FACULTAD DE DERECHO

LA CARACTERIZACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL ORDENAMIENTO JURÍDICO ECUATORIANO

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de

Abogada de los Tribunales y Juzgados de la República

Profesor guía

Diego Alejandro Narváez Solano

Autor

María Cristina Rosero Aguirre

Año

2011

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

…….
Diego Alejandro Narváez Solano
Abogado
170976661-0

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

……
Ma. Cristina Rosero Aguirre
171727407-8

AGRADECIMIENTO

Agradezco a Dios por haberme dado la capacidad de culminar mis estudios y permitirme aprender no solo conocimientos académicos sino formarme con valores morales que son de importante ayuda en mi vida diaria.

DEDICATORIA

Dedico mi trabajo de titulación a mis padres Que con su esfuerzo y constancia supieron guiar mi camino durante toda mi carrera y siempre me ayudaron en mi crecimiento tanto profesional como personal.

Resumen

Los datos de una persona implican información que refleja algunos aspectos íntimos de su vida y en tal sentido su manejo inadecuado puede tener repercusiones graves respecto de su integridad.

Por esta razón, a nivel mundial, el tema de datos personales se ha tratado desde hace 30 años aproximadamente, y la legislación ecuatoriana no ha sido la excepción, aunque dicho tratamiento es novedoso y reciente.

La protección de datos personales en el Ecuador nace como un nuevo Derecho con la Constitución del 2008, en el numeral 19, del artículo 66; es por eso que parte de este trabajo es, analizar el problema relativo al manejo y manipulación no autorizada de los datos de carácter personal; y por otra, la revisión de la importancia del respeto y reconocimiento de este derecho.

Partiendo de la noción de que el marco constitucional ecuatoriano actual necesita mayor control para que el referido Derecho no se vulnere, es necesario precisar aquellas normas jurídicas ecuatorianas, relativas a la protección de datos personales, a fin de delimitar el ámbito de acción dentro del cual las personas pueden desenvolverse en lo que tiene que ver con la protección de la integridad personal, que se podrían vulnerar al momento de un mal uso o uso no autorizado de sus datos personales.

Abstract

Personal data involves information reflects some intímate aspects of people´s life and in that sense its inadequate and improper use can have serious repercussions for our integrity.

Therefore, globally, the issue of personal data has been treated for approximately the last 30 years, and Ecuadorian legislation has not been the exception; although related processes in this matter are new and fresh. The protection of personal data in Ecuador was created as a new law with the Constitution of 2008, included under paragraph 19, article 66, being this the main reason why part of this research is to analyze the problema of handling and tempering with such data, in addition to reviewing the importance of respect and recognition of this right.

Based on the notion that current Ecuadorian constitutional framework needs more control avoid violations of the afore mentioned law, it is necessary to specify those Ecuadorian legal norms concerning the protection of personal data in order to define the scope under which people can act regarding protection of personal integrity; that could be easily damaged or violated upon misuse or unauthorized access.

ÍNDICE

Introducción

Actualmente las tecnologías digitales permiten nuevas formas de injerencia en la vida de las personas. Gran parte de la actividad diaria de una persona queda registrada o filmada en alguna parte. Por esta razón es posible recoger, digitalizar y manipular los datos personales con total desconocimiento por parte del sujeto afectado, además los mismos pueden ser interrelacionarlos y analizados de manera impensable no hace mucho tiempo.

La protección de datos personales, en el ordenamiento jurídico ecuatoriano es un tema realmente nuevo, ya que a partir de la evolución de las nuevas tecnologías de información y su constante intercambio se ha visto la necesidad de proteger la integridad de los individuos, reflejada ésta en los datos que consigna en su diario quehacer; por esta razón, es necesaria la intervención del Derecho que siendo un instrumento regulador de la actividad del hombre en la sociedad, debe servir para la expedición de normas jurídicas.

Así, el Derecho a la protección de datos, atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, partiendo del reconocimiento que éstos van a ser objeto de manejo por parte de responsables públicos y privados. Este manejo impone a los responsables una obligación positiva, al momento de obtener información personal, que consiste en llevarlo a cabo con pleno respeto y reserva la información de una persona.

Con base a lo anterior, y a efecto de proporcionar un conocimiento respecto de los datos personales en el sistema jurídico ecuatoriano, como es su reconocimiento, formación, desarrollo y cuidado, a lo largo del presente trabajo de investigación se expondrá qué son los datos personales, la importancia de protegerlos, la normativa jurídica actual respecto a este tema, tanto a nivel nacional como internacional, y la razón por la cual se propone el reconocimiento normativo en materia de protección a los datos personales además de la creación de un órgano regulador que controle a las entidades públicas y privadas encargadas de manejar gran cantidad de información personal.

Capítulo I

1.- Protección de Datos personales

1.1 Definición:

A fin de delimitar el alcance de este trabajo, es importante determinar el alcance de los siguientes términos:

1.1.1 Dato:

"*Es un elemento circunscripto y aislado, como una referencia. Puede ser descriptivo, indicador, dar una pauta pero no se vincula a la información mientras el conocimiento no se transmita. Lo mismo sucede con las noticias o investigaciones*"[1].

El dato hace referencia a cualquier conjunto de letras, números o signos que tienen un significado. En consecuencia es una mera referencia; pueden ser números o signos que tienen un significado.

Por ende cuando se habla de dato personal es toda información que se refiere a un determinado sujeto y que puede ser su nombre, dirección, etc.

1.1.2 Personal:

Según la real academia de la lengua define el término "personal" como lo perteneciente o relativo a la persona, en otras palabras, esta acepción implica que algo es inherente a la calidad de persona de los seres humanos.

1.1.3 Datos Personales:

Una de las más concretas definiciones sobre datos personales se encuentra en el artículo 2, del Capítulo I, de la Directiva 95/46/CE del Parlamento Europeo y el Consejo, que establece:

[1] GOIZÍNI, Oswaldo (2002). El hábeas Data y la protección de datos. México, editorial Estudios constituciones. p 209

> *"Toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos e2específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social."*

Respecto de la protección de los referidos datos, en el artículo 8, de la Carta de los Derechos Humanos de la Unión Europea[2], aparece:

> *Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.…*

En tal sentido los datos personales deben mantenerse en reserva y de forma confidencial.

Es importante anotar que actualmente para todas las actividades que se realizan, es necesario el proporcionar información personal. Como por ejemplo:

- Al abrir una cuenta bancaria, solicitan tus nombres, apellidos, estado civil, dirección domiciliaria, números de teléfonos celulares y fijos, referencias personales, etc.
- Al momento de comprar algo por internet: en paypal[3], se requieren ciertos datos personales como por ejemplo: nombres, apellidos, número de documento de identificación, dirección de correo electrónico, número de teléfono, dirección domiciliaria, código postal, número de tarjeta de crédito.
- Al contratar un seguro médico, se requiere una serie de datos personales e incluso datos íntimos como es vida sexual, métodos anticonceptivos, enfermedades congénitas, etc., estos son datos

[2] Se proclamo el 7 de diciembre del 2000, busca reforzar la protección a los derechos fundamentales.
[3] Sitio web por medio del cual se pueden hacer compras con tarjetas de crédito.

sumamente sensibles que se proporcionan con la finalidad de asegurar la salud con la medicina pre pagada.

Este tipo de datos, al pertenecen al ámbito privado de una persona, deben ser tratados de manera adecuada, explicando a su titular la finalidad que van a tener y teniendo cuidado de que no sean traspasados a terceros sin expreso consentimiento.

1.1.4.- Protección de datos personales:

Como se anotó, la protección de datos esta prevista en la Carta de los Derechos Humanos de la Unión Europea, y en este sentido, el autor Dávara Rodríguez define a esta expresión como:

"*El amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en sus límites de su intimidad*."

Esta definición es correcta ya que la protección de datos personales busca que los individuos tengan una tutela adecuada para que sus datos no sean utilizados sin su consentimiento; este derecho permite a la persona disponer y controlar los datos que le pertenecen, no obstante éstos sean objeto de un tratamiento por responsables públicos y privados.

Este derechos es fundamental, más un si se toma en cuenta el desarrollo del comercio electrónico y de otras actividades en las que la información juega un rol esencial y su transmisión es prácticamente instantánea. En este sentido se ha establecido el "*data protection*"[4], que para el tratadista Hindious[5], es:

[4] Conjunto de normas y principios que regulan el tratamiento de datos personales en todas sus etapas, hace alusión a la manera como la información de las personas es recolectada, almacenada, procesada, utilizada, divulgada y transferida.

[5] GARCÍA BELAUDE, Domingo (2005). Diferencias entre el Hábeas data y la acción de amparo o tutela constitucional. Perú, editorial Red Ius et Praxis . pág 348

“Aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular del derecho individual a la intimidad respecto del procesamiento manual o autónomo de datos”.

Por lo tanto puede decirse que el derecho a la protección de datos garantiza a la persona su privacidad, además del disfrute y respeto a su propia identidad e integridad.

Respecto del fin que persigue la protección de los datos personales, podríamos decir que es básicamente establecer principios que proporcionen seguridad a la persona y procurar que no se omitan derechos constitucionales que vulneran la dignidad del ser humano.

Finalmente podemos dejar anotado que el derecho fundamental a la protección de datos de carácter personal es un derecho individual, reconocido en la Constitución de la República del Ecuador:

Numeral 19 artículo 66:

“El derecho de protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de ese carácter así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirá la autorización del titular o mandato de la ley”

En el Ecuador la protección de datos personales se ha vuelto un tema de trascendental importancia ya que la sociedad está en contínuo dinamismo y el constante intercambio de información permite que los datos personales sean vulnerados. Como dato histórico podemos mencionar que por primera vez en la Constitución del 2008 se incluyó a la protección de datos personales como un derecho.

1.2- Clasificación de los datos personales:

Los datos personales se clasifican de la siguiente manera:

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

Nominativo: es el dato de una persona física o jurídica conocida e identificada; el dato nominativo se refiere a una persona determinada y a su vez se divide en:

Directos: cuando lo identifica sin necesidad de proceso alguno.

Ej: el nombre

Indirectos: cuando permite la identificación por medio de la agrupación de datos. Ej: lugar donde trabaja

Innominativo o anónimo: es el dato de uso estadístico o científico que no identifica a persona alguna porque la información archivada no se refiere a él sino a sus actividades.

Ej: el numero de alunmos de un universidad.

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

Datos que no afectan la sensibilidad de las personas: se trata de aquellos datos del diario vivir que son de fácil acceso y que no afectan a la persona ni a sus sentimientos más íntimos ni su derecho a la privacidad.

