UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

TRABAJO DIRIGIDO

"CREACIÓN DE UNA NORMA DE PROTECCIÓN DE DATOS INFORMÁTICOS Y EL DERECHO A LA INTIMIDAD"

POSTULANTE : PABLO WALDO MURILLO AREVALO
TUTORA : Dra. KARINA INGRID MEDINACELI DÍAZ

LA PAZ – BOLIVIA
2010

INDICE

ASPECTOS GENERALES

I SECCIÓN DIAGNOSTICA.

CAPITULO I

MARCO HISTORICO
INTIMIDAD INFORMÁTICA Y DATOS PERSONALES

CAPITULO II
MARCO TEORICO
SOCIEDAD DE INFORMACIÓN TECNOLOGÍAS E INTIMIDAD

CAPITULO III
MARCO JURIDICO

II SECCIÓN PROPOSITIVA.

CAPITULO I

LA PROTECCIÓN DE DATOS COMO UN ANUEVA OBLIGACIÓN RESPONSABILIADES Y PRICIPIOS GENERALES

CAPITULO II
OBJETO Y AMBITO DE APLICACIÓN

CAPITULO III
LEGITIMACIÓN

CAPITULO IV
DERECHOS DE LOS CIUDADANOS

CAPITULO V
ESTABLECIMIENTO DE MEDIDAS DE SEGURIDAD

III SECCION CONCLUSIVA

INDICE DE SIGLAS

CPE	Constitución Política del Estado
NCPE	Nueva Constitución Política del Estado.
LOPD	Ley Orgánica de Protección de Datos (España)
DUDH	Declaración Universal de los Derechos Humanos.
ADSIB	Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
TIC´s	Tecnologías de Información y Comunicaciones.
UNESCO	Naciones Unidas Para la Educación la Ciencia y la Cultura.
NN.UU.	Naciones Unidas
D.L.	Decreto Ley.
S.C.	Sentencia Constitucional.
ARCO	Acceso, Rectificación y Cancelación y oposición

DEDICATORIA

A Dios; única fuente de luz y verdad en el camino de la justicia y cuyo fin último es la libertad.

AGREDECIMIENTOS

A mis padres Gaid y Esperanza ejemplo de eterna bondad y sabiduría.

RESUMEN

Estando a fines de la primera década del siglo XXI, nadie puede negar que el majo de la información personal de forma automática a través de los distintos sistemas de información, forman parte indisoluble de nuestras vidas y al mismo tiempo casi de forma inconsciente nos preguntamos: ¿Qué pasa con los nuestros datos personales en manos de instituciones públicas y privadas?, acaso a veces no pensamos que la información que nos piden ¿es excesiva para los fines con que son recogidos?, nuestra información ¿estará protegida por la ley?, ¿de qué medios dispongo para evitar intromisiones?.

Apenas son algunas preguntas que nos hacemos y se han convertido en el centro de debate a nivel internacional a través de importantes organizaciones como la Organización de las Naciones Unidas Para la Educación la Ciencia y la Cultura (UNESCO) con el Monitor de Privacidad y Acceso a la Información, La red Iberoamericana Para la Protección de Datos o la Agencia para el Desarrollo de la Sociedad de Información en Bolivia, pero no es menos cierto que la mayoría de ciudadanos y autoridades de nuestro país, así como muchos de la región no contamos con un *cultura para proteger nuestros datos,* simplemente proporcionamos esta información a cualquier que nos pida, ya sea para una simple encuesta o por *exigencia* de algún funcionario, lo cual es muy serio.

Recordemos que los datos personales tienen un valor económico y de seguridad civil y que sin una adecuada protección, estamos expuestos a ser víctimas de un robo de identidad, robo de tarjetas bancarias o ser candidato de un secuestro. Es por esto que deberíamos saber con absoluta certeza *"donde"* se encuentran nuestros datos de carácter personal, *"quien"* trata dichos datos y *"para qué"* se utilizan.

Haciendo un recorrido por nuestra legislación nos encontramos que ésta en materia de protección de la información personal y el derecho a la intimidad se encuentra muy dispersa y en varias áreas es inexistente, confirmando la falta de Políticas de Estado que incorporen componentes regulatorios de las tecnologías de información y comunicación como parte de la evolución de la Sociedad de Información.

Por ello abordamos; cuáles son los principios rectores en materia de protección de datos y los derechos de acceso, rectificación, cancelación y oposición que nos asisten y que sin embargo a pesar de las garantías constitucionales son insuficientes o poco efectivas.

ASPECTOS GENERALES

1. FUNDAMENTACIÓN DEL TEMA.

Hoy es indudable que el impacto de las tecnologías de información y comunicación en nuestra sociedad contemporánea merece un estudio desde distintos ámbitos como el Sociológico, el Económico o el Derecho, en este sentido se vienen produciendo una autentica revolución en cuanto al régimen jurídico internacional que concierne al tratamiento de datos de carácter personal.

Nuestro país no se encuentra exento del impacto tecnológico; si bien hasta ahora los bancos de datos se iban estructurando de forma manual o semi-mecaninizada en soporte de papel y la transmisión de estos se hacía por medios físicos tradicionales, todo esto está cambiando dando paso de éste tratamiento; a las tecnologías informáticas para: almacenar, gestionar, modificar y transmitir la información a velocidades cada vez mayores y sin límites de distancias.

A la par de tal desarrollo podemos referirnos también a los efectos que producen y que podría afectar a los ciudadanos con respecto a derechos fundamentales; específicamente los concernientes a la privacidad e intimidad de las personas.

La recolección de datos en si mismo tienen en apariencia un carácter inofensivo, cuando se usa esta información para sacar conclusiones individuales, trae consigo un inminente riesgo de afectación a la intimidad personal y/o familiar que si bien gozan hoy en día de protección constitucional en Artículo 21 inciso 2. “a la privacidad, intimidad, honra, honor, propia imagen y dignidad”. Requiere de un tratamiento especial para su protección real.

2. DELIMITACIÓN

a) Delimitación Temática .

Si bien el Derecho a la Intimidad puede interferir con varios derechos fundamentales como el Derecho a Información, libertad de prensa y otros, en nuestro país hoy en día contamos con la protección constitucional de este derecho reconocido como un Derecho Civil en el Artículo.21 numeral 2, elemento que no estaba contemplado en la anterior Constitución, por esto cobra una mayor importancia y a efectos de ésta investigación es materia de estudio del Derecho Informático.

b) Delimitación Espacial

Hoy en día dado el desarrollo vertiginoso de la información, la protección de datos y el derecho a la intimidad son considerados un problema complejo que traspasa las fronteras de cualquier país, por ello será necesario concentrar nuestra atención en la legislación de nuestro país y confrontarla con las dos fuentes importantes de protección de datos informáticos y la intimidad; la norteamericana y europea.

c) Delimitación Temporal

Considerado el problema de la protección de datos informáticos como un fenómeno relativamente nuevo, considero que el tema de estudio puede abarcarse a partir de 19 de marzo de 2002 con la creación de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) al 31 de septiembre de 2010.

3. PLANTEAMIENTO DEL PROBLEMA

¿Cómo garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor e intimidad personal y familiar, en lo concerniente al tratamiento de sus datos personales?

4. DEFINICIÓN DE OBJETIVOS:

a) Objetivo general

Proponer bases legales mínimas para la protección del derecho fundamental de la intimidad en lo concerniente al tratamiento de información de datos personales mediante una normativa especial.

b) Objetivos específicos

1. Demostrar la inexistencia de normativas que regule la protección del derecho fundamental de intimida personal en lo concerniente a tratamiento de datos informáticos personales.
2. Observar qué efectos puede tener la tecnología informática sobre la seguridad y privacidad personal.
3. Establecer los principios esenciales sobre la protección de datos informáticos.

5. ESTRUCTURA METODOLÓGICA Y TÉCNICAS DE INVESTIGACIÓN MONOGRÁFICA

Por las características del tema es necesario el uso del método deductivo y comparativo para determinar las debilidades y encontrar modelos de regulación y protección del derecho fundamental de la intimidad .

I SECCIÓN DIAGNOSTICA.

CAPITULO I

MARCO HISTORICO
INTIMIDAD INFORMÁTICA Y DATOS PERSONALES

1. ANTECEDENTES HISTÓRICOS DEL DERECHO A LA INTIMIDAD.

Para introducirnos en el tema del Derecho a la intimidad debemos retroceder a veinticinco años antes de que se aprobara la Tercera Enmienda de la Constitución de Estados Unidos de América (1789) y fue William Pitt[1] quien dijo: «El hombre más pobre puede, en su choza, oponer resistencia a las fuerzas de la Corona. Puede ser una choza frágil; su techo puede desmoronarse; el viento puede entrar allí, lo mismo que la tormenta y la lluvia; pero el rey de Inglaterra no puede entrar; todas sus fuerzas no se atreverán a cruzar el umbral de la choza en ruinas».

La Corona inglesa se valía de los «*general warrants*» para requisar papeles y domicilios sin ninguna restricción, principalmente en sus colonias de América del Norte para descubrir literatura política sediciosa y para aplicar las leyes sobre impuestos. Quince años antes de la Revolución Americana creció la resistencia a estas requisas intempestivas, y esta experiencia determinó que, una vez conquistada la independencia, se aprobara la Cuarta Enmienda como parte del *Bill of Rights* de 1789.[2]

[1] Británico estadista *Sir William Pitt* 1er Conde de Chatham, 1708- 1778, *habla del derecho de un inglés a vivir seguro en su hogar (1763) E*l famoso comentario de Pitt resume lo que mucha gente consideraba hasta hace poco como la esencia de la privacidad: el derecho de vivir tranquilos en nuestra casa, a salvo de los poderes del gobierno. En los Estados Unidos, la Cuarta Enmienda a la Constitución establece el concepto de que la gente tiene derecho de vivir segura en su hogar, y esta idea se refuerza con la disposición de la Tercera Enmienda que prohíbe al ejército alojar a sus soldados en viviendas particulares.

[2] "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas". LII Legal information Institute Wex: Español [En línea] <http://topics.law.cornell.edu/wex/espanol/legislaci%C3%B3n_sobre_pesquisas_y_confiscaciones_cuarta_enmienda.> [Consulta: 20/10/2010]

Otro antecedente de gran importancia en la literatura americana se encuentra en la obra de los abogados Louis D. Brandeis y Samuel D Warren «*The Right of Privacy*»[3], que en la clase de 1877 de la Harvard Law School habían sido el primer y segundo alumnos, respectivamente. En esta obra publicada el 15 de diciembre de 1890 recapitulaba los derechos individuales, y «...después vino el reconocimiento de la naturaleza espiritual del hombre, de sus sentimientos e intelecto. Gradualmente se ensanchó el ámbito de éstos derechos y ahora el derecho a la vida significa el derecho a gozar de la vida, el derecho a estar solo; el derecho a la libertad incluye el ejercicio de otros derechos civiles, y el término «propiedad» ha llegado a incluir toda forma de posesión, intangible y tangible... Mucho después vino una protección cualificada del individuo contra ruidos y olores molestos, contra el humo, el polvo y la vibración excesiva. Así se entendió que sólo una parte del dolor, el placer y el provecho de la vida está en las cosas físicas. Pensamientos, emociones y sensaciones demandan reconocimiento legal...».

En 1928 llegó a la Corte Suprema de Estados Unidos el caso Olmstead vs. The United States, sobre escuchas y registro de conversaciones telefónicas de comerciantes en alcohol, planteado como violación a la Cuarta y Quinta Enmiendas. El *Chief Justice* William Howard Taft, ex presidente de Estados Unidos, escribió una larga opinión según la cual «no había evidencia de compulsión para inducir a los imputados a hablar por teléfono. Ellos hacían transacciones comerciales contínua y voluntariamente, sin saber que se les interceptaba. Nuestra consideración -decía- debe limitarse a la Cuarta Enmienda... Esta se refiere a requisa de cosas materiales (la persona, la casa, sus papeles y efectos personales). La descripción del mandamiento necesario para que los procedimientos sean legales, es que debe especificarse los lugares a ser requisados y las personas o cosas a secuestrarse. La Cuarta Enmienda no prohíbe lo que se ha hecho acá. No hubo requisa. Se obtuvo la evidencia mediante el uso del sentido del oído. No se penetró en las casas ni en las oficinas de los imputados... La opinión razonable es que quien instale en su casa un instrumento telefónico con cables que lo conectan, se propone proyectar su voz hacia quienes están afuera, y que los cables afuera de su casa y los mensajes que conducen no están protegidos por la Cuarta Enmienda. Quienes

[3] Su obra constituye la base esencial y punto de inicio de numerosos estudios relacionados con la intimidad y fuente de inspiración para el desarrollo de leyes que regulan los conflicto de los medios de comunicación o la tecnología frente a la vulneración del derecho a la intimidad.

interceptaron las voces proyectadas no estaban en la casa de ninguno de los que hablaban por teléfono...»[4].

La argumentación de Taft parecía contundente. Pero el *Justice* Louis D. Brandeis, en uno de los más célebres votos disidentes, se apartó de la interpretación literal de la Cuarta y Quinta Enmiendas. «... El incidente ilícito de la invasión de la intimidad del teléfono -decía- es mucho peor que el de la correspondencia. Cuando se intercepta una línea de teléfono, se invade la intimidad de las personas en ambos extremos de la línea... Aún más, la interceptación de la línea telefónica de un individuo envuelve la interceptación del teléfono de todas las otras personas que él puede llamar, o que le pueden llamar... Los autores de nuestra Constitución se propusieron crear condiciones favorables a la búsqueda de la felicidad. Nos otorgaron, contra el gobierno, el derecho a ser dejados solos, el más amplio de los derechos y el más valioso del hombre civilizado. Para protegerlo, toda intromisión injustificable del gobierno en la intimidad del individuo, cualesquiera sean los medios utilizados, debe considerarse una violación de la Cuarta Enmienda. Y el uso como prueba, en un procedimiento criminal, de hechos revelados por esa intromisión, debe considerarse una violación de la Quinta Enmienda».

Lógica como era la opinión de Brandeis, no fue asumida por la Corte Suprema sino cuarenta años más tarde, cuando en 1967 abandonó su enfoque de la invasión material y en dos decisiones importantes (en los casos Berger y Katz versus United States) admitió que el espionaje electrónico constituye «requisa» en el sentido de la Cuarta Enmienda, cuyo propósito es - dijo la Corte- proteger a las personas, y no simplemente los lugares. [5]

2. CONTENIDO DEL CONCEPTO DE INTIMIDAD.

Hasta el advenimiento de la Revolución francesa, la intimidad carecía de preponderancia en cuanto ella no pasaba de ser un privilegio de los nobles o de los monjes, o de quienes de alguna forma se retiraban de la vida en comunidad, y se constituía en aspiración burguesa sólo por afán imitativo de obtener privilegios, antes pertenecientes a la clase alta. Por ello, la

[4] Morris Ernst and Alan V Schwarts (1962) "**The right to be let alone"**, The Macmillan Company Ney York, p.178, Cit. por Pablo Dermizaky (2000) "El Derecho a la Intimidad" Ius Et praxis Vol 6.No.001. Universidad de Talca Chile

[5] Ibídem

privacidad no pasaba de ser un derecho individualista basado, a su vez, en el derecho de propiedad: la propiedad era condición para acceder a la privacidad.

Como se expuso anteriormente se produce un cambio a fines del siglo XIX en Estados Unidos con Warren & Brandeis en su obra, (el Derecho a la Intimidad) donde se podrá sustentar el derecho a impedir la publicación y la reproducción de las llamadas obras literarias y artísticas" y definen la intimidad como el derecho a la soledad, "*the rigth to be let alone*".

En tal sentido, la palabra intimidad se usa como sinónimo de privacidad, entendido éste último como "el derecho a salvaguardad su intimidad, especialmente sobre los datos relativos a sus personas de que disponen las entidades públicas y privadas."[Larousse; 2009]. En el mismo sentido es definida la palabra inglesa privacy *como "*el estado o condición de estar libre de ser observado o perturbado por otras personas: *su regreso a la privacidad de su propia casa"[Oxford; 2001]*

En la actualidad se tiende a incluir dentro de la Intimidad, la *facultad de ejercer control sobre las informaciones que pueden afectar a las personas*, idea proveniente del derecho norteamericano que posteriormente, ha pasado al derecho europeo, y que tiene hoy una gran importancia en orden a determinar el alcance de ésta en la sociedad tecnológica en pleno desarrollo.

Ahora bien, la esfera de intimidad de la persona reconoce por una parte, una proyección hacia el exterior del individuo que conduce a la protección de valores como la inviolabilidad del domicilio y el secreto de las comunicaciones privadas en todas sus formas como señala la N.C.P.E. Art.25. I;[6] dentro de las cuales se entiende de manera extensiva a los bienes materiales pertenecientes a la persona; por otra parte, existe una proyección hacia el interior del ser humano que se traduce en la protección de bienes propiamente inmateriales como lo son la autoidentificación personal, la honra, el honor la propia imagen, dignidad entre otros (NCPE Art.21). Ambas cualidades deben quedar comprendidas por el concepto de intimidad, sin perjuicio de existir otras que son aún mayormente subjetivas, por así decirlo "más

[6] Artículo 25. I. Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial.

íntimas" y que están presentes en la persona, aún cuando esta ni siquiera lo sepa conscientemente: la filiación, el derecho al mínimo vital (derecho a la dignidad).

