensual. Internet ha frustrado en mayor medida que el fax, los intentos de los gobiernos por controlar la información".[36]

Los nuevos adelantos tecnológicos tienen, como todo avance, aspectos positivos y negativos. Como medios aptos para la diseminación y captación generalizada de la información, el desarrollo de los pueblos y el ejercicio de los más variados derechos, ha llamado la atención y desde luego, provocado el apoyo de la comunidad internacional.[37] Sin embargo, y dado que también pueden provocar perjuicios a las personas, normas de diversas fuentes (internas, regionales e

[36] KINSLEY, George Orwell, *"Selecciones del Reader's Digest"*, agosto 1997, p. 79 a 82.
[37] Por ejemplo, en la Conferencia Internacional sobre Población y Desarrollo (El Cairo, 1994) merecen ser destacadas las medidas 3.8 y 11.14, en las que se elogian las ventajas de la multiplicación e interconexión de los medios de comunicación disponibles, especialmente los que son fruto de las nuevas tecnologías.

internacionales globales) han intentado establecer ciertos límites a la libertad de buscar, recolectar y difundir información, a fin de lograr el respeto de los derechos y la protección de la seguridad nacional, del orden público y de la salud y la moral públicas.[38]

En este mismo sentido, además, y a fin de contrarrestar en alguna medida las consecuencias dañosas de la difusión de informaciones inexactas o agraviantes vertidas a través de los medios de comunicación tradicionales (principalmente diarios, radios, televisión y revistas, aunque las reglas internacionales relativas a la libertad de expresión y sus límites alcanzan a todos los medios de expresión), se crearon ciertos mecanismos específicos de garantía de los derechos que pueden ser transgredidos (por ejemplo el incorrectamente rotulado "derecho" –es una garantía- de réplica, también conocido como amparo informativo, regulado por el artículo 14 de la Convención Americana sobre Derechos Humanos.

Actualmente estos medios tradicionales, no son los únicos que pueden causar perjuicios mediante la compilación y comunicación de información, pues el almacenamiento, elaboración y transmisión de datos, especialmente por vía de la telemática[39] potencia considerablemente aquellos peligros.

A fin de disminuir las indeseadas consecuencias de estos nuevos medios, se han adoptado diferentes respuestas: en algunos países se dictaron sólo normas sectoriales de protección de datos (v. gr., sobre centrales de riesgo); en otros se optó por normas generales (sin perjuicio de algunas sectoriales específicas) que prevén ciertos principios, a los que deben sujetarse esencialmente quienes manipulan datos, y establecen sanciones administrativas y penales para quienes

[38] Entre las normas de fuente internacional, global y regional, cabe citar el artículo 19 párrafo 3º, del Pacto internacional de Derechos Civiles y Políticos, el artículo 13, incisos 2 y 4, de la Convención Americana sobre Derechos Humanos y el artículo 13 inciso 2 de la Convención sobre Derechos del Niño.

[39] Esta voz surge de la conjugación de "telecomunicación" e "informática", y ha sido definida en el Convenio sobre Telecomunicación Internacional de 1973 (Málaga) como "el conjunto de servicios de naturaleza u origen informático que pueden ser prestados a través de una red de comunicaciones".

las violen, y en otros se ha creado –solamente o en conjunción con alguna de las dos variantes mencionadas- un proceso judicial específico de acceso e impugnación de datos de carácter personal, conocido como "habeas data".

Es que el tratamiento de datos no puede dejarse sólo sujeto a las reglas del mercado –opción originalmente adoptada por Estados Unidos, pero que gradualmente ha ido desandando-, pues resulta de toda obviedad que quien cuenta con información cuenta con poder, y quien tiene poder tiende a abusar de él.

La ausencia de regulación y de control a los usos de las técnicas informáticas, podría expandir ilimitadamente el dominio del estado o de los sujetos que disponen de poder informático.

La respuesta del derecho, sin embargo, no se endereza a suprimir este nuevo factor de control social. El habeas data representa apenas un intento incipiente y tímido dirigido a corregir distorsiones extremas del proceso comunicativo informático. De un lado, reduce en cierto grado la invisibilidad de los gestores o titulares de bancos de datos – lo que se logra exigiendo un registro de bancos, una declaración de sus objetivos y de sus procedimientos, etc.-; de otro lado, permite a las personas, en cierta medida, adquirir conciencia de su transparencia externa y de sus condiciones, pudiendo incidir en la elaboración y transmisión de formatos singulares o unidimensionales de su personalidad y de sus acciones.

En el fondo, el derecho legitima el poder informático al convalidar dentro de ciertos límites y condiciones el tratamiento informatizado del sujeto con arreglo a las exigencias funcionales de aparatos públicos y privados que sólo captan a la persona a partir de códigos y gramáticas fraccionadas. De este modo, no sale ileso de su confrontación con la técnica.

La regulación del habeas data, positiva en términos generales e indispensable como forma de sujetar la técnica al derecho, ha tenido de cualquier manera un precio para éste que ha consentido – o se ha visto compelido a hacerlo- y justificado el tipo particular de la antropología que asume la tecnología informática, para la cual la persona humana se convierte en mero dato o conjunto de datos esparcibles y transmisibles a través de sus canales y a tenor de sus pulsaciones.

De lo antes mencionado, es fácil deducir que una política protectora demasiado estricta provocaría graves daños globales a la comunidad.[40] A la vez, una demasiado elástica generaría groseras violaciones a los derechos humanos, en especial porque, a diferencia de muchas otras formas de violación de ellos (v gr., robos, detenciones ilegales), en la mayoría de los casos éstas se producen sin que la persona cuyos datos son objeto de tratamiento se entere- de allí la necesidad de establecer, como lo requiere el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, una serie de principios y derechos específicos, cuya observancia, además, sea controlada por una autoridad independiente-.

En este sentido, PIÑAR MAÑAS agrega que los datos de carácter personal deben ser tutelados por que el derecho a su protección constituye un derecho fundamental según el ordenamiento positivo (y así además surge del proyecto de Constitución Europea, que hace alusión a él en dos ocasiones) y porque además el dato tiene un valor económico que lo hace objeto de múltiples transacciones (ningún emprendimiento comercial de mediana envergadura puede iniciarse con éxito sin bases de datos confiables) y de enormes peligros para quienes figuran en esos sistemas de información.[41]

---

[40] GILS CARBÓ, Alejandra M., *"Régimen legal de las bases de datos y habeas data"*, Bs. As., La Ley, 2001, p. 25 a 27.

[41] PIÑAR MAÑAS, disertación pronunciada en el "Foro sobre protección de datos personales y regulación legal del habeas data", Bogotá, 12/12/03.

2.3. LOS DERECHOS "DE" Y "A" LA PROTECCIÓN DE DATOS.

La potencialidad dañosa sobre los derechos de las personas derivada del tratamiento de datos de carácter personal ha provocado, en especial a partir de la aparición de la informática, un despliegue normativo, doctrinal y jurisprudencial que permite actualmente aludir a una nueva disciplina: "el derecho de la protección de datos", cuyo importante desarrollo proviene, precisamente del reciente reconocimiento del "derecho a la protección de datos"- rotulado por otros "libertad informática", "intimidad informática", "derecho a la autodeterminación informativa o informática", "information control", "data protection", "datenschutz", "habeas data", etcétera-.

Por un lado, el derecho de la protección de datos está integrado por un conjunto de normas y principios, que destinados o no a tal fin, y con independencia de su fuente, son utilizados para la tutela de los diversos derechos de las personas – individuales o jurídicas- que pudieran verse afectadas por el tratamiento (acceso, registro, elaboración, transmisión a terceros, etcétera) de datos de carácter personal.

Por el otro, el derecho a la protección de datos puede ser definido como la facultad conferido a las personas para actuar *per se* y para exigir la actuación de Estado con el fin de obtener la tutela de los diversos derechos que pudieran verse afectados en virtud de aquellas operaciones de tratamiento de los datos de carácter personal que les conciernen.

Desde luego, ambos derechos no se reducen, como pareciera sugerir su rotulación, a la mera protección de los datos en sí, sino que son medios para la tutela de otros bienes jurídicos (lo que no les hace perder la categoría de derechos, pues no alcanzan a reunir las notas típicas de la moderna concepción de las garantías) entre los cuales están implicados los principios rectores de los

derechos humanos (libertad, dignidad e igualdad), y múltiples derechos fundamentales (intimidad, identidad, honor, propiedad sobre los datos, etcétera).[42]

En esta materia se desprende que lo que se busca proteger son los datos de carácter personal, pero únicamente como medio para tutelar los bienes jurídicos que el uso de esos datos puede vulnerar; se protegen de ciertas actividades respecto de tales datos, conocidas técnicamente como "tratamiento" y dentro de las cuales se encuentran el acceso, registro, elaboración y transferencia a terceros, así como 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.

El derecho a la protección de datos puede ser tutelado de diversas formas, de las cuales las más comunes son las que se detallan a continuación:

a) Las normas generales o específicas, convencionales, constitucionales o legales que establezcan:

    1. Ciertas reglas mínimas para el tratamiento de datos de carácter personal y para la habilitación de las bases y bancos de datos, específicamente limitando sus actividades a las estrictamente necesarias para la finalidad para la que son autorizados;

    2. Derechos de los registrados;

    3. Sanciones administrativas y penales para quienes infrinjan las normas (por ejemplo el artículo 8° de los principios de la ONU; el artículo 10 del Convenio

[42] PUCCINELLI, Oscar R, *"Protección de Datos de Carácter Personal"*, Editorial Astrea, Buenos Aires 2004, p.p. 8 y 9.

Europeo de 1981 y el artículo 24 de la directiva europea de 1995);

4. Mecanismos institucionales de garantía (como un órgano de control, con funciones de habilitación y seguimiento de los bancos de datos de carácter personal);

5. Recursos ante ese órgano de control y otras vías administrativas idóneas;

6. Vías judiciales de amparo específicamente amoldadas a la tutela de los datos (por ejemplo el habeas data del constitucionalismo iberoamericano; ó

7. La remisión a mecanismos procesales no específicos, pero que sean aptos para brindar tutela urgente a los derechos fundamentales (amparo, tutela o recurso de protección).

b) Las normas sectoriales que traten aspectos concretos (por ejemplo alcances de los secretos impositivo o estadístico).

c) Los contratos-acuerdo respecto del tratamiento de determinados datos.

d) Los códigos de conducta, deontológicos o de ética.

e) Los instrumentos internacionales (globales o regionales) que regulen ciertos aspectos comunes, en especial lo relativo al flujo de datos transfrontera.

Como se puede apreciar, no hay un sistema único de protección de datos de carácter personal, ya que no todos los sistemas jurídicos lo encaran del mismo modo. Sin embargo, sí hay una tendencia a la homogenización de principios y criterios, a fin de potenciar las interrelaciones (industriales, comerciales, administrativas, etc.) entre los pueblos a través de la transmisión internacional de datos.

Desde luego, de nada sirven las normas que establezcan esos principios a los que debe ajustarse el tratamiento de datos de carácter personal y el reconocimiento de ciertos derechos específicos, si no se diseñan medios efectivos de protección; con tal fin usualmente se establecen sanciones de tipo administrativo a cargo de un órgano de control (multas, inhabilitación), penal (creación de delitos específicos por violación de determinadas previsiones legales) e incluso civil (indemnización tarifada). A ello suelen adicionarse mecanismos específicos (judiciales y administrativos) de tutela de los derechos reconocidos.

ESTADELLA YUSTE, señala que existen dos posibilidades para que los individuos reclamen el cumplimiento de sus derechos: recurrir a la autoridad nacional o a los tribunales ordinarios civiles o administrativos. No en todas las legislaciones nacionales se incluyen ambas modalidades; en concreto, en aquellos países que siguen una legislación sectorial, y que carecen de una autoridad nacional, los individuos tendrán que recurrir a los tribunales ordinarios. En los países con legislación *ómnibus,* es norma general que la primera demanda por violación de los derechos individuales sobre protección de datos se realice frente a la autoridad nacional, quien estudiará los particulares de la demanda así como las argumentaciones del titular del fichero, cuya decisión es apelable ante los tribunales ordinarios civiles o administrativos.[43]

[43] ESTADELLA YUSTE, "*La Protección a la Intimidad frente a la Transmisión Internacional de Datos Personales*" Madrid, Tecnos, 1995, p. 130 y 131.

PÉREZ LUÑO, indica que, a los instrumentos tutelares judiciales se les ha sumado la difusión creciente de instituciones de protección que tienden a completar la función de garantía de los tribunales. En este sentido, debe hacerse notar el protagonismo adquirido por el sistema del *Ombudsman* en defensa de los derechos y libertades de la tercera generación.

El sistema del *Ombudsman* para la protección efectiva de los derechos humanos, presenta las siguientes ventajas:

a) Función dinamizadora, adaptadora y de reciclaje de los derechos fundamentales, realizada básicamente a través de los informes periódicos presentados ante los parlamentos de los que son comisionados;

b) Función orientadora de los ciudadanos, agilizando y clarificando los procedimientos de tutela de las libertades; y

c) Función preventiva de las agresiones y daños de difícil e imposible reparación en el ejercicio de tales derechos (al ejercicio de las libertades es de cabal aplicación el célebre adagio latino: *melius est prevenire Quam reprimere).*[44]

2.4. DE LA PROTECCIÓN DE LA INTIMIDAD AL DERECHO A LA PROTECCIÓN DE DATOS O A LA AUTODETERMINACIÓN INFORMATIVA.

El derecho a la protección de datos, pertenece al contexto de la era informática, y ciertamente resulta atrevido afirmar que esta compleja disciplina legal estuviera ya

[44] PEREZ LUÑO, *"Del habeas corpus al habeas data,* citado por VILLALOBOS, *Derecho de la Informática,* en "Temas para Universidades", Facultades de Derecho y Ciencias Políticas, p. p. 135 y 136.

implícita en las referencias generales al derecho a la intimidad inserta en cuerpos normativos de ámbito nacional o internacional de la era pre-informática.[45]

Salvo el aislado precedente de la Constitución Alemana de 1919, fue recién a partir de 1970 cuando los ordenadores mostraron un notable incremento en los potenciales riesgos del tratamiento de datos de carácter personal, que comenzó el desarrollo normativo del derecho a la protección de datos. Así, los países tecnológicamente más avanzados –en especial los europeos- fueron elaborando paulatinamente legislación específica sobre el tema, apuntando a establecer reglas concretas para enfrentar la nueva problemática.

Sobre algunos de los bienes jurídicos implicados en el tratamiento de los datos de carácter personal (en especial la intimidad de los registrados) se han esbozado las primeras teorías justificatorias de la creación de un derecho autónomo a la intervención sobre los datos; pero ciertamente aquellas no son excluyentes, sino, por el contrario, en la mayoría de los casos, resultan complementarias.

Si bien la doctrina mayoritaria, encuentra en el derecho a la intimidad la fuente del derecho a la protección de los datos de carácter personal, resulta ciertamente difícil sostener que ese mismo derecho se aplique a las personas jurídicas, donde el bien jurídico que se busca tutelar será en todo caso similar, pero no idéntico- *v.gr., el derecho a una esfera de reserva de las operaciones comerciales-.*

En este sentido y aludiendo al paso de la intimidad clásica al derecho de acceso y control de los propios datos, CARRANZA TORRES explica que la formulación contemporánea del concepto de intimidad se debió a dos jóvenes juristas estadounidenses , WARREN y BRANDEIS, quienes lo definieron en 1890, en un artículo publicado en "*Harvard Law Review*", como el derecho a ser dejado solo y que a lo largo de casi la centuria que siguió a dicha formulación, tanto en el

[45] ESTADELLA YUSTE, "*La Protección a la Intimidad frente a la Transmisión Internacional de Datos Personales*" Madrid, Tecnos, 1995, p. 15.

common law como en el derecho continental, fue entendido primordialmente como la facultad de exclusión de terceros respecto de determinadas facetas de la vida de las personas.

Agrega además el autor: "De esta formulación principal se desgajaron, a partir de entonces y hasta el presente, una serie de derechos más específicos. Por ello se dice que el concepto moderno de la privacidad engloba una colección de intereses jurídicamente protegidos, tales como la privacidad de las ideas, la protección de la imagen personal, la privacidad en el domicilio y la protección del honor, entre otros... la forma de regulación jurídica de lo relacionado con el derecho a la intimidad en el derecho internacional parte de entender al mismo como un derecho multidimensional, que en definitiva agrupa a otros que, partiendo de su contenido de base, desarrollan de modo más específico las distintas facetas que el mismo adquiere en contacto con la realidad..."

El concepto de "derecho a la autodeterminación informativa" se construye a partir de la noción de intimidad, *privacy, riservatezza o vie priveé.*

En los años sesenta surge en la doctrina el reconocimiento de un derecho de las personas encaminado a reivindicar la protección jurídica frente a la captación y utilización no autorizada de información personal.

Refiere PALAZZI, que ya en el año 1968 CHARLES FREID definió la *privacy,* concepto jurídico semejante al nuestro de intimidad, como el control que se tiene sobre los propios datos. Tal definición fue de aceptación general de la doctrina. Posteriormente, LAWRENCE TRIBE, en su obra *American Constitutional Law,* se refirió a un derecho a controlar la masa de información por la que se define la identidad de una persona, como parte del derecho que cada persona desea (o no) mostrar a la sociedad".[46]

---

[46] CARRANZA TORRES, "*Habeas Data: La Protección Jurídica de los Datos Personales*" , Cordoba, Alveroni, 2001, p.p. 21 a 25, con cita de PALAZZI, "*el habeas data en el derecho argentino*", p. 5, en http://ulpiano.com.

El derecho a la protección de datos refleja más que una idea individualista de protección a la intimidad, ya que engloba también los intereses de grupo contra el procesamiento, almacenamiento y recolección de información. En definitiva, se puede decir que el derecho a la protección de datos o a la autodeterminación informativa está solapado con una parte importante del derecho individual a la intimidad; ésta es la que hace referencia a la protección de los datos personales de la esfera privada.[47]

A las primigenias elaboraciones doctrinales y normativas se les sumó rápidamente la labor jurisprudencial, que fue perfilando la autonomía del derecho a la protección de datos de carácter personal. Sin duda la sentencia más trascendente, considerada por los autores especializados como el punto de arranque en el despliegue de este nuevo derecho, es la dictada en 1983 por el Tribunal Constitucional (*Bundesverfassungsgericht)* de Karlsruhe[48]. Al declarar en ella la inconstitucionalidad de la ley de censo de la población (*Volkszhlungsgesetz),* el Tribunal construyó un nuevo derecho, "a la autodeterminación informativa" (*rech auf informationelle selbstestimmung)*[49] desde el principio básico del ordenamiento jurídico establecido por la ley fundamental de la República Federal de Alemania (el valor y la dignidad de la persona), a partir del cual ésta queda habilitada para actuar con autodeterminación al formar parte de una sociedad libre, por lo que de la dignidad y de la libertad deriva la facultad de la persona de "*deducir básicamente por sí misma, cuándo y dentro de que límites procede revelar situaciones referentes a su propia vida".* Un orden social y un orden jurídico en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo se sabe sobre él... menoscabaría las oportunidades del desarrollo de la personalidad individual, y también el público, porque la autodeterminación constituye una

---

[47] ESTADELLA YUSTE, "*La Protección a la Intimidad frente a la Transmisión Internacional de Datos Personales"* Madrid, Tecnos, 1995, p. 24 a 26.

[48] Sentencia publicada en el "Boletín de Jurisprudencia Constitucional de España", 1984, Nº 33, p. 152 y 153; ver comentario en EKMEKDJIAN-PIZZOLO, *Habeas Data,* p. 23.

[49] No hay consenso doctrinal respecto de la correcta traducción de esta voz; la más difundida es "autodeterminación informativa", aunque algunos la traducen como "autodeterminación informática" o como "autodeterminación informacional".

condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos.

Desde luego, la tesis del Tribunal Constitucional alemán no lleva este derecho a planos absolutos. Antes bien, como lo indica BERGEL, en el mismo fallo se advirtió que "el derecho a la autodeterminación informática no carece de límites. El ciudadano de un Estado social de derecho –señaló- no tiene un derecho sobre sus datos, en el sentido de una soberanía absoluta e ilimitada, sino que es una persona que se desenvuelve en una comunidad social en la que la comunicación y la información resultan imprescindibles. El individuo –al tenor de la decisión- tiene pues que aceptar determinadas limitaciones de sus derechos a la autodeterminación informática en aras del interés preponderante de la colectividad".[50]

Como bien lo indica GILS CARBÓ al analizar el fallo: "La cuestión que dio lugar a ese pronunciamiento fue la iniciativa del estado de recoger una amplia información sobre los ciudadanos en oportunidad de realizar un censo de la población. Se pretendía requerirles datos sobre sus nombres, apellidos, dirección, teléfono, sexo, fecha de nacimiento, ideología política, religión, nacionalidad, el tipo de convivencia con otras personas, domicilio, clase de trabajo, ingresos, profesión aprendida, duración del periodo de estudios, dirección del trabajo, los medios de locomoción utilizados para ir al trabajo, tiempo promedio utilizado para ese recorrido, duración de la jornada laboral, clase, extensión, dotación y usos de la vivienda, número y uso de las habitaciones, cuantía de los alquileres mensuales. Además se reprimía con la aplicación de sanciones cualquier negativa a suministrar la información.