Ej: el correo electrónico

Datos que afectan la sensibilidad de las personas:

Los datos sensibles son aquellos que al ponerse en conocimiento de terceros pueden afectar la integridad de las personas.

Ej: La salud, la condición racial y social, los pensamientos, los hábitos y costumbres de la persona.

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

Datos públicos o fácilmente conocidos: es aquella información personal que está disponible para cualquier persona por encontrarse en ciertos lugares de fácil acceso al público. El problema se da cuando estos datos no tienen restricción alguna para su conocimiento, esto es los censos, bases de datos de entidades públicas y privadas.

Para Herrán Ortiz[6] El dato accesible al público lo será cuando la fuente sea pública con carácter general, pero no cuando la misma tanga como fundamento un fin predeterminado y establecido entre quienes consienten la publicidad de dichos actos, ya que dicho consentimiento obedece a un interés de la propia persona de darse a conocer dentro del grupo de profesionales.

Datos privados, secretos y confidenciales: el dato privado es aquel que la persona mantiene con el carácter de reservado, en tal sentido, el dato secreto es aquel que solo conoce la persona y quienes están autorizados por ella. El dato confidencial es el que por ser sensible no se puede divulgar ni transmitir a terceros.

- ***Por la subjetividad o pertenencia del dato se clasifica en:***

Datos personales existenciales: son aquellos datos que se refiere a las características personales como es el nacimiento, fallecimiento, matrimonio, divorcio, domicilio, actividad profesional, patrimonio, afiliación política o sindical, confesión religiosa, desplazamientos, enfermedades o encarcelamiento. Estos constituyen una masa de datos que no tienen carácter personal cuando no puedan ser asociados a personas determinadas.

Datos no existenciales: son aquellos vinculados con el patrimonio económico y con la pertenencia de las cosas que identifican a un individuo. Así mismo es dato personal no existencial las informaciones referidas a condiciones personales o materiales relacionadas con cosas o bienes de otras personas.

[6] MÉNDEZ, Luis (2006). El derecho de habeas data. Uruguay. Editorial Real. Pág. 345

- ***Por el secreto que guardan:***

Los datos secretos y confidenciales se refieren a la relación que se debe guardar con alguien. Un claro ejemplo es el secreto profesional.

1.2.1Tipos de Datos Personales que más conocidos:

La doctrina tiene varias clasificaciones de datos personales pero una de las más didácticas y comprensibles es:

- Datos personales sensibles: son aquellos datos que no se pueden dar a conocer libremente por son de carácter íntimo personal o familiar que se guarda con mucha reserva un ejemplo es la orientación sexual.
- Datos personales nominativos: son aquellos datos que el titular entrega voluntariamente a una entidad u órgano con el afán de conseguir un determinado fin.
- Datos personales públicos: son aquellos datos que son de conocimiento abierto esto quiere decir que las personas lo conocen públicamente un ejemplo es el nombre del presidente.

1.3 Objeto de la protección de datos personales:

La protección de datos de carácter personal, tiene como objeto garantizar el derecho al honor y a la intimidad de las personas ya que el conocimiento o empleo por terceros puede afectar a sus derechos personalísimos.

1.4 La Intimidad:

El derecho a la intimidad inicia con el denominado “the right to privacy” que fue el título de un artículo publicado en 1890 en el Harvard Law Review por Samuel D. Warren y Louis D. Brandeis.

Dicho artículo hacía alusión al derecho de las personas de estar solas y de gozar de la vida sin la interferencia de terceras personas, respondía a la necesidad de tener una protección jurídica frente a la actividad realizada por los medios de comunicación que contaban, ya en esa época, con la posibilidad de difundir rápida y extensamente una noticia. Cabe señalar que en ese momento

estaba en auge la fotografía instantánea y ese adelanto tecnológico era utilizado por los periódicos de circulación masiva, con lo que las noticias respecto de los actos de una determinada persona eran acompañadas con imágenes de ésta o de sus actos sin contar con el conocimiento y autorización de las personas pertinentes.

Por este motivo se puede decir que el derecho a la intimidad es típicamente anglo americano apareció en los Estados Unidos de América en 1890 y ha evolucionado conforme lo ha hecho la tecnología en una sociedad que avanza con la tecnología, según la doctrina, el derecho a la intimidad se la concibe de la siguiente manera:

Para los tratadistas Argentinos Pierini, Lorences, y Tornabene "*el derecho a la intimidad es entendido como el poder o potestad de tener un domicilio particular, papeles privados, ejercer actividades, tener contactos personal y pensamientos que no trascienden a terceros en virtud del interés personal de mantenerlos en reserva.*"[7]

El alemán Hans Khler en 1880 menciona por primera vez: "*La existencia de un derecho individual que protege el secreto de la vida íntima de la publicidad no autorizada. En 1890 en un artículo de Harvad Law Review titulado ¨ The right to privacy¨, firmado por Samuel Warren y Louis Bandeis, se define al derecho a la vida privada, por primera vez, con una sencilla expresión: el derecho a ser dejado solo. A partir de allí encontramos el reconocimiento de tratados internacionales.*"[8]

La intimidad es un derecho que inherente al ser humano y que se traduce en el poder excluir a los demás del conocimiento de su vida personal como puede ser sus sentimientos, comportamientos y demás información que estime privada. Es importante mencionar que el ámbito intimo de un ser humano

[7] PIERINI Alicia, LORENCES Valentín, TORNABENE María Inés, (1998)
[8] CONDE ORTÍZ, Concepción (2006). La protección de datos personales, un derecho autónomo con base en conceptos de intimidad y privacidad. Madrid. Dykinson. Pág 232

incluye información que ni siquiera sus más allegados la conocen; es un círculo cerrado, no compartido, a menos que así lo decida.

El derecho a la intimidad está presente también en la sociedad computarizada, en la cual se otorga derechos a los individuos respecto de sus datos personales que son objeto de tratamiento automatizado e impone obligaciones y deberes de aquellos que controlan y tienen acceso a las bases de datos.

Existen tres grados de intimidad, así tenemos:

- La esfera privada
- La intimidad confidencial
- El secreto

El derecho a la intimidad de las personas ha venido en las últimas décadas siendo elaborado sobre la base de la creación de la protección de los datos personales, de tal forma que ha surgido la siguiente clasificación:

1.4.1 Intimidad Física:

- Vida sexual
- Funciones fisiológicas de excreción, así como de hechos y actos relativos al propio cuerpo que son tenidos por repugnantes o socialmente inaceptables
- Defectos, anomalías, enfermedades físicas no ostensibles
- Padecimientos físicos intensos
- El parto y la agonía de un ser humano

1.4.2 Intimidad psicológica:

- Ideas y creencias religiosas, filosóficas, para psicológicas y políticas que el individuo desee sustraerla conocimiento de un tercero.

- Momentos penosos como la muerte de una persona
- En general todo dato, hecho o actividad personal que no sea conocida por un tercero y que si se diera a conocer causara una afectación moral o psíquica.

Ahora bien, la relación entre el derecho a la intimidad y el derecho a la protección de datos personales o a la autodeterminación informativa ha sido analizada de forma diferente por la doctrina.

Groshan sostiene que los términos "*protección de datos" y "protección a la intimidad" son dos nociones distintas ya que el interés de proteger la veracidad de los datos y el uso de que ellos se hacen no está relacionado necesariamente con la protección de la libertad individual*.

La reflexión sobre la intimidad se remonta muy atrás en la historia, muy a menudo ligada con la especulación sobre la libertad. Por ello tiene trascendencia jurídica, sino que es uno de los aspectos más destacados en la historia de las ideas políticas.

1.5 La Privacidad:

Afirma el tratadista Carballo que "*el derecho de privacidad no representa sino la expectativa individual de control que cada persona tiene respecto de la información sobre sí mismo y la forma en que esta es conocida o utilizada por terceros"*

La Privacidad se deriva de la reserva esto es aquello que conocen ciertas personas y únicamente ellas, respecto de su esfera íntima, situaciones especiales, etc., como por ejemplo datos sobre la familia, religión, opinión política; de hecho así lo sostiene Carlos S. Nino[9] según el cual la privacidad es: "*el ámbito de las acciones de los individuos que no afectan a terceros.*

[9] TÉLLEZ VADEZ, Julio (2001). Manual de Derecho Informático. 3ª edición, México. Instituto de Investigaciones jurídicas de la UNAM. Pág 256

Pertenecen a una esfera personal y autorreferente. Son privadas aun cuando no hay limitaciones para el acceso público a su conocimiento."

La naturaleza del ser humano permite que se relacione con los demás en su entorno, sin embargo esta convivencia implica respeto y reserva sobre ciertos aspectos de la vida privada.

Thomas Ermeson menciona:" El Derecho de privacidad es el derecho del individuo para decidir por sí mismo en que medida comparte con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal."

La doctrina determina dentro de la privacidad lo siguiente[10]:

- El respeto a la vida privada de las personas
- El respeto a la vida pública de las personas
- Se asegura el respeto a la honra, honor o buen nombre de la persona y la de su familia.
- Limitación al derecho de publicación.

1.6 Origen de la protección de datos personales.-

A continuación se analizará de manera breve algunos fundamentos, que a nuestro criterio, pueden tomarse como el origen de la protección de datos personales y que están estrechamente relacionados con el derecho a la intimidad.

El derecho a la protección de datos como manifestación del derecho a la intimidad, que engloba el derecho a conocer quién almacena los datos y con qué finalidad, es el derecho de toda persona al control y disposición sobre sus datos personales, que deberá protegerse del mal manejo de los poderes públicos, asimismo, impone a terceros la realización adecuada al tratamiento de datos.

[10] AMANGUE, Juan. (2002*)* Derecho a la información y Hábeas Data e Internet. Buenos Aires. La roca. pág. 234

La protección a la intimidad de una persona, está prevista en la Declaración Universal de los Derechos Humanos (1948)[11], que en su artículo 12 señala:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Todo persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En este artículo se establece el derecho a la intimidad[12] en su sentido general. El derecho fundamental a la intimidad nace antes de la protección a los datos personales, y se traduce en normativa de cada país orientada a la protección del individuo respecto de posibles abusos a su vida privada.

1.6.1.- Convención Americana sobre Derechos Humanos (1969 Pacto de San José)

En su artículo 11 señala:

Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias abusivas o arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o esos ataques.

La sociedad y el intercambio de comunicación, permitió que desde hace muchos años se establezcan normas para garantizar los derechos de los individuos, tal como se puede apreciar en la norma invocada, en donde se establece que toda persona tiene el derecho a tener una vida privada y que nadie puede intervenir en ella ni afectar la honra, la dignidad, o su reputación.