Pretender definir el Derecho a la Intimidad, en la actualidad, podría presentar ciertas dificultades en cuanto depende muchas veces del entorno en el cual éste se desarrolla y hasta donde está dispuesto a llegar las intromisiones en los asuntos de los individuos.

Por lo tanto la Intimidad puede ser considerada en su contenido como provista de los siguientes aspectos:

1) *Privacidad de las informaciones*, o Protección de Datos, Habeas data**,** que impedirá la publicidad de informaciones que pertenecen a la esfera de intimidad de las personas; se plantean problemas entre el Derecho a la Intimidad y el Derecho a las Informaciones. [Gareca; 2004]

2) *Privacidad corporal,* relativa a la protección debida sobre las manipulaciones genéticas, informaciones médicas y similares; plantea debates en torno a la bío-genética, prestaciones médicas, secreto médico y otros.

3) *Privacidad de las comunicaciones,* destinada a proteger los correos, correos electrónicos, teléfonos y en general toda forma de comunicación; plantea los debates sobre necesidades públicas versus privacidad (combate al terrorismo, a la droga); también el problema de la publicidad no requerida (spamming), la utilización indebida de materiales y documentos cubiertos por patentes industriales y propiedad intelectual. [Suárez;1997]

4) *Privacidad territorial,* que recae sobre el medio doméstico y laboral, incluyendo la protección a las grabaciones, filmaciones, intromisiones, etc. Origina problemas en torno a la informática y otras áreas como el derecho laboral (utilización de correos y redes en horario de trabajo, privacidad de sus comunicaciones en computadoras propias de la empresa).

3. DEL DESARROLLO INFORMÁTICO.

No es el objetivo hacer un estudio detenido de la influencia que la Informática ha tenido y tiene en el medio social e individual de todos los países, ni siquiera entrar al extenso campo de la llamada "Informática Jurídica", sino que trataremos de señalar el impacto que la misma ha tenido y tiene dentro del campo jurídico cuando se presenta como un fenómeno que afecta derechos del hombre como, la intimidad individual y familiar.

Desde la muy remota época en que el hombre comenzó a tratar de comunicarse con sus semejantes, mediante sonidos, hasta el presente en que se comunica al mismo tiempo con millones de personas, han transcurrido millones de años, dentro de los cuales ha cruzado por las etapas de la comunicación grabada en piedra a través de las representaciones gráficas, luego con el perfeccionamiento del lenguaje y su expresión en signos y más tarde, luego de la invención del alfabeto, en letras que, posteriormente, fueron capaces de difundirse a través de un nuevo invento que conmocionó la cultura, como fue la imprenta.

Hoy es necesario reconocer que en este siglo el avance de la comunicación entre los hombres ha provocado un evidente impulso de la cultura y, a la vez, ha ampliado aún más las diferencias tecnológicas entre los países desarrollados y aquellos a los que se llama peyorativamente subdesarrollados o en vías de desarrollo.

Comenzaremos entregando un concepto que pueda orientarnos en el estudio de la influencia de la Informática y el delito, para ello nos entrega una noción el jurista italiano Vittorio Frosini, quien dice: "*La Informática puede definirse globalmente como la tecnología de la información; es decir, no sólo su tratamiento técnico por medio de un instrumento como ocurría ya con las distintas formas de registro mecánico, con los archivos mecanográficos de funcionamiento manual, con los aparatos criptográficos; sino su trasposición a un proceso puramente intelectual de control, de movimiento combinatorio y de traducción a nueva fórmula, que fue desenvuelto por el logicario*".

La esencia de la Informática radica en su automatización, en tanto puede reproducirse, corregirse y transmitirse automáticamente. Para este efecto necesita una máquina, cuya

"*parte material de la computadora, llamada hardware, debe distinguirse claramente de la parte meramente lógica del procedimiento de elaboración, de la que se denomina software, y que por eso se podría denominar logicario. Es esta la que da lugar a la denominada inteligencia artificial del computer, y que constituye una prótesis electrónica de la inteligencia humana, por medio de la cual se puede identificar, seleccionar y comparar las informaciones recibidas a una velocidad superior a la del pensamiento humano, cuyo proceso se refleja o mejor se reproduce en el logicario*".[7]

Es un hecho indiscutible que la tecnología de la información se ha universalizado en forma tal que afecta la vida del ser humano, individual o socialmente considerado, tal es así que existen conductas delictivas que utilizan la Informática para consumar delitos y otras conductas irregulares que, no estando tipificadas como delitos, provocan daños de gran peligrosidad en el ámbito económico y de seguridad humanos. En efecto, debemos aceptar que ciertos delitos actualmente constan en las leyes penales y que pueden cometerse a través de la Informática, pero hay gran número de conductas a las que difícilmente se las puede "tipificar" en alguna de las previsiones legales penales que hoy existen, pese a que lesionan importantes bienes jurídicos que merecen la protección del Estado.

En lo que respecta al tema de la protección de la que tiene toda persona a la vida íntima y a la de su familia, que está reconocido universalmente como uno de los derechos humanos que merece especial protección. Nuestra Constitución Política, en el artículo 21, numeral 2 establece como derechos civiles, la privacidad, intimidad, honra, propia imagen y dignidad. Por su parte, en el Código Civil en su artículo 18 (Derecho a la Intimidad), el Código Penal artículo 18 (violación de correspondencia y papeles privados). Es indudable que las anteriores previsiones jurídicas confieren cierta seguridad de que se encuentra protegido en su "intimidad", y que ninguna persona -salvo casos especialmente previstos- puede alterar o menoscabar dicha intimidad.

[7] Revista Jurídica, Facultad de Jurisprudencia y Ciencias Sociales y Políticas Universidad Católica de Santiago de Guayaquil [En línea]; <http://www.revistajuridicaonline.com/index.php?option=com_content&task=view&id=398&Itemid=43> [Consulta: 26/09/2010].

En este punto la Informática ha trastrocado los puntos de vista, antes la intimidad era un derecho que se caracterizaba por ser un derecho que no permitía el ingreso de la acción extraña en el ámbito de la esfera personal, pero con el desarrollo de la Informática, y con la constitución de los "bancos de datos" o "banco de memoria", el criterio ha dado un giro de ciento ochenta grados, pues actualmente se acepta que ese derecho a la privacidad, es el derecho que se le concede a las personas para que tengan acceso a los bancos de datos, para controlarlos cuando se hace referencia a la propia persona, y aun para solicitar la rectificación de la información que se considera falsa, o "sensible", y demandar la eliminación de la misma. [Gareca; 2004]

¿Cómo es que se llegó a ese cambio? La respuesta es; debió a la Informática, con ella se registran los datos personales, unas veces con fines sociales, otras con fines utilitarios y si bien en apariencia tienen un carácter inofensivo pueden poner en peligro el consagrado derecho a la intimidad al "memorizar" todas las referencias de la persona, hasta en sus manifestaciones más recónditas, con el grave peligro de su difusión masiva, de su transferencia para fines que no fueron los que motivaron la captación de los datos individuales.

Esta información que se le ha suministrado a la memoria de la computadora, la cual la mantiene por tiempo indefinido, pudiendo tener acceso a ella, no sólo una persona, sino algunas autorizadas, y otras no autorizadas, así como la información puede ser transferida a un número indefinido de otras computadoras, ante este escenario se elaboraron en distintas legislaciones distintos proyectos destinado a la protección de los bancos de datos, así por ejemplo se tomaron medidas de control con diferentes criterios por ejemplo la legislación americana opta por un control difuso o la legislación europea por un control centralizado pero en ambos casos también se diferencias los datos entre públicos y privados denominados "datos sensibles", entre datos públicos referidos al nombre, residencia, número de identidad personal, profesión, estado civil, lugar de trabajo, etc. y datos privados, como la religión, la opinión política, el estado de salud, su posición económica, etc. pero que aún hoy se encuentran en debate.

De lo dicho se llega, pues, a la conclusión de que las personas, cuyos datos individuales, sin discriminación entre públicos y privados, están dentro de un banco de datos, se encuentran indefensas en cuanto al resguardo de su intimidad y la de su familia, pues el manipuleo de la información puede provocar graves lesiones a los intereses, no sólo del individuo, sino también de toda su familia.

4. LA INFORMÁTICA Y LOS DATOS PERSONALES

En la actualidad existen diversos textos que hablan acerca del impacto de la informática en las libertades individuales y, especialmente, en la denominada esfera de privacidad de las personas y que son consideradas sensibles al desarrollo tecnológico, así por ejemplo encontramos criterios que afirman que "...la informática no es una técnica políticamente neutra: la informatización participa de una dinámica propia que favorece el reforzamiento de los centros de poder (instituciones del Estado y grandes empresas) en perjuicio de las libertades individuales."[Suárez;1997]

Un autor y docente francés reconocido por sus estudios de Medios de Comunicación y Sociedades Francis Balle distingue en la historia de la comunicación posterior a la invención de la imprenta, tres grandes quiebres o rupturas. La primera ruptura corresponde a la que denomina como la *era de las comunicaciones a distancia*. Época que comienza con la invención del telégrafo eléctrico en 1837 y que culmina, pasando por la invención del teléfono, con la aparición de la radio y la televisión transmitida, ambas, por medio de ondas hertzianas.

Una segunda ruptura, se produce a partir de los años cincuenta con el *paso de la electrónica a la microelectrónica*, proceso que se produce gracias a los circuitos integrados y, luego, a los microprocesadores. Esta época se caracteriza porque junto al desarrollo de la informática, la instalación de fuentes de cables y de satélites, expande a escala planetaria la presencia de la radio y la televisión.

Pero, finalmente, la ruptura más impresionante en esta historia de las comunicaciones, es la que comienza a producirse entre los años 1985 y 1990, y que es llamada desde 1991-1992,

tanto en Japón como en los EE.UU., la "*era de la comunicación global"* (llamada por otros autores como la sociedad de la información). Esta nueva y singular etapa se caracteriza porque es la informática la que gobierna los universos por mucho tiempo separados de lo audiovisual, la teledifusión y las telecomunicaciones.[8]

Ante esto la pregunta esencial es, ¿Como la tecnología podría influir en la esfera de la intimida?, considero que se puede responder a esta desde distintos ángulos, en primer lugar nos encontraríamos primero con la *adaptación* como necesidad de la sociedad y el Derecho de encontrar un equilibrio entre el desarrollo de las nuevas tecnologías y procesamiento de datos personales informáticos, un segundo ángulo será *El Control de Tensión,* dado que las tecnologías y la informática en particular presentan dos aristas en toda sociedad, por un lado supone el ideal para la recolección, tratamiento y el proceso de información de datos de carácter personal, pero también supone una verdadera pesadilla en cuanto al surgimiento de nuevas prácticas delictivas dejando a los ciudadanos vulnerables por el tratamiento sensible de datos considerados de carácter personal y privado, un tercer aspecto a considerar será *la persecución de la finalidad,* si consideramos, excluidos de una visión catastrofista del desarrollo tecnológico y asumimos las posturas que propician su control democrático para el resguardo de las libertades como obligación del Estado. Es dentro de esta perspectiva como debemos situar el tema de la libertad frente al fenómeno informático, en este sentido encontramos por ejemplo en el artículo 19 numeral tercero del Pacto de Derechos Civiles y Políticos que deja claro que estas libertades comportan deberes y responsabilidades especiales y que deben ser sometidas a ciertas restricciones, siempre por medio de la ley, en el mismo sentido se expresa la D.U.D.H. en el artículo 12 "nadie será objeto de injerencias en su vida privada, su familia o correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o taques".

Por lo que vemos la influencia de la informática a cambiado los tiempos y distancias en cuanto a la actividad de registro de datos personales; y si bien no sólo es el Estado quien realiza esta labor de registro, censos periódicos y acumulación de información para los más

[8] Francis Balle (1994) **"Medies et sociétés"** Montchrestein , Paris, p 17, Cit. Por Christian Suárez Crothers (1997) " Informatica, vida Privada y los Proyectos Chilenos Sobre Protección de Datos" en: *Ius et praxis:* Talca; Universidad de Talca-Facultad de Ciencias Jurídicas y Sociales; Año 3 N° 1. Pp.321-360.

variados fines, como los que se realizan a través de las instituciones educacionales o de salud, los datos recopilados por la policía o los servicios de inteligencia del Estado y las Fuerzas Armadas y, en fin, a través también del registro cada vez más intenso que realizan las empresas privadas en su afán de competencia, de información y de predominio en los mercados, registro que alcanza a los deudores del comercio y de la banca. Es así que ésta actividad de registro afecta la esfera de privacidad de los individuos. Un sinnúmero de datos son utilizados por los más diversos operadores, a veces sin que existan regulaciones adecuadas que permitan un control personal y jurídico de los mismos, sin que las legislaciones regulen o contemplen instancias de control como una forma de garantía institucional frente a la utilización de estos datos y a su incorporación en registros a partir de los cuales es posible compararlos, confrontarlos y levantar un perfil de la personalidad no aceptado por las personas.

En nuestro país es indudable que esta situación que hoy es estimada como usual y que ha dado lugar a problemas de seguridad y protección de la intimidad y protección de datos se han creado algunas instituciones como el ADSIB (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia) y la Red Iberoamericana de Protección de Datos a generar proyectos en pro de la regulación de las TIC´s. Para El Mejoramiento del Estado y Su Relación con y la Sociedad.

CAPITULO II

MARCO TEORICO
SOCIEDAD DE INFORMACIÓN, TECNOLOGÍAS E INTIMIDAD

1. LA NUEVA SOCIEDAD DE LA INFORMACIÓN.

Hoy el termino *sociedad de la información* puede entenderse como aquella en la cual las tecnologías que facilitan la creación, distribución y manipulación de la información, juegan un papel importante en las actividades sociales, culturales y económicas. La noción de sociedad de la información ha sido inspirada por los programas de los países industrializados. Se encuentra en el centro de los debates de la denominada *brecha digital.*

Esta sociedad de la información es vista como la sucesora de la sociedad industrial junto a otros términos similares utilizados como sociedad post industrial, sociedad post moderna o sociedad del conocimiento.

Aun cuando no existe un concepto mundialmente aceptado de lo que se llama sociedad de la información, la mayor parte de los autores acuerdan en que alrededor de 1970 se inició un cambio de la manera en que las sociedades funcionan. Este cambio se refiere básicamente a que los medios de generación de riqueza poco a poco se están trasladando de los sectores industriales a los sectores de servicios. En otras palabras, se supone que en las sociedades modernas, la mayor parte de los empleos ya no estarán asociados a las fábricas de productos tangibles, sino a la generación, almacenamiento y procesamiento de todo tipo de *información*. Los sectores relacionados con las tecnologías de la información y comunicación desempeñan un papel particularmente importante dentro de este esquema. [Castillo;2008]

Desde la perspectiva de la economía globalizada contemporánea, la sociedad de la información concede a la TIC´s el poder de convertirse en los nuevos motores de desarrollo y progreso. Si en la segunda mitad del S.XX los procesos de industrialización fabriles marcaron la pauta en el desarrollo económico de las sociedades occidentales que operaban bajo una economía de mercado, a principios del S. XXI se habla más bien, de las “industrias

sin Chimenea", es decir, del sector de los servicios y de manera especial, de las industrias de la información.

Muchos críticos han señalado que la llamada sociedad de la información no es sino una versión actualizada del Imperio Cultural ejercido desde los países ricos hacia los pobres, especialmente porque se favorecen esquemas de dependencia tecnológica.

Quienes están a favor de la sociedad de la información sostienen que la incorporación de la TIC´s en todos los procesos productivos ciertamente facilitan la inserción a los mercados globales, donde la intensa competencia obliga a reducir costes y a ajustarse de manera casi inmediata a las cambiantes condiciones del mercado.[Oviedo; 2010]

La sociedad de la información no está limitada a internet, aunque éste ha desempeñado un papel muy importante como un medio que facilita el acceso e intercambio de información y datos, recientemente por ejemplo los weblogs son herramientas que incentivan la creación, reproducción y manipulación de información y conocimientos.

El reto para todas las áreas del conocimiento es vivir de acuerdo con las exigencias de este nuevo tipo de sociedad, estar informados y actualizados, innovar, pero sobre todo generar propuestas y generar conocimiento, conocimiento que surge de los millones de datos que circulan en la red.
De acuerdo con la declaración de principios de la Cumbre de la Sociedad de la Información[9], llevado a cabo en Ginebra (Suiza) en 2003, "la sociedad de la información debe estar centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades

[9] Las conferencias desempeñan un papel clave para encauzar el trabajo de la ONU desde su fundación (1945), estas conferencias han situado problemas difíciles y persistentes, como la pobreza o la degradación del medio ambiente, en los primeros puestos de la lista mundial de prioridades. Han servido para moldear la opinión pública y persuadir a los líderes mundiales para que presten apoyo político sobre distintos temas que reciben atención mundial, como la pionera Cumbre Mundial a favor de la Infancia (1990),

La característica particular de la Cumbre Mundial sobre la Sociedad de la Información es su organización en dos fases: la Cumbre de Ginebra de 2003, que puso los cimientos con la Declaración de Principios y el Plan de Acción, y la Cumbre de Túnez de noviembre de 2005, que ratificó la Declaración de Principios de Ginebra mediante el Compromiso de Túnez y aprobó la Agenda de Túnez para la Sociedad de la Información, que incluye directrices para la implementación y seguimiento de la Cumbre Mundial de la Sociedad de la Información.

y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas…"[10]. Bolivia como Estado miembro originario de las Naciones Unidas desde el 14 de noviembre de 1945 no se encuentra al margen de esta nueva sociedad de información y debe asumir los desafíos que conlleva en pro de garantizar los derechos y libertades de los ciudadanos.