El tribunal superó los parámetros anteriores vinculados a la teoría de las esferas, consagrando la tesis de que ya no existían datos sin interés, sino que todos

[50] BERGEL, "*El habeas data: instrumento protector de la privacidad, Revista de Derecho Privado y Comunitario*" nº 7, p. 127, con cita de PÉREZ LUÑO, *Nuevas Tecnologías, Sociedad y Derecho*, p. 27.

merecían protección en tanto sirvieran para configurar una radiografía de los ciudadanos". [51]

El derecho a la intimidad, sus mecanismos jurídicos de tutela y su ámbito de protección resultaban suficiente garantía para el individuo en el desenvolvimiento de su vida privada. La libertad individual, el libre desarrollo personal y la vida privada y familiar gozaban de un amparo jurídico suficiente hasta la irrupción de la informática, que disponiendo de medios ilimitados para conocer, almacenar, tratar y ceder información personal, invade todos los ámbitos de actuación del ser humano.

RODOTA, acertadamente indica que la nueva concepción de la *privacy* no se reduce ya al derecho a ser dejados solos, sino que hace alusión también al "derecho a controlar el uso que otros hagan de informaciones concernientes a un determinado sujeto". [52] Una doble reflexión puede concluirse de la relación entre los términos intimidad-privacidad, el bien que se tutela a través de la protección de datos personales se resume en:

a) El derecho que compete a toda persona a tener una esfera reservada en la que desarrollar su vida, sin que la indiscreción externa pueda acceder a ella y,

b) En la protección y salvaguarda que se facilita a las personas titulares de datos para evitar el acceso no consentido de terceros a datos relativos a la persona.

La dualidad intimidad- *privacidad* podría resumirse, en la siguiente afirmación: la intimidad no es, en realidad, un sinónimo de *privacidad,* aunque se considera a

---

[51] GILS CARBÓ, Alejandra M., *"Regimen legal de las bases de datos y habeas data"*, Bs. As., La Ley, 2001, p. 14.

[52] RODOTA, Stefano, "*Protection de la vie priveé et controle de l'inforation: Deux sujets d'inquíetude croissante pour l'opinion publique,* OCDE, 1976, P. 40.

veces de este modo al no poseer término apropiado para la noción original de *privacy*. Podría decirse que la privacidad es una noción sociológica al definirse con referencias a un exterior formado por una pluralidad –de personas, grupos...-, y que por el contrario, la intimidad es un concepto psicológico que alude a un "mundo" que se desarrolla en el propio interior. En este sentido, la privacidad contendría a la intimidad.[53] Conforme a esta conclusión intimidad y privacidad no constituyen realidades enfrentadas o contrapuestas, sino que, por el contrario, ambas se identifican con el ser o existir individual, representan dos facetas complementarias de la persona, ambas irrenunciables para la realización y desarrollo personal del individuo; la intimidad referida al mundo interior, profundo y esencial del ser humano, y la privacidad referida a esos otros ámbitos de la persona que la vinculan con el mundo exterior, en las relaciones y actividades sociales.[54]

En consecuencia, toda información, cualquier información personal, merece protección frente al poder informático, no es lo verdaderamente significativo la naturaleza íntima o no de los datos que se conocen o tratan, sino que sea susceptible de afectar al individuo; se pretende evitar la intromisión, la simple invasión en la vida ajena.

Así, pues, el fundamento último del derecho a la autodeterminación informativa consiste no en preservar ocultos y aislados del conocimiento ajeno los actos y vivencias de la realidad personal, sino en mantener la libertad del individuo, evitando la simple fiscalización de su vida y, a través de ello, impedir la instrumentalización del ser humano.

---

[53] BEJAR, Helena, *"Indivídualismo, privacidad e intimidad: precisiones y andaduras"*, en CASTILLA DEL PINO, Carlos (Ed.), "De la intimidad", Barcelona, CRITICA, 1989, p. 44.

[54] No puede hablarse de datos íntimos y de otros que no lo son, por que en definitiva, cualquier información de la persona, por irrelevante que parezca puede comprometer la imagen o la intimidad de la persona con sólo relacionarla adecuadamente con otras informaciones de la persona; en previsión de ello, tal vez la técnica de protección de datos personales, no limita su protección a los datos que pudieran considerarse más comprometedores para los derechos de la persona, sino que la amplía a cualquier dato relativo a la persona, por que el tratamiento informatizado de los datos ofrece innumerables posibilidades de registro, procesamiento e interconexión, que constituyen las auténticas amenazas para la persona.

De las consideraciones expuestas se desprende que el derecho a la autodeterminación informativa se configura como un derecho de la personalidad. No sólo y no siempre se defiende a la persona de los abusos informáticos cometidos por la Administración Pública; igualmente, se protege la vida del individuo cuando ésta se vulnera mediante utilizaciones abusivas de la informática realizadas por sujetos privados. Cierto que la preocupación respecto a la invasión de la informática en la vida privada de los individuos nace como consecuencia de la ilimitada disponibilidad de medios con que contaba el sector público; pero, no es menos cierto, que en la actualidad el sector privado respecto a la capacidad de medios compite en plano de igualdad con la Administración Pública.

Por ello, tanto en el ámbito público, como en el sector privado los derechos del individuo pueden verse afectados; así, el concepto jurídico de libertad informática o como otros prefieren, derecho a la autodeterminación informativa, desde su categorización como derecho de la personalidad permite tutelar los derechos del individuo que frecuentemente quedan a merced de los abusos informáticos. Se impone una definición de este derecho que lo contempla desde la perspectiva que considera su finalidad social. Puede afirmarse que el derecho a la autodeterminación informativa pretende garantizar a la persona el goce y respeto de su propia identidad e integridad en todas sus manifestaciones físicas y espirituales.[55]

Por lo anterior y considerando que el derecho a la autodeterminación informativa constituye un derecho de la personalidad sus caracteres propios y definidores son:

a) Se trata de un ***derecho connatural*** e ***innato*** del hombre, lo que viene a significar que son adquiridos desde el nacimiento de la persona, sin necesidad de ningún otro condicionamiento especial. En efecto, es este un derecho que afecta al núcleo más profundo de la persona, por que en la

[55] LACRUZ BERDEJO, José Luis y otros, *"Parte General del Derecho Civil"*, volumen II, Barcelona, Bosch, 1983, p. 29.

sociedad moderna que mayor ataque a la persona puede reconocerse y protegerse que la revelación y tratamiento no consentido de aquellos aspectos que afectan a su vida privada. Estas intromisiones permiten denunciar la existencia de un ataque a la misma libertad de actuar de la persona en cuanto que el acceso de terceros a la información personal condiciona su proceder y su conducta ante la colectividad.

b) Se trata de un ***derecho subjetivo privado,*** por que tutela el disfrute y protección de derechos de la persona frente a injerencias ajenas. Su fundamento principal se encuentra en el reconocimiento de las garantías que hagan preciso el ejercicio de los derechos individuales frente a las intromisiones procedentes de la informática en su vida privada y personal. Por otro lado, que el afectado ostente capacidad de decisión respecto a sus datos, significa que tiene derecho a conocer de qué información disponen los terceros, con qué finalidad se halla registrada en ficheros informáticos y cuál será su utilización, pero al objeto de prohibir cualquier práctica ilícita. Sin embargo, no reconoce al afectado un derecho de propiedad sobre su información, que significaría la calificación de este derecho como patrimonial, por tanto, el objeto de protección lo constituye la persona, más correctamente, el respeto a sus derechos y al libre ejercicio de los mismos. Cualquier intento de patrimonialización de este derecho representa una negación de la verdadera esencia y naturaleza de este derecho que nace para limitar la abusiva utilización de los medios informáticos garantizando los derechos irrenunciables de la persona. No se pretende garantizar el derecho a la propiedad y disposición de los datos, sino el derecho a controlar y vigilar su adecuada utilización.

c) Se trata de un ***derecho de exclusión,*** entendido como derecho *erga omnes.* Se salvaguarda la esfera privada frente a cualquiera, incluso frente a la administración; ahora bien, ello no significa, sin embargo, que se esté ante un derecho absoluto y sin limitación alguna, esto es, todos los

derechos deben ejercitarse teniendo en cuenta los derechos de los demás, el orden público y la moral.

d) Se califica también como un ***derecho inherente a la persona.*** En otras palabras, que le es propio, necesario para el pleno desenvolvimiento de su personalidad, y sin el cual la persona queda desprovista de su natural esencia y fundamento como individuo; tan es así que el ser humano siente la irreprimible necesidad de retener "en su interior" aquellos aspectos de sí mismo y de sus relaciones con los demás que le definen e identifican. Nada más propio del ser humano que el anhelo de preservar sus comportamientos y actitudes de la curiosidad ajena, que ávida de conocimiento, en la actualidad carece de límites gracias al desarrollo de la informática. Así pues, constituye este derecho un bien inherente a la persona, que le corresponde por la mera circunstancia de tal y, que como instrumento jurídico se fundamenta en su función de garantizar al individuo el respeto mismo a su dignidad personal.

De su carácter de inherente, derivan directamente las siguientes características: por un lado, como ***derecho intransmisible e irrenunciable,*** entendiendo que si dicha renuncia tiene lugar, la misma será nula; otra nota propia es la ***inembargabilidad,*** atendiendo al carácter no patrimonial de este derecho. Asimismo, se caracteriza por su ***indisponibilidad*** y por su ***imprescriptibilidad;*** o lo que es igual, no existe plazo para el ejercicio del mismo, su disfrute es permanente en tanto no se produce agresión o intromisión ilegítima.

CAPÍTULO III

MARCO JURÍDICO INTERNACIONAL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

1. INSTRUMENTOS INTERNACIONALES.

Desde hace varias décadas los países económicamente más desarrollados (los países de la Unión Europea y los de la Organización para la Cooperación y el Desarrollo Económico-OCDE) han promulgado leyes para proteger la privacidad en relación a los datos personales. Estas leyes tienen los siguientes objetivos:

1. Prevenir y eliminar violaciones a las garantías individuales con respecto a la privacidad, tales como el almacenamiento y tratamiento ilegal o incorrecto de los datos personales o la transmisión no autorizada de dichos datos; y

2. Evitar que estas regulaciones dificulten el flujo de la información, necesaria para el eficiente funcionamiento de los mercados y para el adecuado desarrollo de la economía.

La legislación de estos países ha conciliado dos objetivos que en apariencia son contradictorios, pero que la evidencia internacional demuestra que son complementarios. Así, permitir que los datos personales, relevantes para las actividades económicas, tengan un valor en el mercado, fomenta su protección por parte de los tenedores de los mismos. Asimismo, incrementa la confianza de los particulares en el buen uso de los datos, lo que permitirá la conformación de mejores bases de datos.

1.1. PRINCIPIOS DE LA OCDE PARA LA PROTECCIÓN DE LA PRIVACIDAD DE LOS DATOS PERSONALES Y SUS FLUJOS TRANSFRONTERIZOS.

Estos principios son resultado de una vasta experiencia internacional[56]. Diferentes países, con diferentes tradiciones jurídicas y grados de desarrollo heterogéneos, han experimentado, en algunos casos por varios siglos, en el tratamiento que se le debe dar a los datos personales.[57]. Sería ineficiente (y arrogante) pretender una elaboración, desde cero, de estos principios. Dada la poca experiencia mexicana en el tema y la premura para regular este tema, se propone analizar los principios para que los reguladores definan la manera en que la regulación propuesta se apegará (o no) a ellos.

En este y en todos los principios, es pertinente recordar que el Estado puede ser un controlador de datos, y que debe sujetarse a los mismos principios que cualquier otro controlador de datos[58], bajo la supervisión de una institución con suficiente independencia para poder tomar sus decisiones de forma adecuada.

I.- PRIMER PRINCIPIO: LAS BASES DE DATOS PERSONALES DEBEN SER PROCESADAS JUSTA Y LEGALMENTE; Y SU PROCESAMIENTO DEBE CUMPLIR CON CIERTAS CONDICIONES MINIMAS.

En este principio se establecen tres requisitos:

1. Cumplir con las condiciones mínimas de procesamiento;

2. Que el procesamiento sea legal; y,

---

[56] Al final se enuncian los documentos que han servido de referencia para identificar estos principios.

[57] Villar del (2001) es una sobresaliente investigación sobre la protección de datos en América y la Unión Europea.

[58] Ninguno de los países miembros de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) establece un régimen más laxo para los controladores públicos de datos personales. De hecho, la mayoría de ellos establece disciplinas más estrictas para los mismos.

3. Que el procesamiento sea apropiado.

1. CONDICIONES MINIMAS DE PROCESAMIENTO

Para el procesamiento de cualquier dato personal debe cumplirse alguna de las siguientes condiciones:

A. El sujeto de los datos ha dado su consentimiento[59] para el procesamiento; o,

B. El procesamiento es necesario[60] para:

a) La ejecución de un contrato en el que el sujeto de los datos es parte;

b) Que, a solicitud del sujeto de los datos, se tomen los pasos requeridos para establecer una relación contractual,

c) Cumplir con cualquier obligación legal a que es sujeto el controlador de los datos, además de las establecidas en relaciones contractuales;

d) Proteger los intereses vitales del sujeto de los datos. En este caso especifico, se debe considerar si la (calidad de) vida del sujeto de los datos está en serio riesgo o sujeta a un grave daño irreversible;

e) La administración de justicia;

---

[59] El consentimiento debe ser obtenido libre de coacción y basado en información veraz y clara. El consentimiento debe ser comprobable.

[60] ¿En quién radica la facultad de definir si es necesario? Hay diferentes enfoques, algunos países lo acotan a una supervisión *ex ante* de los controladores; eso implica una enorme carga de trabajo para la institución responsable de la protección de los datos personales. Otros países prefieren una supervisión *ex post*, lo que se complementa con fuertes sanciones (y compensaciones para el sujeto) en caso de un error por parte de los controladores.

f) El ejercicio de cualquier función conferida por o bajo cualquier disposición jurídica de carácter general; o,

g) El ejercicio de cualquier función de naturaleza pública desarrollada en el interés público; [61]

Por la naturaleza de los *datos personales sensibles,* el procesamiento específico de estos datos debe cumplir con, al menos, una de las siguientes condiciones:

A. El sujeto de los datos ha dado su consentimiento explícito[62] para el procesamiento de dichos datos;

B. El procesamiento es necesario para:

a) Proteger los intereses vitales del sujeto de los datos o de cualquier otra persona, en caso de que no se pueda obtener el consentimiento del sujeto de los datos;

b) Proteger los intereses vitales de una persona diferente al sujeto de los datos e irrazonablemente se ha retenido dicho consentimiento;

c) Funciones relevantes de administración de justicia; o

d) Ejecutar funciones establecidas por o bajo otras leyes; [63]o

[61] Por ejemplo, la prevención de un crimen.
[62] El consentimiento explícito debe ser claro y acotado. Debe cubrir detalles específicos del procesamiento, sobre los datos a ser procesados, el propósito del procesamiento y sobre los resultados a ser revelados. Numerosos países han establecido estándares técnicos obligatorios para regular la obtención de consentimientos (tanto regulares como explícitos).
[63] Un ejemplo sería el procesamiento de datos para verificar la existencia o ausencia de un trato discriminatorio.

C. La información personal sensible ha sido hecha pública deliberadamente por el sujeto de los datos.

2. PROCESAMIENTO LEGAL.

No todos los marcos regulatorios establecen explícitamente que es un procesamiento legal.[64] El procesamiento legal se refiere a que sus propósitos y méritos se apegan a las siguientes características:

a) No son contradictorios ni opuestos a ninguna ley aplicable; y,

b) Existe justificación legal que permita realizar este procesamiento.

Se presentan dos casos donde estas características son evidentes. El primero se refiere a obligaciones de confidencialidad entre controlador y sujeto de los datos personales. En el caso de información médica o bancaria hay obligaciones legales y explícitas de confidencialidad. La regulación relevante establece restricciones explícitas para que dicha información pueda ser utilizada con un propósito diferente para el cual se autorizó el procesamiento de la misma sin el consentimiento manifiesto del sujeto de los datos. Obviamente, un procesamiento ilegal será aquel que no observe estas restricciones legales.

El segundo caso se refiere a las facultades legales de la autoridad para solicitar información. Dependencias y entidades públicas cuentan con facultades explícitas para procesar datos personales, pero esa misma facultad las limita a procesarlos a de la forma establecida en la regulación correspondiente.

[64] Algunos países prefieren definir procesos ilegales. Lo importante es que la restricción sea a favor de los sujetos de los datos.

3. *PROCESAMIENTO APROPIADO.*

Este requerimiento se refiere a que todas y cada una de las etapas del procesamiento deben ser apropiadas y que además sean apropiadas las consecuencias del procesamiento para el sujeto de los datos.

El procesamiento adecuado debe considerar lo siguiente:

A. La forma en que se obtuvieron/recolectaron los datos debe ser apropiada. Se debe evitar que el sujeto de los datos sea engañado o confundido respecto a los objetivos del procesamiento de sus datos personales. De igual forma, el consentimiento debe ser apropiado (comprobable, claro y certero).

B. La información entregada a los sujetos de los datos debe ser apropiada. Alguna de la información a incluir es:

    a) La identidad del controlador de los datos y la de su representante ante la entidad responsable de la protección de los datos personales;

    b) El propósito o propósitos para los cuales se recolecta la información;

    c) Las consecuencias del procesamiento de la información para el sujeto de los datos (obvias y no obvias);

    d) Potenciales revelaciones de información; y,

    e) En caso de que la información haya sido proporcionada por otro diferente al sujeto de los datos, se debe informar tanto al sujeto de los datos personales así como al que transfirió la información.

Esta información debe ser entregada dentro de un plazo razonable.[65]

II.-SEGUNDO PRINCIPIO: LOS DATOS PERSONALES DEBEN SER OBTENIDOS PARA UNO O VARIOS PROPÓSITOS DEFINIDOS Y LEGALES, Y NO PUEDEN SER PROCESADOS DE UNA FORMA INCOMPATIBLE CON ESTOS PROPÓSITOS ORIGINALES.

En este principio se deben considerar los siguientes aspectos:

1. El controlador de los datos debe hacer explícitos al sujeto de los datos los propósitos del procesamiento de los datos personales.

   A. En el caso de autoridades, también deben hacer explícitas sus facultades para recabar dicha información.

   B. Los propósitos (y las facultades, en caso de autoridades públicas) deben hacerse explícitos antes que inicie el procesamiento de los datos.

   C. Si se modifican los propósitos del procesamiento de los datos, se debe recabar el consentimiento del sujeto.

      a) No es válida una notificación simple al sujeto, es necesario su consentimiento.

      b) Le debe quedar claro al sujeto de los datos las implicaciones de los nuevos propósitos de procesamiento de los datos.

      c) No puede proceder si no se tiene ese consentimiento.

[65] Algunos países establecen un plazo definido que corre desde la recolección, transferencia de los datos personales e información. Otros, lo dejan más abierto.

2. Los propósitos deben ser legales y claros para el sujeto de los datos.

3. el procesamiento siempre debe ser acorde a los propósitos.

4. los propósitos pueden ser generales, y los usos más específicos pero siempre en la misma línea.[66]

III.- TERCER PRINCIPIO: LOS DATOS PERSONALES DEBEN SER ADECUADOS Y NO EXCESIVOS CON RELACIÓN A LOS PROPÓSITOS DEFINIDOS POR LOS CUALES SON PROCESADOS.

Este principio busca que los controladores sean proporcionales y equitativos al recabar los datos personales. Para cumplir con este principio se requiere que los controladores de datos sólo requieran la cantidad mínima de información necesaria para cumplir con los objetivos originales del procesamiento de datos.

Si los controladores requieren información adicional para un subconjunto de sus sujetos (esto es, no para todos), el controlador podría requerirla para este grupo es especifico, pero sería incorrecto recabar un dato que sólo sería ocupado para un grupo.

Tampoco sería aceptable que los controladores recabaran información que consideraran que un futuro podría, de alguna forma aún indeterminada, serles útil. Esto es diferente a recabar información que tendría un propósito determinado pero que no tiene certeza sobre la ocurrencia de dicho evento.[67]

---

[66] Por ejemplo, un particular puede autorizar a un tenedor de los datos la inclusión de sus datos personales con fines de mercadotecnia. Así no tendrá que solicitar autorización cada vez que intente incluir al particular en una lista de clientes potenciales.

[67] Por ejemplo, un registro de información médica que los empleadores conservarían para el tratamiento de potenciales accidentes laborales.

IV.-CUARTO PRINCIPIO: LOS DATOS PERSONALES DEBEN SER CORRECTOS Y, CUANDO SEA NECESARIO, ACTUALIZADOS.

Sin embargo, los controladores no serán responsables por los datos personales incorrectos y entregados de esa forma por los sujetos de los datos, a menos que exista una obligación jurídica del controlador de los datos de verificar la información entregada por el sujeto. Sin embargo, si el controlador tiene una duda razonable sobre la exactitud de los datos, debe establecer un procedimiento de alerta en su propia base de datos. De la misma forma, si un sujeto detecta una información que a su parecer sea incorrecta, y mientras se define la veracidad o no de la información, el controlador estará obligado a anexar el dato en discusión los puntos de vista del sujeto del dato.

Para calificar sobre la necesidad de mantenerlos actualizados, los controladores deben verificar:

Si la obsolescencia del dato registrado causa algún daño al sujeto de los datos;

- Si causa algún daño al controlador de los datos;
- Si causa algún daño a un tercero relacionado con el dato, y
- Si la información obsoleta podría impactar, en alguna forma, la obtención de un beneficio o de una responsabilidad por cualquiera de los involucrados.