---

[11] Es un documento declarativo adoptado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948 en París, que recoge los derechos humanos considerados básicos.

[12] Germán Bidart Campos define a la intimidad como : "la esfera personal que está exenta del conocimiento generalizado de un tercero"

1.6.2. Otros Convenios Internacionales.-

En 1978, la OCDE[13] creó el Grupo de Expertos sobre Barreras Transfronterizas de Información y Protección de Privacidad, al que le fue encomendado desarrollar pautas de consenso general, con la finalidad de armonizar las legislaciones domésticas de los países que fueron publicados el 1 de julio de 1979 como Lineamientos sobre la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales.

En otras legislaciones como la europea nace la protección de datos personales con el Convenio de Estrasburgo, convenio para la protección de las personas con respecto al tratamiento no autorizados de datos de carácter personal, que se celebró el 28 de enero de 1981, entre los miembros del Consejo de Europa, basándose en el respeto particularmente de los derechos humanos y de las libertades fundamentales, teniendo como objetivo ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados. Además persigue garantizar la seguridad de las personas, en el territorio de cada estado miembro, sean cuales fueren su nacionalidad o su residencia.

El 8 de noviembre de 2001 se firmo un protocolo adicional al convenio de 1981[14], que añadía dos nuevos artículos al convenio antes mencionado, estos versan; el primero, sobre la obligación de los Estados partes de establecer una garantía institucional u organismo independiente de control, para supervisar la aplicación de los derechos reconocidos en el convenio de 1981; el segundo por su parte, establece una serie de cautelas en relación con el flujo transfronterizo de datos. Este protocolo hasta ahora no ha entrado en vigor.

---

13 Organización para la Cooperación y el Desarrollo Económico

[14] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (ratificado por España el 27 de enero de 1984 y publicado en el B.O.E de 15 de noviembre de 1985)

Es necesario que entre en vigencia este protocolo, porque como se conoce las tecnologías de información crecen rápidamente y los datos de carácter personal siguen traspasándose a terceros sin ningún control, por lo que existe una enorme vulnerabilidad y peligro a las personas que sin saber, sus datos pueden estarse vendiendo o transmitiendo a otros países sin saber cuál será su finalidad.

1.7 Principios:

El derecho fundamental a la protección de datos está supeditado a otros derechos fundamentales, como el acceso a la información, la protección de la salud, la seguridad nacional u otros intereses públicos regulados legalmente, esto quiere decir que el principio de consentimiento deberá ceder ante tales intereses públicos cuando la ley o la autoridad competente así lo disponga.

La doctrina define algunos principios inherentes de protección de datos de carácter personal:[15]

1.7.1. Principio de consentimiento.-

Consiste en la importancia que tiene el titular de los datos para decidir el tratamiento automatizado de los datos de carácter personal no sólo tratándose del proceso de su recolección, sino también en el de la cesión de estos.

1.7.2. Principio de legalidad.-

Consiste en que no se puede recolectar los datos por medios fraudulentos o ilícitos. Esto es en base a engaños o mecanismos dolosos.

[15] CONDE ORTÍZ, Concepción (2006). *La protección de datos personales, un derecho autónomo con base en conceptos de intimidad y privacidad.* Madrid. Dykinson pág.456

1.7.3 Principio de veracidad.-

Consiste en la exactitud de los datos. Por ello, en caso de inexactitud, total o parcial, o incompleto de los datos de carácter personal registrados, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados

1.7.4 Principio de finalidad.-

Consiste en que los datos personales no puedan usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos. Esto es que sean usados para un determinado fin que conozca el titular que con su voluntad dio sus datos.

1.7.5 Principio de caducidad.-

Tiene que ver con la conservación temporal de los datos, la cancelación de éstos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados. Con esto, se evita que empresas privadas constituyan bases de datos destinadas a comercializar los antecedentes o datos personales de terceras personas, lucrando con datos ajenos y exponiendo a los titulares un profundo riesgo.

1.7.6 Principio de seguridad.-

Se refiere a que el responsable del archivo de los datos personales, tiene que adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

1.8.- Recolección de datos personales:

Como vimos existe un constante requerimiento de datos personales, lo cual implica un enorme flujo de información, que puede obtenerse de la siguiente forma:

- **Directo o voluntario:** cuando se requieren y consigna de una manera verbal (vía telefónica) o por escrito (llenado formularios, internet, encuestas);
- **Indirecto o involuntario:** cuando en el proceso de obtención no necesariamente tiene su consentimiento por ejemplo: por imágenes, por uso de bases de datos, referencias de gente conocida.

1.8.1La recolección de datos deberá llevarse a cabo tomando en cuenta:

No obstante la manera en que se recolecten los datos, deberá tenerse en cuenta:

- Se obtendrán y tratarán de forma leal y legítima;
- Se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;
- Serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;
- Serán exactos y si fuera necesario actualizados;
- Se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

1.9.- Internet y protección de datos personales.-

Como se señaló, es posible el acceso a los datos personales a tavés de varios medios, como por ejemplo el Internet, que hoy por hoy ha revolucionado la comunicación entre las personas, comunidades, estados, etc.

Rafael Gamboa Bernate afirma:"*La velocidad que han alcanzado las comunicaciones en la actualidad se debe en gran parte a los avances tecnológicos en el campo de la informática. La utilización masiva de computadoras en los procesos de escritura ha sido sucedida por la comunicación a través de redes informáticas y en este último fenómeno ha*

permitido la interrelación entre personas separadas físicamente por grandes distancias"[16]

Conforme con esta idea se puede concluir que el Internet es la red informática más grande en la actualidad. Es una fuente inagotable de información que da enormes ventajas para los usuarios, y sus funciones más importantes a nuestro criterio son:

1. Permitir que la gente pueda comunicarse a una gran velocidad, casi de forma instantánea, y a bajo costo, a través del sistema de correo electrónico o redes sociales; y,
2. Posibilita el acceso a una fuente de información casi ilimitada como lo es la World wide web (www).

Entre las actividades y servicios que han surgido en internet y las que implican el manejo de datos personales, con estrictos tratamientos sobre el mismo se pude mencionar:

- Servicio de correo electrónico, que permite intercambiar información de manera interpersonal entre los usuarios de la red.
- Directorios de personas (por ejemplo, directorios de correo) que permiten identificar a los usuarios de internet.
- Bases de datos accesibles desde internet, donde puedan existir datos personales referentes a un individuo, como por ejemplo: las bases de datos de morosidad, bases de datos de jurisprudencia, o bases de datos de médicos.
- Sistemas de intermediación en el mercado laboral, como por ejemplo agencia de empleo que pueden difundir datos personales en sus anuncios de oferta y demanda de empleo a través de internet o teletrabajo.
- Servicios de reservas de medios de transporte y alojamiento.
- Servicios relacionados con actividades de ocio, redes sociales, foros de discusión.

[16] PRADO HERRERA, Gerardo (2009). Los derechos fundamentales y la aplicación en la justicia constitucional. Bolivia. El Cid. Pág 158

- Servicios de venta electrónica, como librerías, programas informáticas.
- Servicios de publicidad y marketing, es decir agencias de publicidad electrónica.
- Servicios bancarios y financieros a través de Internet.
- Bases de datos de clientes (usuarios) abonados a un proveedor de servicio o de información en internet.

La gran cantidad de información almacenada en la red no tendría sentido sino contara con un sistema de comunicación tan eficaz como el que brinda Internet. Así como este sistema sirve no solo para la acumulación de información, sino también para su transmisión, hacemos notar que éstas características pueden ser utilizadas para que una serie de derechos, tales como la intimidad y la privacidad se vulneren y de esta manera se cause daño al ser humano.

En este sentido el tratadita Carlos Saltor*, menciona: "El poder informático se refleja en el poder que tienen las computadoras de acumular información en cantidad ilimitada sobre cualquier aspecto de la vida cotidiana. Esta información es proporcionada por los mismos individuos a bancos de datos públicos y privados para razonas determinadas, puede ser utilizada sin autorización para fines establecidos previamente, invadiendo así la zona de reserva del individuo y por consiguiente afectado su derecho a la intimidad"*[17]

1.9.1 Protección de datos personales en la Contratación Electrónica:

La contratación electrónica se presenta como una nueva forma de contratar, realizar intercambio de bienes y de servicios, la importancia que ha ido adquiriendo a través de los años ha convertido en una materia de interés jurídico por su creciente y constante aplicación práctica convirtiéndose así en uno de los ejes fundamentales de la sociedad. El tratadista español Davara, al respecto, señala que la contratación electrónica "es aquella que se realiza mediante la utilización de algún elemento electrónico cuando este tiene, o

[17] ZÚÑIGA URBINA, Francisco (2005). El derecho a la intimidad y sus paradigmas. Chile. Red ius praxis. Pág 86

puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo".

Con los medios electrónicos las partes pueden contratar fácilmente desde los lugares más lejanos del planeta logrando, de esta manera, unir al mundo en segundos. El consentimiento de las partes contratantes trasciende las fronteras generando, de esta forma, un nuevo mercado en donde las personas mediante el uso de sus computadoras compran, venden, donan, arriendan, intercambian bienes y servicios, realizando cualquier tipo de contratos, haciendo que la riqueza circule en el ambiente electrónico.

Asimismo ahora la contratación ya no se ve limitado a las transacciones de bienes materiales realizados de forma personal, sino que ahora gracias a las nuevas herramientas o medios electrónicos como es Internet, se puede hablar de transferencia de bienes y servicios inmateriales o digitalizados

Por lo tanto al momento de producirse la contratación electrónica los contratantes acceden a dar sus datos personales pero solo para el contrato que se está celebrando en ese momento. Esto significa que los datos deben tener un tratamiento adecuado y no pueden ser utilizados posteriormente para otros fines distintos a los que el titular autorizó,

1.9.2 Uso inadecuado de los datos (delitos informáticos)

A lo largo de este capítulo hemos visto no sólo qué implica un dato personal, los derechos que le resguardan, sino también su manera de recopilarse, ahora bien, en este aparatado revisaremos que ocurre cuando alguien hace un mal uso de datos personales considerado como confidenciales.