2. EL DESARROLLO DE LAS TECNOLOGÍAS Y LA INVASIÓN EN LA ESFERA DE LA INTIMIDAD

La pregunta esencial para abordar este punto es: ¿Por qué proteger los datos personales y su tratamiento?. La repuesta la encontramos en lo sucedido en la II Guerra Mundial con la información personal contenida en los censos poblacionales de Alemania[11] donde se evidenció que el uso indebido de datos personales generó consecuencias catastróficas. Un libro muy controversial escrito por Edwin Black "IBM y el Holocausto; La alianza estratégica entre la Alemania Nazi y la corporación más poderosa de América" sostiene que IBM mediante sus máquinas para tarjetas perforadas dotó al III Reich de capacidad de identificar a judíos, homosexuales y gitanos izquierdistas y no arios, para confiscar sus propiedades, desplazarlos hacia los ghettos y campos de concentración y finalmente exterminarlos.

Una filial de la IBM en Alemania denominada Deutch Holerith Maschinen Gesllschaft diseño una maquina "Hollerith" que permitió clasificar unas tarjetas perforadas que contenían datos personales obtenidos de los censos alemanes de 1933 y 1939. En dichos censos de recolectaron datos que comprendían desde los rasgos étnicos hasta los bienes de las personas. Esta información se incorporó en tarjetas perforadas que luego fueron procesadas en las máquinas clasificadoras permitiendo la creación de perfiles sobre personas. Con estos datos

[10] Declaración de principios Cumbre mundial sobre la sociedad de la información, Documento WSIS-03/ Geneva/4-S de 12 de mayo de 2004 [en línea] <http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-S.pdf> [Consulta: 25/09/2010]

[11] Articulo histórico publicado por Ian Trayno En el periódico "El Guardián el miércoles 23 de junio de 2004 con el título "Gitanos logran el derecho a demandar a IBM sobre el papel en el holocausto"; [en línea]: <http://www.guardian.co.uk/technology/2004/jun/23/secondworldwar.internationalnews> [Consulta: 5/10/2010]

sistematizados, se podía organizar metódicamente confiscaciones de bienes, deportaciones, reclusión en ghettos, explotación laboral y finalmente la aniquilación masiva. [12]

Así, podemos hablar en primer lugar de los peligros en relación a los derechos de la personalidad del individuo, fundamentalmente los ataques a su intimidad personal. En segundo lugar, los peligros relativos al sistema de garantías y contrapesos que caracteriza a la organización del Estado de Derecho. En 1968, por primera vez Naciones Unidas dicta una Resolución en torno a los peligros que pueden derivarse del uso de las nuevas tecnologías y la protección de los derechos fundamentales, como el honor y la intimidad. La Asamblea Parlamentaria recomendó al Consejo de Ministros estudiar los peligros que el uso de los equipos tecnológicos y científicos representaba para los derechos humanos.

De todos los aspectos nos centraremos en los peligros puestos de manifiesto y relacionados directamente con los bancos de datos que contienen información personal, sobre todo su uso a través de las redes informáticas, porque afectan de forma más visible a los Derechos Humanos en lo que se refiere al Derecho de la intimidad personal.

Queda claro que existen peligros directos para los derechos y libertades individuales y hasta ahora los bancos de datos se estructuraban de forma manual, o semi-mecanizada, en soporte papel, la transmisión se hacía por medios tradicionales, todo esto ha cambiado para encargarse las nuevas tecnologías de la información de almacenar, gestionar, transformar y reproducir la información de cualquier tipo a velocidades cada vez mayor, siendo hoy un hecho cotidiano.

Todo el proceso de informatización ha producido una serie de transformaciones tanto en la estructura social como en los comportamientos individuales, cuyo alcance final aún no podemos definir. Se han producido consecuencias de la racionalización, como son el hecho de que las máquinas desplacen a las personas de sus puestos de trabajo, en este sentido se han producido consecuencias que afectan a los ciudadanos y sus opiniones, convirtiéndose

[12] Sobre este hecho, una Corte de Apelación Suiza, decretó que IBM pudo haber ayudado a Hitler al "asesinato en masa de manera más rápida y eficiente de lo que hubiera sido posible sin su colaboración" Ian Trayno Ob. Cit.

en algo dirigible con la ayuda de los sistemas informáticos, estos sistemas permiten un control exhaustivo sobre las personas además de producir ataques a la privacidad, refiriéndonos al acopio de informaciones que forman parte de la intimidad de las personas, pero que no plantean riesgo de ataque a ésta por si solas. El problema de indefensión y violación de la conocida ya como privacidad del individuo se produce cuando se combinan estas informaciones aparentemente inofensivas, para sacar conclusiones a partir de este precipitado, que inciden directamente en el individuo, nos referimos a informaciones tales como las enfermedades sufridas durante la niñez, los ritmos de trabajo, el uso del dinero a través de tarjetas de crédito, etc. Las nuevas tecnologías permiten hacer los combinados a los que nos venimos refiriendo y pueden dar un retrato robot del candidato o candidata al puesto de trabajo, con el peligro incluso de que los datos manejados sean erróneos, o aún siendo ciertos, el resultado de su combinación no coincida con la personalidad del demandante. [Ballesteros; 2005].

Hoy por hoy, factores como la velocidad, la potencia y la capacidad de almacenamiento de los ordenadores pueden suponer una seria amenaza al derecho a la intimidad y privacidad de las personas, riesgo que se ve aumentado cuando se facilita la comunicación entre terminales separados por miles de kilómetros, y no existiendo ningún impedimento técnico para el tratamiento de los datos personales.

La privacidad debe ser considerada como uno de los valores humanos fundamentales, que sirve a los ciudadanos para mantenerse libres, el hecho de preservar nuestras privacidad es una labor importante sobre todo a la hora de recoger y utilizar la información.

2.1 El Derecho a la intimidad frente a otros derechos

El derecho a la intimidad puede interferir con otros derechos como la libertad de prensa, la libertad de información, la igualdad ante la ley y el interés general. ¿Cómo conciliar estos derechos cuando aparecen contrapuestos en determinadas circunstancias? ¿Cuál debe prevalecer en los casos en que no puedan concurrir? ¿Son inevitables esas interferencias?. Estas preguntas se plantean ahora al constituyente y al legislador, tanto como al juzgador, lo que supone estudio y reflexión para los hombres de Derecho. Suponen, asimismo, estas

preguntas que el progreso científico impulsado por el hombre, a su servicio, hiere algunos de sus atributos, como lo reconocieron la Conferencia Internacional de Derechos Humanos realizada en Teherán, en mayo de 1968 [13], y la Asamblea General de las Naciones Unidas en la "Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad"[14],de 10 de noviembre de 1975.

La interferencia resulta de un conflicto de intereses, más que de derechos: la intimidad es invadida y avasallada por razones económicas y políticas. En el primer caso, la competencia por vender más induce a los medios de información a traspasar todas las vallas, todos los límites, aun aquellos que oponen la moral y la convivencia social. En el segundo caso, el espionaje político por razones de "seguridad pública" que esgrimen los gobiernos autoritarios y pocos "democráticos", invade y destruye el derecho a la intimidad. La informática y la cibernética plantean otras formas de invasión insidiosa de la intimidad contra las cuales se tiene un arduo trabajo. Los casos anotados de interferencia se reducirían, o desaparecerían, si la información y la autoridad actuaran dentro de los límites que les señala la ley. En consecuencia, la intimidad "sólo puede ser objeto de limitaciones en guarda de un verdadero interés general que responda a los presupuestos establecidos por el Artículo 13. de nuestra Constitución "Los derechos reconocidos por esta Constitución son inviolables, universales, interdependientes, indivisibles y progresivos. El Estado tiene el deber de promoverlos, protegerlos y respetarlos".

2.2 El Derecho a la información y derecho a ser informados

Los modernos adelantos tecnológicos, incluidos el de la informática hace que la intimidad de las personas se encuentre cada vez más amenazada y uno de los medios más idóneos para atentar contra la intimidad dada su repercusión social es el ejercicio abusivo del derecho a la información; derecho que claro esta tiene un carácter absoluto por lo que habrán de fijarse ciertos límites apoyados en razones legales y motivos de carácter ético y moral un avance en torno al manejo de la información podemos encontrarla en el proyecto de Ley de

[13] "Proclamación de Teherán Proclamada por la Conferencia Internacional de Derechos Humanos en Teherán el 13 de mayo de 1968", [en línea]: <http://www.acnur.org/biblioteca/pdf/1290.pdf> [Consulta:25/09/2010]

[14] Asamblea General de la ONU Resolución 3384 (XXX), 10 de noviembre de 1975 [en línea]: <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/INST%2024.pdf> [Consulta: 25/09/2010]

Transparencia y acceso a la información pública, en su Art. 1 inciso c) Establecer normas de protección de los datos personales en posesión de las entidades del sector público. Y en cuanto a las excepciones en el Art.18 a. Relativa a la intimidad o privacidad de la persona o que estén protegidos por el secreto profesional.

Podemos observar que si bien existen intentos de regulación en torno al derecho a la información, llama la atención que se orientan más, a un control difuso de este derecho confiando en la ética de los funcionarios y la autorregulación por parte de las empresas públicas y privadas.

3. PROTECCIÓN DE DATOS PERSONALES

Como hemos considerado anteriormente el fenómeno de la tecnología trae consigo implicaciones positivas y negativas pues las computadoras, al permitir un manejo rápido y eficiente de grandes volúmenes de información, facilita le concentración automática de datos referidos a las personas, constituyéndose así en un verdadero factor de poder.

Tal es así que deben desarrollarse una normativa específica que contenga principios rectores, determinación de datos sensibles, medidas necesarias para su protección y hacer este derecho efectivo, como también establecer los derechos que asiste a cada ciudadano y las sanciones para los responsables del manejo de datos, establecimiento de un sistema de monitoreo y poner énfasis en la difusión de estos derechos y obligaciones a la población e instituciones.

3.1 Recopilación de datos personales

De manera casi generalizada en el mundo y no es la excepción nuestro país que pasada la década de los setenta y en Bolivia los ochenta, que comienzan a surgir numerosos archivos informáticos con información de tipo personal, con un conjunto mínimo de datos como filiación, fecha y lugar de nacimiento, domicilio, estado civil, etc., hasta otro tipo de datos con carácter aún más distintivo como raza, religión, inclinaciones políticas, ingresos, cuentas bancarias, historias clínicas, etc. Dichos datos, al ser recopilados en diferentes centros de acopio, como lo son los registros censales, civiles, parroquiales, médicos, académicos, bancarios, laborales y tantos otros, ya no por medios exclusivamente manuales, sino con el

apoyo de medios automatizados, provocan una gran concentración y sistematización de instantánea disponibilidad de ese tipo de información para diferentes fines. Tanto es así que al entrar en esta etapa de sociedad de la información, el mundo jurídico ha evolucionado y continúa haciéndolo en lo concerniente a la protección de esta información. Para ésta tarea se deben considerar algunos principios básicos: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; e) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; f) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. [Arango, Rueda, et al; 2005)

3.2 Destino de datos e implicaciones

Este tipo de datos no son vulnerables por si, sino según el destino del que puedan ser objeto, pudiendo ser variada. De esta forma, dichas informaciones pueden ser empleadas para fines publicitarios, comerciales, fiscales, policiales, etc., convirtiéndose en un instrumento de opresión. La variedad de los supuestos posibles de indefensión frente al problema provoca que los individuos estén a merced de un sinnúmero de situaciones que pudiera alterar sus derechos fundamentales en sociedad, provocados por discriminaciones, manipulaciones, persecuciones, asedios, etc., todo ello al margen de un control jurídico adecuado.

A veces uno tiene la sensación de que todo es una catástrofe y lo más grave es que es cierto, sin embargo puestos a analizar el origen de este derecho cuando la información se guardaba en ficheros manuales, hemos progresado. Ahora el derecho de la intimidad supera el concepto unipersonal de ser dejado a solas, y se impone la autodeterminación informática: mis datos son míos, y sólo Yo puedo autorizar su disposición porque soy el dueño.

Esa protección también se extiende más allá de nuestras fronteras. La Argentina por ejemplo ha obtenido la calificación de país adecuado para transferir datos personales por parte de la

Unión Europea. De esta manera es calificada como el quinto país del mundo fuera de la Unión Europea que ha obtenido esta calidad. El punto culminante para el otorgamiento de esta calificación fue la existencia de un órgano de control para la protección de los derechos personales de la gente.

¿Qué significa este reconocimiento en los hechos? Significa que a partir de ése reconocimiento es un país seguro para la transferencia de datos, precisamente, porque cuenta con mecanismos de protección de datos personales.

De aquí en adelante se tendría seguridad de que, en principio, hay defensas para proteger invasiones a la privacidad no autorizadas, pero lo importante a veces no es solamente tener una herramienta legal a nuestra disposición, sino conocer que existe y que podemos utilizarla. Aquí entonces se supera la distancia entre saber y poder. [Piñara; 2003]

CAPITULO III

MARCO JURIDICO

1. EL DERECHO A LA INTIMIDAD EN LA LEGISLACIÓN BOLIVIANA

1.1 NUEVA CONSTITUCIÓN POLÍTICA DEL ESTADO.

El capítulo tercero, sobre derechos civiles y políticos, sección I, **artículo 21**, establece:
Las bolivianas y los bolivianos tienen los siguientes derechos:

2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad.
De manera mucho más clara y explícita que en la anterior constitución, hace referencia a cada uno de estos derechos, recordemos que en la anterior constitución se habla solamente de dignidad, libertad, inviolabilidad de la propiedad privada y correspondencia o comunicaciones. El **artículo 22** La dignidad y la libertad de la persona son inviolables. Respetarlas y protegerlas es deber primordial del Estado.

Aquí se reafirma la obligación del Estado a defender y proteger la dignidad, de la cual se desprenden la privacidad e intimidad. El **artículo 25.I**. Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial.
II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, éstos no podrán ser incautados salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente.
III. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones o comunicaciones privadas mediante instalación que las controle o centralice.
IV. La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal.

En esa misma línea detallada de proteger los derechos de las personas y su privacidad, se establece en el Capitulo Segundo sección III, la posibilidad que todo ciudadano tienen de actuar para proteger su privacidad.

Artículo 130. I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.
II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

1.2. CÓDIGO CIVIL

Aprobada por D.L. No 12760 de 6 de agosto de 1975
El artículo 15 (Nulidad), "Son nulas toda confesión y toda manifestación de voluntad obtenidas por procedimientos lesivos a la personalidad".

El artículo 16 (Derecho a la Imagen),**I.**Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga cesar el hecho lesivo. II.Se comprende en la regla anterior la reproducción de la voz de una persona.

El artículo 17 (Derecho al Honor), Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes.

El artículo 18 (Derecho a la Intimidad) Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley,
El artículo 19 (Inviolabilidad de las comunicaciones y papeles privados), I Las comunicaciones, la correspondencia epistolar y otros papeles privados son inviolables y no

pueden ser ocupados sino en los casos previstos por las leyes y con orden escrita de la autoridad competente.

1.3 CÓDIGO PENAL

Aprobado por Ley 1768 del 18 de marzo de 1997 .

Inviolabilidad de domicilio y secretos

El artículo 298, (allanamiento de domicilios o dependencias). El que arbitrariamente entrare en domicilio ajeno o sus dependencias, o en un recinto habitado por otro, o en un lugar de trabajo, o permaneciere de igual manera en ellos, incurrirá en la pena de privación de libertad de tres meses a dos años y multa de treinta a cien días.

Se agravará la sanción en un tercio, si el delito se cometiere de noche, o con fuerza en las cosas o violencia en las personas, o con armas, o por varias personas reunidas.

El capítulo III artículo 300, (violación de correspondencia y papeles privados). El que indebidamente abriere una carta, un pliego cerrado o una comunicación telegráfica, radio-telegráfica o telefónica, dirigidos a otra persona, o el que, sin abrir la correspondencia, por medios técnicos se impusiere de su contenido, será sancionado con reclusión de tres (3) meses a un (1) año o multa de sesenta (60) a doscientos cuarenta (240) días.

Con la misma pena será sancionado el que de igual modo se apoderare, ocultare o destruyere una carta, un pliego, un despacho u otro papel privado, aunque estén abiertos, o el que arbitrariamente desviare de su destino la correspondencia que no le pertenece.

Se elevará el máximo de la sanción a dos (2) años, cuando el autor de tales hechos divulgare el contenido de la correspondencia y despachos indicados.

1.4 INVIOLABILIAD EN LA LEY DE TELECOMUNICACIONES

Esta Ley 1632 fue aprobada el 5 de Julio de 1995,

Artículo 37, capítulo IX, referido a "Inviolabilidad de las comunicaciones",

Los servicios de telecomunicaciones son declarados de utilidad pública. Salvo disposición judicial en favor de autoridad competente, queda terminantemente prohibido interceptar, interferir, obstruir, alterar, desviar, utilizar, publicar o divulgar el contenido de las telecomunicaciones.

Su intercepción sólo es posible cuando el interés público prevalece ante el privado e íntimo a través de orden judicial. Esto supone también que, además de no ser posible interrumpir o acceder a las comunicaciones privadas, no se puede difundirlas.

1.5 CÓDIGO NIÑO, NIÑA Y ADOLESCENTE RESERVA DE IDENTIDAD EN NIÑOS, NIÑAS Y ADOLESCENTES

Ley 2026 del 27 de octubre de 1999.