En caso de que alguna respuesta sea positiva, es evidente que será necesario actualizar los datos.

V.- QUINTO PRINCIPIO: LOS DATOS PERSONALES NO DEBEN MANTENERSE MÁS ALLÁ DE LO NECESARIO PARA CUMPLIR CON LOS PROPÓSITOS PARA LOS CUALES FUERON PROCESADOS.

Los controladores serán responsables de depurar los datos personales en su responsabilidad y destruir los datos que ya no utilicen. En este sentido, se puede establecer una caducidad determinada de los datos personales, y si después de "n" años, no ha habido un nuevo registro, el dato se pueda eliminar en la base activa de datos.

De la misma forma, se debe establecer que aquellos controladores que dejen de operar puedan deshacerse de sus bases de datos de una forma adecuada (si es destrucción, que esta sea total, si es transferencia, que sea bajo principios claros y ciertos, que no vulneren los derechos de los sujetos ni la seguridad de las bases de datos).

VI.-SEXTO PRINCIPIO. EL CONTROLADOR DE LOS DATOS PERSONALES DEBE ESTABLECER Y MANTENER LAS MEDIDAS TÉCNICAS Y ORGANIZACIONALES ADECUADAS PARA EVITAR EL PROCESAMIENTO ILEGAL O NO AUTORIZADO DE LOS DATOS PERSONALES, ASÍ COMO PARA EVITAR LA PÉRDIDA, DESTRUCCIÓN ODAÑO ACCIDENTAL A LOS MISMOS.

El primer concepto a definir de este principio es que se entiende por "adecuadas". Para auxiliar en este punto las autoridades regulatorias presentan algunas sugerencias:

A. Se debe considerar el estado de la tecnología y el costo de implementar dicha tecnología. En todo momento se debe asegurar que nivel de seguridad es apropiado para:

a) El daño que podría surgir de una violación a la seguridad; y,

b) La naturaleza de los datos a proteger.

B. El controlador de los datos debe asegurarse (y será responsable) de la confiabilidad de su personal que tendrá acceso a los datos bajo su resguardo.

Además, se debe buscar que los sistemas sean adecuados tanto en el diseño, su infraestructura y en su operación.

Es relevante que la Ley contemple la posibilidad de establecer regulación secundaria que permita determinar si el grado de seguridad es el adecuado. Algunas naciones han establecido estándares técnicos para medir la confiabilidad y seguridad del sistema.[68]

VII.-SÉPTIMO PRINCIPIO: LOS DATOS PERSONALES NO SE DEBEN TRANSFERIR A PAÍSES QUE NO PROTEJAN, AL MENOS CON LA MISMA SEGURIDAD, LOS DATOS PERSONALES.

La OCDE ha establecido las *Directrices de la OCDE para la Protección de la Privacidad de los Datos personales y sus Flujos Transfronterizos.* Las directrices de la OCDE constituyen estándares mínimos para los países miembros los cuales se pueden complementar con medidas adicionales para la protección de la privacidad y las libertades individuales. Los objetivos que se establecen en las directrices se pueden perseguir de diferentes maneras dependiendo de los instrumentos legales y las estrategias con los que cuenten los países para su implementación. Por su importancia, se transcriben las directrices relacionados al flujo transfronterizo de los datos personales.

[68] En México debería contemplarse en el reglamento respectivo la posibilidad de establecer normas oficiales mexicanas al respecto.

Principios básicos de aplicación internacional.

1. Los países miembros deben tomar en consideración las implicaciones que tienen el procesamiento interno y la re-exportación de datos personales sobre otros países miembros.

2. Los países miembros deben tomar las medidas razonables y adecuadas para asegurar que el flujo transfronterizo de datos personales, incluyendo el tránsito a través de un país miembro, sea ininterrumpido y seguro.

3. Un país miembro debe evitar restringir los flujos transfronterizos de datos personales entre sí mismo y otros países miembros, excepto cuando estos últimos no han observado adecuadamente las directrices o cuando la re-exportación de los datos puede infringir su legislación doméstica sobre privacidad y para las cuales otros países miembros no tienen protección equivalente.

4. Los países miembros deben evitar desarrollar leyes, políticas o prácticas bajo el nombre de protección de privacidad y libertades individuales que puedan crear obstáculos al flujo transfronterizo de datos personales que excedan los requerimientos de protección. Este principio intenta balancear los intereses de protección de privacidad contra los de flujos libres transfronterizos de datos personales. Se deben eliminar las barreras artificiales al flujo de los datos desde el punto de vista de protección de la privacidad y libertades individuales.

1.2. DIRECTIVA 95/46/CE RELATIVA A LA PROTECCION DE LAS PERSONAS FISICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ÉSTOS.[69]

Con el fin de lograr una unión cada vez mas estrecha entre los pueblos europeos, pero sobre todo para garantizar a todas y cada una de las personas físicas la protección de las libertades y de los derechos fundamentales y en particular del derecho a la intimidad, en lo referente a la protección de los datos personales, entró en vigor 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 éstos".[70]

La directiva está conformada por exposición de motivos, 34 artículos divididos en 7 capítulos y disposiciones finales.

El objeto de esta directiva es que en los Estados miembros se garantice la protección de las libertades y de los derechos fundamentales de las personas físicas y en particular el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. El tratamiento de los datos se encuentra amparado bajo esta directiva únicamente cuando se realiza de forma automatizada o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos e un archivo estructurado, según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata. [71]

La directiva define los datos personales como "toda información sobre una persona física identificada o identificable, llamada "el interesado". Se entiende por

---

[69] García Corona, Irene Gabriela; "*La protección de datos personales en la Comunidad Europea, desde la perspectiva alemana y española*". En Villanueva, Ernesto, Luna Pla Issa (eds), Derecho de Acceso a la Información Pública, Valoraciones Iniciales, Instituto de Investigaciones Jurídicas, 1ª edición , UNAM 2004, p.p. 94-100.
[70] DOCE L 281 23/11/1995 p. 31-50.
[71] Véase considerando numero 15 de la Directiva 95/46/CE.

identificable 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.[72]

En cuanto a su ámbito de aplicación será según su artículo 3, respecto del tratamiento total o parcialmente automatizado de datos personales, así como del tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Se entiende por tratamiento de datos personales como "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".[73] Fichero de datos personales comprende "todo conjunto estructurado de datos personales accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".[74]

Asimismo, esta directiva plantea las Condiciones Generales para la Licitud del Tratamiento de Datos Personales, Recursos judiciales, responsabilidad y sanciones, la transferencia de datos a países terceros, Códigos de conducta que deben ser elaborados por la Comisión Europea y los estados miembros, Autoridad de Control y grupo de protección de las personas y las medidas de Ejecución Comunitarias.

---

[72] Véase articulo 2 Definición de Datos Personales de la Directiva 95/46/CE.
[73] Confróntese artículo 2 Directiva 95/46/CE.
[74] Ibidem.

2. LEYES DE PROTECCIÓN DE DATOS. EVOLUCIÓN DE LA PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO AUTOMATIZADO DE LA INFORMACIÓN QUE LE AFECTA.

No es el caso en este apartado, el estudio detallado de todas las leyes de protección de datos existentes, sino y a través del estudio de algunas de ellas, caracterizar cada una de las etapas de evolución legislativa en este campo, destacando aquellas innovaciones que supusieron avances sustanciales en la protección de los datos personales.

Desde principios de la década de los setenta aparecen, tanto en Europa como en los Estados Unidos de América, una serie de disposiciones que tienen por objeto la protección de las personas frente al tratamiento automatizado de sus datos. Se inicia en ese momento según PÉREZ LUÑO, "el proceso de positivación de los derechos integrantes de la tercera generación, en particular (...) el derecho a la autodeterminación informativa"[75].

En las distintas leyes de protección de datos aparecidas desde esas fechas hasta hoy, se pueden apreciar diferencias respecto al grado de protección que ofrecen, su ámbito de aplicación, los derechos que otorgan a los individuos y en el modo de realizar sus fines. Estas diferencias, así como la fecha en que fueron aprobadas nos permite agruparlas en tres etapas o, en tres generaciones sucesivas de leyes de protección de datos personales.

[75] PÉREZ LUÑO, A.E., "Los derechos humanos en la sociedad tecnológica". En LOSANO, M.G. Y OTROS: "Libertad informática y leyes de protección de datos personales", Cuadernos y Debates número 21, Centro de Estudios Constitucionales, Madrid 1989, p. 145.

2.1. PRIMERA GENERACION: LA LEY DE PROTECCION DE DATOS DE HESSE DE 1970 Y LA LEY SUECA DE 11 DE MAYO DE 1973[76].

A. LEY DE HESSE DE 7 DE OCTUBRE DE 1970.

Es una ley breve compuesta de 13 artículos y dividida en 2 secciones. Su finalidad es "proteger el derecho de la personalidad restringiendo la utilización de datos personales que pudiera afectar a los ciudadanos por parte de la administración".

En esta ley hace falta un contenido más completo del derecho de autodeterminación informativa, en especial al no garantizar expresamente el derecho de acceso de los ciudadanos a los propios datos. No obstante, esta es una característica propia de las primeras leyes de protección de datos, pues, hasta la segunda generación, no encontraremos garantizado el derecho de acceso.

Esta carencia se subsana, con la figura establecida en la sección segunda de la ley. En ella se fija el sistema de control de la información y de su tratamiento a través de la figura del Comisario para la protección de datos. La protección de los ciudadanos se instrumentaliza a través de esta figura cuya misión principal es la de velar por la aplicación de la ley *"mediante la inspección y control de los servicios públicos informatizados"*[77]. De esta forma, la Ley de Hesse de 1970 acoge el modelo *ombudsman*[78] para garantizar la libertad de los ciudadanos.

---

[76] Los textos legales que se citan proceden del volumen: *Informática. Leyes de Protección de Datos, Documentación Informática n° 2, Serie verde/Legislación,* Servicio Central de Publicaciones, Secretaría General Técnica. Presidencia del Gobierno, Madrid, 1977. Confrontados, en su caso, con *Secretaría General del Congreso de los Diputados:* Protección de Datos Personales (Documentación preparada para la tramitación del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal.), B.O.C.G. Congreso, Serie A, n° 59, de 24 de julio de 1991.

[77] PÉREZ LUÑO, A.E., *"Los derechos humanos en la sociedad tecnológica"*, op. Cit., p. 146.

[78] Para FAIRÉN GUILLEN, el medio más adecuado para controlar y supervisar a la Administración es la queja del ciudadano contra la misma, *"ante el ombudsman cuando estime que se ha vulnerado un interés legítimo o un derecho subjetivo de aquel"*. De esta manera el ombudsman realiza su supervisión examinando las quejas recibidas y realizando las inspecciones e investigaciones que estime necesarias (En FAIREN GUILLEN, V., El defensor del pueblo-

Esta ley de 1970 es fruto de la tecnología informática de su época. Tiempo en el que, si bien ya se era consciente de los peligros que, para la libertad de las personas podían derivarse de su uso incorrecto, no estaba generalizado el uso ni la propiedad de los ordenadores, cuyo número aún era escaso y se trataba de equipos fácilmente localizables por su gran volumen.

Son varias las carencias que la primera ley de protección de datos presenta, explicadas sin duda por la situación descrita, aunque tiene el mérito de ser la primera en dar respuesta a una nueva situación de agresión a los derechos fundamentales.

En primer lugar, se echa en falta la protección de los datos personales automatizados por entidades privadas, al limitar el ámbito de aplicación de la ley a la Administración pública.

En segundo lugar, debe destacarse que la protección a los ciudadanos se instrumenta principalmente a través de la figura del Comisario de protección de datos, del principio de seguridad de éstos, que garantiza su integridad y la imposibilidad de acceso al personal no autorizado y del deber de secreto de quienes tuviesen conocimiento de los datos personales o del resultado de su tratamiento.

Por el contrario, debe destacarse, que el conjunto de garantías que la ley establece no se completa con un contenido más amplio y perfeccionado del derecho de las personas a controlar los datos que les conciernen.

Ombudsman- tomo I, Parte General, Centro de Estudios Constitucionales, Madrid, 1982, p. 75.

B. DATA LAG DE 11 DE MAYO 1973 DE SUECIA.

El mayor logro de esta ley es responder al principio de publicidad de los bancos de datos personales informatizados y el haber creado un registro especial en el que deberían inscribirse los bancos de datos[79].

En esta época, los datos personales se almacenaban en grandes ordenadores centrales, por lo que resultaba extremadamente difícil detectar la presencia de una información. Y, aún cuando se conocía que una información determinada se encontraba almacenada en un fichero informatizado, público o privado, resultaba prácticamente imposible acceder a ella. Por estas razones se crea *"un sistema de registro masivo (...) diseñado precisamente para dar nuevos derechos a los particulares afectados, y para imponer nuevas responsabilidades a las organizaciones del sector, fueran estas públicas o privadas"*[80].

La ley sueca ofrece, en primer lugar, la definición de aquellos conceptos fundamentales en torno a los cuales van a girar las disposiciones de la misma.

Esta estructura normativa, consistente en aportar las definiciones básicas en los primeros preceptos de la ley, ha sido imitada posteriormente. En especial cabe destacar el Convenio para la Protección de las Personas (108) del Consejo de Europa y la propia Ley Española de Protección de Datos.

Uno de los aspectos más relevantes de esta ley, es que ésta amplía su ámbito de aplicación a los ficheros privados, con lo que primera vez los legisladores toman conciencia de que los riesgos de lesión de derechos fundamentales de las

[79] Sin embargo, la creación del Registro no aparece en la Ley, sino en un Reglamento de datos *(Datakungörelse)*, relativo principalmente al procedimiento para solicitar la autorización administrativa de creación y explotación de archivos de datos personales.

[80] DRESNER,S.H., *"Panorama de la legislación europea sobre protección de datos personales"*, Traducción de Santiago Ripio Carulla, en *Informática y Derecho, número 6-7*, UNED, Centro Regional de Extremadura, Mérida, 1994, p. 390.

personas derivados del acopio, tratamiento y uso de las informaciones personales automatizadas, no sólo pueden provenir del sector de las Administraciones Públicas, sino también y, en ocasiones en mayor medida, del ámbito de las empresas privadas.

Otro avance importante es que se introducen dificultades a la creación de ficheros de datos especialmente sensibles; aunque es criticable, no obstante el intento de súper proteger estos datos, que la ley no establezca cuales serían esas razones especiales, en orden a una mayor seguridad jurídica. De esta forma, se deja en manos de la discrecionalidad de la inspección de datos el decidir cuando existen y cuando no, las antedichas razones.

Otros logros de esta ley es la de establecer la figura del responsable del archivo, al que corresponde, como contrapartida a la posibilidad de crear un archivo de datos personales, velar por la integridad del titular de estos, involucrándole personalmente en su protección a través de las obligaciones que la ley le impone, que en caso de incumplimiento supondrían sanción, incluso penal. Es decir, el responsable del fichero está obligado a garantizar activamente, a través de la adopción de las medidas oportunas y del cumplimiento de los deberes legales, la integridad del afectado.
Finalmente se establecen en la ley sanciones penales y responsabilidades indemnizatorias por los daños causados según las infracciones que se cometan contra lo allí establecido.

C. LA LEY DE INFORMACIÓN CREDITICIA DE 1973.

En el mismo año de promulgación de la Ley de protección de Datos, el Reino de Suecia aprobó una ley especial para la protección y control de la información de carácter económico: la Ley de Información Crediticia de 1973.

Dicha ley se aplicaría a la actividad de información sobre solvencia ejercida de forma profesional[81]. Se pretende, al igual que con la Ley de Protección de Datos garantizar que no se produzcan intrusiones indebidas en la integridad de las personas.

La importancia de esta ley reside en que se amplia la protección que la ley de datos ofrece a los ficheros manuales, aunque solo a aquellos cuyo objeto sea recabar, almacenar y proporcionar información sobre el estado financiero de una persona.

Es importante señalar que la ley prohíbe la recolección almacenamiento y comunicación de las informaciones relativas a la raza o color de una persona, ideas políticas, creencias religiosas, antecedentes penales, enfermedades o trastorno psíquicos o físicos y nacionalidad. También de aquellas noticias relativas a impagos que no hubieran sido declarados probados en juicio o los que hubieran dado lugar a suspensión de pagos o solicitud de quiebra en convenio con los acreedores.

Se garantiza, por lo tanto, el derecho al olvido de las informaciones sobre solvencia económica de una persona. Se garantiza el derecho de acceso del interesado a los datos de carácter económico que sobre él hubiese almacenados. Se establece que se faciliten esos datos por escrito, aunque se permite el cobro de un *justo precio* por parte de quien ejerce la actividad de información sobre solvencia crediticia.

Se establecen medidas semejantes a las de la Ley de Protección de Datos en orden a la rectificación y cancelación de datos inexactos o erróneos, así como semejantes poderes y facultades a la Inspección de Datos para garantizar la observancia de la ley.

[81] Es indiferente a la Ley que la información sobre solvencia se trate informática o manualmente.

Igualmente se establecen sanciones penales e indemnizaciones de daños y perjuicios para los transgresores de dichas disposiciones.

La Ley de Información Crediticia supone un complemento a la Data Lag, aunque sólo en lo que se refiere a los datos de tipo económico o sobre solvencia patrimonial.

Por lo demás, existe prácticamente una completa identidad entre las funciones de la inspección de datos, derechos de los afectos y deberes de quienes se dedique a esta actividad, recogidas en la Ley de información sobre solvencia crediticia y los desarrollados en la Ley sueca de protección de Datos.

2.2. SEGUNDA GENERACIÓN DE LEYES DE PROTECCIÓN DE DATOS PERSONALES.

A. PRIVACY ACT DEL 31 DE DICIEMBRE DE 1974[82].

La segunda etapa en la evolución de las leyes de protección de datos se inicia, según PEREZ LUÑO[83], el 31 de diciembre de 1974, fecha de promulgación de la Privacy Act norteamericana. Esta fase se caracteriza por asegurar a las personas el acceso a las informaciones que les conciernen.

La Privacy Act del 74 persigue la protección de la vida privada de las personas frente a los cada vez más numerosos y sofisticados sistemas informáticos de acopio y almacenamiento de datos por parte del Gobierno Federal. Limita, por tanto, su ámbito a los ficheros de titularidad pública.

---

[82] El nombre completo con el que fue publicado el 31 de diciembre de 1974 fue el de *"Ley por la que se modifica el Título 5 del Código de los Estados Unidos, insertando una sección 552ª para salvaguardar la privacidad individual frente al uso indebido de los registros federales, disponer que los individuos tengan acceso a los registros que les conciernen, llevados por órganos federales; crear una comisión de estudio de la Protección de la Privacidad y para otros fines"*.

[83] PÉREZ LUÑO, A.E., "Los derechos humanos en la sociedad tecnológica", op. Cit., p. 147.

Sus aspectos más relevantes son:

1. Esta ley limita el uso de los datos relativos a las personas, estableciendo restricciones a su recogida y conservación. Solamente se conservará la información que sea pertinente y necesaria para realizar el fin, que en virtud de una disposición legal, fuera competencia del órgano del titular del fichero[84].

2. El gobierno deberá comunicar al interesado[85], cuando le solicite información que le afecte, el uso que de la misma va a hacer. La información deberá recabarse, a ser posible, directamente de éste y, en todo caso, cuando dicha información pudiese perjudicarle en sus derechos o privilegios en aplicación de un programa federal.

3. Se requiere a las Agencias públicas para que creen un registro en el que se haga constar que información personal se ha facilitado a terceras personas y la identidad de éstas últimas.

4. Se garantiza a los interesados el derecho de acceso, el derecho a obtener una copia de los propios datos y a exigir su rectificación y su cancelación, cuando hayan sido indebidamente procesados. Sólo se podrán limitar estos derechos cuando una necesidad de orden público lo justifique, en virtud de lo establecido en una disposición legal.

---

[84] Para GUIDO ALPA, por sí, la adquisición de un dato personal no supone una gran violación de la privacy, puede no sólo no ser dañosa, sino que podría suponer un beneficio para el titular del dato personal cuando se trate de acceder a un servicio público de tipo asistencial, para cuya obtención sea necesario comunicar ciertos aspectos de la vida privada. El problema más grave, a su juicio, es el que deriva del uso y de la difusión de la información.
Para él, este problema en la Privacy Act queda resuelto con la estricta observación de las Agencias, en la ejecución de su actividad, del principio de finalidad según el cual los datos habrán de usarse de para finalidades compatibles con la finalidad para la que hubiere sido recogido. (ALPA, G.: "Privacy e statuto dell'informazione (Il privacy act, 1974 e la loi relative á l'informatiqeu, aux fichiers et aux libertés n. 78-17 del 1978) en Il Diritto alla riservatezza in Italia ed in Francia, Edizioni Cedam, Padova, 1988, p. 296).

[85] Que podrá ser todo ciudadano de los Estados Unidos o extranjero legalmente autorizado para residir permanentemente.

5. Ante la negativa de la Administración a facilitar o rectificar los datos personales de un consumidor cuando éstos estuviesen errados, el afectado podrá solicitar de los Tribunales la revisión de la decisión administrativa.

6. La ley americana establece la responsabilidad civil de los entes y órganos federales por daños y perjuicios producidos por una actuación dolosa o intencionada de atentar contra los derechos individuales reconocidos en esta ley.