El acceso, uso o modificación de un dato personal sin la autorización de su titular, puede ser considerado como delito, así Téllez Valdés[18] conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a las "*las conductas antijurídicas tipificadas como tales, en las que se utilizan a las*

[18] TÉLLEZ VADEZ, Julio (2001). *Manual de Derecho Informático*. 3ª edición, México. Instituto de Investigaciones jurídicas de la UNAM. Pág. 134

computadoras como instrumento o fin; y, por las segundas, las actitudes ilícitas en que se tienen a las computadoras como instrumento a fin"

Por otra parte para, respecto de este tipo de delitos, el tratadista Ruiz Vadillo, sostiene: [19] "*por un lado, al hablar de la delincuencia informática en particular, establece que a su juicio son tres las zonas a las que se dirige la delincuencia informática;*

La parte patrimonial, el espionaje y la intimidad de las personas, siendo, a su juicio, en esta última donde hay que centrar la gravedad del problema y por otro al referirse a los medios concretos de realización de la delincuencia informática teniendo en cuenta la naturaleza del bien jurídico afectado. "

Para Bueno Arús[20] *le parece discutible la expresión delito informático por ser un concepto ambiguo con el que se puede concluir lo siguiente:*

Primero a los delitos que recaen sobre los objetos pertenecientes al mundo de la informática (destrucción o sustracción de programas o de material, alteración o reproducción de datos almacenados, utilización indebida de los ordenadores.

Segundo se refiere a la comisión de los delitos más variados y tradicionales (delito contra la intimidad, contra la fe pública contra el patrimonio)

En adelante se hablara de los delitos informáticos partiendo de la noción del tratadista referido, por cuanto al momento de invadir la intimidad de una persona, como en el caso de la manipulación de datos personales a través de medios electrónicos, existe un mayor riesgo de daño al titular de los mismos que cuando dicha manipulación se la lleva a cabo mediante medios físicos. No hay que olvidar que la comunicación a través de redes electrónicas es muy rápida y en este sentido más efectiva que la llevada a cabo mediante medios físicos.

[19]CANIHUA FLORES, Rubén (2007). Elaboración de una medida tecnológica que permita garantizar y proteger el adecuado tratamiento de los datos personales en el Internet de tercera generación. Chile. Campo verde. Pág 323

[20] CANIHUA FLORES, Rubén (2007). Elaboración de una medida tecnológica que permita garantizar y proteger el adecuado tratamiento de los datos personales en el Internet de tercera generación. Chile. Campo verde. Pág 323

Existe una serie de clasificaciones a los delitos informáticos, en esta tesis se cita la tradicional clasificación formulada por LAMPE[21], que responde a un criterio sistematizado, vinculado a las características del procesamiento automático de datos y a una separación de los diversos tipos criminológicos de conducta, y que agrupa las siguientes:

1. Manipulaciones de datos y programas, o fraude informático.
2. Copia ilegal de programas
3. Obtención y utilización ilícita de datos o espionaje informático.
4. Destrucción o inutilización de datos y programas o sabotaje informático.
5. Agresiones en el hardware o soporte material informático.

Veamos algunas de las maneras en que suele accederse a datos personales son contar necesariamente con la autorización del titular de los mismos.

1.9.3 Tipos de Delitos Informáticos:

- **Phishing:** es la pesca de claves a través de internet, la cual puede ser realizada por medio de programas especiales que pueden instalarse en la PC del usuario cuando este visita determinadas páginas o bien a través del envío de virus o programas adjuntados a los mail como troyanos, incluso en algunos casos se han presentado intrusiones directas por técnicas de hacking o más propiamente de cracking para la instalación de estos programas espías que envían información hacia otros equipos[22].

Como operan los estafadores en internet:

- En la primera fase, la red de estafadores se enfoca a los usuarios de chat, foros o correos electrónicos, a través de mensajes de ofertas de

[21] SALAZAR, Miguel (2005). El Derecho informático en la sociedad. Argentina Buenos Aires. Becerra. Pág 210

[22] ANGULO MARCIAL, Noel (2009). Manual de Tecnologías y Recursos de la información. México. Tecnology. P 124

empleo con una gran rentabilidad o disposición de dinero (hoax o scam[23]). En el caso de que caigan en la trampa, los presuntos intermediarios de la estafa, deben rellenar determinados campos, tales como: Datos personales y número de cuenta bancaria.

- Se comete el phishing, ya sea el envío global de millones de correos electrónicos bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria o con ataques específicos.
- El tercer paso consiste en que los estafadores comienzan a retirar sumas importantes de dinero, las cuales son transmitidas a las cuentas de los intermediarios a estas personas se las denomina muleros.
- Los intermediarios realizan el traspaso a las cuentas de los estafadores, llevándose éstos las cantidades de dinero y aquéllos, los intermediarios, el porcentaje de la comisión.

Trapping: consiste en la práctica de introducir interrupciones en la lógica de los programas con objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante. A pesar de que muchos confunden esta técnica con el phishing, su potencialidad es mucho mayor, ya que se trata de ataques mucho más avanzados ya que sólo obtiene claves bancarias.

Data leakage: o divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa.

Data diddiling: o introducción de datos falsos, es una manipulación de datos de entrada al ordenador con el fin de producir o lograr movimientos falsos en transacciones de una empresa ora otorgarle solvencia moral y económica a una persona que no la tiene. También puede ocurrir de publicar datos sensibles, como los referentes a las convicciones religiosas, políticas o a la vida íntima de las personas.

[23] Estafas o engaños.

Pharming: consiste en manipular direcciones DNS[24] para engañar al usuario y cometer fraude. Este realiza su ataque sobre estos servidores y su objetivo es cambiar la correspondencia numérica del servidor y hacer que en lugar de ir a una dirección o pagina web se desvié y se conecte con una web que es de delincuentes.

Spamming: es un término que se utiliza para indicar el fastidioso y no solicitado envió de mensajes publicitarios o comunicaciones y es una violación abierta a su intimidad personal on-line. Por esta razón se ha implantado mecanismo técnicos, jurídicos y de autodisciplina para contrarrestar tales comportamientos.[25]

1. 10 Bienes jurídicos protegidos:

La protección de los datos personales implica la protección de los siguientes bienes jurídicos:

1. La integridad de la persona. Si sus datos se vulneran podría ponerse en peligro su vida o al menos su salud, ya que el conocimiento de ciertos datos personales puede significar agresión, lesiones, tortura o muerte;
2. La intimidad. Porque al vulnerar los datos de un individuo se afecta un área muy sensible del ser humano que tiene repercusión en los ámbitos emocional y psicológico.
3. La dignidad. En concordancia con lo indicado en el numeral 1, el mal manejo de la información personal puede implicar vejaciones al titular de la misma.
4. El patrimonio. Ya que si se roba información de la misma se puede acceder, por ejemplo, a cuentas bancarias y así apropiarse de manera ilegal de dinero u otros bienes..

[24] Consiste en el servidor de la red de internet
[25] REYES KRAFFT, Alfredo (2009) Las firmas electrónicas y las entidades de certificación. México. Panamericana. Pág 187

Una vez ocurrida la vulneración de los datos de una persona, es menester determinar y ponderar qué bien protegido se vulneró y de qué manera se afectó al titular de la información confidencial, para de esta manera establecer la manera de resarcir el daño causado a la persona.

Capítulo II

2.- Análisis de las normas jurídicas ecuatorianas:

La protección de datos en Ecuador:

Como se analizó en el capítulo I, el manejo indebido de los datos personales, a más de causar serios daños al bienestar de una persona, puede poner en riesgo su vida; en este capítulo se analizará el alcance de la normativa jurídica ecuatoriana emitida para proteger los datos de carácter personal.

Antes de pasar a la revisión de la normativa referida, es importante destacar que existe discrepancia en la doctrina respecto de la concepción de “protección de datos”, como un concepto autónomo o como una derivación del derecho a la intimidad, así tenemos que:

Es un concepto autónomo porque tiene consecuencias propias, si bien está relacionado con el derecho a la intimidad, éste no se agota en aquel, sino que va más allá ya que incorpora características propias que pueden servir de base para una acción legal, independientemente de las acciones que pudiesen interponerse con base en la violación al derecho a la intimidad. Además porque la protección de datos constituye un derecho nuevo, que inicia a partir del derecho a la intimidad, pero es más general ya que este tipo de datos no necesariamente incluyen referencias íntimas de su titular. En el Ecuador se lo toma como un concepto autónomo porque nace como un sólo derecho independiente.

Por lo tanto puede decirse que el derecho a la protección de datos garantiza a la persona el disfrute y respeto a su propia identidad e integridad en todas las manifestaciones, físicas y espirituales.

Para los que afirman que la protección de datos personales es una concreción del derecho a la intimidad, ellos tienden a relacionar la noción de “dato personal” con la de “intimidad”, a tal punto que consideran que el simple hecho

de transmitirlos a un tercero afectaría a la persona, criterio con el que no compartimos ya que constantemente los datos personales están siendo entregados tanto a instituciones públicas como privadas, por lo tanto si se toma esta posición se entendería que todos los datos personales son íntimos y que no pueden ser conocidos, esto es un argumento bastante ambiguo y que en una sociedad que está en constante evolución no sería aplicable.

2.1 El Hábeas Data

En el Ecuador nace la protección de datos como un derecho a partir de la Constitución de la república del 2008[26], anteriormente solo se contemplaba del hábeas data como una garantía de los ciudadanos para acceder a los archivos y controlar su veracidad y difusión.

2.1.1 Antecedentes: Constitución Política de la República (1998)[27]:

Art. 94 Hábeas Data: "*Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.*

Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.

La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional."

[26] Públicado el 20 de Octubre de 2008 en el registro oficial 449.
[27] Aprobada por la Asamblea Nacional Constituyente, RO No 1 de 11 de agosto de 1998

En esta norma se concebía al hábeas data como una herramienta para conocer, acceder, usar, rectificar, actualizar, eliminar, anular, adoptar de medios de seguridad, demanda de perjuicios de un archivo.

El bien jurídico protegido era la veracidad de información. Concordantemente Vanossi[28] interpreta que el hábeas data protege lo inherente a la propia persona que es el derecho a su perfil y el derecho a su imagen. El referido derecho contempla dos aspectos: El primero relativo a los archivos y el segundo la modificación del registro en dos casos principales:

a) Cuando los datos son falsos.
b) Cuando los datos requieren de actualización.

Por lo tanto se puede afirmar que el Hábeas Data no procede si la información contenida en un banco de datos no es ni errónea ni incompleta, por lo que, si la información es correcta, completa y fue recolectada en forma legítima, esta garantía constitucional no resulta procedente.

> **Art. 23 de los derechos civiles:** *"Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes:*
>
> ***(…)***
>
> ***8.** El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona.*

En esta constitución se contemplaban los derechos invocados pero no el derecho a la protección de datos de carácter personal con lo cual aparentemente estos quedaban desprotegidos. Hay que tomar en cuenta que al vulnerar los datos personales, se está afectando además los derechos mencionados que son parte del ser humano, cuya protección consta en distintos tratados internacionales reconocidos a nivel mundial.