En el artículo 10, (reserva y resguardo de identidad), Las autoridades judiciales y administrativas tienen la obligación de resguardar la identidad de los niños, niñas y adolescentes que se vean involucrados en cualquier tipo de procesos, salvo los casos expresamente previstos por este Código. La identidad de los niños debe ser resguardada por encima de cualquier interés, salvo excepciones previstas por Ley.

Artículo 229, sección II de derechos individuales, sobre protección de registro, se establece otro tipo de reserva para los casos en los que algún niño ha tenido alguna participación.
Los organismos policiales no podrán registrar en sus archivos datos personales del adolescente que incurra en una infracción. El registro judicial de infracciones será reservado y sólo podrá certificar antecedentes mediante auto motivado.
Se trata de disposiciones que protegen los derechos de los niños, entre los que se destacan los de la personalidad, honor, honra, vida privada e intimidad.

1.6 SECRETO PROFESIONAL EN LA LEY DE LA ABOGACIA

Disposición aprobada por Decreto Ley N° 16793, durante la presidencia del General de División David Padilla Arancibia, el 10 de julio de 1979.

En artículo 10 establece la inviolabilidad de los documentos y objetos que estén en manos de abogados en ejercicio de sus funciones. Refiriéndose a dicho concepto, dice textualmente: Son también inviolables su consultorio jurídico, los documentos y objetos que le hayan confiado sus clientes para asumir su defensa, salvo previa y expresa resolución motivada de juez competente.

La excepción es definida por alguna autoridad, quien evalúa la prevalencia de intereses colectivos sobre los individuales.

El artículo 24 se refiere a la responsabilidad ética del abogado, quien está comprometido a guardar confidencialidad sobre la información que maneja en cada caso que atiende, tanto de la acusación como de la defensa.

Todo abogado, individualmente, o como miembro de una sociedad de abogados, tiene el deber de guardar el secreto profesional, que es inviolable.

1.7 LEY DE BANCOS Y ENTIDADES FINANCIERAS EL SECRETO BANCARIO

Aprobado el 14 de abril de 1993, del capítulo I, Título sexto,

El artículo 86. Las operaciones bancarias en general estarán sujetas al secreto bancario. No podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a la persona que lo representa legalmente.

El artículo 87. El secreto bancario será levantado únicamente:

1. Mediante orden judicial motivada, expedida por un juez competente dentro de un proceso formal y de manera expresa, por intermedio de la Superintendencia.
2. Para emitir los informes ordenados por los jueces a la Superintendencia en proceso judicial y en cumplimiento de las funciones que le asigna la ley.
3. Para emitir los informes solicitados por la administración tributaria sobre un responsable determinado, que se encuentre en curso de una verificación impositiva y siempre que el mismo haya sido requerido formal y previamente; dichos informes serán tramitados por intermedio de la Superintendencia.
4. Dentro de las informaciones que intercambian las entidades bancarias y financieras entre sí, de acuerdo a reciprocidad y prácticas bancarias.
5. Para emitir los informes de carácter general que sean requeridos por el Banco Central de Bolivia.

1.8 INTIMIDAD DEL PACIENTE EN EL CÓDIGO DE ÉTICA MÉDICA

Ley del Ejercicio Profesional Médico

La Ley Nº 3131 del Ejercicio Profesional Médico de fecha 8 de agosto de 2005.

Artículo 3. En el ejercicio profesional médico, inclusive en la enseñanza de la medicina, el secreto médico es inviolable salvo las excepciones previstas en la presente Ley.

Artículo 4. SECRERO MEDICO: "Toda información identificada durante el acto médico sobre el estado de salud o enfermedad del paciente, su tratamiento y toda otra información de tipo personal, debe mantenerse en secreto, inclusive después de su muerte, para salvaguarda de la dignidad del paciente".

Artículo 12 Deberes del Médico:
k) Guardar el secreto médico, aunque haya cesado la prestación de sus servicios.

Artículo 13 Derechos de Paciente:

c) La confidencialidad.
d) Secreto médico
g) Reclamar y denunciar si considera que sus derechos humanos han sido vulnerados durante la atención médica.
i) Respeto a su intimidad.

1.9 LEY DE TRANSPARENCIA EN LA GESTIÓN PÚBLICA DEL PODER EJECUTIVO Ley 28168 de 17 de mayo de 2005

ARTÍCULO 19º (PETICIÓN DE HABEAS DATA). I. Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público.

II. La petición de Habeas Data se resolverá en el plazo máximo de cinco (5) días hábiles. En caso de negativa injustificada de acceso a la información, la autoridad jerárquica competente,

adicionalmente tendrá un plazo de quince (15) días hábiles para proporcionar la información solicitada.

III. La petición de Habeas Data no reemplaza ni sustituye el Recurso Constitucional establecido en el Artículo 23 de la (anterior) Constitución Política del Estado. El interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial. *El acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa*

1.10 LEY Nº 004 LEY DE LUCHA CONTRA LA CORRUPCION, ENRIQUECIMIENTO ILICITO E INVESTIGACION DE FORTUNAS "MARCELO QUIROGA SANTA CRUZ" de 31 de marzo de 2010.

Artículo 17. (Protección de los Denunciantes y Testigos).III. El Ministerio de Transparencia Institucional y Lucha Contra la Corrupción, guardará reserva de la identidad de las personas particulares y servidoras o servidores públicos que denuncien hechos y/o delitos de corrupción y guardará en reserva la documentación presentada, recolectada y generada durante el cumplimiento de sus funciones.

Artículo 20. (Exención de Secreto Bancario para Investigación de Delitos de Corrupción).
I. No existe confidencialidad en cuanto a las operaciones financieras realizadas por personas naturales o jurídicas, bolivianas o extranjeras, en procesos judiciales, en los casos en que se presuma la comisión de delitos financieros, en los que se investiguen fortunas, en los que se investiguen delitos de corrupción y en procesos de recuperación de bienes defraudados al Estado.

1.11 LEY CONTRA EL RACISMO Y TODA FORMA DE DISCRIMINACIÓN

Ley N° 045, de 8 de octubre de 2010

Artículo 22. Protección de Testigos.- El Estado garantizará la seguridad física y emocional a la persona que denunciare delitos de racismo y discriminación. En el marco de esta ley, las autoridades públicas y funcionarios que no garanticen la protección de los testigos serán sometidos a procesos disciplinarios y sanciones con suspensión de sus cargos temporal o definitiva.

1.12 PROYECTO DE LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACION PÚBLICA

Ministerio de Justicia y Derechos Humanos CAPITULO III Información Pública

Artículo 8. (Oficial de Información).”… se creará el cargo del Oficial de Información, quien tendrá bajo su responsabilidad el proceso administrativo de acceso a la información, en la recepción de solicitudes, gestión y entrega de la información. En las entidades que por razones presupuestarias este cargo no pueda ser creado, se designará a un funcionario responsable de estas.”

2. CONVENIOS INTERNACIONALES

2.1 Privacidad en el Pacto de San José de Costa Rica

Bolivia es país signatario del “Pacto de San José” que promulgó la “Convención Americana sobre Derechos Humanos”, entre el 7 y el 22 de noviembre de 1969. Posteriormente, el Estado boliviano reconoció y ratificó la vigencia y suscripción a través de la Ley 1430 del 11 de febrero de 1993

El artículo 11, referido a la “Protección de la Honra y de la Dignidad”, ratifica que el respeto a la honra y la dignidad de las personas es irrenunciable. Protege al ciudadano de injerencias en su vida privada, su domicilio, correspondencia y agresiones a la honra y reputación.
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.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

2.2 Pacto Internacional de Derechos Civiles y Políticos de 16 de diciembre de 1966

El Artículo 17 señala numeral 1. señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida, su familia, su domicilio o correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias

2.3 Declaración Americana de los Derechos y Deberes del Hombre (1948)

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

Artículo XVIII. Toda persona puede ocurrir a los tribunales para hacer valer sus derechos. Asimismo debe disponer de un procedimiento sencillo y breve por el cual la justicia lo ampare contra actos de la autoridad que violen, en perjuicio suyo, alguno de los derechos fundamentales consagrados constitucionalmente.

3. SENTENCIAS CONSTITUCIONALES

HABEAS DATA: HOY ACCIÓN DE PROTECCIÓN DE PRIVACIDAD (NCPE)[15]

3.1 Alcance (SC 0965/2004-R)

Linea Jurisprudencial : "(...) la garantía del hábeas data, instituida en Bolivia con la reforma de la Constitución Ley 2631 de 20 de febrero de 2004(...) "(...)es una modalidad de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación". "(...)el hábeas data se define como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informática". Es una garantía constitucional que, sin desconocer el derecho a la información, al trabajo y al comercio de las entidades públicas o privadas que mantienen centrales de información o bancos de datos, reivindica el derecho que tiene toda persona a verificar qué información o datos fueron obtenidos y almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, se impida su difusión y, en su caso, se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referido a la honra, buena imagen o el buen nombre". "Partiendo de los conceptos referidos, se puede inferir que el hábeas data es una garantía constitucional por lo mismo se constituye en una acción jurisdiccional de carácter tutelar que forma parte de los procesos constitucionales previstos en el sistema de control de la constitucionalidad. Es una vía procesal de carácter instrumental para la defensa de un derecho humano como es el derecho a la autodeterminación informática". (Jurisprudencia reiterada 1511/2004-R)

[15] En materia de Habeas Data, hoy llamada Acción de Protección de Privacidad, El Tribunal Constitucional ha sentado la línea jurisprudencial para la materia en su página web [en línea]
<http://www.tribunalconstitucional.gob.bo/gpwtc.php?name=jurisprudencia&file=indiceletras&raiz=6582&eltema=> [Consulta: 26/09/2010]

3.2 Acción subsidiaria (SC 0965/2004-R)

Linea Jurisprudencial : "Tomando en cuenta sus fines y objetivos , así como la aplicación supletoria de las normas previstas por el art. 19 de la CPE, dispuesta por el art. 23 parágrafo V antes referido (hoy Art.130 NCPE), se entiende que el hábeas data es una acción de carácter subsidiario, es decir, que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que inducen a discriminaciones, y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume inmediatamente la acción solicitada. Dicho de otro modo, el hábeas data se activa exclusivamente cuando la persona demuestra que ha acudido previamente ante la entidad pública o privada para pedir la restitución de su derecho lesionado y no ha podido lograr la reparación a dicha vulneración". (Jurisprudencia Reiterada 1511/2004-R)

3.3 Dimensiones de la persona que están bajo su tutela (SC 0965/2004-R)

Linea Jurisprudencial : "(...)Las dimensiones de la persona que están bajo la tutela del hábeas data pueden sintetizarse en las siguientes: 1) El propio cuerpo, referido a la salud de la persona o de los miembros de su familia; 2) Las ideas y creencias religiosas, filosóficas, políticas; 3) La vida pasada, relacionada con el ámbito que a la persona podría generarle bochorno al estar compuesta por pasajes desagradables o ingratos; 4) La vida doméstica, relacionada con los hechos o situaciones que se producen dentro del hogar; 5) La vida familiar concerniente con el matrimonio y la filiación; 6) La vida amorosa , relaciones de amistad, la vida sexual; 7) El ámbito de las comunicaciones personales que comprende las diferentes vías de comunicación; 8) La situación económica de las personas referidas al nivel de ingreso, patrimonio, inversiones, obligaciones financieras".

3.4 Legitimación activa y legitimación pasiva (SC 0965/2004-R)

Linea Jurisprudencial : "La legitimación activa del hábeas data recae en la persona natural o jurídica -aunque el precepto constitucional no lo determina de esa manera en forma expresa, se entiende que dentro de la protección de este recurso se puede y debe abarcar tanto a las personas físicas como a las jurídicas, de quienes también se pueden registrar datos e informaciones- respecto de la cual la entidad pública o privada haya obtenido y tenga registrados datos e informaciones que le interesen a aquella conocer, aclarar, rectificar, modificar, o eliminar, y que no haya tenido respuesta favorable por la citada entidad para lograr esos extremos. La legitimación pasiva de esta acción, tomando en consideración que protege a la persona en el ejercicio de su derecho a la autodeterminación informativa contra cualquier manejo impropio de sus datos personales registrados o almacenados en bancos de datos públicos o privados, recae en el personero legal de la entidad pública o privada que tengan los archivos o bancos de datos personales de quien se sienta afectado en el ejercicio del citado derecho".

3.5 No se activa contra difusión de información por medios de comunicación social. No es medio para establecer censura previa o correctiva (SC 0965/2004-R)

Linea Jurisprudencial : "(...)En cuanto a los límites del hábeas data, es importante remarcar que, como vía procesal instrumental, protege a la persona en su derecho a la autodeterminación informática, activándose contra el poder informático. De manera que cabe advertir que existe un límite en cuanto a los alcances del hábeas data que se establece en el ejercicio de la libertad o derecho de información y libertad de expresión. En efecto, el hábeas data no se activa contra la difusión de información a través de los medios masivos de comunicación social, toda vez que este medio no es el adecuado para viabilizar el derecho de réplica por parte de un medio de prensa con relación a una información difundida que la persona considere inexacta o que agravia su derecho al honor. La honra o la buena imagen, o lesione su vida privada o íntima. Debe quedar claramente establecido que el hábeas data no es un medio para ejercer control sobre los medios de comunicación social y el ejercicio de la libertad de expresión e información, no es un mecanismo para establecer censura previa ni correctiva".

3.6 Ámbitos de protección (SC 0965/2004-R)

Linea Jurisprudencial : "(...) La protección que brinda el hábeas data abarca los siguientes ámbitos: *a) Derecho de acceso a la información o registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada*, para conocer qué es lo que se dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal; *b) Derecho a la actualización* de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona*; c) Derecho de corrección o modificación de la información o los datos personales inexactos* registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona; *d) Derecho a la confidencialidad* de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona; *e) Derecho de exclusión de la llamada "información sensible"* relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado; *f) En consecuencia, el hábeas data es una garantía constitucional que tiene por objetivo el contrarrestar los peligros que conlleva el desarrollo de la informática* en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona; y tiene por finalidad principal el proteger el derecho a la autodeterminación informática, preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios a la persona. El hábeas data tiene la función primordial de establecer un equilibrio entre el "poder informático" y la persona titular del derecho a la autodeterminación informática, es decir, entre la entidad pública o privada que tiene la

capacidad de obtener, almacenar, usar y distribuir la información sobre datos personales y la persona concernida por la información.

3.7 No procede para modificación, rectificación o adiciones de partidas en Reg. Civil (SC 1511/2004-R)

(..)de acuerdo al entendimiento jurisprudencial contenido en la SC 965/2004-R, de 23 de junio, "Tomando en cuenta sus fines y objetivos, así como la aplicación *supletoria* de las normas previstas por el art. 19 de la CPE, dispuesta por el art. 23 parágrafo V antes referido, se entiende que el hábeas data es una acción de carácter *subsidiario*, es decir, que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que inducen a discriminaciones, y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume inmediatamente la acción solicitada. Dicho de otro modo, el hábeas data *se activa exclusivamente cuando la persona demuestra que ha acudido previamente ante la entidad pública o privada para pedir la restitución de su derecho lesionado y no ha podido lograr la reparación a dicha vulneración".*

II SECCIÓN PROPOSITIVA.

CAPITULO I

LA PROTECCIÓN DE DATOS COMO UN ANUEVA OBLIGACIÓN RESPONSABILIADES Y PRICIPIOS GENERALES

1. LA PROTECCIÓN DE DATOS COMO UNA NUEVA OBLIGACIÓN.

Como observamos en desarrollo de la monografía La Protección de Datos es un hecho que ha tomado importancia producto del desarrollo de las tecnologías hoy considerado como un derecho fundamental de las personas, consagrado el derecho a la intimidad en la DUDH de 1948 en su artículo 12; el Pacto Internacional de los Derechos Civiles y Políticos de 1966 en su artículo 17.1 y en la Convención Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 en su artículo 8.1

El derecho fundamental al que hacemos referencia tiene una estrecha relación con el derecho a la intimidad y al honor, encuadrándose todos ellos dentro del artículo. 21. de nuestra actual Constitución. Este "nuevo derecho" fundamental adopta la denominación de libertad informativa o autodeterminación informática, protegiendo el "control que a cada una de las personas le corresponde sobre la información que les concierne personalmente, sea íntima o no, para preservar el libre desarrollo de la personalidad".[Gareca;2004]

Siguiendo lo establecido en el modelo de LOPD, ésta establece obligaciones básicas que se pueden resumir en:

a) Legalizar. Todos los ficheros de datos de carácter personal deberían estar inscritos y legalizados ante un organismo independiente y con autonomía administrativa y con capacidad fiscalizadora y sancionador encargado de Protección de Datos,

b) Legitimar. Todos los datos de carácter personal recogidos por una institución pública o privada, deberían contar con el consentimiento del afectado, así como cumplir una serie de principios básicos como son:

- Principio del consentimiento del afectado.
- Principio de información
- Principio de calidad de los datos

c) Proteger. Esta parte está orientada a tomar las Medidas Técnicas necesarias de Seguridad[16], que garanticen la seguridad de los datos de carácter personal, medidas que habrán de adoptarse, implementarse por la empresa o profesional que almacene estos datos. Entre estas medidas se incluye la elaboración de un Documento de Seguridad en el que se detallarán los datos almacenados, las medidas de seguridad adoptadas, así como las personas que tienen acceso a esos datos.