7. Finalmente, se fijan por la Ley sanciones penales para los responsables de los ficheros automatizados con datos personales que revelasen dolosamente, en contra de una prohibición reglamentaria, el contenido de los mismos; así como para quien tuviera conocimiento de ellos por razón de su cargo. También, se sanciona penalmente al responsable del fichero por el incumplimiento de las normas referentes a la publicidad del registro y a quien obtuviese, con engaños, acceso a un registro con datos personales.

B. INFORMÁTIQUE, AUX FICHIERS ET AUX LIBERTÉS, DE 6 DE ENERO DE 1978.

Con anterioridad a la Ley de Informática, Ficheros y Libertades de 1978, el legislador francés había modificado el artículo 9 del Código Civil, por la Ley de 17 de junio de 1970, para consagrar el derecho a la vida privada de la persona, amenazado notablemente por la informática. Sin embargo, esta medida resultó insuficiente ante la creciente preocupación sobrevenida por ciertos proyectos del gobierno francés. Fueron especialmente contestados, en este sentido, e proyecto SAFARI de 1971, que pretendía atribuir una única identificación para cada ciudadano de manera que se pudiesen interconectar los distintos ficheros existentes y el proyecto GAMIN, de Gestión Automatizada de Medicina Infantil de 1975. Esta preocupación social animó a los poderes públicos a aprobar una ley general sobre la materia en 1978.

La finalidad de la ley francesa de protección de datos es la protección de la identidad humana, de los derechos humanos, de la vida privada y de las libertades individuales o públicas de los ciudadanos frente a la informática.

Los derechos que garantiza a todas las personas son los siguientes[86]:

1. El derecho a conocer y discutir las informaciones y razonamientos utilizados en los tratamientos automáticos cuyos resultados le sean adversos[87].

2. A ser informados, en el momento de la recogida de sus datos personales[88], de carácter voluntario u obligatorio de sus respuestas y de las consecuencias de su negativa a proporcionar dichos datos.

3. A ser informados de la identidad de los destinatarios de los datos personales recogidos y tratados y de que tiene derecho a acceder y a rectificar los mismos.

Las personas tienen derecho a negarse al tratamiento automatizado de sus datos cuando existan razones que justifiquen esta negativa, excepto cuando los destinatarios de los datos sean autorizados por la ley, por un acta reglamentaria y por la Comisión Nacional de Informática y Libertades.
Derecho de acceso, rectificación y de cancelación de las informaciones nominativas equivocadas.

---

[86] Para GILLES LEBRETON, la ley francesa reconoce a cada persona tres derechos fundamentales: *"le droit d'acceder aux informatioms nominatives la concernant, le droit d'en obtenir la rectification en cas d'erreur, et le droit d'en obtenir l'enffacement en cas d'atteinte illegale au respect de la vie privee"*. (En LEBRETON, G., Libertés publiques et droits de l'homme, Armand Colin, Paris, 1995, p. 265.)

[87] Artículo 3 de la Ley de informática ficheros y libertades de 1978.

[88] La Ley Francesa los denomina informaciones nominativas que define en su artículo 4° como las *"informaciones que permitan bajo cualquier forma, directa o indirectamente, la identificación de las personas físicas, tanto si el tratamiento es efectuado por personas físicas o por personas morales"*. Esta definición es para PEREZ LUÑO uno de los aspectos centrales de la norma francesa. (En PEREZ LUÑO, A.E., *"Los Derechos Humanos en la sociedad tecnológica"*, ob. cit., p. 148).

La ley de 6 de enero de 1978, no consagra expresamente el derecho a la confidencialidad de la información tratada automatizadamente. Sin embargo, si está contenido el derecho al respecto de la vida privada y al mismo tiempo, por primera vez, establece un derecho a la identidad humana.

Como complemento a estos derechos de los afectados, la ley prohíbe la "recogida de datos por cualquier medio fraudulento, ilegal, ilícito". Asimismo, se prohíbe que las decisiones administrativas o privadas se basen como único fundamento, en un "tratamiento automático de información que pretenda dar una definición del perfil o de la personalidad del interesado"

Esta prohibición se extiende a los Tribunales, que en ningún caso podrán fundar su fallo en una información tratada por medios automáticos para obtener el perfil de una persona.

La ley de 1978, da un paso más en la protección de las personas frente al procesamiento y tratamiento automatizado de sus datos, al impedir que la Administración Pública, los Tribunales y las entidades privadas tomen una decisión que podría perjudicar al interesado, basándose únicamente en el perfil que resultase al someter una serie de datos (seguramente incompletos y posiblemente erróneos) a un programa informático determinado. Es decir, además de garantizar unos derechos a los afectados para controlar la calidad de sus datos personales, se impide que se tomen decisiones basándose en el resultado de combinar informáticamente los mismos.

La ley de 1978 supone un avance, también desde otro punto de vista, al ampliar el ámbito de protección a aquellos datos personales que se encuentran en manos de entidades privadas.

Otro aspecto que debe destacarse es el de las diferentes categorías de informaciones nominativas contempladas por la Ley de 1978, en orden a establecer distintos grados de protección.

C. LA LEY FEDERAL DE 18 DE OCTUBRE DE 1978 DE AUSTRIA.

La Ley de Austria establece, en primer lugar, el derecho de toda persona a exigir y a hacer valer en juicio que los datos automatizados que le conciernen sean mantenidos en secreto, en la medida que esto fuese necesario para garantizar el respeto a su vida privada y familiar[89].

Este derecho así enunciado solo cederá ante intereses legítimos de otros o cuando se establezcan limitaciones por una ley en virtud de lo dispuesto en el artículo 8°, párrafo segundo, de la Convención Europea para la protección de los Derechos Humanos y las Libertades Fundamentales. Es decir, el derecho a la protección de la intimidad y a vida privada de las personas podría ceder cuando existiese una habilitación legal en ese sentido[90] y "constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás"[91].

---

[89] Este derecho esta contenido en el artículo primero de la Ley y tiene rango de norma constitucional.

[90] Según la Jurisprudencia del Tribunal europeo de Derechos Humanos, la habilitación legal que limite el derecho garantizado en el artículo 8.1 del Convenio ha de cumplir el doble requisito de la existencia de una base legal en el Derecho interno y de la calidad de la ley. Bajo la rúbrica << calidad de la ley>>, el Tribunal de Europeo de Derechos Humanos ha englobado varias exigencias que debe cumplir la ley: su accesibilidad, en el sentido de que la ley tiene que ser cognoscible y accesible para los afectados, de forma que el ciudadano disponga de suficiente información y su previsibilidad, que significa que la ley debe formularse con la suficiente precisión de manera que permita al ciudadano adecuar su conducta. (En RUIZ MIGUEL, C. *El Derecho a la Protección de la Vida Privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos,* Cuadernos Civitas, Civitas, Madrid, 1994, p. 89-97).

[91] Artículo 8°, párrafo segundo de la Convención Europea para la protección de los Derechos Humanos y las Libertades Fundamentales.

El ámbito de aplicación de la Ley de Austria lo forman, tanto los ficheros de titularidad pública, como aquellos que pertenecen al sector privado. Con ello se amplía el nivel de protección de las personas, pues, si en un primer momento se pensó que los mayores peligros para la identidad de las personas provenían de las Administraciones Públicas, con el avance de la tecnología informática y su recepción en las empresas privadas, éstas se convirtieron en potenciales y, en ocasiones, reales violadores de la vida privada de las personas al mismo nivel o incluso, a veces, en mayor grado que las Administraciones Públicas[92].

La Ley de 1978 acude al sistema de establecer una serie de definiciones legales clarificadoras de cuál es el bien jurídico protegido, sobre los usos y operaciones automáticas que se pueden llevar a cabo sobre los datos y sobre la persona que realiza esas operaciones.

Cabe destacar que esta Ley protege no sólo los datos relativos a las personas físicas, sino también a las personas jurídicas.

Si bien el objeto de las leyes de datos es la protección de la persona física frente a las posibles agresiones de algunos usos de la informática que impiden el normal ejercicio de las libertades y los derechos fundamentales, ésta se garantiza mejor protegiendo, también, los datos relativos a las personas jurídicas, que en último término son datos, aún indirectamente, referentes a las personas físicas que las integran.

Esta es la filosofía que subyace en la Ley de Protección de Datos Austriaca, ya que, aunque en un primer momento enuncia un derecho fundamental a la protección de datos de toda persona natural, extiende su protección a los datos relativos a las sociedades mercantiles u otras personas jurídicas.

---

[92] Como podrá apreciarse a lo largo de la exposición, la inclusión de los ficheros de titularidad privada en el ámbito de aplicación de las leyes de protección de datos, es una característica general de las leyes de segunda generación.

Por otra parte, no se establece un único régimen jurídico para la protección de los datos, sino dos, uno para el sector público y otro para el privado.

La ley austriaca es muy restrictiva en lo que se refiere a la obtención y elaboración de datos personales a través de medios automáticos. Solamente podrán llevarse a cabo estas operaciones para una posterior cesión de los mismos cuando exista una disposición legal que expresamente lo autorice.

Dentro del específico contenido del derecho a la autodeterminación informativa, se garantiza al titular de los datos informatizados los siguientes derechos:

1) Derecho a ser informado acerca de la identidad del titular del fichero, del contenido de los datos, de la fuente de donde proceden y de la finalidad del tratamiento automatizado. Esta información deberá serle trasmitida por escrito y en forma tangible, en el plazo de cuatro semanas.

2) Derecho a exigir la rectificación de los datos inexactos o erróneos y a que los datos obtenidos o elaborados indebidamente sean cancelados.

Esta ley prevé no solamente el tratamiento de los datos sobre los ficheros nacionales, amplía su campo al tráfico internacional de datos.

Asimismo, la ley contempla sanciones penales y administrativas para las infracciones contra lo dispuesto en esta ley.

D. LEY DE 9 DE JUNIO DE 1978 DE NORUEGA.

La ley establece que su ámbito de aplicación se extenderá a los registros de las personas y de sus datos personales cuya titularidad sea estatal o municipal o aquellos que se encuentren en el seno de las actividades económicas, asociaciones o fundaciones y, tanto a los registros manuales como a los

electrónicos, requiriéndose para la creación de estos últimos la autorización del Rey.

Crea la inspección de datos, claramente influida por la Ley sueca de 1973. la inspección estará dirigida por un Consejo de Administración compuesto por siete personas nombradas por el Rey.

Para poder cumplir con sus funciones de control, la inspección cuenta con el poder de solicitar la información que fuese necesaria, así como acceder a los lugares en donde se encuentren los bancos de datos y los medios auxiliares y practicar las pruebas y controles oportunos.

Como es común en las leyes de segunda generación, la ley noruega incluye disposiciones especiales para determinado tipo de datos, los denominados sensibles[93]. Se establece que, excepto cuando sea estrictamente necesario no podrán registrarse los datos relativos a la raza, ideología política o religiosa, antecedentes penales, salud o consumo de drogas, vida sexual y a la situación familiar, aunque en este último supuesto, con excepción de los datos relativos al estado civil, al parentesco y a las relaciones patrimoniales entre los cónyuges u obligación de alimentos.

Se establece, por otra parte, el principio de finalidad de los datos según el cual los datos deberán responder a la actividad del órgano o empresa titular del registro.

Por otra parte se garantizan los derechos de información y acceso para el titular de los datos. No obstante, estos derechos no serán aplicables a los ficheros con fines estadísticos o de investigación y planificación general. Además, el derecho que la ley denomina de consulta no será aplicable a los datos que pudiera considerarse imprudente que el interesado conociera por hacer referencia a su

[93] Aunque, con anterioridad, la Ley sueca de 1973 sobre solvencia económica, se había referido a esta clase de datos personales.

salud o a sus relaciones con personas allegadas. Con esta última limitación al derecho de acceso e información se está prohibiendo su ejercicio en aras de la protección del interesado <frente a sí mismo>, lo que, como mínimo, resulta contradictorio. Parece que e legislador noruego considera que los derechos fundamentales de la persona pueden limitarse cuando su ejercicio pudiera, incluso potencialmente, perjudicar a su titular[94] y, asumiendo fundamentaciones paternalistas, considera que el interesado "no conoce cuáles son sus propios intereses y que (el legislador) conoce mejor que es lo mejor para él[95].

Por otra parte, tal limitación, no sólo afecta a la dignidad de las personas[96] a las que se protege de esas informaciones desagradables, sino también a lo que DWORKIN denomina derecho a la autonomía, "es decir, un derecho a tomar, por sí mismos, decisiones importantes definitorias de sus propias vidas"[97].

Dentro de las garantías que ofrece la Ley para el afectado se incluye también la obligación para las empresas de cancelar los datos referentes a una persona a solicitud de ésta. Asimismo deberá informársele sobre cuál ha sido la fuente utilizada por la empresa para su recabación.

Dicha Ley regula también la transferencia internacional de datos. Como en el caso de Austria, se va asumiendo paulatinamente que la protección de los datos personales no puede terminar en las fronteras de los Estados, estableciendo normas de control con su exportación a otros países.

---

[94] El artículo 7 establece que *"el derecho de consulta no será aplicable a los datos que pudiere estimarse imprudente que el interesado los conozca, por hacer referencia a su salud o a sus relaciones con personas allegadas"*

[95] DWORKIN, R., *El dominio de la vida,* Traducción de Ricardo Caracciolo y Victor Ferreres, Ariel, Barcelona, 1994, p. 251.

[96] Entendida como dominio sobre la propia vida, es decir, como el *"valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión de respeto por parte de los demás".* (Sentencia del Tribunal Constitucional 53/1985).

[97] DWORKIN, R., *El dominio de la vida,* ob.cit., p. 290.

Por último, la ley prevé sanciones penales e indemnizaciones por daños y perjuicios.

E. LA CONSTITUCIÓN PORTUGUESA DE 1976 Y LA ESPAÑOLA DE 1978.

Dentro de la segunda generación de leyes de protección de datos se inscriben las dos primeras constituciones que recogen, entre su articulado, la protección de las personas frente al procesamiento informático de sus datos.

Para PEREZ LUÑO supone, las Normas fundamentales de Portugal de 1976 y de España de 1978, "las primeras consagraciones"[98] del derecho fundamental a la autodeterminación informativa o, como dice FROSINI, del "nuevo derecho a la libertad"[99].

a) Artículo 35 de la Constitución de Portugal de 1976.

Dicho artículo sienta los principios básicos que deberán ser incorporados y desarrollados por una futura ley de protección de datos personales.

- Reconoce a los ciudadanos el derecho a conocer las informaciones que les conciernen almacenadas en archivos, su finalidad y la posibilidad de rectificarlas o actualizarlas, contiene el principio básico del derecho al control sobre los datos personales.

- Contiene dos importantes principios: el derecho a la confidencialidad de los datos y el principio de prohibición de la interconexión o del cruzamiento de los datos personales, excepto los casos previstos en la ley.

---

[98] PEREZ LUÑO, A.E., *"Los derechos humanos en la sociedad tecnológica"*, Ob. Cit., p. 149.
[99] FROSINI, V., *Informática y Derecho*, Ob. Cit., p. 111.

- Prohíbe el tratamiento informático de los datos referentes a convicciones políticas o religiosas o a la vida privada, salvo que se trate de datos no identificables con fines estadísticos.

- Reenvía a la Ley ordinaria la adopción de la definición de datos personales y de base de datos.

- Prohíbe que a cada ciudadano se le asigne un único número nacional de identidad dificultándose así la interrelación de los datos a él referidos en diferentes ficheros automatizados y, de ésta manera se complica la obtención del perfil de un individuo de forma automática.

Destaca MARTÍN PALLÍN que el control sobre los individuos alcanza su punto más elevado cuando se agiliza al máximo el sistema de difusión de la información y se "acude a procedimientos en los que la identificación personal de los ciudadanos se hace fundamentalmente a través de un número identificador que sigue al individuo donde quiera que va como la sombra sigue al cuerpo"[100]. En estas circunstancias el control se vuelve asfixiante para el ciudadano, difuminándose su personalidad y convirtiéndose la uniformidad identificadora "en un lazo inmovilizador que maniate cualquier capacidad de autodeterminación"[101].

Por último, se establece que la Ley deberá definir el régimen aplicable a los flujos fronterizos de datos, estableciendo formas adecuadas de protección de datos personales y de otros cuya salvaguarda se justifique por razones de interés nacional.

---

[100] MARTÍN PALLÍN, J.A., *"Constitucionalidad del número de identificación único"*, en Jornadas sobre el Derecho Español de la Protección de Datos Personales, Agencia de Protección de Datos, Madrid, 1996, p. 66.
[101] Ibídem.

El artículo 35 de la Constitución Portuguesa, aunque con la brevedad propia de una norma constitucional toca todos los temas claves en la protección de los datos personales. En primer término esboza un completo derecho a controlar los propios datos garantizando los derechos de acceso, rectificación y actualización, así como el derecho de información acerca del fin de los ficheros, prohibiéndose la interrelación de los datos, el acceso de terceros y la asignación de un único número identificador.

En segundo lugar y al igual que la mayoría de las leyes de segunda generación siente una preocupación especial por los datos sensibles, restringiendo su captación y tratamiento a los datos anónimos para fines estadísticos.

Y por fin deja para un posterior desarrollo legislativo otras cuestiones en las que también predominan las características de las leyes de ésta generación, como son la inclusión de la definición de aquellos conceptos básicos para delimitar el alcance la protección de la ley y su ámbito de aplicación y la regulación al tráfico internacional de datos, lo que comienza a ser nota común en otras leyes de esta misma etapa.

b) La Constitución Española de 1978.

Establece en su artículo 18.4 que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

En el artículo 105 b) se garantiza "el acceso de los ciudadanos a los archivos y registro administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de la persona".

En torno a estos dos preceptos constitucionales y a la Ley 1/82, de 5 de mayo, sobre Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a

la Propia Imagen[102], ha girado la protección de los datos personales en este país hasta la Ley Orgánica 5/92, de 29 de octubre.

El artículo 18.4 recoge el mandato constitucional de regular mediante ley orgánica el uso de la informática para que éste no perturbe el derecho al honor y a la intimidad y el normal ejercicio de los derechos de las personas.

Según el Tribunal Constitucional Español:

"Dada la conexión necesaria que ha de existir entre el derecho en cuestión (derecho a la intimidad) y la esfera reservada para sí por el individuo, en los más básicos aspectos de su autodeterminación como persona, resulta por lo menos cuestionable, que en abstracto pueda entenderse vulnerada su intimidad por la exigencia de transmitir información sobre actividades desenvueltas en el tráfico económico y negocial"[103].

El artículo 105 b) consagra el principio de transparencia administrativa[104]. Este precepto supone un medio de control de la actuación administrativa en un doble aspecto: de un lado, el control por parte del ciudadano que se encuentra vinculado a un procedimiento administrativo; de otro, el de todos "los ciudadanos a estar informados (...) del funcionamiento ordinario y cotidiano de las administraciones"[105].

Por otro lado, hay que entender incluido en este artículo, el derecho de acceso a los archivos y registros de todas las administraciones territoriales, institucionales y

---

[102] La disposición transitoria primera de la Ley Orgánica 1/82, de 5 de mayo establece que "*en tanto no se promulgue la normativa prevista en el artículo 18, apartado 4, de la Constitución la protección Civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley*".
Esta Disposición Transitoria fue derogada por la Disposición Derogatoria Única de la Ley Orgánica 5/92, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

[103] Sentencia del Tribunal Constitucional 143/1994, de 9 de mayo, fundamento jurídico 6°.

[104] Principio considerado por DEBBASCH como un nuevo derecho integrado dentro de una nueva generación de derechos humanos, en MESTRE DELGADO, J.F., *"el derecho de acceso a archivos y registros administrativos,* Civitas, Madrid, 1993, p. 29.

[105] MESTRE DELGADO, J.F., *"el derecho de acceso a archivos y registros administrativos"*, ob.cit., p. 103.

corporativas y de los organismos autónomos, "en la medida en que desarrollan o desempeñan funciones públicas, de interés o servicio público"[106].

También, y por esa misma razón, el derecho de acceso alcanza a todos aquellos sujetos que colaboran o participan en el ejercicio de funciones públicas.

Los límites y excepciones al derecho de acceso a los archivos y registros administrativos están contenidos en el propio precepto y son los siguientes:

1) Informaciones que afecten a la seguridad y a la defensa del Estado.

2) La averiguación de los delitos. Este es el segundo límite expresamente recogido por el artículo 105 b) de la Constitución española en base al cual es posible restringir el derecho de los ciudadanos a acceder a los registros y archivos administrativos.

3) La intimidad de las personas. El derecho a la intimidad es un derecho fundamental garantizado en el artículo 18.1 de la Constitución. Por ello no es necesario su expresa inclusión en el artículo 105 b) para que actuase como límite al derecho de acceso a los archivos y registros administrativos. Junto al derecho a la intimidad, están consagrados en el artículo 18.1, los derechos al honor y a la propia imagen, por lo que aunque no figuren de manera expresa, igualmente limitan el acceso de los ciudadanos a dichos archivos.

Por otra parte, los derechos garantizados en el artículo 18 de la Constitución española, no deberán limitar el acceso a los propios datos recogidos por las administraciones, puesto que el conocimiento de éstos por su titular en ningún caso puede afectar a su honor, intimidad o imagen. Por esta razón éste límite debe entenderse sólo al acceso a los datos ajenos, pero nunca a los propios[107].

---

[106] MESTRE DELGADO, J.F., *"el derecho de acceso a archivos y registros administrativos"*, ob. Cit., p. 103.