[28] GARCÍA BELAUDE, Domingo (2005)

2.2.- La Constitucion de la República del Ecuador(2008)[29]:

> **Art. 92 Hábeas Data: "***Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.*
>
> *Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.*
>
> *La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados."*

En esta nueva constitución, a diferencia de la de 1998, se toma en cuenta los denominados "datos sensibles" porque pertenecen a una categoría tal, que su manipulación no se relaciona con su veracidad o no, sino con los principios que su utilización puede ocasionar, que dada su naturaleza, para su difusión es necesaria la autorización por el titular de los mismos. Para su archivo se debe implementar mecanismos de seguridad tales que garanticen su integridad.

[29] Registro Oficial 449 públicado el 20 de Octubre de 2008.

2.2.1 Artículo 66 de la Constitución de la República:

- **Numeral 19:** *"El derecho de protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de ese carácter así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirá la autorización del titular o mandato de la ley"*

En concordancia con el art. 92 en este numeral se reconoce el derecho a la protección de datos de carácter personal que comprende:

1. La información que se quiere proporcionar, es decir que no pueden obligar a revelar ciertos datos cuya resera puede preferir a su titular; y
2. La autorización del titular de los datos para el archivo, recolección, procesamiento o difusión de los mismos.

- **Numeral 11:** *"El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica."*

En este numeral se establece claramente que nadie puede ser obligado a declarar de sí mismo. Ni revelar información personal o datos sensibles de terceras personas sin su consentimiento.

- **En el numeral 20:** "El derecho a la intimidad personal y familiar."

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 hogar, de la correspondencia, de la documentación personal, y en general de las comunicaciones privadas, dentro de las cuales debe

entenderse un cuidado extensivo a bienes materiales pertenecientes a la persona.

- **Numeral 21 :** *"El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación*."

En este numeral la protección de datos personales se encuentra de una manera implícita ya que el secreto a la correspondencia tanto física como virtual. Actualmente la sociedad de la información, a través de internet, emite una serie de datos que si son mal manejados, pueden poner en riesgo la integridad física, emocional, económica y hasta familiar de una persona. Como establece claramente la Constitución nadie puede violar este derecho al secreto de correspondencia.

- **Artículo 40 numeral 5:** *"Se reconoce a las personas el derecho a migrar. No se identificará ni se considerará a ningún ser humano como ilegal por su condición migratoria.*

  El Estado, a través de las entidades correspondientes, desarrollará entre otras las siguientes acciones para el ejercicio de los derechos de las personas ecuatorianas en el exterior, cualquiera sea su condición migratoria:

  (…)

  5. Mantendrá la confidencialidad de los datos de carácter personal que se encuentren en los archivos de las instituciones del Ecuador en el exterior."

Determina que los datos personales serán confidenciales cuando se encuentren en los archivos de las instituciones del Ecuador en el exterior, esto es para proteger la información personal aun cuando no se encuentre en el territorio nacional.

2.3La ley de comercio electrónico , firmas y mensajes de datos[30]:

Como se observa en la Constitución de la República del Ecuador, ya se habla del derecho a la protección de datos personales que tienen todos los individuos.

2.3.1 En el artículo 9 de esta Norma preceptúa:

"Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

[30]Ley 67 (Registro oficial suplemento 557 publicado el 17 de abril del 2002)

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo."

Este artículo hace relación a las bases de datos y al consentimiento del titular de la información que se recopila. Para su análisis deberá tomarse en cuenta las siguientes nociones que establece la Constitución:

1. **Intimidad:** es un derecho personalísimo que deriva de la dignidad de la persona e implica necesariamente la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás. Es la esfera personal es inalienable porque no le corresponde más que al individuo. Lo amparan tratados internacionales en el mundo entero y en el Ecuador la constitución en el numeral 20 del artículo 66.
2. **Privacidad:** constituye una esfera más amplia que el de la intimidad porque puede mantenerse en reserva ciertos elementos del conocimiento de terceros.
3. **Confidencialidad:** se refiere a cierta información que es conocida no sólo por una persona sino varias pero que debe quedar en reserva porque puede causar afectaciones a terceros.

En el Art. 5 de la ley de comercio electrónico, firmas y mensajes de datos: *"Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia."*

En concordancia con la Constitución que establece garantías a las personas, como son estos derechos personalísimos, en este artículo dispone la confidencialidad y reserva de los mensajes de datos ya que al igual que se protege la información física de igual manera debe existir una regulación para

lo que es información electrónica que se utiliza mediante un medio digital el cual tiene las mismas afectaciones e incluso peores ya que un mensaje de datos se puede enviar por la red y llegar al conocimiento de varias personas.

- **La disposición general novena de la norma invocada, establece:**

"Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica."

La ley de comercio electrónico, firmas y mensajes de datos establece las disposiciones generales para que se entienda a que se refiere con datos personales autorizados como se entiende son aquellos que el titular con su consentimiento, esto es su voluntad de entrega información personal a determinada persona u entidad para un fin específico. Aquí entra el principio de finalidad que la doctrina establece que cuando se recolecta datos personales tienen que tener un fin determinado y los datos que fueron entregados no pueden ser destinados para un fin distinto del que el titular de los datos dio su consentimiento.

2.4Ley Orgánica de defensa al consumidor.-

Art. 4.- *Derechos del Consumidor.- Son derechos fundamentales del consumidor, a más de los establecidos en la Constitución de la República, tratados o convenios internacionales, legislación interna, principios generales del derecho y costumbre mercantil, los siguientes:*

(…)

> *Numeral 4. Derecho a la información adecuada, veraz, clara, oportuna y completa sobre los bienes y servicios ofrecidos en el mercado, así como sus precios, características, calidad, condiciones de contratación y demás aspectos relevantes de los mismos, incluyendo los riesgos que pudieren prestar;*

Vale la pena citar a este articulado porque, los consumidores al momento de celebrar un contrato, entregan una serie de datos personales, los cuales deberían ser destinados para la finalidad del documento suscrito y para lo posterior estos datos ya no deberían ser tomados en cuenta; aquí se puede observar que por la falta de una regulación estrictamente en materia de datos personales en la realidad no se brinda un control ya que se traspasan los datos sin contar con la autorización de su titular.

2.5 Código Penal Ecuatoriano[31]:

> Artículo… (202.1), contempla la pena de 6 meses a 1 año de prisión y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica;
>
> *"El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad".*

Claramente el código penal establece como sanción por los delitos contra la inviolabilidad al secreto en este caso se está lesionando bienes que son jurídicamente protegidos como es la intimidad y la confidencialidad al acceder a información personal por medios electrónicos o informáticos violando claves.

[31] Registro Oficial 160, de 29 de marzo de 2010, reformado.

> Artículo.... (202.2) contempla la pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica;
>
> *"La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares"*

Este artículo hace especial referencia a los datos personales que sin autorización de su titular son conocidos por un tercero y manipulados. Es necesario conocer que la información personal no se puede violentar porque se afecta a otros derechos personalísimos que no solo afectan a la integridad de un individuo sino que pueden llegar a perjudicar la integridad familiar y como se ha estudiado hasta poner en riesgo la vida de las personas.

2.6 El código de ética médica[32]:

El secreto profesional es aquella información que se conoce por la actividad profesional en el ejercicio de un cargo determinado. El código de ética médica establece que los médicos por su profesión pueden llegar a conocer información personal muy sensible como son enfermedades géneticas; u otras que son única y exclusivamente de conocimiento de la persona; por lo que los profesionales de la salud deben guardar confidencialidad con respecto a lo que descubran en su profesión.

No hay que olvidar el famoso juramento de Hipócrates que es parte de la ética de los médicos y en su parte pertiene dice:

"*Guardaré silencio de todo aquellos que en mi profesión o fuera de ella oiga o vea de los hombres y que no deba ser público, manteniendo estas cosas en forma que no se pueda hablar de ella"*

[32] Código de ética médica, Registro oficial 300 publicado el 20 de octubre de 1993.

En el Capítulo IX Del Secreto Profesional

El Art. 66 establece:

"El secreto profesional es un deber que nace de la esencia misma de la profesión. El interés público, la seguridad de los enfermos, la honra de las familias, la responsabilidad del profesional y la dignidad de la ciencia médica, exigen el secreto. Los médicos tienen el deber de conservar en secreto todo cuanto observen, escuchen o descubran en el ejercicio de su profesión. ."

A continuación el Código de Ética Medica establece que el médico puede revelar el secreto profesional solo en los casos puntuales que se menciona acontinuación;

Art. 67*.- El médico no incurre en responsabilidad cuando revela el secreto profesional en los siguientes casos:*

a). Cuando en su calidad de perito actúa como médico de una compañía de seguros rindiendo informe sobre la salud de los candidatos que ha examinado, el que enviará en sobre cerrado al médico jefe de la compañía, quien tendrá la misma obligación del secreto;

b). Cuando es comisionado por la autoridad competente para reconocer el estado físico y mental de una persona; 8

c). Cuando ha sido designado por la autoridad competente para practicar necropsias o peritajes médicos legales de cualquier género, así en lo civil como en lo penal;

d). Cuando actúa con carácter de médico funcionario de los servicios sanitarios del país;

e). Cuando en su calidad de médico tratante hace declaración de enfermedad infecto - contagiosa ante la autoridad sanitaria y cuando expida certificado de defunción;

f). Cuando tratándose de menores de edad o mayores incapacitados mentales, lo exijan sus padres o representantes;

g). Cuando el médico es acusado o demandado bajo imputación de un daño culposo en el ejercicio de su profesión;

h). Cuando revela o denuncia los delitos que tenga conocimiento en el ejercicio de su profesión para que no cometa un error judicial; e,

i) Cuando a pedido expreso del paciente extienda una certificación sobre su afección o enfermedad.

La protección de los datos personales contenidos en las historias clínicas de los hospitales, resulta un tanto difícil y esto conlleva a invasiones arbitrarias o ilegales a la vida privada de las personas, así como la utilización de los datos personales para fines distintos por los que fueron recolectados por primera vez.

El dato de salud, por su naturaleza, es considerado como un dato sensible y como al resto de los datos personales, le es aplicable los principios de protección internacionalmente reconocidos, además que se debe contar con medidas de seguridad más altas que garanticen la confidencialidad, integridad y disponibilidad de la información personal.

Además sólo en estos casos especiales el médico queda libre de la responsabilidad de guardar el secreto, que por su conocimiento profesional llegue hacia él. Pero en ningún otro caso un médico podrá revelar o divulgar información estrictamente personal.