El cumplimiento de cada una de estas obligaciones tan sólo exige un pequeño esfuerzo de las empresas y profesionales, que junto al asesoramiento adecuado, evitará disgustos y la imposición de sanciones por ejemplo económicas.

2. IMPLICACIONES Y RESPONSABILIDADES DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Para poder tomar verdadera conciencia por parte de las instituciones de nuestro país que tratan con el manejo de Datos Personales es en la actualidad una tarea indispensable si acaso se pretende cumplir con los deberes de un Estado de Derecho y los compromisos asumidos por éste ante organismos internaciones como la Declaración de las Naciones Unidas Sobre la Utilización del Progreso Científico y Tecnológico en Interés de La Paz y en Beneficio de la Humanidad [17] o el compromiso asumido en La Declaración de la Antigua durante la

[16] El ámbito de la protección en la legislación española se encuentra en el Reglamento de medidas de seguridad (RD 994/1999, de 11 de junio) y establece tres niveles de seguridad en cuanto al grado de sensibilidad de los datos.

[17] Asamblea General de la ONU Resolución 3384 (XXX), 10 de noviembre de 1975 " …Proclama solemnemente que: **1.** Todos los Estados promoverán la cooperación internacional con objeto de garantizar que los resultados del progreso científico y tecnológico se usen en pro del fortalecimiento de la paz y la seguridad internacionales, la libertad y la independencia, así

celebración de la XII Cumbre Iberoamericana celebrada en la ciudad Santa Cruz de la Sierra en noviembre de 2003 párrafo 45[18], es así que el deber de las instituciones tanto públicas como privadas no sólo consistirá en la adaptación a una normativa vigente, sino también en la aplicación práctica de principios de protección de datos en el seno de la las instituciones, dentro de cada uno de los departamentos, involucrando a todo el personal... Las consecuencias del incumplimiento de la normativa no se quedan sólo en las sanciones de una institución, sino que van más allá y afectan a todos.

La Protección de Datos de Carácter Personal, adquiere una gran importancia desde el momento en que las consecuencias de su incumplimiento conllevan grandes responsabilidades tanto para las Institución como para el personal que trata o accede a los datos de carácter personal, es decir, se deben tomar todas las medidas necesarias para capacitación del personal encargado del manejo de los datos personales para un adecuado tratamiento de esta información sensible y evitar sanciones que si bien la ley 15/1999 de Protección de Datos española en su Titulo VII establece infracciones y sanciones económicas de hasta 600.000 de Euros para las instituciones privadas, pero no sancionadas económicamente a las públicas, estableciendo simplemente acciones disciplinarias.

Claro está que dichas sanciones no eximen de la responsabilidad civil o penal que dichos actos desencadenen. Así los recomienda el principio octavo de la Resolución 45/95, 14 de diciembre de 1990.[19]

como para lograr el desarrollo económico y social de los pueblos y hacer efectivos los derechos y libertades humanos de conformidad con la Carta de las Naciones Unidas.

2. Todos los Estados tomarán medidas apropiadas a fin de impedir que los progresos científicos y tecnológicos sean utilizados, particularmente por órganos estatales, para limitar o dificultar el goce de los derechos humanos y las libertades fundamentales de la persona consagrados en la Declaración Universal de Derechos Humanos, en los Pactos Internacionales de derechos humanos y en otros instrumentos internacionales pertinentes."

[18] **45.-** "los participante subrayan su reconocimiento de que la protección de datos personales es un derecho fundamental de las personas y destacan la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de la Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de la Comunidad."

[19] …"En caso de violación de las disposiciones de la legislación interna promulgada y en virtud de los principios enunciados, deberían preverse sanciones penales y de otro tipo así como recursos individuales apropiados."

3. PRINCIPIOS GENERALES DE LA PROTECCIÓN DE DATOS.

Las leyes sobre protección de datos se basan fundamentalmente en los mismos *principios* que regulan esta materia en la mayor parte de los Estados Democráticos. Ellos se han venido desarrollando a partir de la década de los setenta, conforme a un documento del Consejo Económico y Social, de 1972 de Naciones Unidas [20]. Ellos han sido posteriormente recogidos en la Convención del Consejo de Europa sobre *protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* de 1981 y sistematizado en la Resolución 45/95 de la Asamblea general de las Naciones Unidas de 14 de diciembre de 1990. Ellos son:

1) Principio de licitud y lealtad. La utilización de ficheros debe ser consecuente con los principios de NN.UU. sin que se puedan obtener datos por medios ilícitos o desleales. No podrán del mismo modo llevarse datos sobre matanzas, genocidios, deportaciones u otros medios semejantes.

2) Principio de exactitud. Las personas encargadas de la creación de un fichero o de su funcionamiento deberían tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completo posible a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando

3) Principio de finalidad. Los datos deben ser pertinentes al objeto y fin perseguidos. No deben ser utilizados ni difundidos – salvo acuerdo con el afectado – con otros fines. Los datos además no deben ser mantenidos sino el tiempo necesario para su objeto.

4) Principio de acceso. El interesado tiene derecho a saber si sus datos personales son conformes con el objetivo del fichero. Debe tener acceso de manera inteligible, sin demora ni gastos excesivos. Tiene derecho a las rectificaciones y destrucciones de los datos indebidos

[20] Principios rectores aplicables a los ficheros computarizados de datos personales. (Resolución 45/95 de 14 de diciembre, de la Asamblea General de las Naciones Unidas (documento E/CN.4/1990/72.20 de febrero de 1990). [En línea]: < http://www.un.org/spanish/documents/ga/res/45/list45.htm> [consulta: 20/09/2010]

(ilícitos, injustificados, inexactos). Cuando se transmitan datos tiene derecho a conocer los destinatarios.

5) Principio de no discriminación. Queda prohibida la utilización de informaciones sensibles cuyo uso pueda engendrar discriminaciones ilegítimas o arbitrarias.

6) Principio de establecer excepciones. Solo para los principios 1 y 4 si es necesario para proteger la seguridad nacional, orden público, salud o la moral pública y en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por ley.

7) Principio de seguridad. Los ficheros deben estar debidamente protegidos contra riesgos naturales y humanos (acceso no autorizado, utilización indebida de datos o contaminaciones por virus informáticos).

8) Control y sanciones. Debe existir una autoridad que controle el respeto a los principios señalados, la que deberá ser imparcial e independiente respecto de las personas u órganos responsables del tratamiento de datos y de su utilización, y con la adecuada competencia técnica. Debe además preverse las sanciones penales y de otros tipos y los recursos individuales pertinentes.

9) Flujo de datos a través de las fronteras. Cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada territorio. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, y solo en la medida en que así lo exija la protección de la vida privada.

10) Campo de Aplicación. Debe aplicarse a todos los ficheros computarizados, tanto públicos como privados y por su extensión facultativa a los ficheros manuales. Podrían también hacerse extensiva a las personas jurídicas que dispongan de información sobre personas físicas

4 PRINCIPIOS DE LA LEY 15/1999, DE 13 DE DICIEMBRE.

Debemos también, hacer mención a otros principios básicos en el tratamiento de datos automatizados de carácter personal, la Constitución de España en el Titulo Primero, Capítulo II, artículo18.4 establece: "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 tal sentido los principios recogidos por la ley 15/1999 LOPD que por su importancia detallamos a continuación son:

a) Principio de calidad de los datos

La aplicación de este principio supone que los datos de carácter personal sólo podrán recogerse para su tratamiento cuando sean **adecuados, pertinentes** y **no excesivos** para el cumplimiento de las finalidades del fichero.

b) Principio de la información en la recogida de datos

El responsable del fichero debe arbitrar la fórmula que permita informar a los afectados de determinados extremos en el momento de la recogida de los datos, de modo que esta información sea conocida por el afectado antes de prestar su consentimiento.

Sólo cuando el ciudadano ha sido informado de forma expresa, precisa e inequívoca de la finalidad de la recogida de sus datos, podrá decidir si quiere que éstos estén, o no, almacenados en un fichero y que se utilicen, o no, para una determinada finalidad.

c) Principio de consentimiento.

Este principio va íntimamente unido al anterior principio de información, y podríamos decir que es el principio legitimador de todo tratamiento. El consentimiento permite al afectado ejercer el control del uso de sus datos personales, lo que viene denominado como derecho de autodeterminación informativa.

Se establece algunas excepciones como cuando el tratamiento tenga como finalidad proteger un interés vital del interesado y éste se encuentre física o jurídicamente incapacitado para dar su consentimiento, cuando los datos figuren en fuentes accesibles al público. En todo caso, la excepción del consentimiento no exime de la obligación de informar en los términos que hemos visto en el punto anterior, relativo al principio de información, ni permite el tratamiento de cualquier dato sino únicamente aquellos que cumplan el principio de calidad (datos adecuados, pertinentes y no excesivos).

d) Principios de datos especialmente protegidos.

El tratamiento especial de determinados datos, aquellos relativos a la ideología, la afiliación sindical, la religión o las creencias, el origen racial, la salud y la vida sexual, se constituye en un principio más del tratamiento de datos personales.

La Ley Orgánica 15/1999 prevé la necesidad de proteger especialmente unos datos que, por la información a la que se refieren, pueden generar con mayor facilidad lesiones en otros derechos fundamentales, además del propio derecho a la protección de datos.

Podemos pensar que un tratamiento inadecuado de datos relativos al origen racial o a la salud, puede vulnerar el derecho a la igualdad y a la no discriminación. El derecho a la libertad de pensamiento o a la libertad religiosa, puede ser lesionado por el tratamiento de datos relativos a la ideología o las creencias sin las debidas garantías, etc. Precisamente para evitar estos peligros, la Ley establece una serie de refuerzos, con el fin de que se preste un especial cuidado en el tratamiento de estos datos, de manera que:
Prohíbe expresamente la creación de ficheros con la finalidad exclusiva de almacenar datos especialmente protegidos.

Exige el consentimiento expreso y por escrito del afectado si los datos son de ideología, afiliación sindical, religión o creencias; y consentimiento expreso cuando los datos se refieran al origen racial, la salud o la vida sexual.

Debe recomendarse que siempre que se traten datos especialmente protegidos, con independencia de cuáles sean, se procure obtener constancia del consentimiento expreso en forma escrita, puesto que recae sobre el responsable del tratamiento la carga de la prueba de demostrar que se disponía del consentimiento, con ese especial atributo de expreso.

Exige el establecimiento de medidas de seguridad de nivel alto para los ficheros que contienen datos especialmente protegidos, también llamados sensibles.

Establece que los datos personales relativos a la comisión de infracciones penales o administrativas sólo pueden ser incluidos en ficheros de titularidad de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Establece que los datos personales relativos a la comisión de infracciones penales o administrativas sólo pueden ser incluidos en ficheros de titularidad de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

No obstante todo lo anterior, la propia Ley Orgánica 15/1999 establece una excepción al consentimiento expreso y por escrito del afectado para el tratamiento de datos especialmente protegidos: cuando dicho tratamiento resulte necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

Resulta también importante el aporte que hace el autor Pedro Gareca en su obra "El Habeas data y aporta con nuevos principios para el tratamiento de datos que complementan a los anteriores, estos son:

e) El Principio de celeridad.

Ante toda solicitud de datos que formulen los titulares de los derechos, las autoridades y representantes legales de los ficheros públicos y privado; estarán obligados a conocer y decidir en plazos perentorios que no sobrepasen los 15 días las peticiones.

f) Principio de gratuidad.

Los afectados en sus derechos podrán efectuar sus peticiones a los responsables o encargados de los ficheros públicos o privados, en forma gratuita.

g) Principio al olvido.

Considerado también como un derecho donde los datos personales que hubieren cumplido con la finalidad que motivaron su cesión, o se estimaren no ser suficientes o necesarios para alcanzar esa finalidad, serán suprimidos o cancelados aún de oficio por los responsables de ficheros. Por tanto, el titular del derecho en estos supuestos y en otros que eviten el almacenamiento indefinido de sus datos (caducos u obsoletos), tiene el derecho de peticionar a la administración la cancelación de los mismos.

CAPITULO II

OBJETO Y AMBITO DE APLICACIÓN

1. BIEN JURÍDICO PROTEGIDO PARA LA NORMATIVA SOBRE PROTECCIÓN DE DATOS PERSONALES.

Consientes que hoy vivimos en una nueva era de desarrollo llamada sociedad de la información es evidente que su vertiginoso avance provoca la utilización de datos personales, que van más allá de la esfera de la intimidad, afectando la parcela de la privacidad, que convierten a la administración pública y las empresas privadas en fuentes inagotables de conocimiento e información. Este conocimiento confiere a quienes poseen la información, un poder de control y seguimiento de las diversas actividades de las personas, cuyo relacionamiento o conexión pueden incidir negativamente en los derechos fundamentales de ellas.

Por tanto, debe reconocerse que con la informatización, tanto el ámbito íntimo, privado, pueden verse fácilmente afectados, producto de un conocimiento no autorizado por el interesado, de una divulgación en que cabía guardar en reserva, o de un inadecuado tratamiento de sus datos.

Ante una amenaza de tratamiento nada ético de los datos personales, que registra y almacenan los órganos de la administración pública como privada, se sugiere el desarrollo de un nuevo derecho, siguiendo las pautas del derecho español que han creado el denominado "Derecho a la autodeterminación informativa" [21]El Objeto de una norma que proteja estas áreas sensibles de la vida intima de las personas es lo que se denomina, el Bien Jurídico Protegido. Si bien para alguna parte de la doctrina y parte de la jurisprudencia, este es un derecho que

[21] "Entendido como la libertad de la persona para determinar quién, qué y con qué ocasión pueden los entes públicos y privados conocer informaciones que conciernen a cada uno".

se deriva del derecho a la intimidad, se le ha querido configurar como un derecho fundamental autónomo, básicamente por dos razones fundamentales:

La primera indica que con el indebido uso de los datos personales en Bancos de Datos, no sólo pueden ser objeto de violación aquellas esferas de la vida privada de las personas que pueden ser protegidas mediante el derecho a la intimidad, sino que también pueden ser vulnerados derechos de otra índole que no sean necesariamente fundamentales (derechos de tipo económico, por ejemplo) que de esta manera verían disminuidas sus posibilidades de defensa. De esta forma el derecho a la autodeterminación informativa, protegería un bien jurídico distinto, el de la privacidad, que abarcaría la protección de más facetas de nuestra personalidad que quedarían bajo la salvaguardia de esta facultad.

La segunda apunta a diferenciarlas desde el punto de vista del individuo frente al derecho correspondiente, porque mientras en el derecho a la intimidad se asume un papel pasivo, no intromisión en sus asuntos privados, en el derecho a la autodeterminación informativa toma un papel activo, exige el adecuado manejo de los datos que ha decidido o le ha tocado revelar.

La Acción de Protección de Privacidad, en estricto sentido, no sería un derecho fundamental, sino que se trataría de una vía procesal pertinente para asegurar que los derechos a la intimidad o a la autodeterminación informativa sean efectivamente salvaguardados.

Mediante el ejercicio de este derecho es posible entonces materializar el objetivo de hacer valer los derechos a la intimidad o a la autodeterminación informativa, para conocer, actualizar o exigir la rectificación de las informaciones personales que reposen en ficheros o Bancos de Datos.

Para algunos, en lo que respecta a la libertad informática, el habeas data o denominada hoy Acción de Protección de Privacidad, cumple una función paralela a la que cumple el habeas corpus tratándose de la libertad personal, pues mientras en el primero se protegen aspectos internos como la intimidad, la dignidad, o la autodeterminación, en el segundo se preservan aspectos externos como el derecho a la locomoción.

2. ÁMBITO DE APLICACIÓN ¿QUÉ DATOS SE DEBE REGULAR? Y ¿CUÁLES NO?

Siguiendo lo establecido por la doctrina española, para la determinación de qué ficheros o datos de carácter personal entran dentro del ámbito de aplicación de una norma de protección de datos, debemos tener en cuenta tres conceptos: "dato personal", "fichero" y "tratamiento".

*"**Dato de carácter personal**",* entendido como cualquier información concerniente a personas físicas, identificadas o identificables; es decir, toda información numérica, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Entonces; dato de carácter personal es cualquier elemento que permite determinar, de manera directa o indirecta, la identidad física, fisiológica, psíquica, económica, cultural o social de una persona física.

"Fichero", Debe ser entendido como conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Es, por tanto, el soporte físico, sea automatizado o no, en el que se recoge y almacena, de manera organizada, el conjunto de datos que integra la información.

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

Si bien entendemos que los ficheros de datos de carácter personal que se mantengan en soporte informático o telemático no presentan grandes dudas para su determinación, puesto que para su creación se exige, con carácter previo, la grabación, depuración y estructuración de una forma determinada, no sucede lo mismo para los ficheros en soporte papel (o ficheros no automatizados).

Para poder determinar cuando los datos registrados en soporte papel son susceptibles de tratamiento, y en consecuencia, se encuentren incluidos en el ámbito de aplicación de una Ley de Protección de Datos, hay que atender a los siguientes requisitos:

- Que el tratamiento no automatizado se refiera a datos comprendidos en un Fichero en soporte papel.

-Y, que dichos datos se encuentren organizados estructurados u ordenados por criterios específicos. no considerándose, en consecuencia Fichero, la existencia de carpetas no estructuradas, aunque estás contengan datos de carácter personal (por ejemplo: en una consulta médica las carpetas o fichas de pacientes ordenadas alfabéticamente por el nombre de los mismos, se consideraría un fichero susceptible de tratamiento, siéndole por tanto de aplicación la Ley).