[107] En este mismo sentido, para EMBID IRUJO los sujetos legitimados para el acceso a los documentos y registros administrativos que contengan datos que afecten a la intimidad *"son sólo*

2.3. TERCERA GENERACION DE LEYES DE PROTECCION DE DATOS.

A. EL CONVENIO 108 DEL CONSEJO DE EUROPA.

La tercera generación de leyes de protección de datos comienza "con el reconocimiento a escala internacional, de las facultades jurídicas que dimanan de la libertad informática"[108]. Reconocimiento que se produce con la aprobación del convenio de 28 de enero de 1981, Para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

En 1968, la Asamblea Parlamentaria del Consejo de Europa invita, a través de su recomendación 509, al Comité de Ministros a estudiar si es suficiente la regulación interna de cada estado miembro para garantizar la protección de la vida privada en relación con la evolución de la moderna tecnología. Constatada, en un estudio preliminar, la insuficiencia de estas para la protección de la vida privada y de otros derechos e intereses de la persona, el Comité de Ministros adopto en 1973 y 1974, dos resoluciones sobre la protección de la vida privada de las personas en relación con los bancos del sector privado (R(73)22) y del sector publico (R(74)23), respectivamente.

Los principios más importantes contenidos en ambas resoluciones para garantizar la protección de los individuos frente al tratamiento automatizado de sus datos, fueron recogidos en las leyes sobre protección de datos aprobadas en diferentes países del entorno del consejo de Europa. Sin embargo, pronto se puso de manifiesto que los progresos legislativos en esta materia "podían ser minimizados o dejados sin efecto por el desarrollo del flujo transfronterizo de datos"[109]. Por esta razón y ante la evidente necesidad de elaborar una norma internacional

---

las personas respecto a las que se poseen esos datos y quienes, también, pueden pedir la rectificación de menciones incompletas o inexactas". (EMBID IRUJO, A., *"El ciudadano y la Administración"*, Ministerio para las Administraciones Públicas, Madrid, 1994, p. 97).

[108] PEREZ LUÑO, A.E., *"Los Derechos humanos en la sociedad tecnológica"*, ob. Cit., p. 149.

[109] BUQUICCHIO, G., *"Informática y Libertades :Balance de quince años de actividad en el seno del Consejo de Europa"*, traducción de Isabel Hernando, en *Jornadas Internacionales sobre informática y Administración Pública,* Instituto Vasco de Administración Pública, Oñate, 1986, p. 99.

obligatoria, que evitase la aparición de <paraísos de datos>, el Comité de Ministros del Consejo de Europa encargo, en 1976, a un comité de expertos la elaboración de un Convenio para la protección de la vida privada en relación con el tratamiento automatizado de datos personales en el extranjero y en relación con la transmisión internacional de datos, proyecto que culminaría con la aprobación del Convenio 108 del Consejo de Europa.

El Convenio 108 firmado en Estrasburgo, "tiende a conciliar dos derechos fundamentales contrapuestos (...): la protección de datos personales y, la posibilidad de garantizar una libre circulación de las informaciones incluso a través de las fronteras"[110]. Su finalidad es garantizar a las personas físicas, en el territorio de cada parte, el respeto de sus derechos y libertades fundamentales, concretamente el derecho a la vida privada, con respecto al tratamiento automatizado de sus datos personales (Art. 1)

Sin embargo, si bien en principio el Convenio restringe su protección a los datos referentes a las personas físicas, en su artículo 3 abre la posibilidad de que los Estados contratantes amplíen esta protección "a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto de personas físicas, tengan o no tengan personalidad jurídica".

El ámbito de aplicación del Tratado son los ficheros automatizados[111] de carácter personal de los sectores públicos o privados, con la posibilidad de que los Estados parte amplíen la protección a los ficheros y archivos manuales (Art. 3.2.c). Por otra parte se autoriza a excluir determinadas categorías de ficheros automáticos.

---

[110] Ibídem.

[111] El propio convenio dice lo que debe entenderse por fichero automatizado. En el artículo 2°, dedicado en exclusiva a definir los conceptos básicos sobre los que se edifica el Tratado, se entiende que fichero automatizado "*significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado*" (art. 2° b). Por tratamiento automatizado se entienden las siguientes operaciones: registro de datos, aplicación de esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión, siempre que dichas operaciones hayan sido *"efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados"* (art. 2° c)

El capítulo II del Convenio se refiere a los principios básicos para la protección de datos. Estos son los siguientes:

1. Principio de calidad de los datos (Art. 5). Que a su vez se articula en los siguientes subprincipios:

    a) Principio de lealtad que supone que los datos personales que vayan a ser tratados automatizadamente deberán obtenerse y tratarse leal y legítimamente, es decir, sin engaños y sin utilizar procedimientos desleales o ilícitos.

    b) Principio finalista. El registro de los datos deberá hacerse de acuerdo con una finalidad legitima y determinada, no pudiéndose utilizar esos datos de forma incompatible con dicha finalidad.

    c) Los datos deberán ser adecuados y pertinentes en relación con los fines para los que se recogen y, en ningún caso, deberán de ser excesivos para dichas finalidades. Este principio de Pertinencia de los datos completa al anterior, ya que los datos han de guardar relación con el objetivo que se persigue con su tratamiento y finalidad. Por ello mismo, no podrán registrase datos que excedan de este ni utilizarse para un fin distinto del previsto.

    d) Principio de exactitud o veracidad. Los datos serán exactos y actualizados.

    e) Principio de limitación temporal. Según este principio los datos solo se conservaran de forma que permita la identificación de la persona a la que se refieran durante el tiempo necesario para cumplir los fines para los que se recabaron y registraron. Supone la consagración por parte del convenio 108 del derecho al olvido.

2. El segundo principio se centra en la protección de determinadas categorías de datos personales: los datos sensibles. Según el articulo 6 del Convenio 108, "los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, (los) relativos a la salud o a la vida sexual (...) o los referentes a condenas penales, no podrán tratarse automatizadamente salvo que el derecho interno prevea garantías aprobadas. Significa, por tanto la prohibición del tratamiento de este tipo de datos excepto cuando se garantice su uso correcto y su seguridad.

En ningún caso dice el Convenio cuales deberán ser estas garantías dejando a la normativa interna de cada Estado firmante la labor de establecerlas. Debe entenderse que las medidas que protejan estos datos deberán ser mayores que para el resto de los datos personales y, en todo caso suficientes.

3. Principio de seguridad de los datos. Se establece la necesidad de que se incorporen medidas apropiadas de seguridad para evitar que los ficheros de los datos personales sean destruidos o perdidos y para garantizar la imposibilidad del acceso no autorizado a los mismos, así como su difusión o modificación. Al igual que en el caso anterior, será el derecho interno de cada país el encargado de concretar dichas medidas.

4. Bajo el epígrafe de "Garantías complementarias para la persona concernida", el artículo 8 del Tratado consagra los siguientes derechos para las personas:

    a) Derecho a conocer la existencia de un fichero automatizado de datos personales, su finalidad y la identidad y domicilio habitual de la autoridad controladora del mismo.

b) Derecho a ser informado de si sus datos personales se encuentran o no en un fichero automatizado, y a que se le comunique cuales figuran en el mismo.

c) Derecho de rectificación y cancelación de los datos obtenidos infringiendo las normas de derecho interno que desarrollen los principios antes enunciados.

d) Derecho a recurrir la resolución que hubiese desatendido alguno de los derechos anteriores.

Las facultades contenidas en el articulo 8º suponen *"el reconocimiento, a escala europea, de la libertad informática (al) garantizar el acceso y control de las personas (habeas data) de aquellos datos que les conciernen"*[112].

Los principios y derechos enunciados en los artículos 5 y siguientes no son absolutos, estableciéndose en el artículo 9 algunas excepciones. Podrán limitarse los derechos de las personas garantizados por el Convenio así como los principios de calidad de los datos personales y las especiales normas referentes a los datos sensibles cuando ello sea necesario *"en una sociedad democrática*:

a) para la protección de la seguridad del estado, de la seguridad pública, para los intereses monetarios del estado o para la represión de las infracciones penales;

b) para la protección de la persona concernida y de los derechos y libertades de otras personas".

También podrán establecerse restricciones a los derechos de las personas cuando la ley interna así lo provea para los ficheros que se utilicen con fines estadísticos o

[112] PEREZ LUÑO, A.E., *"Los Derechos humanos en la sociedad tecnológica"*, ob. Cit., p. 169.

de investigación científica, siempre que no existan riesgos manifiestos *"de atentado a la vida privada de las personas concernidas"*. Este tipo de ficheros son necesarios para llevar a cabo determinadas investigaciones científicas por lo que parece razonable que siempre que se garantice por órganos de control y normas internas el respeto a los derechos fundamentales de las personas, puedan tratarse automáticamente datos personales.

El capítulo III del Tratado de Estrasburgo regula la circulación internacional de datos personales.

El convenio, tal y como se expresa en su preámbulo, persigue conciliar, por una parte, el respeto a la vida privada de las personas y, por otra, garantizar la libertad de información a través de la libre circulación de la información entre los pueblos, sin tener en cuenta las fronteras. Para garantizar el cumplimiento de este fin, el articulo 12.2, establece que un estado parte *"no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte"*.

Podrá parecer que en el Convenio 108 del Consejo de Europa, prima de manera absoluta la libertad de circulación internacional de datos frente al derecho ala vida privada de las personas. Sin embargo, al relacionar este precepto con su punto tercero se establece la posibilidad de que una parte no permita la exportación de datos personales cuando el destinatario final de los mismos sea un estado no contratante y se puedan burlar las normas establecidas en el Tratado respecto a la protección de las personas y, en segundo lugar, cuando la legislación interna prevea para determinado tipo de datos y ficheros una protección especial y en el país de destino estos no cuenten con una protección equivalente.

El cumplimiento del convenio por los países contratantes se estructura a través del principio de colaboración entre las partes (Art. 13).

Por último, prevé el Tratado 108 sobre protección de datos, la constitución de un Comité consultivo. Dicho comité estará compuesto por un representante y un suplente de cada parte. Aquellos estados miembros del Consejo de Europa, que no lo sean del Convenio, podrán estar representados en este órgano por un observador.

El convenio entro en vigor con carácter general el 1 de octubre de 1985

B. DATA PROTECTION ACT DE 1984. REINO UNIDO.

La Ley Inglesa de Protección de Datos está inspirada en los principios fundamentales del Convenio 108 del Consejo de Europa.

Su objetivo es regular el uso de la información automatizada relativa a personas y no el establecimiento de un derecho general a la intimidad[113] ni su protección.

El ámbito de aplicación de la ley se limita a los ficheros automatizados, tanto del sector público como del privado[114], quedando excluidos los ficheros manuales.

La Privacy Act se estructura en 5 partes, divididas en secciones y parágrafos, reguladoras de cuestiones de carácter general, y se complementa con 4 apéndices que regulan los principios de protección de datos (apéndice 1), el registro de protección de datos y el tribunal de protección de datos (apéndice 2), el

---

[113] El derecho británico desconoce, a diferencia de los derechos continentales un derecho general a la intimidad de elaboración legislativa y tampoco, como sucede en los Estados Unidos, de elaboración jurisprudencial. Esta última opción, "*la creación por elaboración jurisprudencial de un derecho de accionar* (ante una violación de la intimidad personal o familiar) *ha sido considerada imposible en Inglaterra*". Así lo confirmó el caso Kayes Robertson, que impidió a los acusados la publicación de unas fotografías tomadas al demandante en un hospital como si éste voluntariamente hubiese consentido la entrevista o que le fotografiasen, por maliciosa falsedad y no para garantizar el derecho a la intimidad de aquel. (En MUNRO, C., *"La libertad de prensa en Inglaterra: Como la bestia fue domada"),* traducción de Carlos González Alvarez, en Revista de Administración Pública, Centro de Estudios Constitucionales, Mayo-Agosto, 1993.)

[114] la sección 38 dispone que los Departamentos del Gobierno estarán sujetos por las mismas obligaciones y responsabilidades que se establecen en esta ley para las personas privadas y los funcionarios públicos pueden ser perseguidos por las mismas infracciones que los usuarios de datos privados.

procedimiento de apelación (apéndice 3) y los poderes de acceso e inspección (apéndice 4).

La característica más destacada de la Privacy Act de 1984 son las numerosas excepciones a las normas protectoras de las personas frente al tratamiento automatizado de sus datos de carácter personal.

Las excepciones más evidentes son las relativas a informaciones contenidas en las bases de datos de las Fuerzas Armadas y de la Policía, pero también existen numerosas excepciones al derecho de acceso del titular de los datos y a la obligación del usuario de los datos de impedir los accesos y las revelaciones no autorizadas.

Por otro lado, el complejo sistema de excepciones de la Ley no excluye en bloque todos los derechos y deberes correspondientes a ciertos sujetos, *"pero –caso por caso,- conforme a la tradición jurídica de aquel país- excluye alguno o todos los derechos o deberes de algunos o de todos los sujetos"*[115].

Hay que destacar que la Privacy Act otorga numerosos poderes y funciones al Registrador de Protección de Datos, limitando bastante el número y contenido de los derechos de las personas afectadas por el tratamiento informático de sus datos, por lo que la tutela de sus intereses y el cumplimiento de los principios y fines de la ley se realizarán en mayor medida a través de actuaciones del registrador que mediante demandas interpuestas por ellos ante los Tribunales ordinarios.

---

[115] LOSANO, M.G., *"Il Diritto pubblico dell'informatica, corso di informatica guridica"*, Piccola Biblioteca Einaudai, Torino, 1986, p. 124.

C. LEI N° 10/91, DE 29 DE AVRIL, DA PROTECCAO DE DADOS PESSOAIS FACE Á INFORMÁTICA.

En la legislación portuguesa de protección de datos puede constatarse tres niveles de protección. Un primer nivel, en lo alto de la pirámide, en el que se sitúa el artículo 35 de la Constitución que establece los principios básicos para la defensa de los ciudadanos frente al tratamiento automatizado de sus datos.

En un segundo nivel. Encontramos, por un lado, el artículo 181 del Código Penal y, por otro, la Ley Portuguesa de Protección de Datos. En el primero se tipifica como delito <<la indagación por medio de la informática>> ; en un segundo apartado, el artículo dispone que será castigado con prisión de hasta dos años, quien procesara o mandara procesar datos de carácter personal relativos a convicciones políticas, religiosas, filosóficas u otras relativas a la intimidad, contraviniendo lo que la ley establezca.

Es característica común a los distintos niveles de protección de la legislación portuguesa de protección de datos, una preocupación muy especial por el tratamiento que reciban los datos sensibles.

En un tercer nivel se encontrarían las relativas a otras materias que contienen referencias a la protección de datos personales. Esto supone la adopción de un sistema mixto de protección "tendente a conjugar una disciplina unitaria con un marco jurídico adaptado a las exigencias de determinados aspectos jurídicos (...) o tecnológicos específicos"[116]

El principio general inspirador de esta ley, es el uso transparente de la informática en el estricto respeto de la vida privada y familiar y de los derechos, libertades y garantías fundamentales del ciudadano[117] (art. 1°). El objetivo de la ley no es el de

[116] PEREZ LUÑO, A.E., *"Manual de Informática y Derecho"*, Ariel, Barcelona, 1996, p. 54.
[117] La Constitución Portuguesa consagra en su primera parte, titulos I y II, los derechos, libertades y garantias de que gozan todos los ciudadanos. Los derechos garantizan el status positivus y el

prohibir el tratamiento automatizado de las informaciones de carácter personal, sino de que este tratamiento se haga respetando los derechos y libertades fundamentales de las personas[118].

Es importante destacar que, si bien bajo la denominación de <<dados pessoais>> sólo se incluyen las informaciones relativas a una persona singular identificada o identificable, el artículo tercero amplía el ámbito de aplicación de la Ley a los soportes informáticos relativos a personas jurídicas siempre que contuvieran datos personales. Es decir, la Ley portuguesa de Protección de Datos Personales, adopta una postura intermedia.

Esta extensión del régimen de protección a las personas jurídicas es "una clara manifestación de que el bien jurídico protegido no es exclusivamente la intimidad personal y familiar[119] que, en sentido estricto, sólo puede referirse a las personas físicas.

Como es habitual en las leyes de protección de datos modernas, especialmente las aprobadas con posterioridad al Convenio 108 del Consejo de Europa, la ley portuguesa dedica un capítulo al flujo internacional de datos personales; asimismo, un capitulo de delitos.

Después de haber realizado un análisis sobre la evolución de las legislaciones de datos personales, cuyo objetivo no fue el estudio profundo de cada una de ellas, podemos advertir que prácticamente todos los países europeos y, también, otros no europeos como Japón, Estados Unidos o Canadá cuentan con este tipo de regulación.

---

status activus, como dercehos inherentes al hombre como individuo o como participante en la vida política; las libertades son los medios de defensa de la esfera jurídica de los ciudadanos frente a los poderes públicos y suponen un status negativus y las garantias o medios procesales adecuados para la defensa de los derechos integran el status processualis. (En GOMES, CANOTILHO, J.J.; Directo Constitucional, Almedina Coimbra, 1995, p. 530.)

[118] No se trata de garantizar la intimidad de las personas sino el pleno ejercicio de todos sus derechos, libertades y garantías constitucionales como máxima expresión de la dignidad de la persona, en la que, según el artículo 1° de la Constitución portuguesa, debe basarse la República de Portugal para la consecución de una sociedad libre, justa y solidaria.

[119] ASPAS ASPAS, J.M., *"El derecho a la autodeterminación informativa en la Ley Portuguesa de Protección de Datos de 1991. sujetos, contenido y garantías" p. 283.*

Por supuesto, en cada etapa se adoptaron determinados mecanismos de protección y determinadas garantías, que respondían al estado de la tecnología en ese momento y, al mismo tiempo, al estado de concienciación sobre el problema de los Gobiernos, los Parlamentos y los ciudadanos.

En la primera generación, las leyes de protección de datos intentaron crear instrumentos de garantía con los que se pudiese establecer límites a la utilización de la informática. Al encontrarse los registros de datos personales en grandes centros de información, fáciles de localizar y proteger, las leyes organizaron sus mecanismos de protección en torno a dos principios básicos: la autorización previa a la constitución de los bancos y ficheros de datos y su control e inspección posterior.

La segunda etapa podríamos calificarla como aquella en la que, de forma generalizada, los Estados asumen la necesidad de brindar una protección efectiva a las personas frente al uso automatizado de sus datos. La asunción de este objetivo se manifiesta muy especialmente en la inclusión en las constituciones, del derecho fundamental de la personas a ser protegidas frente a aquellos usos. Así sucede en los casos de Austria, Portugal y España.

En los demás casos, es decir, cuando los Estados no optan por la inclusión de un nuevo derecho fundamental en sus Normas Fundamentales, la solución legislativa es la de aprobar una ley de protección de datos.

Esta segunda generación de leyes está marcada por el intento de "asegurar la calidad de los datos"[120]. Este objetivo se consiguió, principalmente, mediante el asentamiento de dos tipos de disposiciones. Por un lado, se regularon los derechos individuales de los afectados para que pudiesen, de manera efectiva, controlar la información personal que les concierne y, por otro, a través del

[120] DEL PESO NAVARRO, E. y RAMOS GONZÁLEZ, M., *"Confidencialidad y Seguridad de la información: La LORTAD y sus implicaciones socioeconómicas"*, Díaz de Santos, Madrid, 1994, p. 200.

establecimiento de cláusulas específicas para la protección de "las informaciones consideradas <<sensibles>>, por su inmediata incidencia sobre la intimidad y el ejercicio de las libertades"[121].

Así, en las leyes de segunda generación se combinaron las medidas de tutela estática, basadas en asegurar la calidad de los datos, con "un sistema de protección dinámica, centrada en el control de los programas y en su utilización[122].

A este fin de garantizar la calidad de los datos procesados contribuyó el establecimiento de los denominados principios de protección de datos. En este momento las leyes de protección de datos comienzan a incluir entre sus disposiciones, normas que hacen referencia a los principios de lealtad, de finalidad y de pertinencia de los datos personales recogidos. Así sucede desde la Privacy Act de 1974 hasta nuestros días, aunque, en la tercera generación de leyes, esas disposiciones que determinan que principios generales han de ordenar la recogida, tratamiento y cesión de los datos personales se han completado con otros principios.

De otro lado, con la proliferación del uso de ordenadores cada vez más potentes y pequeños, menos fáciles de localizar, se hace necesario añadir estas medidas a las adoptadas en la primera etapa. De esta forma, los poderes y las facultades de las Autoridades de Protección de Datos se complementan con la posibilidad de los titulares de datos personales de ejercer su control por sí mismos. Sólo en caso de incumplimiento de las disposiciones legales, acudirán en demanda de protección de sus intereses, bien ante los Tribunales ordinarios, bien ante el especial creado para tal efecto.

Por otra parte, en este momento se amplía, con carácter general, a los datos contenidos en ficheros de titularidad privada, el ámbito de aplicación de estas normas.

---

[121] PEREZ LUÑO, A.E., *"Los derechos humanos en la sociedad tecnológica"*, ob.cit., p. 152.
[122] PEREZ LUÑO, A.E., *"Manual de informática y Derecho"*, ob.cit., p. 55.

Finalmente, la tercera generación de leyes de protección de datos se caracteriza por intentar armonizar el principio de libre circulación internacional de datos personales con la defensa de los derechos y las libertades de las personas[123]. Responden al estado actual de la tecnología que ha supuesto la masiva utilización de ordenadores personales en todos los ámbitos y sectores, económicos y sociales, públicos y privados. Por ello, estas normas se caracterizan, también, por incidir en mayor medida que en etapas anteriores en las medidas de seguridad que los responsables de los ficheros de datos personales deben adoptar, al haber aumentado alarmantemente las formas de eludirlas.