Es necesario destacar que la información de una persona, como la referida a una enfermedad infecto-contagiosa no debe ser revelada hacia terceras personas, ya que el afectado puede sufrir de discriminación o incluso de que su integridad personal, situación ésta que afectaría a los derechos constitucionales en especial los derechos de libertad que se establecen en el art. 66

2.7 El código municipal para el distrito metropolitano de Quito:

> ***Art. 3)*** *La Municipalidad del Distrito Metropolitano de Quito, en relación al uso de las Tecnologías de la Información y Comunicación, y en general a los temas de gobierno electrónico, se regirá por los siguientes principios:*
>
> *h) Principio de Confidencialidad, Seguridad y protección de datos.- Todo el proceso administrativo de la Municipalidad del Distrito Metropolitano de Quito se enmarca en una infraestructura segura y confiable por la cual se garantiza el respeto a la intimidad que procura esta interacción;*

El gran avance de la tecnologia ha permitido que la comunicación sea cada vez mas eficiente. En los medios electrónicos se almacena gran cantidad de información por lo que para la correcta protección de los datos personales es necesario establecer principios que regulen el acceso público a los mismos.

Estos procesos administrativos garantizan la protección a las personas en ámbitos tales como el patrimonio, integridad física y su intimidad.

2.8 Resolución de la Superintendencia de Bancos 306[33]:

A continuación se señala la importancia que los datos de carácter personal tienen al momento de realizar actividades en entidades bancarias que mediante esta resolución se regula que los datos tengan una protección específica en cuanto a esto se refiere los bancos tienen la obligación de guardar reserva y confidencialidad.

> **En el *Art. 14 preceptúa:***
>
> *"El usuario tendrá derecho a recibir protección y a demandar la adopción de medidas efectivas que garanticen la seguridad de las operaciones financieras, del defensor del cliente, de la Superintendencia de Bancos y*

[33] Resolución aprobada el 5 de Julio del 2006 tal como consta en la página Web de la Superintendencia de Bancos. No promulgada en el Registro Oficial.

Seguros o de otras instancias administrativas o judiciales pertinentes, especialmente en los siguientes casos:

14.2 Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos o servicios financieros. La información sobre dichos datos personales solo podrá ser otorgada por la institución del sistema financiero, en caso de consentimiento libre y expreso, específico, inequívoco e informado, por parte del usuario, de disposición judicial o del mandato de la ley;

14.3 Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos y servicios financieros prestados por vía electrónica. Las instituciones financieras adoptarán específicamente las medidas de seguridad necesarias para este tipo de operaciones financieras;

14.4 Obtener protección de los datos personales sobre su solvencia patrimonial y crediticia, y a que las instituciones financieras respeten las normas relativas a la reserva y sigilo bancario;

14.5 Exigir rectificación de la información de los datos personales en las bases de datos cuando esta sea inexacta o errónea;

14.6 Demandar protección cuando las instituciones financieras empleen métodos de cobranza extrajudicial que atenten contra su privacidad, dignidad personal y/o familiar;"

Es importante que se tomen medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados como es la información crediticia, contra el acceso, la modificación o la difusión no autorizada de información que es única y exclusivamente de una persona.

"Datos personales autorizados son aquellos que el titular ha accedido a entregar de forma voluntaria para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados. Datos Sensibles del consumidor son aquellos de información

financiera de cualquier tipo de números de tarjetas de crédito o similares que involucran transferir dinero o datos a través de los cuales pueden cometerse fraudes o ilícitos"

Aquí se puede analizar que los datos personales se los mencionan pero no se garantiza que estén protegidos verdaderamente; puesto que, el concepto es restringido y se los enumera de forma general no especificando la relevancia jurídica que estos puedan tener al momento que un tercero logre conseguir esta información. Muchas personas desconocen todo lo que abarca los datos personales y en la sociedad actual es fácil conseguir dichos datos, en varias ocasiones empresas privadas tan solo con una llamada telefónica logran conseguir información, o ciertas compañías logran realizar cierto tipo de encuestas que tienen como finalidad recolectar la mayor información posible de las personas y las mismas proporcionan esta información sin contar que está siendo utilizada para otros fines.

Capítulo III

3.- Breve análisis de la Normativa Internacional:

Luego de lo analizado, observando la necesidad que tiene el Ecuador de contar con una norma específica respecto de la protección de datos; una norma que brinde seguridad jurídica y que sirva para garantizar y proteger el tratamiento de datos personales, y todo lo que esto conlleva, es decir, las libertades públicas y los derechos fundamentales de las personas, especialmente los derechos al honor, intimidad personal y a la integridad. El referido ordenamiento jurídico debe tomar en cuenta la naturaleza de los datos, la finalidad y la duración del manejo.

Es importante tomar en cuenta la experiencia legislativa en otros países, un claro ejemplo es la europea, así, los países que conforman la Comunidad Europea llevan muchos años trabajando en este tema y son verdaderos expertos en la protección de datos, sin embargo, esto no significa que el legislador se limite a hacer una copia de la norma europea, por ejemplo la española, sino más bien legislando en virtud de las necesidades y características del medio ecuatoriano.

Al respecto, debe considerarse lo que dice al respecto el "Grupo de Trabajo Protección sobre Datos" de la Unión Europea[34], que sostiene que la regulación de un país, a más de principios de contenido y procedimientos de protección de datos personales, es necesario que incluya mecanismos y autoridades que efectivamente velen por la protección de dicha información. Los principios de la protección se establecen como base de parámetros al manejo de los datos personales, esto significa que basándose en estos principios las personas

[34] El grupo de trabajo creado por el artículo 29 de la Directiva 95/45/CE, es un órgano consultivo sobre protección de datos y vida privada. Sus funciones se definen en el artículo 30 de citada Directiva y en el artículo 14 de la Directiva 97/66/CE

puedan dar sus datos con la seguridad que no va a existir un abuso o manipulación de la que ellos no autorizaron.

Hay que tomar en cuenta que todo manejo de datos personales debe efectuarse de forma lícita y leal con respecto al interesado, dicha licitud se basa en el consentimiento informado del interesado.

La Directiva Comunitaria Europea considera que los datos personales deben ser:

a) Recogidos con fines determinados, explícitos y legítimos y no ser tratados posteriormente de manera incompatible con dichos fines;
b) Adecuados, pertinentes y no excesivos en relación con los fines para los que se recaben y para los que se traten posteriormente;
c) Exactos y actualizados; y,
d) Conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines que fueron recogidos.

Además ha incorporado en los respectivos ordenamientos jurídicos de los países de la Unión Europea[35], los lineamientos tales como:

- **La protección de datos;** quiere decir que los individuos que proporcionen datos tendrán la seguridad de que los mismos se encuentran protegidos de la manipulación de terceros.
- **La calidad de los datos:** Los datos de carácter personal podrán ser sometidos a tratamiento siempre y cuando sean adecuados, pertinentes y no excesivos de acuerdo a la finalidad para la cual han sido recabados;

[35] La Unión Europea (UE) es una comunidad política de Derecho constituida en régimen de organización internacional *sui generis*, nacida para propiciar y acoger la integración y gobernanza en común de los pueblos y de los Estados de Europa. Está compuesta por veintisiete Estados europeos, y su Unión fue establecida con la entrada en vigor del Tratado de la Unión Europea (TUE), el 1 de noviembre de 1993.

- **El derecho a la información en la recogida de datos:** Los interesados respecto de la prestación de un servicio o acceso a un bien, a los que se soliciten datos personales, deben estar informados de manera expresa, precisa e inequívoca, respecto del manejo que se dará a su información;
- **El consentimiento del afectado:** Se refiere a la aceptación del titular al momento de dar sus datos personales.;
- **Los datos especialmente protegidos:** Ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual;
- **Los datos relativos a la salud:** Potestad que tienen las instituciones, centros sanitarios públicos y privados y los profesionales respecto de la cesión de datos correspondientes a la salud;
- **La seguridad de los datos:** Obligaciones del responsable y del encargado del manejo del fichero;
- **El deber de secreto:** El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de datos personales deben guardar el secreto profesional respecto de los datos contenidos en los ficheros;
- **La comunicación de los datos:** La comunicación de los datos a un tercero debe contar con la previa autorización del titular de los datos; y
- El acceso a los datos por cuenta de terceros.

Tomando en cuenta estos lineamientos, se determina que una autoridad de control encargada de supervisar la actuación de los administradores de bancos de datos, quien ejercería sus funciones con plena independencia. Esto constituiría un elemento esencial de la protección de las personas, en lo que respecta al tratamiento de datos personales y a la vigilancia y efectividad de las normas sobre la materia.

Como corolario podemos manifestar que el Ecuador no debe ocupar el último grupo de países, en lo que protección de datos personales se refiere, tomando en cuenta que en el mundo existen tres grandes grupos; el primero, en donde se encuentran los Estados donde existe legislación (ejemplo : los estados miembros de la Unión Europea); el segundo, formado por aquellos países en los que se está trabajando en *pro* de una legislación; y, finalmente el tercero, que está integrado por aquellos países donde la legislación en materia de protección de datos ni siquiera existe.

3.1 En América Latina:

Tomando como ejemplo a la República de Argentina, que acogiendo los principios de la Directiva Comunitaria Europea, elaboró un conjunto de normas redactadas con el fin de garantizar los derechos al honor, a la intimidad y a la integridad familiar de las personas; esto permitió que sea reconocido como un país con un nivel de protección adecuado, indispensable para la transferencia internacional de datos.

En este país se promulgó una Ley sobre protección de datos personales (Ley N° 25326)[36], que desarrolló y amplió lo dispuesto en su Constitución, y que contiene normas sobre los principios generales de protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones. (También en el ámbito legislativo promulgó el Decreto Reglamentario Nº 1558/2001[37], que introdujo las normas de aplicación de la ley.)

---

[36] Promulgada en Buenos Aires-Argentina el 30 de Octubre de 2000. Ley de protección de los datos personales.

[37] Reglamentación de la Ley Nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Promulgada en Buenos Aires-Argentina el 29 de noviembre del 2001.

De esta forma se creó un órgano de control de protección de datos[38], encargado de realizar todas las acciones necesarias para cumplir los objetivos y preceptos de la ley, y que se denomina: “Dirección Nacional de Protección de Datos Personales”, DNPDP; y tiene a su cargo el Registro Nacional de las Bases de Datos, utilizado para conocer y controlar las bases de datos que circulan en el país, esta Dirección está bajo el control del Ministerio de Justicia, Seguridad y Derechos Humanos.