De este modo, la Ley concibe los Ficheros protegidos desde una perspectiva dinámica; es decir, no los entiende como un mero depósito de datos, sino, como una globalidad de procesos o aplicaciones que se llevan a cabo con los datos almacenados (por ejemplo: en la consulta médica en la que los datos de los pacientes están recogidos en fichas, las mismas no suponen un mero deposito de datos, sino que permiten al médico efectuar un análisis de las distintas visitas que ha efectuado el paciente, revisar la historia clínica del paciente, y ofrecer un tratamiento o diagnóstico que se adapte a las circunstancias concretas de cada paciente).

También debemos aclara que no todo dato es susceptible de protección por parte de una Ley de Protección de Datos de carácter personal, así por ejemplo la ley 15/1999 establece en su artículo 2 y 3 que no será susceptible de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domesticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero

comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Y que se regirán por disposiciones especiales:

a) Los ficheros regulados por el régimen electoral.

b) Los de fines estadísticos

c) Los que son controlados por el régimen de las Fuerzas Armadas.

d) Los derivados del Registro Civil.

CAPITULO III
LEGITIMACIÓN

1. OBTENCIÓN DEL CONSENTIMIENTO DE LOS TITULARES DE DATOS.

El principio del consentimiento es el eje fundamental de la Protección de Datos estableciéndose como exigencia. Así lo indica al establecer la ley española LOPD en su artículo 6.1 "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"-.

El consentimiento no es más que la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de sus datos personales.

Este consentimiento debe tener las siguientes características.

a) **Libre**: deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento.
b) **Específico**: referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del Responsable del Fichero.
c) **Informado**: el usuario debe conocer, con anterioridad al tratamiento, la existencia y las finalidades para las que se recogen los datos.
d) **Inequívoco**: es preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento (no resulta admisible el consentimiento presunto).

Hay que señalar que el consentimiento general que se debe exigir para el tratamiento de datos, va íntimamente ligado a la obligación de informar, ya que a partir de dicha información el afectado es consciente y toma conocimiento de la existencia del tratamiento que se va a realizar, las finalidades y los derechos que le asisten.

También esta ley dispone en su artículo 7.2 para determinadas categorías de datos un tipo elevado de consentimiento. Así, encontramos que: "Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas

y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado"-.

Excepciones al consentimiento.

En cuanto a las excepciones al consentimiento para el tratamiento de sus datos personales se fijan los siguientes casos:

- Tratamiento realizados por Administraciones Públicas en el ejercicio de sus competencias propias.

- Tratamientos realizados dentro del mantenimiento de una relación precontractual, contractual, laboral o administrativa..

- Protección de un "interés vital" del interesado, como en caso de que el afectado se encuentre física o jurídicamente incapacitado para dar su consentimiento.

- Cuando procedan de fuentes accesibles al público. No será necesario el consentimiento del afectado cuando, recogidos los datos de fuentes accesibles al público, el tratamiento sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del fichero (casos de publicidad y prospección comercial, principalmente).

Revocación del consentimiento.

Un aspecto interesante que plantea esta ley española es la revocatoria del consentimiento, así lo establece su artículo.6.3 "El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos".

Así entonces la revocación sería otra declaración de voluntad. Así y en este sentido lo entiende la propia Ley citada, para los casos de cesión de datos o cuando los datos se destinen a fines promocionales y/o publicitarios.

2. CALIDAD DE LOS DATOS.

Son cuatro las condiciones u obligaciones en la legislación española para adecuarse a este fin.

1º.- deben de adecuarse a la finalidad para la que fueron recabados. Cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido.

2º.- Deben ser exactos y actualizados. Significa que los datos tienen que ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Ello no significa que las empresas deban mantener exactos los datos cuando no tengan medios para conocer la exactitud o veracidad de los datos; pero, si tienen conocimiento de la inexactitud de un dato, deben proceder a actualizarlo.

3º.- No deben mantenerse indefinidamente sin justificación. Esto impide que los datos se usen para finalidades incompatibles o distintas con aquellas para las que hubiesen sido recogidos, si bien no se considera incompatible el tratamiento posterior de éstos datos con fines históricos, estadísticos o científicos.

4º.- Deben haber sido recogidos de forma lícita. Se impone la prohibición de recoger los datos por medios fraudulentos, desleales o ilícitos

3. DEBER DE SECRETO.

Trata de la revelación de datos considerados altamente sensibles, es decir, la revelación de datos como: ideología, religión, creencias, salud, origen racial o vida sexual, caso de la víctima se tratar de un menor de edad o un incapaz.

Este deber de secreto está relacionado con el secreto profesional que tendría sobre sí el encargado o responsable de un fichero que contenga datos de ésta naturaleza, haciéndose responsable éste encargado aún en el caso de ser un tercero el autor de revelar esta información sensible. Esto implica que toda persona encargada de manejar datos personales debe tener especial cuidado en torno a las medidas de seguridad adoptadas para su protección.

CAPITULO IV

DERECHOS DE LOS CIUDADANOS

Siguiendo la línea de la LOPD española, estos derechos son conocidos como los Derecho ARCO (Acceso, Rectificación y Cancelación y oposición) y constituyen la base y garantía para el ejercicio pleno del ciudadano en materia de autodeterminación informática, por lo que pasamos a describirlos brevemente a continuación.

1 DERECHO DE ACCESO

a). El interesado tendrá derecho a recabar de la persona responsable, cuando así lo solicite, información relativa a los concretos datos de carácter personal objeto de tratamiento, así como al origen de dichos datos, a las finalidades de los correspondientes tratamientos y a los destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos.

b). Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo.

c). La legislación nacional aplicable podrá limitar el ejercicio reiterado de estos derechos, que obligaría a la persona responsable a responder múltiples solicitudes en intervalos cortos de tiempo, excepto en aquellos casos en los que el interesado haga constar en su solicitud un interés legítimo

2 DERECHO DE RECTIFICACIÓN Y CANCELACIÓN

1. El interesado tendrá derecho a solicitar a la persona responsable la rectificación o cancelación de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.
2. Cuando proceda, la persona responsable rectificará o cancelará los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos.
3. La cancelación no procederá cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable por la

legislación nacional aplicable o, en su caso, por las relaciones contractuales entre la persona responsable y el interesado.

3. DERECHO DE OPOSICIÓN

1. El interesado podrá oponerse al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal.
2. No procederá el ejercicio de este derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable.
3. Cualquier interesado podrá oponerse, igualmente, a aquellas decisiones que conlleven efectos jurídicos basadas únicamente en un tratamiento automatizado de datos de carácter personal, excepto cuando la decisión hubiese sido expresamente solicitada por el interesado o sea precisa para el establecimiento, mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el propio interesado. En este último caso, el interesado debe tener la posibilidad de hacer valer su punto de vista, a fin de defender su derecho o interés.

4) EJERCICIO DE ESTOS DERECHOS

Los derechos previstos podrán ser ejercidos:

a. Directamente por el interesado, que deberá acreditar adecuadamente su identidad ante la persona responsable.
b. Por medio de representante, que deberá acreditar adecuadamente tal condición ante la persona responsable.

2. La persona responsable deberá implementar procedimientos que permitan a los interesados ejercer sus derechos de forma sencilla, ágil y eficaz, y que no conlleven demoras o costes indebidos, ni ingreso alguno para la persona responsable.
3. Cuando la persona responsable aprecie que, de acuerdo con la legislación nacional aplicable, no procede el ejercicio de los derechos previstos en la presente Parte, informará cumplidamente al interesado de los motivos que concurran en su apreciación.

CAPITULO V
ESTABLECIMIENTO DE MEDIDAS DE SEGURIDAD

Es importante señalar que tanto la Ley 15/1999 como el Real Decreto 994/1999 que fijan lineamientos de Seguridad ligan el concepto de seguridad de los datos a los conceptos de: a) Confidencialidad: entendido como el acceso autorizado a los datos. b) Exactitud: la información no debe sufrir alteraciones no deseadas, en cuanto a su contenido y c) Disponibilidad: sólo las personas autorizadas pueden tener acceso a la información.

1. MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO.

Deberían ser aplicados para todos los ficheros que contengan datos de carácter personal.

Se trata de un documento que deberá contener, como mínimo, los siguientes aspectos:

a. especificación detallada de los recursos protegidos.
b. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido
c. Funciones y obligaciones del personal.
d. Estructura de los ficheros con datos de carácter personal
e. Procedimiento de notificación, gestión y respuesta ante las incidencias.
f. Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

El documento debería mantenerse en todo momento actualizado.

2. MEDIDAS DE SEGURIDAD DE NIVEL MEDIO.

Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia y crédito.

Además de lo exigido en el documento para el Nivel Básico, se tiene:

- la identificación del responsable o responsables de seguridad,
- (auditoría interna y externa) Son los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.
- Identificación y autenticación. De todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
- Gestión de soportes. Estableciendo un sistema de registro de entrada y salida de soportes informáticos, fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable.
- Cuando un soporte vaya a ser desechado o reutilizado, las medidas para impedir cualquier recuperación posterior y se procede a su baja en el inventario.
- Registro de incidencias. Ante denuncias

3. MEDIDAS DE SEGURIDAD DE NIVEL ALTO.

Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

Se suma al documento de Nivel Básico y Medio el cifrando dichos datos o bien cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Registro de accesos.

1. De cada acceso se deben guardar, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad revisará los control registrados y los problemas detectados al menos una vez al mes.

Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas.

Telecomunicaciones.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros

III SECCIÓN CONCLUSIVA

CONCLUSIONES:

Del estudio monográfico realizado se pueden extraer las siguientes conclusiones:

- Producto de la evolución tecnológica y la informática, el manejo y tratamiento de datos personales tanto en la administración pública como privada se ha visto transformada de manera radical, acortando tiempos y distancias; poniendo así en riesgo el derecho de la intimidad de los ciudadanos.

- Nuestro país en la actualidad dispone de diversas leyes y en distintas áreas del Derecho que tratan sobre la intimidad de las personas; hoy como derecho fundamental, esto no reduce en nada el peligro de invasiones en la esfera de este derecho, dado el carácter disperso de las normas que apunta en su generalidad a un derecho reparador y no tienen un carácter preventivo que garantice una seguridad efectiva del ciudadano.

- Como ciudadanos de un Estado de Derecho, cada uno de nosotros deberíamos estar informados sobre el derecho que tenemos a controlar toda la información relativa a nosotros mismos (nuestros datos de carácter personal) y en este marco, quién utiliza dicha información y con qué fines, para evitar que el tratamiento de nuestra información pueda llegar a suponer injerencias en nuestra privacidad.

- Nuestras instituciones como responsables del manejo de nuestra información personal no cuentan con reglamentos específicos que definan responsables, obligaciones, restricciones en la recogida de datos en función a la finalidad perseguida, niveles de seguridad bajo; medio o alto, ni sanciones ante posibles infracciones.

- Existe desconocimiento por parte de instituciones y ciudadanos de los denominados Derechos ARCO (acceso, rectificación, cancelación y oposición).

RECOMENDACIONES:

Para poder mejorar la calidad de nuestra sociedad democrática y el Estado de Derecho, será necesario mejorar la calidad del Derecho a la privacidad que tenemos como ciudadanos a través de:

- Creación de una norma específica que regule la privacidad y protección de datos personales enmarcado en los principios rectores que rigen la materia.

- Creación de una Autoridad Independiente del Estado que tenga atribuciones de Control y Fiscalización, y con facultades de sanción.

- Fomentar la cultura de protección de datos personales en la sociedad y concientizar, sobre el peligro que implica el uso indiscriminado de los mismos.

- Exigir capacitación por parte de las instituciones a los responsables del tratamiento de datos personales.

GLOSARIO DE TERMINOS.

SOCIEDAD DE LA INFORMACIÓN.- El vocablo informática proviene del francés informatique, acuñado por el ingeniero Philippe Dreyfus para su empresa «Société d'Informatique Appliquée» en 1962. Pronto adaptaciones locales del término aparecieron en italiano, español, rumano, portugués y holandés, entre otras lenguas, refiriéndose a la aplicación de las computadoras para almacenar y procesar la información.

Es un acrónimo de las palabras *information* y *automatique* (información automática). En lo que hoy día conocemos como informática confluyen muchas de las técnicas, procesos y máquinas (ordenadores) que el hombre ha desarrollado a lo largo de la historia para apoyar y potenciar su capacidad de memoria, de pensamiento y de comunicación.

En el Diccionario de la Real Academia Española se define informática como: Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores

Conceptualmente, se puede entender como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización en ordenadores (computadoras), con el fin de almacenar, procesar y transmitir información y datos en formato digital.

TIC´s. Aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

BRECHA DIGITAL.- La brecha tecnológica es un término que hace referencia a la diferencia socioeconómica que existe entre aquellas comunidades que tienen Internet y aquellas que no, se refiere también a las desigualdades que se reflejan en todas las nuevas tecnologías de la información y la comunicación (TIC), tales como el computador personal, la tecnología móvil, la banda ancha y otros dispositivos.

WEBLOGS.- Blog o bitácora. Es un sitio web personal donde se escriben periódicamente, como un diario on line, sobre distintos temas que le interesan al propietario. Cada escrito está ordenado cronológicamente y en general posee enlaces a otras páginas.

Para abril de 2007, existían 71 millones de blogs según Technorati, y se crean 120 mil nuevos blogs diarios. La misma fuente también informa que el 37% de los blogs están en japonés, el 36% en inglés, 8% en chino, 3% en español, 3% en italiano y 13% en otros idiomas.

Para el mismo mes de 2006, no llegaban a los 40 millones de blogs, en tanto para abril de 2005 ni siquiera llegaban a los 10 millones.

AUTO DETERMINACIÓN INFORMATIVA.- Concebido como la libertad de la persona para determinar quién, qué y con qué ocasión pueden los entes públicos y privados conocer informaciones que conciernen a cada uno

DATO DE CARÁCTER PERSONAL. entendido como cualquier información concerniente a personas físicas, identificadas o identificables; es decir, toda información numérica, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, tratamiento o transmisión concerniente a una persona física identificada o identificable. Entonces; dato de carácter personal es cualquier elemento que permite determinar, de manera directa o indirecta, la identidad física, fisiológica, psíquica, económica, cultural o social de una persona física.

FICHERO.- Debe ser entendido como conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Es, por tanto, el soporte físico, sea automatizado o no, en el que se recoge y almacena, de manera organizada, el conjunto de datos que integra la información.

TRATAMIENTO, entendido como las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Si bien entendemos que los ficheros de datos de carácter personal que se mantengan en soporte informático o telemático no presentan grandes dudas para su determinación, puesto que para su creación se exige, con carácter previo, la grabación, depuración y estructuración de una forma determinada, no sucede lo mismo para los ficheros en soporte papel (o ficheros no automatizados).

Sistemas de información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

Recurso: cualquier parte componente de un sistema de información.

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Soporte: objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

IV BIBLIOGRAFIA

- Dermizaky Peredo, Pablo (2000), "El derecho a la intimidad"; en: *Ius et praxis:* Talca; Universidad de Talca-Facultad de Ciencias Jurídicas y Sociales; Año 6 N° 1.

- Christian Suárez Crothers (1997) " Informatica, vida Privada y los Proyectos Chilenos Sobre Protección de Datos" en: *Ius et praxis:* Talca; Universidad de Talca-Facultad de Ciencias Jurídicas y Sociales; Año 3 N° 1. Pp.321-360

- Louis D. Brandeis y Samuel D Warren (1890), "El Derecho a la Privacidad" . Harvard Law Review Vol.IV 15 de diciembre 1890 No 5. Editado por Stephen R.LAniel Universidad de Lawrence.1999.

- Castillo Jimenez Cintia (2008) "Protección del Derecho a la Intimidad y usos de las Nuevas Tecnologías de la Información" Universidad de Sevilla.

- Arango Rueda Adriana, Zuleta Lodoña Alberto, et. al.(2005) "El habeas data y la protección de datos personales" Documentos GECTI; Bogota

- Fundación COSO (2003), "Veracidad y objetividad. Desafíos éticos en la sociedad de la información"; 1.er Congreso Internacional de Ética y Derecho de la Información; Valencia.

- Piñara Mañas Juse Luis; Red Iberoamericana de Protección de Datos (2003) "Proteccion de Datos de Carácter Personal; II Encuentro Iberoamericano de Protección de Datos la Antigua – Guatemala2003" Edita Tirant Lo Blanch Valencia.

- Pedro Gareca Perales (2004), "El Habaeas Data en Bolivia en el Constitucionalismo Iberoamericano". Editorial Gaviota del Sur", 1ra edición. Sucre Bolivia

- Miguel Ángel Davara Rodriguez (2004), "Guía Práctica de Protección de Datos Para Abogados". Editorial DaFeMa España.

- Luis Ángel Ballesteros (2005), "La Privacidad Electrónica". Editorial Tirant Lo Blanch, Valencia España.

- Agencia de Protección de Datos (2005), "Protección de Datos Personales". Editorial ATIG, S.L. Rio Ebro, Madrid España.

- Nelson Remolina Angarita (2005), "Documentos GECTI Sobre el Habeas Data y la Protección de Datos Personales". Bogotá, octubre 20 de 2005.

- Erick Iriarte Ahon(2007), "Informe de Análisis y Propuestas en Materia de Acceso a la Información y Privacidad en América Latina". ONG Alfa Redi, Editorial Coroforma Primera edición.