También se completan los principios relativos a la calidad de los datos enunciados en la etapa anterior. A los principios de lealtad, finalidad o pertinencia, se añaden ahora los principios de exactitud, seguridad, conservación de los datos limitada en el tiempo, etc.

[123] Si bien es cierto que en la etapa anterior ya se incluían frecuentes disposiciones legales reguladoras del tráfico internacional de datos, sólo ahora, estas se producen con tanta frecuencia y habitualidad y es tal la calidad de los datos que son transferidos de un Estado a otro, que se hace necesario uniformizar las distintas legislaciones nacionales de forma que sus diferencias no supongan un obstáculo a ese tráfico internacional. A este fin responde la firma del Convenio 108 del Consejo de Europa y la Directiva 95/46/ CE, de la Unión Europea, ya que ambos tratados pretenden conciliar la libre circulación de información entre los Estados con la protección de las libertades del individuo.

CAPITULO IV

RECONOCIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO.

1. PROTECCIÓN DE DATOS PERSONALES EN ARCHIVOS GUBERNAMENTALES.

1.1. LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL (LFTAIPG).

En el año 2002, se aprobó la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la cual tiene como finalidad proveer lo necesario para garantizar el acceso a toda persona a la información en posesión de los Poderes de la Unión, los Órganos Constitucionales Autónomos o con autonomía legal, y cualquier otra entidad federal. Entre los objetivos de la Ley, el artículo 4 establece el de garantizar la protección de los datos personales en posesión de los sujetos obligados, es decir, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental obliga a proteger los datos personales que obren en archivos de los órganos federales. Para el caso que nos ocupa, no avocaremos al estudio de lo relativo a la protección de la información (datos) de carácter personal.

En primera instancia y antes de abordar la regulación de los datos personales en nuestro país, es importante definir que debemos entender por *"dato personal"*, por lo que como referencia señalaremos los siguientes conceptos:

Por dato personal debe entenderse aquel que es relativo o propio de una persona, es decir perteneciente a una persona; o según el Convenio Europeo de 1981, de

Protección de Datos, *"cualquier información relativa a una persona física identificada o identificable".*[124]

Para el Parlamento Europeo los «datos personales» se definen como: *"toda información sobre una persona física identificada o identificable (el«interesado»); se considerará identificable 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".*[125]

En nuestro país, dato personal se define como *" la información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales u otras análogas que afecten su intimidad".*[126]

Cabe señalar que el concepto que reconoce la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental enuncia una serie de datos, lo que en modo alguno de considerarse una lista taxativa.

De este mismo ordenamiento, se desprenden una serie de disposiciones relativas a la protección de datos personales los cuales serán precisados a continuación:

Artículo 18. *Como información confidencial se considerará:*

---

[124] Artículo 2° a) del Convenio de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de sus Datos de Carácter Personal.

[125] Artículo 2° a) de la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[126] Artículo 3°, fracción II de la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental, México, D.O.F., 11 de junio de 2002.

I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y

II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.

No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público.

Asimismo, existe en el cuerpo de la referida Ley un capítulo completo destinado a la protección de datos personales, en poder únicamente del sector público y donde se establece la responsabilidad de los sujetos obligados detentores de los datos personales, mismos que a continuación se transcriben:

Capítulo IV

Protección de datos personales

Artículo 20. *Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:*

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. *Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;*

IV. *Procurar que los datos personales sean exactos y actualizados;*

V. *Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y*

VI. *Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.*

Artículo 21. *Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.*

Así, se garantiza el derecho de acceso a los datos personales, el principio de proporcionalidad (tratamiento de datos cuando sea pertinente y no excesivo) el principio de finalidad (propósito del tratamiento de los datos) y el principio de seguridad.

En el artículo 22 encontramos la obligación de lealtad (prohibición de la comercialización de los datos) y las excepciones para el consentimiento (principio del consentimiento del titular) de obtención de datos.

Artículo 22. *No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:*

I. (Se deroga).

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales.

Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes.

***Artículo 23.** Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales.*

***Artículo 24.** Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por*

escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

Artículo 25. *Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición.*

Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

Artículo 26. *Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.*
En esta misma Ley se impone la obligación al sector público de declarar todos los sistemas de datos personales al Instituto Federal de Acceso a la información (IFAI). Además los ciudadanos mexicanos podrán interponer un recurso de revisión si previamente se les negó el acceso a la información (derecho de impugnación). Este recurso se interpondrá ante el IFAI, el cual es el órgano encargado de controlar la información pública en México.

1.2. LINEAMIENTOS DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE INFORMACION DE LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL.[127]

Estos lineamientos fueron expedidos por el Instituto Federal de Acceso a la Información Pública y publicados en el Diario Oficial de la Federación el 18 de agosto de 2003, por lo que hace a la información confidencial (datos personales) señala en su capítulo tercero lo siguiente:

Trigésimo.- Los documentos y expedientes clasificados como confidenciales no podrán difundirse si no media en cada caso, el consentimiento del titular de dicha información, sin perjuicio de las excepciones establecidas en la Ley, el Reglamento y los presentes Lineamientos. Dicho consentimiento podrá solicitarse de conformidad con el artículo 41 del Reglamento.

Trigésimo Primero.- La información confidencial que además se ubique en alguno de los supuestos establecidos por los artículos 13 y 14 de la Ley, será clasificada como reservada.

Trigésimo Segundo.- Será confidencial la información que contenga datos personales de una persona física identificada o identificable relativos a:

I. Origen étnico o racial;

II. Características físicas;

III. Características morales;

IV. Características emocionales;

---

[127] http://portaltransparencia.gob.mx/pot/mrcoNormativo/buscar.do?method=buscar&_idDependencia=06738 , **tomado de los Lineamientos de Clasificación y Desclasificación de Información de las Dependencias y Entidades de la Administración Pública Federal.**

V. Vida afectiva;

VI. Vida familiar;

VII. Domicilio particular;

VIII. Número telefónico particular;

IX. Patrimonio;

X. Ideología;

XI. Opinión política;

XII. Creencia o convicción religiosa;

XIII. Creencia o convicción filosófica;

XIV. Estado de salud física;

XV. Estado de salud mental;

XVI. Preferencia sexual, y

XVII. Otras análogas que afecten su intimidad, como la información genética.

Trigésimo Tercero.- Los datos personales serán confidenciales independientemente de que hayan sido obtenidos directamente de su titular o por cualquier otro medio.

Trigésimo Cuarto.- Se considerarán como confidenciales los datos personales referidos a una persona que ha fallecido, a los cuales únicamente podrán tener acceso y derecho a pedir su corrección, el cónyuge supérstite y/o los parientes en línea recta ascendente y descendente sin limitación de grado, y en línea transversal hasta el segundo grado.

En caso de que no existan las personas a que se refiere el párrafo anterior, tendrán acceso y derecho a pedir la corrección de datos personales del fallecido, sus parientes en línea transversal hasta el cuarto grado.

Cuando el titular de los datos personales haya fallecido, y la dependencia o entidad reciba una solicitud de acceso o corrección de los mismos presentada por una persona distinta de las mencionadas en los párrafos anteriores, el Comité podrá solicitar el consentimiento de cualquiera de éstas.

Trigésimo Quinto.- La información confidencial que los particulares proporcionen a las dependencias y entidades para fines estadísticos, que éstas obtengan de registros administrativos o aquellos que contengan información relativa al estado civil de las personas, no podrán difundirse en forma nominativa o individualizada, o de cualquier otra forma que permita la identificación inmediata de los interesados, o conduzcan, por su estructura, contenido o grado de desagregación a la identificación individual de los mismos.

Trigésimo Sexto.- Sin perjuicio de las excepciones establecidas en la Ley, el Reglamento y los presentes Lineamientos, los particulares podrán entregar a las dependencias y entidades con carácter de confidencial, aquella información a que se refiere la fracción I del artículo 18 de la Ley y de la cual sean titulares, entre otra:

I. La relativa al patrimonio de una persona moral;

II. La que comprenda hechos y actos de carácter económico, contable, jurídico o administrativo relativos a una persona, que pudiera ser útil para un competidor por ejemplo, la relativa a detalles sobre el manejo del negocio del titular, sobre su proceso de toma de decisiones o información que pudiera afectar sus negociaciones, acuerdos de los órganos de administración, políticas de dividendos y sus modificaciones o actas de asamblea, y

III. Aquella cuya difusión esté prohibida por una cláusula o convenio de confidencialidad.

Cabe hacer mención que se contempla el caso de fallecimiento del titular de los datos personales; así como lo que corresponde a ciertos aspectos respecto de personas morales.

1.3. LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES.

Por lo que respecta al tratamiento que deben tener los datos personales se han expedido los Lineamientos de Protección de Datos Personales (IFAI), los cuales son de carácter general y observancia obligatoria para la Administración Pública Federal, mismos que en su quinto lineamiento señalan expresamente que las dependencias y entidades deberán observar los principios de *licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión*, los cuales se describen brevemente a continuación:

a) Licitud, es decir que exista justificación legal que permita la posesión de los mismos, lo que se traduce en que debe contemplarse dentro de las atribuciones legales o reglamentarias de las dependencias o entidades de la Administración Pública, además de que los mismos deben ser obtenidos a través de los medios previstos en los instrumentos jurídicos y con una finalidad u objetivo específico.

b) Calidad; El "tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea"[128].

En este sentido el tratamiento que reciban los datos personales deberá cumplir con un propósito en particular, deberán ser veraces y utilizados exclusivamente para el fin u objetivo para el que fueron recabados, lo que se traduce en que se deberán mantener las medidas de seguridad necesarias para su manejo, además de que únicamente se debe requerir la cantidad de información necesaria para cumplir con el objetivo previsto, a través del personal legalmente facultado para ello.

c) Acceso y corrección; lo que implica que siempre deberá garantizarse al titular de los datos personales el acceso y en su caso la corrección de los mismos, para de esta forma mantener su información como cierta; lo cual deberá de hacerse conforme a los procedimientos previstos en los ordenamientos jurídicos correspondientes.

d) De información, lo que obliga al manejador de los datos a manifestar la razón jurídica y causa que ha dado lugar a su recopilación, así como el objetivo o fin para los cuales han sido obtenidos.

e) Seguridad; lo que se traduce en que los tenedores de los datos deberán garantizar que estos se encuentren debidamente resguardados a través de medidas que eviten su alteración, pérdida o menoscabo, transmisión, procesamiento ilegal o acceso no autorizado de los mismos, avalando de esta forma la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales.

---

[128] Artículo séptimo, Lineamientos de Protección de Datos Personales, D.O.F., 30 de septiembre de 2005.

f) Custodia y cuidado de la información; esto implica que el resguardo y conservación de los datos personales dependerá de quienes estén debidamente autorizados y facultados para ello en términos de la legislación aplicable.

g) Consentimiento para la transmisión, es decir que invariablemente para que exista transferencia de datos, deberá contarse con la aprobación del titular de los mismos para hacerlo, salvo en los casos expresamente previstos en las leyes u ordenamientos jurídicos correspondientes.

De esta breve descripción podemos advertir que se han considerado en la elaboración de los Lineamientos de Protección de Datos Personales, los principios rectores previstos por la Organización para la Cooperación y el Desarrollo Económico (OCDE) así como de otros instrumentos jurídicos internacionales en lo relativo a la protección de la privacidad de los datos personales y sus flujos transfronterizos; con lo que nuestro país al ser miembro de dicha organización pretender dar cumplimiento a sus recomendaciones y de esta forma tener una regulación compatible a nivel mundial.

Por lo que hace a los derechos del titular de los datos personales, en este aspecto podemos determinar que tomando en consideración las disposiciones legales existentes en el Sistema Jurídico Mexicano, tales como la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), su Reglamento, así como los Lineamientos de Protección de Datos Personales, los derechos inherentes a los titulares de los datos son básicamente el acceso, rectificación, así como a la cancelación de los datos personales, actualmente considerado en la reforma constitucional al artículo 16.

Cabe señalar que esta normatividad expedida por el IFAI tiene por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a

la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.[129]

Si bien se requiere la expedición de una Ley de Protección de Datos Personales, la normatividad citada aunque es un ejercicio modesto respecto del universo de datos que deben protegerse, constituye el primer antecedente importante en la materia, aplicable exclusivamente al sector público.

2. REFORMA AL ARTÍCULO 6° DE LA CONSTITUCIÓN POLITICA DE LOS ESTADOS UNIDOS MEXICANOS.[130]

La promulgación y entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental es una de las adquisiciones democráticas más importantes de México en los años recientes. Su vigencia ha contribuido a la apertura del Estado, al conocimiento público de los asuntos importantes para la nación, ha puesto en manos de los ciudadanos una gran cantidad y variedad de datos, cifras y documentos para la toma de sus propias decisiones y ha ayudado a remover inercias gubernamentales indeseables como el secretismo, el patrimonialismo, la corrupción y la discrecionalidad.

La actual Ley Federal es el resultado de una construcción plural y de una acción legislativa concertada. El compromiso con la transparencia y el acceso a la información ha alcanzado y reforzado un amplio consenso en el ámbito político, social y académico de la nación.

La expedición de la Ley se sustentó en el artículo 6° Constitucional, cuya reforma en 1977 adicionó "el derecho a la información será garantizado por el Estado".

---

[129] Artículo primero, Lineamientos de Protección de Datos Personales, D.O.F., 30 de septiembre de 2005

[130] Instituto Federal de Acceso a la Información Pública *"Reforma al artículo 6° constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos"*, junio 2007.

En 2007 se reforma nuevamente el artículo constitucional en comento, la redacción que se propuso, respetó la secuencia natural del párrafo inicial del artículo 6° constitucional que no se modificó, y establece con precisión los principios de las bases para el ejercicio del derecho de acceso a la información.

La nueva versión incluye de un modo explícito y congruente las bases principales para el funcionamiento de los mecanismos clave para la publicidad de la información en posesión de cualquier autoridad, entidad órgano u organismo federal, estatal y municipal.

Cabe destacar que la adición en el texto del artículo 6° constitucional tiene una implicación de grandes consecuencias para el país, a saber: consolidar la idea de que el acceso a la información es un derecho fundamental que debe ser reconocido en la Constitución como una garantía de los individuos frente al estado mexicano en todos sus niveles, poderes, órganos y entidades.

Derivado del trabajo conjunto realizado por instituciones académicas y las comisiones o institutos de transparencia locales y el federal, se logro dar cabida a la propuesta de reforma. Es mediante esta reforma que por primera vez la Constitución Política de los Estados Unidos mexicanos reconoce la existencia del derecho de protección de datos personales.

La reforma al artículo 6° constitucional se publicó en el Diario Oficial de la Federación el 20 de julio de 2007 en los términos siguientes:

Artículo 6°.- *La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.*

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. *Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.*

II. *La información que se refiere a la vida privada y* ***los datos personales será protegida*** *en los términos y con las excepciones que fijen las leyes.*

III. *Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.*

IV. *Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.*

V. *Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.*

VI. *Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.*

VII. *La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.*

En ese sentido, la reforma de mérito constituyó no sólo un avance importante en el ejercicio del derecho de acceso a la información, sino también el reconocimiento a nivel constitucional del derecho de protección de datos personales, como un derecho diverso del derecho a la privacidad.

3. REFORMA DE LOS ARTÍCULOS 16 Y 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MÉXICANOS.

Ahora bien, es pertinente señalar avances significativos orientados a la construcción de un marco jurídico completo en materia de protección de datos personales.

Los inicios para la conformación de una regulación completa son visibles en sendas reformas a la Constitución Política de los Estados Unidos Mexicanos, las cuales dada su relevancia para la presente investigación, a continuación se transcriben:

a) Decreto por el que se adiciona la fracción XXIX-Ñ al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.

Artículo Único. Se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73. El Congreso tiene facultad:

I. a XXIX-N. ...

XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.

XXX. ...

b) Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos

Artículo Único. Se adiciona un segundo párrafo recorriéndose los subsecuentes en su orden al artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal de procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado cuando menos con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.
(...)

4. INICIATIVAS DE LEY PRESENTADAS EN EL CONGRESO DE LA UNIÓN.

a) Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales, a cargo del Diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI.[131]

La iniciativa está fundada en prevenir el mal uso de los datos personales y por consiguiente el daño que se pudiera causar a los ciudadanos (los titulares de los datos personales) por ese mal uso. La iniciativa no se centra solamente en sancionar el mal uso de los datos, sino de proveer a los individuos de mecanismos para ejercer efectivamente los derechos Arco.

Asimismo, hace una importante distinción entre los datos personales que tienen una naturaleza sensible y que en sí mismo no son necesarios para llevar a cabo actos meramente comerciales, contractuales o laborales.

Se centra en proveer a los titulares de información sobre los datos que se recopilan de ellos y con qué propósito. Esto se logra por medio del aviso de privacidad que los responsables del tratamiento de los datos personales (entendido de la forma más amplia posible) tienen que presentar a los titulares especificando no solamente que datos recopilarán, sino los fines para lo que lo hacen y cualesquiera fines secundarios para los que pudieran utilizarse dichos datos.

La iniciativa especifica la necesidad de que la información esté completa y la mantenga, en la medida de lo posible, actualizada.

---

[131] http://gaceta.diputados.gob.mx/, tomado de la Exposición de Motivos de la iniciativa con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales, a cargo del Diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI.

Determina la existencia de una autoridad central que sea responsable del cumplimiento de la ley y que pueda establecer sanciones en la esfera administrativa. Esta autoridad está particularmente enfocada al cumplimiento de las obligaciones que los responsables de los datos tienen que dar para permitir el acceso y corrección de los datos a los titulares de éstos.

Para efectos de la designación de la autoridad y buscando minimizar los costos del estado propone que el ente especializado en la materia, dependa de la Secretaría de Economía, quien tiene entre sus atribuciones y órganos desconcentrados o especializados la protección de otros derechos como el del consumidor por medio de la Procuraduría Federal del Consumidor (Profeco) o el de la protección de la propiedad industrial por medio del Instituto Mexicano de la Propiedad Industrial (IMPI).

Asimismo reconoce la necesidad de que los responsables de los datos establezcan medidas de seguridad para proteger estos y finalmente establece dos procedimientos fundamentales para otorgar protección efectiva para los titulares de los datos. El primero, es el procedimiento de acceso ante el responsable; En segundo lugar se establece un procedimiento ante la autoridad que tiene el objeto de corregir faltas u omisiones que el responsable haya podido cometer, que es la verdadera necesidad del titular, estableciendo sanciones ante el incumplimiento.

La iniciativa se presentó en la sesión del 11 de diciembre de 2008. se turnó a la Comisión de Gobernación, con opinión de la Comisión de presupuesto y Cuenta Pública.

b) Iniciativa con proyecto de decreto por el que se expide La Ley de Protección de Datos Personales en Posesión de Particulares, a cargo del Diputado Luis Gustavo Parra Noriega, del Grupo Parlamentario del PAN [132]

De la exposición de motivos de este proyecto se desprende que se busca crear dicha ley de protección de datos personales en posesión de datos personales en atención a que los ciudadanos se convierten en seres vulnerables ante el desarrollo estrepitoso de la tecnología, ya que ante la ausencia de una regulación en la materia, quienes posean bases de datos personales tienen a su alcance una radiografía clara y precisa de los titulares de la información.

El diputado argumenta que es precisamente el uso indebido de los datos personales, lo que puede tener consecuencias graves para una persona que pueden ir desde la provocación de actos de molestia al titular de los datos, consistente en el envío ilimitado de información no solicitada; pasando por actos de discriminación, toda vez que mediante el cruce de información de una persona, se puede configurar un perfil respecto de sus gustos, creencias, afinidades o que decir de su estado de salud o mental, que pueden influir negativamente al momento de solicitar se le proporcione un servicio o adquiera un bien; hasta la comisión de delitos graves como el secuestro o el robo de identidad. El uso perverso de la información puede crear problemas muy serios que han convertido a la persona en un ser vulnerable que vive con la amenaza latente de ser observado en forma permanente.

Asimismo señala que el respeto a la dignidad de la persona constituye la base fundamental de la protección de datos personales, en cuanto a que se refiere a una expresión de su vida privada, toda vez que este derecho se basa en el poder

---

[132] http://gaceta.diputados.gob.mx/, tomado de la Exposición de Motivos; *IV. Elementos para la construcción de la iniciativa de Ley de Protección de Datos Personales;* de la iniciativa con proyecto de decreto por el que se expide La Ley de Protección de Datos Personales en Posesión de Particulares, a cargo del Diputado Luis Gustavo Parra Noriega, del Grupo Parlamentario del PAN.

de disposición de los datos por su titular, y de decir, en la mayoría de los casos, a quienes y bajo qué condiciones los entrega; lo anterior implica que la persona que tenga a su cargo el tratamiento de datos personales, los debe utilizar con estricto respeto a los derechos del interesado.

En consecuencia, si los datos sometidos a tratamiento son datos ajenos y su utilización ha de hacerse en el marco del respeto a la dignidad de la persona y a su poder de disposición sobre los datos, es necesario que en la recopilación y tratamiento de datos se observen ciertos principios[133] (licitud, consentimiento, información, calidad, confidencialidad, derecho al olvido y seguridad) que garanticen plenamente seguridad en el manejo de los mismos.