Otra de las funciones de esta Dirección, consiste en asesorar y asistir a los titulares de datos personales, tramitando las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos. Las denuncias que se hagan ante la DNPDP, revelan deficiencias o incumplimientos de las normas aplicables en el tratamiento de los datos personales que hagan los archivos, registros bancos o bases de datos ya que si se cumplen con las normas y se da el debido tratamiento a los datos no debería existir denuncias.

3.2 En Europa:

No obstante lo mencionado de la Unión Europea en acápites anteriores, reparamos en España, uno de los países que ha legislado este tema y actualmente se encuentra muy avanzado en la búsqueda del equilibrio entre el derecho a la intimidad y el derecho a la información en el camino a la protección del dato personal, que como vimos, a pesar de ser conceptos distintos, guardan mucha relación entre sí.

La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), es una Ley Orgánica española que 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

[38] El mismo que fue creado en el año 2002 en cumplimiento de la Ley Nº 25.326 para la efectiva protección de los datos personales. Su sede se encuentra en la Ciudad Autónoma de Buenos Aires

personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

La referida norma ***[39] introduce el concepto de tratamiento de datos, por medio de los ficheros que no se los entiende sólo como un deposito de datos sino como algo activo, en constante reforma y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, sin llegase a conectarse entre sí, de configurar el perfil personal.

Esta ley está motivada por la idea de implantar mecanismos cautelares que prevengan las violaciones a la privacidad que pudieran resultar del tratamiento de la información.

3.2.1 Agencia Española de Protección de Datos (AEPD)

Régimen de Protección:

> En España se creó la Agencia Española de Protección de Datos (AEPD) encargada de velar por el cumplimiento de la normativa sobre protección de datos, garantiza y tutela el derecho fundamental a la protección de datos de carácter personal. Es independiente en el ejercicio de sus funciones y su principal función es, como mencionamos, la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, tomando en cuenta los derechos de información, acceso, rectificación, oposición y cancelación de datos.

---

[39] Ley Orgánica de Protección de Datos de Carácter Personal. Publicada el 13 de diciembre de 1999.

Sin perjuicio de lo anterior, entre sus funciones, consta:

- Emitir autorizaciones previstas en la Ley.
- Requerir medidas de corrección.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
- Ejercer la potestad sancionadora.
- Recabar ayuda e información que precise.
- Autorizar las transferencias internacionales de datos.
- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

Deber de información de la Agencia Española de Protección de Datos:

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso:

1. 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.

2. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

3. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

4. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

5. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

El tratamiento de datos de carácter personal sin haber sido recolectados directamente del afectado o interesado, aunque no se exime de la obligación de informar de forma expresa, precisa e inequívoca, por parte del responsable del fichero o su representante.

En conclusión, como se puede ver, tanto en América Latina, así como en la comunidad Europea, el Derecho a la Protección de Datos Personales se ha convertido hoy en día una de las ramas del Derecho de mayor importancia a nivel mundial. El legislador nacional no debe ser ajeno a esa realidad y debe ser consciente de la cantidad de problemas que han surgido en la actualidad por la masificación de los medios y el avance tecnológico alcanzado que no ha hecho otra cosa que suprimir barreras de tiempo y espacio

3.3. Ecuador.-

Respecto de este país, se estima recomendable que, como medida organizativa, se cree un organismo (ente autónomo) que ejerza funciones de control, supervisión, fiscalización, inspección y sanción en materia de protección de datos, es decir, un organismo que se encargue de velar por el cumplimiento de la legislación sobre datos personales y controlar su aplicación, a más del control de todas las personas, empresas e instituciones que manejen archivos y bases de datos personales.

Otra actividad a su cargo podría ser la de auditar a las empresas, tanto públicas como privadas, en lo referente al tratamiento adecuado de los datos de cada persona, cuidando que los mismos sean destinados para el fin que fueron recolectados.

En conclusión a más de la legislación que se emita, la creación del ente estatal mencionado, lograría que en el país exista seguridad jurídica y que observe el cumplimiento de los demás derechos fundamentales que están ligados a este tema.

En tal sentido debería seguirse los ejemplos argentino y español, referentes directos en materia de protección de datos.

3.3.1 Propuesta de un órgano de control en Ecuador.-

Tomando en cuenta que el Ecuador es un país que aun no cuenta con ninguna regulación en cuanto a este tema, se estima, como se señaló antes, que a más de un marco jurídico concreto, se debe crear un órgano a cargo del control de la recolección, uso y manejo de las bases de datos, así recomendamos lo siguiente:

Departamento ecuatoriano de Protección de datos personales:

La entidad sugerida tendría las siguientes características:

Visión:

Ser una entidad de control comprometida con la excelencia, reconocida por altos estándares de desempeño, apoyada en un equipo profesional, capacitado para auditar el adecuado tratamiento y manejo de datos personales.

Misión:

Brindar seguridad jurídica con respecto a los derechos personalísimos, al tratamiento de los datos, velando el cumplimiento y aplicación de la ley de protección de datos personales.

Valores:

- Integridad: Actuación pública sustentada en la prudencia, entereza, rectitud y firmeza.
- Responsabilidad: trabajar con profesionalismo, diligencia, experiencia e independencia.

- Lealtad: Se garantiza la consolidación y mejoramiento de la entidad manteniendo los valores y el fortalecimiento del Recurso Humano

Objetivos:

Sus objetivos serían:

- Proteger los derechos de los individuos en cuanto a la calidad de los datos.
- Garantizar la calidad, la seguridad de la información personal y el servicio informático del almacenamiento de datos, con tecnología de punta.
- Fortalecer el marco legal y normativo de acuerdo a principios, mejoras prácticas y estándares a nivel internacional vigentes.
- Fortalecer la gestión organizacional y la administración del recurso humano.

Regulación Normativa:

- La aprobación del proyecto de Ley de protección datos personales por la asamblea nacional del Ecuador
- La aprobación del Reglamento de protección datos personales por la asamblea nacional del Ecuador

La normativa de protección de datos personales establecerá principios cuyo cumplimiento es obligatorio para los responsables de las entidades públicas que manejan el tratamiento de datos, como vía para garantizar al ciudadano el respeto a su derecho fundamental a la intimidad y otros derechos personalísimo además que se dispondrá la creación de un órgano regulador hacia estas entidades para que cumplan con el procedimiento adecuado en el manejo de datos que se estipula en la ley.

Naturaleza Jurídica:

Sería un ente de derecho público, con personalidad jurídica propia y plena capacidad en los ámbitos público y privado; actuará con independencia de las

administraciones públicas en el ejercicio de sus funciones. Conformado por 5 miembros, a saber:

1.- Un delegado de la superintendencia de compañías, un delegado de la superintendencia de bancos y seguros y un delegado de la superintendencia de telecomunicaciones, los mismos que tendrán que tener pleno conocimiento de la materia de Protección de datos personales;

De entre ellos se nombrara al Director de esta entidad de control, el mismo que tendrá un período de dos años, así consecutivamente serán todos elegidos como director

2.- Un delegado de la Contraloría General del Estado; y,

3.- Un delegado de la Procuraduría General del Estado.

Por lo tanto tendrá la siguiente estructura:

El Consejo Directivo de Protección de Datos

El Consejo Directivo de Protección de Datos, previsto en la Ley de protección de datos personales estará conformado por 5 miembros, que deberán conocer la ley de protección de datos personales, su reglamento y en general tener noción de la regulación que regula esta materia, tanto a nivel nacional como internacional.

Director del Departamento

El Director del Departamento es la persona que tiene que controlar que todo el Departamento Ecuatoriano de Protección de Datos Personales opere correctamente y cumpla con los objetivos planteados. Además determinará las políticas y directrices respecto de programas de capacitación y de sistemas adecuados de atención de las quejas presentadas por el público en general, respecto del mal uso, manejo inadecuado o falta de confidencialidad acerca de los datos personales.

Tendrá un período de dos años porque este tiempo es suficiente para poder desempeñar sus funciones y lograr con sus objetivos además que debe ser rotativo entre los tres miembros del Consejo Directivo que corresponde los delegados de la Superintendencias de Bancos y Seguros, Compañías y telecomunicaciones, los mismos que tendrán pleno conocimiento de la materia y ley de protección de datos personales.

Funciones:

- Controlar a cada una de las entidades públicas en cuanto al registro lícito de datos personales.
- 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.
- Tutelar los derechos y garantías de las personas naturales.
- Sancionar a las entidades públicas que no están dando un tratamiento correcto a los datos personales.
- Autorizar las transferencias internacionales de datos, una vez que el Ecuador suscriba tratados con otros países argumentando que cuenta con una normativa sólida en el campo de protección de datos personales.
- Supervisar a las entidades públicas sobre el correcto manejo de los datos personales.
- Lograr una adecuada administración de los datos personales mediante el fortalecimiento de los procesos de supervisión de las entidades controladas.

Obligaciones:

- Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones, así como otras personas físicas, en relación con los

tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de la ley.

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

Trámite:

El trámite que llevará a cabo la entidad de control en caso de que un organismo no proporcione la información correcta será por la vía administrativa por tratarse de entidades públicas.

Sanciones:

A las entidades públicas que manejen datos personales y no cumplan con la ley de protección de datos tendrán como sanción multas por el mal manejo de la información, o por su divulgación no autorizada. Además la entidad de control hará un informe a la Contraloría General del Estados para que tome las medidas pertinentes si las entidades no cumplen con las medidas necesarias para proteger los datos personales.

Capítulo IV

4.1 Conclusiones:

- El derecho a la protección de datos atribuye a una persona el poder de disposición y control sobre datos que le conciernen, partiendo del reconocimiento de que tales datos van a ser objeto de un tratamiento que se lleve a cabo con pleno respeto a derechos personalísimos que desemboca esta protección. En ocasiones se ha planteado que el derecho a la protección de datos constituye una barrera para la tutela de otros derechos fundamentales o intereses públicos como la libertad de información, transparencia y acceso a la información que obre en poder de entidades públicas y la respuesta es que frente a estas afirmaciones debe destacarse que no se producen propiamente conflictos entre unos y otros, sino que debe existir una ponderación de derechos y claro esta como se hablo en esta tesis existen excepciones a la protección de datos personales por ejemplo cuando se trata de seguridad del estado, o que por orden de la autoridad competente se tenga que revelar cierta información. Sin embargo, no puede olvidarse que sólo respetando el derecho fundamental de todos a la protección de sus datos personales se conseguirá un marco jurídico equilibrado donde se respete los derechos inherentes al ser humano.