- Diego Sanchez Montenegro (2007), "Informe Situacional de la Privacidad y Acceso a la Información en América Latina" ONG Alfa Redi,. Edición Coroforma Primera edición.

- Boletin oficial del Estado de Madrid (2008) "Reglamento de Protección de Datos de Carácter Persona"; Edición Departamento de Programación Editorial, Documentación e Información del Boletin Oficial del Estado. España.

- Karina Ingrid Medinaceli Díaz (2009) "Proyecto de Ley de Transparencia y acceso a la información pública y el derecho fundamental a la Intimidad y privacidad personal o familiar, o su propia imagen, honra y reputación" Informe ADSIB.

- Diccionario Larousse (2009) Editorial Larousse S.A.de C.V. Mexico D.F.

- Oxford English Dictionary, (2010)

- Oviedo Albán Jorge (2010) "Obligaciones y Contratos en el Derecho Contemporaneo". Universidad de La Sabana 1ra Edición, Colombia.

- ENCUENTROS IBEROAMERICANOS DE PROTECCIÓN DE DATOS: DECLARACIONES.
  Red Iberoamericana de Protección de Datos; Cartagena de Indias 23 de mayo de 2004

PAGINAS WEB

- Declaración de principios Cumbre mundial sobre la sociedad de la información, Documento WSIS-03/ Geneva/4-S de 12 de mayo de 2004 [en línea] <http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-S.pdf> [Consulta: 25/09/2010]

- "La informática y el derecho a la intimidad" Revista Jurídica, Facultad de Jurisprudencia y Ciencias Sociales y Políticas Universidad Católica de Santiago de Guayaquil [En línea] <http://www.revistajuridicaonline.com/index.php?option=com_content&task=view&id=398&Itemid=43> [Consulta 26:/09/2010]

- Principios rectores para la reglamentación de los Ficheros Computarizados de Datos Personales. Adopción: Asamblea General de la ONU Resolución 45/95, 14 de diciembre de 1990: [en línea].
  <http://www.un.org/spanish/documents/ga/res/45/list45.htm>
  [Consulta 20/09/2010]

- Declaración de principios Cumbre mundial sobre la sociedad de la información, Documento WSIS-03/ Geneva/4-S de 12 de mayo de 2004 (fuente: página oficial de la "Cumbre Mundial de la Sociedad de Información Ginebra 2003) [en línea]. <http://www.itu.int/wsis/docs/geneva/official/dop-es.html> [Consulta 25/09/2010]

- Proclamación de Teherán Proclamada por la Conferencia Internacional de Derechos Humanos en Teherán el 13 de mayo de 1968", [en línea]: http://www.acnur.org/biblioteca/pdf/1290.pdf [Consulta:25/09/2010]

- Asamblea General de la ONU Resolución 3384 (XXX), 10 de noviembre de 1975; [en línea]:
  http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/INST%2024.pdf
  [Consulta: 25/09/2010]

ANEXO 1

LEY ORGANICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España

I. Disposiciones generales
JEFATURA DEL ESTADO
23750 LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

JUAN CARLOS I
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I
Disposiciones generales
Artículo 1. Objeto.

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2. Ámbito de aplicación.

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.
2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.
No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.
3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:
a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

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

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:
a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.
j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.
Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II
Principios de la protección de datos
Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.
No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho de información en la recogida de datos.
1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.
2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado.
1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos.

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado
a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros
mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
3. Los datos de carácter personal que hagan referencia
al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión
de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las
respectivas normas reguladoras. 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud.
Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. Seguridad de los datos.
1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto.
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos.
1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:
a) Cuando la cesión está autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.
En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.
3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.
5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso a los datos por cuenta de terceros.
1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III
Derechos de las personas

Artículo 13. Impugnación de valoraciones.
1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre elloso que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho de consulta al Registro General de Protección de Datos.
Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.
1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

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

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.
1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.
2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos.
1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.
3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.
4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho a indemnización.
1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.
2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.
3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV
Disposiciones sectoriales
CAPÍTULO I
Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.
1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.
2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.
3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. Comunicación de datos entre Administraciones públicas.
1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del ficheroo por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.
3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.
4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.
1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos
de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.
3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.
4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.
1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones quese estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados.
1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.
2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II
Ficheros de titularidad privada

Artículo 25. Creación.
Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral.
1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.
2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.
3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.
4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.
5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. Comunicación de la cesión de datos.
1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.
2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. Datos incluidos en las fuentes de acceso público.
1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.
2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial. Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes. La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.
3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.
4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.
3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.
4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, amás de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.
1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.
2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.
3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.
4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. Censo promocional.
1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.
2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.
3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado
4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. Códigos tipo.
1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.
2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.
3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V
Movimiento internacional de datos

Artículo 33. Norma general.
1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.
2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En

particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de

26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director.

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas. En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

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

Artículo 37. Funciones.

Son funciones de la Agencia de Protección de Datos:

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

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

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

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
g) Ejercer la potestad sancionadora en los términosprevistos por el Título VII de la presente Ley.
h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
k) Redactar una memoria anual y remitirla al Ministerio de Justicia.
l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.
n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. Consejo Consultivo.
El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros: Un Diputado, propuesto por el Congreso de los Diputados. Un Senador, propuesto por el Senado.
Un representante de la Administración Central, designado por el Gobierno. Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias. Un miembro de la Real Academia de la Historia, propuesto por la misma.
Un experto en la materia, propuesto por el Consejo Superior de Universidades. Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente. Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma. Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente. El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.
1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.
2. Serán objeto de inscripción en el Registro General de Protección de Datos:
a) Los ficheros de que sean titulares las Administraciones públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones a que se refiere la presente Ley.
d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.
3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad de inspección.
1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.
2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos. Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.
Artículo 41. Órganos correspondientes de las Comunidades Autónomas.
1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.
2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.
3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas

podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII
Infracciones y sanciones

Artículo 43. Responsables.

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. Tipo de sanciones.
1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.
2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.
3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.
6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.
7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones públicas.
1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.
2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.
3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción.
1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.
2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.
3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.
4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.
5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.
6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador.
1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.
2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.
Artículo 49. Potestad de inmovilización de ficheros.
En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. Ficheros preexistentes.
Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente. En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. Ficheros y Registro de Población de las Administraciones públicas.

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. 2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. Tratamiento de los expedientes

de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social. Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos. En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. Modificación del artículo 112.4 de la Ley General Tributaria.

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción: «4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado.

En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. Competencias del Defensor del Pueblo y órganos autonómicos semejantes.

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2.o de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción: «Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley. También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación. En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado.»

Disposición transitoria primera. Tratamientos creados por Convenios internacionales

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. Utilización del censo promocional.

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional.

Disposición transitoria tercera. Subsistencia de normas preexistentes.

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993,

de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. Derogación normativa. Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. Habilitación para el desarrollo reglamentario.

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. **Preceptos con carácter de Ley ordinaria**

. Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional

cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. Entrada en vigor.

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley Orgánica.

Madrid, 13 de diciembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno,

JOSÉ MARÍA AZNAR LÓPEZ

ANEXO 2

SENTENCIA CONSTITUCIONAL 0965/2004-R
Sucre, 23 de junio de 2004

SENTENCIA CONSTITUCIONAL 0965/2004-R
Sucre, 23 de junio de 2004

Expediente: 2004-08860-18-RHD
Distrito: La Paz
Magistrada Relatora: Dra. Elizabeth Iñiguez de Salinas

En revisión, la Resolución 14/2004, cursante de fs. 35 a 36, pronunciada el 8 de abril por la Sala Civil Primera de la Corte Superior del Distrito Judicial de La Paz, dentro del recurso de hábeas data interpuesto por José Carrasco Vidaurre contra Gerardo Tórrez Ossio, Gerente General del periódico "La Razón" y Efraín Oscar Alarcón Bautista, alegando la vulneración de sus derechos al honor, a la dignidad, a la intimidad y a la privacidad.

I. ANTECEDENTES CON RELEVANCIA JURÍDICA
I.1.Contenido del recurso
I.1.1.Hechos que motivan el recurso

En el memorial presentado el 30 de marzo de 2004 (fs. 9 a 12 vta.), y en el de subsanación, de 3 de abril (fs. 14 y 15), el recurrente asevera que en 14 y 21 de marzo de 2004, Efraín Oscar Alarcón Bautista, mediante el periódico "La Razón" publicó avisos por los que le señalan, al igual que a su hija Marcela Carrasco López como deudor moroso, en contra de su imagen, honorabilidad e intimidad.

Aduce que la intimidad en su concepto constitucional no solamente protege la esfera privada de los ciudadanos, como un tema donde se excluyen del conocimiento de los otros una serie de datos e informaciones, salvo manifiesta expresión del afectado, sino que también resguarda su pleno desarrollo como persona, de modo que al amparo de lo establecido por el art. 23 de la Constitución Política del Estado (CPE) tiene la potestad de plantear este recurso para que se eliminen o rectifiquen los datos registrados en "La Razón", en el que se ha divulgado su vida íntima, sin conocer la realidad de los hechos, dado que dicho medio de prensa debió negar a Efraín Alarcón Bautista la publicación que solicitó y persuadirlo que acuda a la vía pertinente.

I.1.2. Derechos y garantías supuestamente vulnerados

El recurrente estima que se han conculcado sus derechos al honor, a la dignidad, a la imagen, a la intimidad y a la privacidad.

I.1.3. Personas recurridas y petitorio
Por lo anotado, interpone recurso de hábeas data contra Gerardo Tórrez Ossio, Gerente General del periódico "La Razón" y Efraín Oscar Alarcón Bautista, solicitando sea declarado procedente, se disponga la supresión, rectificación y eliminación inmediata "de tales y demás avisos publicitarios", se remitan fotocopias legalizadas al Ministerio Público para la instauración y persecución por delitos cometidos y se califiquen costas, daños y perjuicios.

I.2. Audiencia y Resolución del Tribunal de hábeas data

En la audiencia pública de hábeas data realizada el 8 de abril de 2004 (fs. 31 a 34 vta.) se suscitaron las siguientes actuaciones:

I.2.1. Ratificación y ampliación del recurso

El abogado del recurrente, actuando además como apoderado en base al instrumento 140/2004, de 7 de abril (fs. 18), ratificó y reiteró los términos de su demanda, agregando que: a) José Carrasco Vidaurre es2 un profesor de gran trayectoria, ha recibido muchas condecoraciones, inclusive la medalla de la Gran Orden Boliviana de la Educación, lo que demuestra que es una persona distinguida y conocida en nuestro medio, que ha visto vulnerado su derecho a la intimidad con la publicación de su nombre como deudor moroso; b) Efraín Alarcón pretende hacer justicia por mano propia al mandar la publicación del
nombre de su representado como una persona deudora y morosa; c) se debe tener en cuenta que cada día se vende un millar de ejemplares del periódico "La Razón" o sea que es un banco de datos que informa a muchas personas,

que “seguramente mañana” van a llegar a insinuar o a prohibir a su mandante a realizar ciertos actos y ejercer algunos derechos constitucionales al haber visto su nombre como deudor moroso; d) se trata de una información sensible para su representado, sobre un dato “netamente íntimo”, que solamente le incumbe al interesado; e) “La Razón” tendrá que publicar una satisfacción hacia José Carrasco Vidaurre para hacer viable la rectificación.

A la pregunta de la Presidenta de la Corte de hábeas data, el apoderado respondió que no acudió “a las entidades demandas” para pedir la restitución de los posibles derechos lesionados, porque no existe ningún medio legal.

I.2.2.Informe de los recurridos

Efraín Oscar Alarcón Bautista a través de su abogada, informó lo siguiente: a) el recurso ha sido totalmente equivocado, pues conforme a la doctrina y al art. 23 de la CPE, el hábeas data se refiere al “delito” de distorsión de información en medios públicos, cuando hay manipulación de la verdad, datos errados que dañan la dignidad de la persona u otros derechos constitucionales, lo que no ha sucedido en este caso por cuanto la publicación de prensa no vulnera ninguno de los méritos y distinciones que ha recibido el recurrente a lo largo de su vida; b) existe un contrato reconocido ante Notario de Fe Pública en el que se establece la deuda de $US5.000.- del actor a favor suyo y que no ha sido cancelada, ante ese incumplimiento, el 26 de febrero de 2004 remitió una carta notariada al recurrente solicitando el pago de la obligación, lo que no fue atendido por José Carrasco; c) en la citada carta le advirtió que, de no pagar la deuda, recurriría a publicaciones de prensa, pues tiene necesidad del dinero; d) la hija del recurrente es garante mancomunada del deudor principal, por eso también publicó su nombre, pero en ningún caso se atentó en la publicación de prensa contra sus derechos; e) este recurso constitucional no es sustitutivo de otros medios legales a los que podía acudir el recurrente; f) la información sensible es la que puede dañar a la persona como un hecho de violación, un adulterio, pero pedir que se pague una deuda no afecta a los derechos fundamentales; g) no ha existido nunca la intención de hacer daño, sino de solicitar el pago de una obligación pecuniaria, puesto que deber dinero no es delito, no se ha sindicado al recurrente de cometer un hecho ilícito; h) la realidad de la deuda no ha sido tergiversada, la obligación existe y debe ser pagada. Solicitó se declare improcedente el recurso.

Los abogados del Gerente General del periódico “La Razón”, afirmaron que: a) según lo establecido por la Ley de Imprenta, cualquier publicación es de responsabilidad del director del medio de comunicación, por ende, el recurrido debió ser el Director de la “Razón” y no su Gerente General; b) este recurso no ha cumplido las formalidades diseñadas por el Tribunal Constitucional, ya que el hábeas data se ha asimilado al amparo constitucional, por lo que tiene el carácter de subsidiariedad, y en este asunto, el recurrente no ha agotado previamente las vías que tenía a su alcance para reclamar y lograr la anulación o supresión de la publicación que considera atenta contra sus derechos; c) “La Razón” tiene el cuidado de pedir se entregue el texto que se quiere publicar, asimismo, solicita fotocopia de la cédula de identidad y la firma del que está realizando la publicación; d) el periódico no ha establecido el derecho de ninguna persona, se ha limitado a publicar un aviso que fue pagado por Efraín Alarcón; e) ese medio de prensa no ha restringido ni amenazado ningún derecho constitucional ni garantía fundamental, toda vez que no es un banco de datos, es un instrumento por el que se exteriorizan ideas, sin que le sea posible a “La Razón” verificar si esas opiniones, avisos, etc., son veraces o no; f) estamos en un sistema democrático en el que la libertad de ideas es fundamental, y en ese marco, “La Razón” no tiene porque dar una satisfacción pública al recurrente, la misma debería ser pedida a la persona que solicitó se publique el aviso; g) el único “filtro” que tiene el periódico para publicar anuncios y otros, es el de la moral y las buenas costumbres

I.2.3. Resolución

La Resolución 14/2004, cursante de fs. 35 a 36, pronunciada el 8 de abril de 2004, por la Sala Civil Primera de la Corte Superior del Distrito Judicial de La Paz, declara improcedente el recurso, bajo estos fundamentos: 1) si bien de acuerdo al art. 17 del Código civil (CC), toda persona tiene derecho a que sea respetado su buen nombre, dicha protección legal se traduce en la reparación civil; 2) el hábeas data como acción tutelar es de carácter subsidiario, procede cuando el titular del derecho lesionado reclama, ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos y almacenados, o en su caso la actualización, rectificación o supresión, y no obtiene una respuesta positiva, y en el caso presente no se ha evidenciado que el recurrente haya acudido ante las personas demandadas solicitando la supresión de la información que considera ilegal, agraviante y falsa.

II. CONCLUSIONES

Hecha la debida revisión y compulsa de los antecedentes se llega a las conclusiones que se señalan seguidamente:

II.1. Por documento privado de 2 de junio de 2003 (fs. 230 y 21), con reconocimiento de firmas de 1 de agosto del mismo año (fs. 19), Alberto José Carrasco Vidaurre reconoció adeudar la suma de $US5.000.- a Efraín Oscar Alarcón Bautista, obligándose a pagarla hasta el 30 de noviembre de dicha gestión. Marcela Ludnila Carrasco López, hija del actor, figura como garante solidaria y mancomunada.

II.2. Por carta notariada de 26 de febrero de 2004 (fs. 25 y 26), el co – recurrido Efraín Oscar Alarcón Bautista solicitó al demandante cancele la obligación hasta el 4 de marzo, caso contrario acudiría a los medios de comunicación, reservándose el derecho de seguir las acciones legales que correspondan.

II.3. El 14 y 21 de marzo de 2004 (fs. 3 y 4), en el periódico "La Razón", sección páginas azules, Efraín Oscar Alarcón Bautista publicó un aviso bajo el título de "DEUDOR MOROSO", que rezaba: "Al señor: ALBERTO CARRASCO VIDAURRE (DEUDOR) y MARCELA CARRASCO LÓPEZ (GARANTE), Propietario COLEGIO AMAUTA (Ciudad Satélite) comunicarse al Telf.: 72084685 y cancelar la deuda pendiente, caso contrario se acudirá a las instancias legales correspondientes" (sic).

La publicación del 28 de marzo de 2004 (fs. 5), añadió que la cancelación de la deuda pendiente se realice hasta el 1 de abril de este año. Respecto de esta publicación, a fs. 29 corre el talón de "Páginas Azules del Loro de Oro", al que se encuentra adherida la leyenda que Efraín Oscar Alarcón Bautista –cuya cédula de identidad también está adosada (fs. 30)- pidió se publique.