Establece autoridad administrativa en la materia, la Comisión Nacional de Protección de Datos Personales con la naturaleza jurídica de un organismo descentralizado de la Administración Pública Federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio; contando con plena autonomía técnica y de gestión, así como para dictar sus resoluciones.

Las principales atribuciones de la Comisión serán la promoción y protección de los datos personales en posesión de particulares; el desarrollo, fomento y difusión de análisis, estudios e investigaciones en materia de protección de datos personales en posesión de particulares; el establecimiento de los lineamientos que en materia de seguridad en el tratamiento de los datos personales, deban observar los particulares; la emisión de las disposiciones necesarias para la operación, funcionamiento y control del registro de bases de datos previsto en la ley; la difusión de los compromisos asumidos por el Estado mexicano en los instrumentos; procurar la solución de las diferencias entre los titulares de datos personales y los particulares; elaborar el Programa Institucional en materia de Protección de Datos Personales en posesión de particulares; conocer y resolver

[133] Capítulo Segundo del Proyecto de Ley de Protección de Datos Personales en Posesión de Particulares.

los procedimientos de declaración de infracción administrativa; resolver los recursos de revisión interpuestos en contra de sus resoluciones, así como imponer las sanciones correspondientes.

La iniciativa se agendó para presentarse en la sesión del 07 de octubre de 2008. No se presentó sino hasta la sesión del 04 de noviembre de 2008 y se turnó a la Comisión de Gobernación, con opinión de la Comisión de Presupuesto y Cuenta Pública.

c) Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales, a cargo de la Diputada Sheyla Fabiola Aragón Cortés, del Grupo reglamentario del PAN.[134]

Esta iniciativa señala en su exposición de motivos destaca la evaluación de ciertos elementos mismos que a continuación se precisan:

1. Que la responsabilidad de esta soberanía para legislar en materia de protección de la privacidad de los datos personales de los individuos es impostergable, no sólo por tratarse de un tema de protección de derechos humanos y libertades fundamentales, sino porque tiene un origen y efectos esenciales sobre la economía nacional y el aseguramiento del comercio irrestricto entre las entidades federativas, y con la regulación del comercio con otros Estados extranjeros.

2. El Congreso de la Unión está expresa y exclusivamente facultado para legislar en materia de comercio, incluyendo la facultad para legislar en todo cuanto impida que existan restricciones en el comercio entre las entidades de la Federación, como ocurre con el

[134] http://gaceta.diputados.gob.mx/, tomado de la Exposición de Motivos de la iniciativa con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales, a cargo de la Diputada Sheyla Fabiola Aragón Cortés, del Grupo Parlamentario del PAN.

establecimiento de marcos legislativos diversos en materia de protección de datos personales en jurisdicción distinta de la federal, en la medida en que éstos puedan resultar contrarios a los lineamientos adoptados por los organismos internacionales de los cuales forma parte el Estado mexicano, y crear de hecho obstáculos o restricciones al comercio entre las entidades de la Federación.

3. La iniciativa se circunscribe en el contexto de la legislación en materia de comercio y en la intervención de esta soberanía federal para impedir el eventual establecimiento de medidas que puedan constituir obstáculos o restricciones al comercio entre las entidades de la Federación, por lo que la facultad de legislar sobre la materia que nos ocupa está expresamente reservada a la Federación, en términos de las fracciones IX, X y XXX del artículo 73 de la Constitución federal.

4. Que la iniciativa es consistente, armónica y complementaria con las disposiciones existentes en materia de protección de datos personales que esta soberanía ha expedido en la jurisdicción federal y en el ámbito del derecho administrativo, como las contenidas en relación con la protección de los datos personales por las entidades del sector público obligadas bajo la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de las cuales es garante el Instituto Federal de Acceso a la Información Pública, o las contenidas en relación con la protección de datos personales compartidas en relaciones de consumo, según lo previsto en la Ley Federal de Protección al Consumidor.

5. Que si bien es cierto que el Instituto Federal de Acceso a la Información Pública, creado por virtud de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, es

por definición la institución a cargo de la detentación y manejo de información por parte del sector público y no de los particulares, también lo es que la exigencia de razones presupuestarias, obligan a esta soberanía a tener en cuenta la conveniencia de aprovechar las instituciones existentes para dotar de eficacia al marco legal propuesto, y que sea el Instituto quien tenga las facultades para sancionar la eventual violación de las normas de privacidad en que pudieren incurrir los sujetos obligados.

6. Que en todo caso, la iniciativa deja a salvo para su regulación especial, sea que ésta competa a esta soberanía o al Ejecutivo federal por la vía reglamentaria, si las disposiciones legales pertinentes ya existieren en las leyes especiales por cada materia, los casos en que la protección de datos personales corresponda, por su naturaleza, a cuerpos normativos e institutos especiales, como lo es en materia financiera, de seguros y fianzas y otras especificadas en la misma, así como las que involucran otras entidades o dependencias del sector público en relación con funciones electorales, de seguridad nacional y demás indicadas en el cuerpo de la iniciativa.

En resumen la iniciativa busca la protección de la privacidad de los datos personales, detentados y usados por particulares; así como considera conveniente en razón de economía, que sea el propio Instituto Federal de Acceso a la información quien tenga a su cargo la función de ejecución de las disposiciones para garantizar la protección de los datos personales.

La iniciativa se presentó en la sesión del 22 de marzo de 2006 y fue turnada a la Comisión de Gobernación.

d) Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Datos Personales, a cargo del Diputado David Hernández Pérez, del Grupo Parlamentario del PRI.[135]

Esta iniciativa se sustenta en 9 principios básicos, los cuales se han integrado al cuerpo de la misma, mismos que a continuación se precisan:

A) De Información: La obligación de una persona física o moral de informar a los individuos de los propósitos para los que recolecta información personal; de cómo contactar a quién colecta dicha información con respecto de preguntas o quejas sobre dicha práctica; los tipos de entidades a los que se pudiera revelar dichos datos, si ello aplicare, y las opciones y medios por los que un individuo puede limitar el uso y publicación de dicha información.

B) De Elección: Principio que busca asegurar que los individuos sobre los que un tercero posea información, puedan ejercer sus derechos sobre la misma. Esto incluye el derecho de un individuo a decidir sobre el uso de su información y el derecho de decidir sobre cómo y si su información es compartida con terceros, cuando esta acción es incompatible con el propósito original de la autorización.

C) De Transferencia: Principio que garantiza la capacidad de asegurar que la información no es transmitida fuera del control del responsable, sin salvaguardar sus derechos y manteniendo el mismo nivel de protección establecido cuando se recolectó.

D) De Seguridad: Principio que asegura que las entidades que tratan los datos personales de los individuos, utilizan medidas razonables de

[135] http://gaceta.diputados.gob.mx/, tomado de la Exposición de Motivos de la iniciativa con proyecto de decreto por el que se expide la Ley Federal de Datos Personales, a cargo del Diputado David Hernández Pérez, del Grupo Parlamentario del PRI.

seguridad de carácter físico, técnico y organizacional para salvaguardar la integridad de dichos datos.

E) De Integridad: Principio que incluye el derecho de los individuos a asegurar que su información, que obre en posesión de un tercero, es precisa, completa y actual, teniendo el derecho de rectificarla en caso necesario.

F) De Acceso: Principio que otorga a los individuos el derecho a conocer su información personal que obre en posesión de un tercero.

G) De Cumplimiento: Principio que busca que las personas que tratan datos personales cuenten con las estructuras necesarias para dar cumplimiento con la Ley y que exista una autoridad encargada de velar por su cumplimiento y efectiva aplicación.

H) De Conocimiento El derecho del individuo de conocer con que finalidades son recolectados sus datos personales mismos que deben ser adecuados, pertinentes y no excesivos conforme a los fines planteados y las leyes respectivas.

I) De Consentimiento: El derecho del individuo de permitir el uso de sus datos personales que obren en bases de datos de un tercero y de igual forma poder solicitar la cancelación de su información en dichas bases de datos.

En términos generales, la iniciativa propone un sistema de protección de datos personales a cargo del IFAI quien tendrá las funciones de interpretación y vigilancia de la Ley; establece que habrá obligación para todo aquel que maneje datos personales de hacer del conocimiento del titular de los mismos, un aviso de

privacidad que debe atender ciertos principios, que le conceden al ciudadano el control de sus datos, lo que le otorga certidumbre.

La iniciativa se presentó en sesión del 23 de febrero de 2006 y fue turnada a la Comisión de Gobernación.

e) **Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales, a cargo del Senador Antonio García Torres, del Grupo Parlamentario del PRI.**

El proyecto propone la Creación del Instituto Federal de Protección de Datos personales, en manos del sector privado. Busca proteger los datos personales, sin que ello afecte la actividad económica del país.

Considera la necesidad de que el control de la aplicación de esta Ley quede en manos del nuevo Instituto Federal de Protección de Datos Personales, como un órgano distinto al IFAI.

La iniciativa se presentó en sesión del 02 de febrero de 2006 y se turnó a las Comisiones Unidas de Gobernación y de Estudios Legislativos.

f) **Iniciativa con proyecto de Ley Federal de Protección de Datos Personales, a cargo del Diputado Jesús Martínez Álvarez, del Grupo Parlamentario CONVERGENCIA.**

Esta iniciativa tiene como objetivo garantizar la protección de los datos personales que se encuentren contenidos en documentos, archivos, registros, bancos de datos, ya sean de carácter público o privado.

Busca asegurar los derechos de las personas a la vida privada y a la intimidad, así como el acceso a la información que sobre las mismas se registre, en términos de

los artículos 6, 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos.

La iniciativa se presentó en sesión el 01 de diciembre de 2005 y turnada a la Comisión de Gobernación.

g) Iniciativa con proyecto de Ley Federal de Protección de Datos Personales, a cargo del Diputado Luis Miguel Barbosa Huerta, del Grupo Parlamentario PRD.[136]

Esta iniciativa parte de que el derecho a la privacidad es uno de los derechos humanos esenciales que dan contenido y substancia a la dignidad humana.

El texto del proyecto se estructura con una parte general y otra especial. En la parte general se establecen las normas delimitadoras del ámbito de aplicación de la ley, principios reguladores del acopio, registro y uso de datos personales y, sobre todo, garantías de los titulares o afectados.

En la parte especial del proyecto se propone la creación del Registro Nacional de Protección de Datos, como el ente encargado de coadyuvar en el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Cabe mencionar que hace referencia especial respecto de la regulación de la denominada acción de acción de protección de datos personales o *habeas data* (exhibe el dato) como una garantía de toda persona para acceder a la información y a los datos que sobre sí misma obren en registros privados u oficiales; para

[136] http://gaceta.diputados.gob.mx/, tomado de la Exposición de Motivos de la iniciativa con proyecto de decreto por el que se expide la Ley de Protección de Datos Personales, a cargo del Diputado Miguel Barbosa Huerta, del Grupo Parlamentario del PRD.

conocer el uso que se haga de los mismos y de su finalidad, y para solicitar la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegalmente sus derechos.

La iniciativa se presentó en sesión el 06 de diciembre de 2001 y turnada a las Comisiones Unidas de Gobernación y Seguridad Pública.

- **PROTECCIÓN DE DATOS PERSONALES EN ARCHIVOS PRIVADOS.**

A manera de referencia, cabe señalar que actualmente en México, sólo existe una Ley de Datos Personales (Colima) de junio de 2003. Entre los motivos que existían para la creación de esta ley, es que se consideraba que en nuestro país, la protección de los ciudadanos estaba incompleta. Que era necesario promover y facilitar el uso de las tecnologías de la información y brindar al ciudadano una protección adecuada contra el posible mal uso de la información que le concierne, sin que esto implique la creación de obstáculos para el desarrollo de las nuevas tecnologías en México.[137]

Esta ley establece como finalidad la protección y la garantía de los derechos de protección de los datos de carácter personal como un derecho fundamental. El ámbito de aplicación de la ley es para los datos de carácter personal que sean registrados en cualquier soporte que permita su procesamiento, con algunas excepciones (archivos detenidos por personas físicas para uso personal, los archivos clasificados por la ley y los archivos penales).

En su artículo 3° también define lo que se entiende como dato de carácter personal: *son los datos relativos a las personas físicas o morales que de manera directa o indirecta puedan conectarse con una persona específica. Se incluyen a manera ilustrativa, los datos representados en forma de texto, imágenes, datos*

[137] Véase la exposición de motivos de la Ley.

biométricos como la huella digital, datos sobre el DNA de las personas o cualquier otro que corresponda intrínsecamente a una persona determinada.

Los datos deberán ser obtenidos por medios lícitos, previamente a su obtención el interesado deberá ser informado y sus datos podrán ser almacenados en un tiempo limitado. Además, el titular de los datos dispone de un derecho de acceso mediante la figura del *habeas data,*[138] que es una acción procesal para solicitar información de sus datos de carácter personal, impugnar actos o decisiones privadas que deriven de las informaciones obtenidas de datos de carácter personal, y para solicitar que se realicen gratuitamente las rectificaciones y cancelaciones de los datos de carácter personal que les correspondan; y en su caso, recibir una indemnización proporcional al daño o lesión ocasionada en sus bienes o derechos.[139]

Para controlar la efectiva aplicación de esta Ley, en Colima se creó una autoridad denominada Comisión de Protección de Datos. Es necesario informar a la misma de toda creación de archivos de datos de carácter personal[140], ya sean privados o públicos. Es lo que se conoce como la declaración de la creación de archivos.

Esta ley es un ejemplo para la protección de datos de carácter personal, sin embargo, a nivel federal aún no contamos con una ley en la materia.

5. RETOS FRENTE A LA LEGISLACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

El reconocimiento en la Constitución Política de los Estados Unidos Mexicanos del derecho de protección de datos personales implica la inminente expedición de una

[138] La cual ya existe en otras legislaciones latinoamericanas como es el caso de Argentina.
[139] Véase el artículo 7° de la Ley de Protección de Datos de Colima.
[140] Excepto aquellos que están exentos en la Ley, como es el caso de los archivos de datos para fines privados.

Ley en la materia, la cual tendrá por objetivo particular regular el tratamiento de los datos personales en el sector privado.

En ese sentido, se presentan diversas interrogantes que habrán de definirse en la nueva ley ¿qué autoridad deberá encargarse de garantizar la protección de datos en el sector privado? ¿Qué modelo de protección deberá adoptar México? ¿Deben las legislaciones estatales y la federal que protegen datos en archivos públicos modificarse? ¿La Ley de Protección de Datos Personales debe regular de manera específica a todos los sectores? O bien, ¿Debe una legislación de esta naturaleza establecer los principios y dejar que se expida normatividad secundaria que regule cada sector –salud, educación, comercio, entre otros?

En razón de lo anterior, se hará un breve análisis respecto de los elementos que deben ser considerados para la expedición de una ley en esta materia.

5.1 ORGANO GARANTE DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES.

Podrá observarse que hay países en los que el órgano que protege datos personales de igual forma tiene encomendada la tarea de garantizar el derecho de acceso a la información gubernamental y otros países en los que el órgano que garantiza la protección de datos personales es diverso al que se encarga de garantizar el derecho de acceso a la información.

En el caso de España, la Agencia Española de Protección de Datos Personales tiene la naturaleza de ser un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada; actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Tiene como objetivo velar por el cumplimiento de la legislación sobre la materia, en especial en lo

relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.[141]

En Argentina la Dirección Nacional de Protección de Datos Personales es el órgano de control creado en el ámbito nacional, para la efectiva protección de los datos personales. Tiene a su cargo el registro de las bases de datos, instrumento organizado a fin de conocer y controlar las bases de datos. Asesora y asiste a los titulares de los datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos. En este sentido, tiene por función investigar si la base de datos denunciada da cumplimiento o no a los principios que establece la ley y las disposiciones reglamentarias.[142]

En el caso del Reino Unido, el órgano encargado de la protección de la información personal es la Oficina del Comisionado de Información (ICO)[143], cuya naturaleza es la de ser un órgano público independiente del Reino Unido establecido para fomentar el acceso a la información oficial y proteger la información personal. Lleva a cabo este cometido promocionado prácticas recomendables, dictaminando en quejas que reúnen las condiciones exigidas, proporcionando información a personas físicas y organizaciones y tomando las medidas adecuadas cuando se infringe la ley.

Su objetivo general es básicamente hacer pública la información oficial a menos que existan buenas razones para no divulgarla y asegurar que se proteja adecuadamente la información personal.

---

[141] https://www.agpd.es/portalweb/conozca/naturaleza/index-ides-idphp.php, Agencia Española de Protección de Datos Personales.
[142] http://www.jus.gov.ar/dnpdpnew/, Dirección Nacional de Protección de Datos Personales.
[143] http://www.ico.gov.uk/about_us/other_languages/espanol/overview_what_we_do.aspx

La oficina del Comisionado es independiente del Gobierno Británico, y su Comisario, es oficialmente nombrado por la Reina, está bajo las órdenes directas del Parlamento y su función es principalmente nacional, aunque también tiene algunas responsabilidades de protección de datos a nivel internacional.

ICO se encarga de hacer cumplir y supervisar la Ley de Protección de Datos, la Ley de Libertad de Información, las Regulaciones para la Información Medioambiental y las Regulaciones de Comunicaciones Electrónicas.[144]

Por otra parte y a manera de comparación, es de importancia destacar el caso de Canadá, toda vez que son órganos distintos los que regulan estos aspectos, por una parte el que garantiza la protección de datos personales y por otra el que garantiza el derecho de acceso a la información.

La Oficina del Comisionado de Privacidad de Canadá (OPC), está dividida en 2 partes, la que se hace cargo de la información personal en poder de departamentos del gobierno federal y agencias (Privacy Act); y por otra parte lo relativo al sector privado (*Personal Information Protection and Electronic Documents Act (PIPEDA)*,).

La misión de la oficina del comisionado es proteger y promover el derecho a la privacidad de los individuos; esta oficina trabaja de forma independiente a cualquier otra parte del gobierno, para investigar las quejas de los individuos respecto del sector público federal y el sector privado. En el caso del sector público, los individuos deberán quejarse acerca de cualquier tema especificado en la sección 29 del Privacy Act. Esta acta plica para la información personal en poder de instituciones del gobierno de Canadá.

Por otra parte, La Comisión de Información de Canadá es un organismo autónomo, no adscrito a ningún poder estatal; está dotado de independencia de

[144] Idem.

criterio, autonomía presupuestaria y facultades de delegación de atribuciones; asimismo, la Ley le otorga competencias sancionadoras en contra de cualquier persona que destruya, falsifique ó esconda información pública.

Tiene amplias facultades para establecer su organización interna: el artículo cincuenta y ocho de la Ley de Acceso a la Información determina que cualquier funcionario público o empleado, que sea necesario para el adecuado funcionamiento de los deberes del Comisionado de la Información, será puesto a su disposición con base en las disposiciones de la Ley de Trabajadores del Servicio Público "58. Such officers and employees as are necessary to enable the Information Commissioner to perform the duties and functions of the Commissioner under this or any other Act of Parliament shall be appointed in accordance with the *Public Service* Employment Act".

El Comisionado de Acceso a la Información goza de fuero: el artículo sesenta y seis ordena que ningún procedimiento penal o civil puede iniciarse en contra del comisionado o en contra de cualquier persona que actúe bajo su representación o dirección. Es importante señalar que ningún otro titular de autoridad fiscalizadora del derecho a la información que esté supeditado a la administración pública, goza de este mecanismo de protección jurídica.

> *66. No criminal or civil proceedings lie against the Information Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith in the course of the exercise or performance or purported exercise or performance of any power, duty or function of the Commissioner under this Act.*

El comisionado de la información es propuesto por el titular del poder ejecutivo (Governor in Council), previa aprobación del Senado y de la Cámara de los Comunes; asimismo su destitución debe ser ordenada ambas cámaras y ejecutada por el titular del ejecutivo.

Tiene facultades para tramitar las quejas presentadas ante denegación de información pública y compeler a las autoridades administrativas a publicar y entregar cualquier tipo de documento o información.[145]

En nuestro país existe el Instituto Federal de Acceso a la Información Pública (IFAI), el cual fue creado mediante decreto publicado en el Diario Oficial de la Federación el 24 de diciembre de 2002, como un Organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propios; con autonomía operativa, presupuestaria y de decisión, encargado fundamentalmente de promover el ejercicio del derecho de acceso a la información; resolver sobre la negativa de las solicitudes de acceso a la información y la ***protección de los datos personales*** en poder de las dependencias y entidades.

De lo anterior se desprende que existe en nuestro país un órgano que regula la protección de datos personales en posesión de órganos federales pero no en archivos privados, situación que con excepción de Colima se repite en todas las entidades federativas. De esta suerte, el legislador tendrá que determinar si en nuestro país debe crearse un órgano que garantice la protección de datos personales en todo el sector privado o bien, si se otorgan estas facultades al IFAI, organismo que en el ámbito federal conoce de esta materia respecto de los órganos del Estado.

5.2. MODELOS DE PROTECCIÓN DE DATOS PERSONALES

En este apartado se pretende reflejar que no en todos los países se ha adoptado el mismo régimen de protección de datos personales, por lo que otra de las disyuntivas a las que se enfrentará el legislador es la que se refiere a determinar qué modelo de los que se señalan a continuación debe adoptar nuestro país.

---

[145] Tomado de **Autoridades reguladoras independientes en materia de acceso a la información, en http://www.juridicas.unam.mx/publica/rev/decoin/cont/9/art/art4.htm**

a) MODELO EUROPEO.

Para poder garantizar una libre circulación de personas, de mercancías y de capitales, es necesario tener políticas de armonización de las leyes de los estados miembros de la Unión europea, las directivas europeas forman parte de las mismas.

En la Unión Europea existe desde hace algunos años un esfuerzo para proteger directa o indirectamente este tipo de datos personales. En este caso existe una protección bien establecida, diversas directivas, tienden a eliminar los obstáculos a la circulación de los datos personales. Para eliminar estos obstáculos, el nivel de protección de los derechos y libertades de las persona, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los estados miembros.

En consecuencia busca armonizar las legislaciones que protegen los datos personales y ofrecer un nivel máximo de garantía a los ciudadanos de la Unión Europea. Su objetivo es garantizar la protección de los derechos y libertades de las personas físicas; en particular, de su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. En este tenor, son los Estados Miembros y la Comisión europea los encargados de informarse en qué casos estiman que un país tercero no asegura un nivel de protección adecuado.

b) MODELO AMERICANO.

En Estados Unidos existe un arsenal jurídico en materia de privacidad pero esto no ha impedido que se desarrollen alternativamente políticas de autorregulación.

Estas últimas se han dado sobre todo para proteger a los sectores más sensibles de la sociedad como son los enfermos, y la protección y la confidencialidad de la información que proporcionen menores de edad a sitios de Internet.

En lo que corresponde a las bases de datos personales del sector público, se aplica el *Freedom of Information Act;* para el proceso de datos de los consumidores la *Fair crédito Reporting Act.* Finalmente es la *Finantial Information Privacy Protection Act,* la que regula la protección de los datos personales propios al sector financiero.

En conclusión, en Estados Unidos no existe un derecho general relativo a la protección de la vida privada, sino una multitud de legislaciones federales y estatales que pueden aplicarse. Es lo que va más acorde con su concepto de *privacy*, que en ocasiones lo traducimos como el respeto a la vida privada pero que es diferente. Este término, utilizado por primera vez como un derecho a estar solo, surgió como una respuesta para frenar el poder de intromisión desarrollado en la época por la prensa estadounidense. Este concepto tiene su fundamento legal en la Enmienda IV de la Constitución, al tenor del cual se hace referencia tanto a la libertad de los bienes personales como de la propia persona.[146]

c) MODELO CANADIENSE.

Canadá ha preferido seguir con políticas de regulación sobre privacidad y protección de datos con la adopción de un marco regulatorio, donde no existe una excesiva regulación de gobierno pero tampoco una libre autorregulación de las empresas. Canadá combina la legislación conjuntamente con políticas de autorregulación que responden a las necesidades individuales de los nacionales.

Por medio de las mismas protege los derechos de los consumidores y de los ciudadanos canadienses sin imponer obstáculos a las empresas.

La vía escogida por Canadá es la del consenso entre todos los interesados, como son los empresarios, las asociaciones de consumidores, las organizaciones no

[146] Se puede leer esta decisión en www.supremecourtus.gov/opinions/02pdf/01-729.pdf

gubernamentales, los académicos y los ciudadanos. Es el caso de *"The Personal Information Protection and Electronic Documents Act", PIPED Act* de abril de 2000.

Se trata de una ley federal que establece estándares mínimos de protección a la privacidad en el sector privado. En el caso de que alguna de las provincias que integran Canadá no cumpliese con los requisitos de esta *Act*, el gobierno puede desconocer esta ley local y por ende la misma quedaría sin validez jurídica.[147] Y sería la *PIPED Act,* la ley federal, la que se aplicaría directamente.

5.3. ALCANCES DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES.

En este sentido habremos de analizar qué será lo más apropiado para regulación de la protección de datos personales en nuestro país; es decir si lo más conveniente es que nuestro país tenga una Ley con marco de aplicación en todos los sectores (educativo, salud, bancario, seguridad, etc.) o bien si sería más adecuado proponer la creación de una ley que abarque o señale de manera general los principios aplicables a los diversos sectores y permitir que la normatividad secundaria regule de manera específica cada sector.

Al respecto y atento a las diversas propuestas de Leyes de Protección de Datos Personales, es evidente que el modelo más conveniente de adopción para el Estado Mexicano es el que maneja el modelo canadiense, toda vez que en nuestro país existe como órgano garante de la protección de datos en poder de entidades públicas, el Instituto Federal de Acceso a la Información (IFAI) quien bien podría asumir la responsabilidad del tratamiento de los datos personales en archivos privados.

[147] http://www.privcom.gc.ca/legislation/02_06_01_e_asp

Asimismo, es importante precisar que resulta más conveniente la expedición de una Ley Federal de Datos personales de aplicación nacional en razón de que se debe unificar la tutela de este derecho en todo el territorio nacional y en consecuencia evitar que exista un tratamiento distinto en cada entidad federativa respecto al mismo derecho fundamental.

Por otra parte, cabe destacar que al expedirse la Ley de Protección de Datos Personales se proporcionará certeza jurídica a los titulares de los mismos, ya que se garantizará su debido uso y transmisión.

Asimismo, al expedirse una ley de esta naturaleza atendiendo a los principios internacionales, el país se verá favorecido en sus relaciones comerciales primordialmente y de cualquier otra índole, ya que al cumplir con los estándares de seguridad se verá fortalecido como Estado y será más competitivo.

Es importante hacer notar que la tarea que tiene nuestro legislativo no es nada sencilla, pues al buscar expedir una ley en esta materia, deberá ser muy preciso y meticuloso para no perjudicar a los titulares de la información.

Finalmente, cabe hacer mención que recientemente en marzo del presente año, la Comisión de Gobernación, aprobó por mayoría el dictamen por el cual se expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares, donde satisface los elementos básicos que garantizan la protección de los datos personales: principios, derechos, procedimientos, definición de autoridades reguladora y garante.

CONCLUSIONES

PRIMERA: Intimidad es el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con la libertad de decidir a quién se le da acceso al mismo, según la finalidad que persiga, que impone a todos los demás la obligación de respetar y que solo puede ser obligado a develar en casos justificados cuando la finalidad perseguida por la develación sea licita.[148]

SEGUNDA: El Derecho a la Intimidad es un derecho fundamental del ser humano. A lo largo de la historia de la civilizaciones, la intimidad así ha sido considerada, todos los individuos tenemos conciencia de ello, por la propia naturaleza del hombre. El derecho a la intimidad tutela la zona más reservada de la persona, referida a la conciencia de sí mismo como ser humano libre en su ámbito moral e intelectual.

TERCERA: El Derecho a la Vida Privada, es un derecho fundamental de la personalidad, consistente en la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público; se caracteriza por ser un derecho esencial del individuo, un derecho extrapatrimonial, y un derecho imprescriptible e inembargable.

CUARTA: El derecho a la vida privada se manifiesta a través de la realización de actividades y comportamientos en un ámbito estrictamente personal, de amistad o familiar en que el sujeto decide desarrollar su existir, preservando esa esfera de su existencia del conocimiento general.

---

[148] Meján, Luis Manuel, *"El Derecho a la Intimidad y la Informática,* Porrúa, México, 1994, p. 87

QUINTA: La Declaración Universal de Derechos Humanos, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, el Pacto Internacional de Derechos Civiles y Políticos, la Declaración Americana de los Derechos y Deberes del Hombre, reconocen la personalidad jurídica y vida privada de las personas, lo cual es un primer esfuerzo que da pauta al reconocimiento del derecho a la protección de datos personales.

SEXTA: La Convención Americana sobre Derechos Humanos (Pacto de San José), amplía la esfera de protección de los derechos esenciales del hombre; al reconocer el derecho de rectificación de información.

SÉPTIMA: En el artículo 3° de la Declaración sobre la Libertad de Expresión, así como en la Carta de Derechos Fundamentales de la Unión Europea, se infiere que hay ya un reconocimiento de otro derecho, *el derecho a la protección de los datos personales*, que se configura como un derecho fundamental de carácter personalísimo y como un derecho autónomo.

OCTAVA: Se puede definir a la sociedad de la información como un nuevo 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 vía 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.

NOVENA: El derecho de la protección de datos está integrado por un conjunto de normas y principios que, con independencia de su fuente, son utilizados para la tutela de los diversos derechos de las personas que pudieran verse afectadas por el tratamiento (acceso, registro, elaboración, transmisión a terceros, etcétera) de datos de carácter personal.

DÉCIMA: El derecho a la protección de datos puede ser definido como la facultad conferida a las personas para actuar *per se* y para exigir la actuación de Estado con el fin de obtener la tutela de los diversos derechos que pudieran verse afectados en virtud de aquellas operaciones de tratamiento de los datos de carácter personal que les conciernen.

DÉCIMO PRIMERA: Existe una tendencia en todos los sistemas jurídicos, para homogeneizar sus principios y criterios de protección de datos de carácter personal, a fin de potenciar las interrelaciones (industriales, comerciales, administrativas, etc.) entre los pueblos a través de la transmisión segura a nivel internacional de datos; en los cuales destacan los que adoptan una legislación sectorial y por otra parte los que adoptan una legislación nacional.

DÉCIMO SEGUNDA: El derecho a la autodeterminación informativa efectivamente se construye a partir de la noción de intimidad; toda vez que ésta es la que hace referencia a la protección de los datos personales de la esfera privada.

Sin duda la sentencia del Tribunal Alemán en la que declaró inconstitucional de la ley de censo de la población (*Volkszhlungsgesetz),*se constituyó un nuevo derecho, "a la autodeterminación informativa" (*rech auf informationelle selbstestimmung)*[149] a partir del cual deriva la facultad de la persona de "*deducir básicamente por sí misma, cuándo y dentro de que límites procede revelar situaciones referentes a su propia vida".*

DÉCIMO TERCERA: El derecho a la autodeterminación informativa constituye un derecho de la personalidad cuyos caracteres propios y definidores son:

[149] No hay consenso doctrinal respecto de la correcta traducción de esta voz; la más difundida es "autodeterminación informativa", aunque algunos la traducen como "autodeterminación informática" o como "autodeterminación informacional".

1. Un ***derecho connatural*** e ***innato*** del hombre, es decir, que son adquiridos desde el nacimiento de la persona, sin necesidad de ningún otro condicionamiento especial;

2. Un ***derecho subjetivo privado,*** por que tutela el disfrute y protección de derechos de la persona frente a injerencias ajenas;

3. Un derecho un ***derecho de exclusión,*** entendido como derecho *erga omnes; a través del cual se* salvaguarda la esfera privada frente a cualquiera, debiendo tomarse como límites los derechos de los demás, el orden público y la moral.

4. Un ***derecho inherente a la persona,*** es decir, que le es propio, necesario para el pleno desenvolvimiento de su personalidad, y sin el cual la persona queda carente de su natural esencia y fundamento como individuo.

Cabe hacer mención que de su carácter inherente se desprenden las siguientes características: como ***derecho intransmisible e irrenunciable,*** entendiendo que si dicha renuncia tiene lugar, la misma será nula; ***derecho inembargable,*** atendiendo al carácter no patrimonial de este derecho, derecho ***indisponible*** e ***imprescriptible;*** en otras palabras, debe entenderse que no existe plazo para el ejercicio del mismo, su disfrute es permanente en tanto no se produce agresión o intromisión ilegítima.

DÉCIMO CUARTA: Los países económicamente más desarrollados han promulgado leyes para proteger la privacidad en relación a los datos personales, cuyos objetivos son:

1. Prevenir y eliminar violaciones a las garantías individuales con respecto a la privacidad, tales como el almacenamiento y tratamiento ilegal o incorrecto de los datos personales o la transmisión no autorizada de dichos datos; y

2. Evitar que estas regulaciones dificulten el flujo de la información, necesaria para el eficiente funcionamiento de los mercados y para el adecuado desarrollo de la economía.

Si bien dichos objetivos en apariencia son contradictorios, la experiencia internacional ha demostrado que son complementarios; por un lado permite que los datos personales, relevantes para las actividades económicas, tengan un valor en el mercado, fomentando su protección por parte de los tenedores de los mismos y por otro incrementa la confianza de los particulares en el buen uso de los mismos, lo que permitirá la conformación de mejores bases de datos y desarrollo económico entre los países que legislen su regulación..

DÉCIMO QUINTA: La primera generación de leyes de protección de datos centró la organización de sus mecanismos de protección en torno a dos principios básicos: la autorización previa a la constitución de los bancos y ficheros de datos y su control e inspección posterior.

DÉCIMO SEXTA: La segunda etapa podríamos calificarla como aquella en la que, de forma generalizada, los Estados asumen la necesidad de brindar una protección efectiva a las personas frente al uso automatizado de sus datos.

Esta segunda generación de leyes se caracteriza por el aseguramiento de la calidad de los datos; es decir, se regularon los derechos individuales de los afectados para que de manera efectiva, controlaran la información personal que les concierne y, por otro, el establecimiento de cláusulas específicas para la protección de la información considerada sensible, por su inmediata incidencia sobre la intimidad y el ejercicio de las libertades de cada uno de los individuos.

DÉCIMO SÉPTIMA: La tercera generación de leyes de protección de datos se caracteriza por armonizar el principio de libre circulación internacional de datos personales con la defensa de los derechos y las libertades de las personas

DÉCIMO OCTAVA: La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental tiene entre sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, es decir, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental obliga a proteger los datos personales que obren en archivos de los órganos federales.

DÉCIMO NOVENA: Se puede definir al dato personal como aquel que es relativo o propio de una persona, es decir que pertenece a la misma; en nuestra legislación dicho termino se acuñó de la siguiente forma: *" la información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales u otras análogas que afecten su intimidad".*[150]

VIGÉSIMA: Para el tratamiento de los Datos Personales deberán observarse los siguientes principios: licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión.

1. Licitud; es decir que exista justificación legal que permita la posesión de los mismos; deben haberse obtenido por medios previsto en la ley y con un objetivo especifico.

[150] Artículo 3°, fracción II de la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental, México, D.O.F., 11 de junio de 2002.

2. Calidad: El "tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea"[151].; lo que significa que se deberán mantener las medidas de seguridad necesarias para su manejo, además de que únicamente se debe requerir la cantidad de información necesaria para cumplir con el objetivo previsto, a través del personal legalmente facultado para ello.

3. Acceso y corrección; lo que implica que siempre deberá garantizarse al titular de los datos personales el acceso y en su caso la corrección de los mismos, para de esta forma mantener su información como cierta.

4. De información, es decir que se obliga a quien maneja los datos a manifestar la razón jurídica y causa que ha dado lugar a su recopilación, así como el objetivo o fin para los cuales han sido obtenidos.

5. Seguridad; es decir que se deberá garantizar que estos se encuentren debidamente resguardados avalando de esta forma la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales.

6. Custodia y cuidado de la información; esto es que el resguardo y conservación de los datos personales dependerá de quienes estén debidamente autorizados y facultados para ello conforme a la ley.

7. Consentimiento para la transmisión, es decir que para que exista transferencia de datos, deberá contarse con la aprobación del titular de los mismos para hacerlo, salvo en los casos expresamente previstos en las leyes.

---

[151] Artículo séptimo, Lineamientos de Protección de Datos Personales, D.O.F., 30 de septiembre de 2005.

VIGÉSIMA PRIMERA: Respecto al órgano garante del Derecho de Protección de Datos Personales y tomando en consideración que existen países que contemplan figuras donde un mismo órgano es el encargado de garantizar el acceso a la información y la protección de datos personales; y por otra parte aquellos donde son figuras distintas los que se encargan de garantizar ambos derechos; es necesario considerar que para el caso de nuestro país resultaría conveniente que el Instituto Federal de Acceso a la Información Pública fuera el encargado de garantizar la protección de datos personales en archivos privados; en razón de ser la institución más especializada en el tema aunado a que por razones de economía resultaría más conveniente.

VIGÉSIMA SEGUNDA: Por lo que hace al modelo de protección de datos personales y derivado de la breve reseña de los más representativos resulta más apropiado considerar el Modelo Canadiense, ya que resulta ser un modelo moderado a diferencia del Europeo que es más restrictivo y del Americano que indica ser más permisivo. La idea de tomar un modelo de protección de datos personales deberá ser acorde a las necesidades nacionales, considerando que sería de más favorable la expedición de una Ley Federal de Protección de Datos Personales que establezca los estándares mínimos de protección de los datos en sector privado y cada uno de los estados hiciera lo propio en su respectiva competencia. Para el caso de que las legislaciones locales en la materia fueran insuficientes, se podrá recurrir a la legislación federal para la resolución de cualquier controversia; con lo que se estaría al principio de jerarquía de leyes.

VIGÉSIMA TERCERA: Por lo que hace al contenido de la Ley Federal de Protección de Datos Personales en archivos privados, resulta más apropiado considerar la expedición de un ordenamiento que abarque o señale de manera general los principios aplicables a los diversos sectores (educativo, salud, bancario, seguridad, etc.), ya que de ninguna manera se puede dar el mismo tratamiento a los datos; se deberá permitir que la normatividad secundaria regule de manera específica cada sector.

VIGÉSIMA CUARTA: Finalmente, es importante destacar que la finalidad de la expedición de una Ley de Protección de Datos Personales, primordialmente debe buscar garantizar el derecho humano y constitucional del derecho a la privacidad y permitir al titular su acceso, rectificación, cancelación y oposición de sus datos personales, tal como plantea en el artículo 16 constitucional. Con esto nuestro país estaría acorde a las disposiciones Internacionales como la OCDE y la Unión Europea y consecuentemente estará en posibilidad de realizar sus actividades comerciales y de cualquier otra índole de manera más eficiente, lo que le hará más competitivo a nivel mundial.

BIBLIOGRAFÍA

BURGOA ORIHUELA, Ignacio. *Las Garantías Individuales*. Porrúa, México, 2005.

CABEZUELO ARENAS, Ana Laura. *Derecho a la Intimidad*. Tirant lo Blanch, Valencia 1998.

CAMPUZANO TOMÉ, Herminia. *Vida Privada y Datos Personales: Su protección Jurídica frente a la Sociedad de la Información*. Madrid, 2000.

CARBONELL, Miguel. *La Libertad de Expresión en la Constitución Mexicana*. IIJ-UNAM, México, 2003.

CONCHA CANTÚ, Hugo A., LÓPEZ AYLLÓN, Sergio (Coord.). *Transparentar al Estado: La Experiencia Mexicana de Acceso a la Información*. IIJ-UNAM, México, 2004.

FERNÁNDEZ RODRÍGUEZ, José Julio. *Lo Público y lo Privado en Internet: Intimidad y Libertad de Expresión en la Red*. IIJ-UNAM, México, 2004.

FERREIRA RUBIO, Delia Matilde. *El Derecho a la Intimidad*. Editorial Universidad, Buenos Aires, 1982.

GARRIGA DOMÍNGUEZ, Ana. *La Protección de Datos Personales en el Derecho Español*. Universidad Carlos III de Madrid, Dykinson, 1999.

HERRÁN ORTIZ, Ana Isabel. *La Violación de la Intimidad en la Protección de Datos Personales*. Dykinson. Madrid, 1999.

MEJÁN, Luis Manuel. *El Derecho a la Intimidad y la Informática*. Porrúa, México, 1994.

MURILLO DE LA CUEVA, Pablo Lucas. *El Derecho a la Autodeterminación Informativa*. Tecnos, Madrid, 1990.

OVILLA BUENO, Rocío. *La protección de los Datos Personales en México.* Porrúa, México, 2005.

PUCCINELLI, Oscar Raúl. *Protección de Datos de Carácter Personal.* Astrea, Buenos Aires, 2004.

REBOLLO DELGADO, Lucrecio. *El Derecho Fundamental a la Intimidad.* Dykinson. Madrid, 2000.

SALAZAR UGARTE, Pedro (Coord.). *El Derecho de Acceso a la Información en la Constitución Mexicana. Razones, Significados y Consecuencias.* IIJ-UNAM-IFAI, México, 2008.

VILLANUEVA, Ernesto. *Derecho de la Información, Conceptos Básicos.* Quipus, CIESPAL, Quito, Ecuador 2003.

VILLANUEVA, Ernesto, LUNA PLA, Issa (editores). *Derecho de Acceso a la Información Pública. Valoraciones Iniciales.* IIJ-UNAM, México, 2004.

VILLANUEVA, Ernesto. Temas Selectos de Derecho de la Información. IIJ-UNAM, México, 2004.

WARREN Samuel/ BRANDEIS Louis. *El Derecho a la Intimidad.* Edición a cargo de Benigno Pendás y Pilar Baselga, Madrid, 1995.

Legislación

Constitución Política de los Estados Unidos Mexicanos

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Lineamientos de Clasificación y Desclasificación de Información de las Dependencias y Entidades de la Administración Pública Federal.

Lineamientos de Protección de Datos Personales.

Páginas de Internet

www.ifai.org.mx

www.un.org/es/documents/udhr/

www.cinu.org.mx/onu/documentos/pidcp.htm

https://cidh.oas.org/Basicos/Basicos1.htm

https://cidh.oas.org/Basicos/Basicos13.htm

http://www.europarl.europa.eu/charter/pdf/text_es.pdf

http:/gaceta.diputados.gob.mx/

https://www.agpd.es/portalwebAGPD/index-ides-idphp.php

http://www.jus.gov.ar/dnpdpnew/

http://www.juridicas.unam.mx/publica/rev/decoin/cont/9/art/art4.htm

http://www.ico.gov.uk/

www.supremecourts.gov.opinions/02pdf/01-729.pdf

http://www.privcom.gc.ca/legislation/

http://www.ordenjuridico.gob.mx/