II. 4.En el cuaderno procesal de hábeas data remitido a este Tribunal, no se constata la existencia de ninguna reclamación o pedido que hubiera efectuado el actor a los recurridos en lo concerniente a las publicaciones que denuncia como atentatorias a sus derechos.

III. FUNDAMENTOS JURÍDICOS DEL FALLO

El recurrente arguye que se han vulnerado sus derechos al honor, a la dignidad, a la intimidad y a la privacidad, al haber publicado en el periódico "La Razón" un aviso en el que figura como deudor moroso. En ese sentido, corresponde, en revisión, analizar si en la especie se debe otorgar la tutela pretendida.

III.1. Con el fin de dar una cabal comprensión a la garantía del hábeas data, recientemente instituida en Bolivia con la reforma de la constitución Ley 2631 de 20 de febrero de 2004, resulta imperioso efectuar una introducción doctrinal sobre este instituto.

A lo largo de toda su vida, una persona es objeto de innumerables formas de identificación o individualización que se registran en otros tantos bancos de datos. Desde el registro del nacimiento hasta el mismo momento de la defunción se realiza un sinfín de actividades en ese sentido. La individualización y anotación con un nombre, el otorgamiento de un documento de identidad numerado, la extracción de fichas dactiloscópicas, la obtención del pasaporte, la elaboración de la ficha de ingreso laboral, la apertura de cuentas corrientes o cajas de ahorro bancarias, las fichas de ingreso a un club deportivo, el registro en una entidad de salud, la historia clínica y tantas otras más, implican la existencia de una serie
de datos personales que, merced al avance tecnológico, se encuentran interconectados, pudiendo establecerse una posible fusión o complementación o conoce de los datos, sin autorización expresa ni conocimiento por parte de la persona a la cual están referidos.

Para resguardar los derechos del titular de dichos datos, se ha instituido la acción del hábeas data, que es una modalidad de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación.

Siguiendo la doctrina del Dr. José Antonio Rivera Santivañez en su obra "Jurisdicción Constitucional", el hábeas data se define como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informática". Es una garantía constitucional que, sin desconocer el derecho a la información, al trabajo y al comercio de las entidades públicas o privadas que mantienen centrales de información o bancos de datos, reivindica el derecho que tiene toda persona a verificar qué información o datos fueron obtenidos y

almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, se impida su
difusión y, en su caso, se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referido a la honra, buena imagen o el buen nombre.

Partiendo de los conceptos referidos, se puede inferir que el hábeas data es una garantía constitucional por lo mismo se constituye en una acción jurisdiccional de carácter tutelar que forma parte de los procesos constitucionales previstos en el sistema de control de la constitucionalidad. Es una vía procesal de carácter instrumental para la defensa de un derecho humano como es el derecho a la autodeterminación informática.

Como una acción tutelar, el hábeas data sólo se activa a través de la legitimación activa restringida, la que es reconocida a la persona afectada, que puede ser natural o jurídica. En consecuencia, no admite una activación por la vía de acción popular, es decir, no se reconoce la legitimación activa amplia. Así, el hábeas data como un proceso constitucional de carácter tutelar, tiene la finalidad de brindar tutela efectiva, inmediata e idónea a la persona en el ejercicio de su derecho a la autodeterminación informática. La protección que brinda el hábeas data abarca los siguientes ámbitos:

a) Derecho de acceso a la información o registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo que se dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal;

b) Derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona;

c) Derecho de corrección o modificación de la información o los datos personales inexactos registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona;

d) Derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona;

e) Derecho de exclusión de la llamada “información sensible” relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado;

En consecuencia, el hábeas data es una garantía constitucional que tiene por objetivo el contrarrestar los peligros que conlleva el desarrollo de la informática en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona; y tiene por finalidad principal el proteger el derecho a la autodeterminación informática, preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios a la persona. El hábeas data tiene la función primordial de establecer un equilibrio entre el “poder informático” y la persona titular del derecho a la
autodeterminación informática, es decir, entre la entidad pública o privada que tiene la capacidad de obtener, almacenar, usar y distribuir la información sobre datos personales y la persona concernida por la información.

La doctrina ha clasificado los diversos tipos e hábeas data que pueden presentarse, a saber:

a) Hábeas data informático, que permite a la persona ejercer su derecho a la autodeterminación informática accediendo a los registros o bancos de datos públicos o privados destinados a proveer información para que pueda recabar toda la información obtenida, almacenada y registrada en torno a su persona. Aquí se tienen las variantes de:

a.a) Hábeas data exhibitorio, para que la persona que lo plantea tome conocimiento de sus datos,almacenados en bancos de datos;
a.b) Hábeas data finalista, para que la persona sepa para qué o para quién se almacenaron sus datos;
a.c) Hábeas data autoral, para que la persona conozca quién tuvo, almacenó y registró sus datos.

b) Hábeas data aditivo, permite a la persona lograr que se actualice el registro de sus datos, y se adicione un dato personal que no fue inserto en el banco de datos;

c) Hábeas data rectificador, a efecto de otorgar la tutela a la persona perjudicada en su derecho a la libertad informática, disponiendo que los encargados del banco de datos procedan a sanear los datos falsos o incorrectos almacenados;

d) Hábeas data reservador, es el que permite a la persona conservar el ámbito de su intimidad frente la divulgación de información obtenida y almacenada en los registros públicos o privados, información que en su criterio es sensible y debe mantenerse en reserva;
e) Hábeas data cancelatorio o exclusorio, por medio del que se logra se borren los datos conocidos como información sensible.

Dentro de ese marco, a efectos de delimitar el campo de acción de este recurso constitucional, es necesario expresar que para la aplicación del hábeas data existen distintos posibles planteamientos:

1) El primero está referido a la constatación sobre la existencia del registro. Esta cuestión parte de un primer problema relativo a la existencia misma del banco de datos, ya que si él no existiera, no habría solicitud atendible alguna. Acreditada la existencia, y ante la sospecha de la inclusión de datos suyos, la persona podrá solicitar la constatación sobre el contenido del asiento a ella referido, su finalidad y uso concreto;

2) El segundo planteamiento concierne al control del contenido. La persona que accedió al registro realizado respecto suyo, ahora puede controlar y analizar el contenido de los datos. Este control puede materializarse en un actuar concreto dirigido a diferentes acciones, tales como:

a) Anular el asiento, cuando el dato no responde a la realidad de los hechos, cuando nunca existió la circunstancia que anota, o si, habiendo existido, desapareció o se extinguió por diferentes causas;

b) Actualizar el asiento, cuando en el registro figuran algunos datos ciertos y otros que se han modificado por el tiempo o por alguna acción del titular, por lo que se solicita que toda la información se relacione con las actuales circunstancias del afectado;

c) Rectificar o modificar, si en el registro se ha consignado información que es incorrecta, falsa o mendaz;

d) Aclarar, si en el registro existe información que, si bien es cierta, está dada en una forma incorrecta o equívoca respecto de la real situación;

e) Anulación de registros referidos a datos “sensibles”, cuando dichos datos sólo le pertenecen e incumben al titular, y están referidos a temas, circunstancias, y en general a todo lo que, de ser conocido públicamente, puede generar perjuicios o discriminación.

f) Reserva de datos, cuando la información resulta correcta, y también lo es su origen, pero no se trata de información susceptible de darse indiscriminadamente o publicarse sin autorización del titular. La acción tiende a preservar que los datos sean revelados, salvo que obedezca a la solicitud de autoridad competente o del interesado, debidamente fundada;

g) Datos que importen discriminación, implicarán necesariamente su anulación, por ser ilegítima la posesión de este tipo de información;

La garantía del hábeas data se desarrolla en dos etapas: la prejudicial y la judicial propiamente dicha: a) etapa prejudicial, se produce cuando la persona que pretende la exhibición del registro y, si es el caso, la corrección de los

datos asentados en él, debe notificar fehacientemente a la empresa titular del banco de datos, su pretensión de que se le exhiban sus datos incluidos en el registro, y pedir, si así estima necesario, sean rectificados, corregidos, modificados o eliminados. Si la entidad requerida consiente en lo solicitado, queda consumado el ejercicio del derecho con esa sola fase prejudicial. Si el interesado no
recibe respuesta alguna o se le da una negativa a lo solicitado, puede válidamente pasar a la siguiente fase; b) etapa judicial, que se realiza -se reitera- cuando el titular del registro se niega a exhibir los datos, hace caso omiso del requerimiento, o si exhibiéndolos, pretendiera mantener los datos cuestionados, negándose a rectificarlos o a cancelarlos en su caso, entonces es procedente la vía constitucional del hábeas data.

Las dimensiones de la persona que están bajo la tutela del hábeas data pueden sintetizarse en las siguientes:

1) El propio cuerpo, referido a la salud de la persona o de los miembros de su familia;
2) Las ideas y creencias religiosas, filosóficas, políticas;
3) La vida pasada, relacionada con el ámbito que a la persona podría generarle bochorno al estar compuesta por pasajes desagradables o ingratos;
4) La vida doméstica, relacionada con los hechos o situaciones que se producen dentro del hogar;
5) La vida familiar concerniente con el matrimonio y la filiación;
6) La vida amorosa, relaciones de amistad, la vida sexual;7
7) El ámbito de las comunicaciones personales que comprende las diferentes vías de comunicación;
8) La situación económica de las personas referidas al nivel de ingreso, patrimonio, inversiones, obligaciones financieras.

En cuanto a los límites del hábeas data, es importante remarcar que, como vía procesal instrumental, protege a la persona en su derecho a la autodeterminación informática, activándose contra el poder informático. De manera que cabe advertir que existe un límite en cuanto a los alcances del hábeas data que se establece en el ejercicio de la libertad o derecho de información y libertad de expresión. En efecto, el hábeas data no se activa contra la difusión de información a través de los medios masivos de comunicación social, toda vez que este medio no es el adecuado para viabilizar el derecho de réplica por parte de un medio de prensa con relación a una información difundida que la persona considere inexacta o que agravia su derecho al honor. La honra o la buena imagen, o lesione su vida privada o íntima.

Debe quedar claramente establecido que el hábeas data no es un medio para ejercer control sobre los medios de comunicación social y el ejercicio de la libertad de expresión e información, no es un mecanismo para establecer censura previa ni correctiva.

III.2.En Bolivia, la Ley de Necesidad de Reforma a la Constitución 2410 de 1 de agosto de 2002, determinó la reforma del art. 23 de la Ley Fundamental, introduciendo la garantía del hábeas data.

La Constitución Política del Estado, a partir de la Ley 2631 de 20 de febrero de 2004, que ha reformado la misma, en su art. 23 determina lo siguiente:

"I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Habeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.

II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.

III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.

IV. El recurso de Habeas Data no procederá para levantar el secreto en materia de prensa.
V. El recurso de Habeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19° de esta Constitución".

El nuevo texto constitucional anotado contiene normas de carácter sustantivo, porque en su primer parágrafo instituye el hábeas data como una garantía constitucional y determina su alcance; y, establece normas de carácter procesal dando la configuración básica en cuanto al trámite de esta acción tutelar.

Tomando en cuenta sus fines y objetivos , así como la aplicación supletoria de las normas previstas por el art. 19 de la CPE, dispuesta por el art. 23 parágrafo V antes referido, se entiende que el hábeas data es una acción de carácter subsidiario, es decir, que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que inducen a discriminaciones, y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume inmediatamente la acción solicitada. Dicho de otro modo, el hábeas data se activa exclusivamente cuando la persona demuestra que ha acudido previamente ante la entidad pública o privada para pedir la restitución de su derecho lesionado y no ha podido lograr la reparación a dicha vulneración.

La legitimación activa del hábeas data recae en la persona natural o jurídica –aunque el precepto constitucional no lo determina de esa manera en forma expresa, se entiende que dentro de la protección de este recurso se puede y debe abarcar tanto a las personas físicas como a las jurídicas, de quienes también se pueden registrar datos e informaciones- respecto de la cual la entidad pública o privada haya obtenido y tenga registrados datos e informaciones que le interesen a aquella conocer, aclarar, rectificar, modificar, o eliminar, y que no haya tenido respuesta favorable por la citada entidad para lograr esos extremos.

La legitimación pasiva de esta acción, tomando en consideración que protege a la persona en el ejercicio de su derecho a la autodeterminación informativa contra cualquier manejo impropio de sus datos personales registrados o almacenados en bancos de datos públicos o privados, recae en el personero legal de la entidad pública o privada que tengan los archivos o bancos de datos personales de quien se sienta afectado en el ejercicio del citado derecho.

III.3. En la especie, el recurrente, Alberto José Carrasco Vidaurre, interpone el recurso contra Efraín Oscar Alarcón Bautista, por haber hecho publicar un aviso en un medio de prensa escrito, en el que se lo identifica como “Deudor Moroso” y se le invita a cancelar su deuda, siendo dicho aviso publicado en el periódico “La Razón”, motivo por el que dirige su acción también contra el Gerente General de ese órgano.

Entendida la figura del hábeas data, caben realizar las siguientes puntualizaciones en el caso objeto de estudio. En primer término, Efraín Oscar Alarcón no posee un “archivo” o “banco de datos” que registre información sobre el actor, sino que se trata de un acreedor que acudió ante un periódico para publicar una exhortación a quien supuestamente le debe una suma de dinero con el fin de que la misma le sea cancelada, por un lado, y por otro, en el cuaderno procesal del recurso, no existe nota o literal alguna que evidencie que el recurrente hubiera pedido al nombrado acreedor retire la publicación mencionada, razón
que determina en este aspecto, la improcedencia del hábeas data por ser un recurso subsidiario como se tiene expresado.

Si bien el art. 2 de la Ley de Imprenta establece que “son responsables de los delitos cometidos por la prensa o por cualquier otro modo de exteriorizar y difundir el pensamiento: 1) los que firmen como autores una publicación; 2) los directores de diarios, revistas y publicaciones periodísticas; 3) los editores”, en el caso presente no se está procesando la comisión de un hecho ilícito, sino un acto presuntamente ilegal que agravió al recurrente en sus derechos fundamentales.

De los datos el expediente se tiene que “La Razón” tampoco posee un banco de datos sobre aspectos que interesan al recurrente, es un medio de prensa que, además de emitir información general, publica avisos a través de un contrato celebrado con la persona que desea hacer conocer algo a la población. Dentro de esa lógica, el hábeas data no puede activarse contra la difusión de información a través de los medios masivos de comunicación social, toda vez que este medio no es el adecuado para viabilizar el derecho de réplica por parte de un medio de prensa con relación a una información difundida que la persona considere inexacta o que agravia su derecho al honor, la honra o la buena imagen, o lesione su vida privada o íntima. Este recurso constitucional extraordinario no es una vía para ejercer control sobre los medios de comunicación social, existiendo para ello la vía expedita que el ordenamiento jurídico establece.

Al margen de lo expresado, en autos se tiene clara constancia que el recurrente no solicitó a "La Razón", antes de plantear su recurso, la supresión del aviso, motivo que corrobora la improcedencia antedicha.

Cabe manifestar que le asiste al recurrente el derecho de rectificación o respuesta, también llamado derecho de réplica, previsto en el Pacto de San José de Costa Rica -ratificado por Bolivia mediante Ley 1430- cuyo art. 14 establece que 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 establece la ley. En el país, la Ley de Imprenta en su art. 62 inc. 3) prevé como obligación de los editores responsables, y en su caso de los impresores, publicar las vindicaciones y defensas de las personas ofendidas en el mismo periódico, cobrando media tarifa. Entonces, el actor tiene el derecho de publicar, en el mismo periódico donde se emitió el aviso de "Deudor Moroso", las aclaraciones que estime corresponden a la realidad precautelando sus intereses y derechos.

De todo lo analizado, se tiene que en el caso revisado, por una parte, los recurridos no pueden revestir la condición de sujetos pasivos de esta acción tutelar, por cuanto ni Efraín Oscar Alarcón Baustista, ni el periódico "La Razón" tienen en su poder bancos de datos o registros que pudieran afectar al recurrente en sus derechos al honor, a la dignidad, a la intimidad y a la privacidad; y por otra, que el actor tiene la posibilidad de solicitar directamente a ese órgano de prensa la rectificación del aviso, si contiene datos incorrectos o falsos, en mérito de lo cual no puede otorgarse la protección que hoy busca, más aún si se toma en cuenta que en ningún momento realizó reclamo alguno ni ejercitó su derecho de rectificación y respuesta respecto del aviso publicado los días 14, 21 y 28 de marzo del presente año.

De todo lo examinado, se concluye que la Corte de hábeas data, al haber declarado improcedente el recurso, ha evaluado correctamente los datos del proceso y las normas aplicables al mismo.

POR TANTO

El Tribunal Constitucional, en virtud de la jurisdicción que ejerce por mandato de los arts. 23 y 120.7ª de la CPE, con los fundamentos expuestos APRUEBA la Resolución 14/2004, cursante de fs. 35 a 36, pronunciada el 8 de abril por la Sala Civil Primera de la Corte Superior del Distrito Judicial de La Paz.

Regístrese, notifíquese y publíquese en la Gaceta Constitucional

No firma el Presidente, Dr. Willman Ruperto Durán Ribera, por encontrarse con licencia.

Fdo. Dr. René Baldivieso Guzmán
PRESIDENTE EN EJERCICIO

Fdo. Dra. Elizabeth Iñiguez de Salinas
DECANA EN EJERCICIO

Fdo. Dr. José Antonio Rivera Santivañez
MAGISTRADO

Fdo. Dra. Martha Rojas Álvarez
MAGISTRADA