- Si bien en la vida diaria se van a requerir datos personales constantemente, el temor a que éstos sean utilizados ya sea de una manera inapropiada o no autorizada, no quiere decir que las personas se deban aislar de la sociedad, al no proporcionar información de carácter personal, sino al contrario, implica que deben hacerlo, pero tomando las medidas cautelares del caso y exigiendo un tratamiento correcto como se propone en el proyecto de ley. En suma, el titular de un dato personal debe procurar, a través de los medios a su alcance, ya sean físicos o legales, que su información personal no sea captada,

almacenada o manipulada sin su autorización. Es importante hacer hincapié en que el titular de los datos personales debe informarse acerca del manejo que van a recibir sus datos esto quiere decir que se apliquen los principios establecidos y sus datos no sean traspasados o manipulados sin control alguno.

- Se debe proteger los datos personales desde dos puntos de vista: primero la seguridad integral, esto se refiere a que el titular de los datos es el que decide que información va a proporcionar ya que existen datos que por su sensibilidad no pueden ser conocidos por cualquier persona y sólo en casos especiales se podrían obtener, ya sea con la autorización de la persona o con una orden de autoridad competente; y, la segunda se refiere a la seguridad normativa, basada en leyes que ampare a las personas respecto de la obtención, manipulación o modificación no autorizada de sus datos, a través de la interposición de las acciones legales pertinentes.

- Existe comentarios acerca de si la protección de datos personales es lo mismo que el Hábeas Data y definitivamente la respuesta es no puesto que el hábeas data no procede si la información contenida en un banco de datos no es ni errónea ni incompleta, por lo que, si la información es correcta y es completa, y fue acopiada en forma legítima, aún causando discriminación esta garantía constitucional no resulta procedente. Es lo que sucede con los bancos de datos destinados a brindar informes de carácter económico, respecto de los cuales en el Ecuador se ha reconocido como de rango superior al derecho a la privacidad de las personas, el derecho de la colectividad a conocer los antecedentes crediticios de los individuos en sus relaciones comerciales y patrimoniales con los restantes miembros de la sociedad.

- Existe discrepancia en la doctrina acerca de si la protección de datos es un concepto autónomo o es una derivación del derecho a la intimidad y se concluye que es un derecho nuevo, autónomo porque para proteger

un dato personal no necesariamente tiene que ser íntimo. Partiendo de dos directrices que es la libertad informática que consiste en la potestad de vigilar los datos personales contenidos en archivos y la autodeterminación informática que es el poder de controlar los datos.

- El avance tecnológico es indispensable para el desarrollo de la sociedad, pero a su vez este pone en riesgo a las personas que no conocen como proteger su información personal, un claro ejemplo esta en el Internet, debido a la gran cantidad de información que se suele suministrar a través de esta red, o a través de redes sociales, en donde es fácil acceder al perfil de una persona. Si no se establecen seguridades correctas como el manejo de la privacidad, individuos totalmente ajenos pueden acceder y conocer el perfil de una persona. Otro ejemplo son ciertas actividades que requieren información crediticia que llega a formar parte de bases de datos y que tan solo con ingresar el nombre completo de una persona se conoce su estado financiero y demás, esto resulta peligroso ya que puede ser traspasado a terceros si ningún control y claramente se puede vulnerar el derecho a la protección de datos personales porque, no existe el consentimiento de la persona en que se establezcan límites en cuanto a la información que se va a conceder.

- Tener una normativa específica en materia de protección de datos personales permitiría al Ecuador tener mayores beneficios no solo porque se evitaría una serie de abusos en cuanto al uso indebido de la información sino porque permite proyectarse a una sociedad digital donde el internet proporciona una gran cantidad de ventajas tanto tecnológicas como culturales, pero así mismo se ha desencadenado una serie de inconvenientes que deben ser vistos desde el punto tecnológico y el jurídico, se debe resaltar que la mayoría de riesgos son aun desconocidos debido a la manera como se desarrolla la tecnología la cual contribuye un cambio diario en el mundo. Por la misma filosofía de la sociedad de la información son innumerables las diversas conductas

que se pueden considerar lesivas y ciertamente es muy difícil determinar a la persona que se encuentra tras un computador debido a que no se cuentan con parámetros jurídicos sólidos para determinar la responsabilidad, en esta era digital nace la necesidad de crear organismo de control en el Ecuador que no solo regulen el manejo indebido de los datos sino que los individuos tengan una tutela que brinde a mas de protección, formas de instruir a las personas para que estas conozcan y no permitan que sus datos se vulneren.

4.2 Recomendaciones:

- La protección de datos personales es un derecho que debe ser tutelado por la Ley y sus titulares deben conocer cómo y ante quien pueden exigirlo es necesario equilibrar los vacios legales existentes en la actualidad donde solamente se ha legislado en el ámbito del derecho al acceso a la información. Como se mencionó la información de una persona es valiosa y en tal sentido, no cualquiera puede conocerla ya que de ser así se podría poner en riesgo una esfera muy delicada del ser humano que es su intimidad, privacidad, integridad, etc. El Derecho es evolutivo y va cambiando para satisfacer las necesidades de la sociedad por esta razón, proteger los datos personales se vuelve indispensable ya que la mayor parte de ésta es asequible para un gran número de personas.

- Se debe mirar el modelo europeo en cuanto a materia de protección de datos personales ya que poseen bases sólidas del tratamiento adecuado de los datos de un individuo además que existen convenios entre países europeos para cuidar los datos personales que cada vez se van ampliando no solo por cuidar la intimidad de las personas sino porque mejoran el comercio internacional ya que las grandes tecnologías de la información permiten perfeccionen contratos via internet con varias personas a nivel mundial.

- Actualmente se guarda una cantidad de información personal en computadores laptop, teléfonos celulares (smartphones), y en tal virtud, sus dueños o tenedores deben tomar precauciones, esto quiere decir que se debe utilizar claves con alto grado de seguridad que incluyan, por ejemplo letras y números para que si alguien diferente a su dueño llegara a poseerlos no pueda acceder y robar esta información.

- Con respecto a las nuevas tecnologías de la información es importante que los padres hablen a sus hijos sobre el peligro de poner sus datos personales en internet ya que por este medio la información se traspasa rápidamente y sin pensarlo pueden caer en manos de personas peligrosas que usen esa información para otros fines.

4.3 Proyecto de ley a la Protección de Datos Personales.-

Después de haber analizado la importancia de la protección de datos personales en el Ecuador, considero importante sugerir una norma específica en este tema, en la cual se regule el manejo de los datos personales, a través de entidades encargadas de su recolección y su almacenamiento.

En el numeral 19, del artículo 66 de la Constitución de la República del Ecuador, se garantiza, en forma expresa el derecho a la protección de datos de carácter personal, el cual incluye el acceso, la decisión sobre información y datos de ese carácter, así como la correspondiente protección; así mismo se dispone, que la recolección, archivo, procesamiento, distribución, difusión de datos personales o información, requerirán para ello la autorización de su titular o por mandato de la ley; y que en la misma norma, se garantiza el derecho a la intimidad personal y familiar.

Además en el artículo 92, de la norma invocada, se preceptúa como garantía constitucional, al hábeas data, estableciendo que toda persona tiene derecho a conocer de la existencia y acceder a los documentos, datos genéticos, bancos, archivos de datos personales e informes sobre sí misma, o sobre sus bienes,

que consten en entidades públicas o privadas, en soporte material o electrónico. Además se señala que tendrán derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Sólo con autorización los responsables de los bancos y archivos de datos personales podrán difundir información. O por mandato de la ley;

4.3.1 CAPÌTULO I

Art. 1.- **(Objeto)** Esta ley, tiene por objeto garantizar y proteger los datos personales, específicamente en su tratamiento, aquellos que se encuentren en ficheros, archivos, registros, bases o bancos de datos físicos, digitales o tecnológicos de entidades públicas destinadas a proporcionar información o recolectar la misma. En ningún caso se podrá afectar bases de datos y fuentes de información periodísticas.

Art. 2.- (Ámbito) La presente Ley, se aplicará a los datos personales registrados en soporte físico, electrónico o digital, susceptibles de tratamiento, y a toda forma de uso posterior que manejen las entidades públicas como órganos de control. El responsable del tratamiento no establecido en territorio nacional, se sujetará a las normas de esta Ley, en cuanto fuere aplicable, conforme a las normas del Derecho Internacional Público, como también cuando no esté establecido en territorio nacional y utilice medios de tratamiento ubicados en Ecuador, salvo que éstos se utilicen únicamente con fines de tránsito.

Con excepción de los siguientes casos esta ley no será aplicable, al tratamiento de datos:

- La seguridad pública,
- La defensa y la seguridad el Estado

- Actividades sobre investigación del terrorismo y formas graves de delincuencia organizada al igual que investigación de delitos de corrupción y de lesa humanidad.

No se aplicará a los archivos que, se encuentren en el sistema de régimen electoral, los que sirvan para fines exclusivamente estadísticos, los que tengan por objeto el almacenamiento de datos contenidos en los informes personales de calificación de las Fuerzas Armadas, los derivados del Registro Civil y del Registro de Antecedentes Penales, los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas Armadas, Policía Nacional y otros órganos de seguridad, conforme a las leyes pertinentes. No se sujetan a esta ley, el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

4.3.2 CAPÌTULO II

De los principios

Art. 3.- (Licitud). La elaboración de archivos o bases de datos, sea por medios electrónicos o no, deberá ser lícita, observando en su procedimiento los principios establecidos en esta Ley y el reglamento que se dicte; no pueden tener finalidades contrarias a las leyes, a las buenas costumbres o a la moral pública.

Art. 4.- (Calidad). Los datos personales recolectados y que sean objeto de tratamiento, deben someterse a los siguientes requerimientos de calidad:

a. Deben ser lícitos, legítimos, ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad;

b. No podrán ser utilizados para fines distintos e incompatibles con aquellas que motivaron su obtención, salvo por asuntos históricos, estadísticos o científicos.

c. La recolección no podrá hacerse por medios arbitrarios, desleales, fraudulentos o ilícitos.

d. Los datos serán exactos y recientes, se pondrán al día de forma que respondan con certeza a la realidad del afectado.

e. Los datos personales, total o parcialmente inexactos o incompletos, serán de oficio cancelados y sustituidos o en su caso completados por el responsable del archivo o base de datos, sin perjuicio de los derechos y garantías de los afectados.

f. Serán almacenados de manera que, permitan a su titular el ejercicio del derecho de acceso, salvo que sean legalmente o por orden judicial, cancelados.

g. Serán cancelados y destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hayan sido recolectados o registrados.

h. No serán conservados, de modo que permita identificar al interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

El Reglamento establecerá por excepción, el procedimiento para el mantenimiento integro de determinados datos, atendiendo valores históricos, estadísticos o científicos de acuerdo con la legislación específica.

Art. 5.- (Recolección). En la recolección de datos personales, previamente se deberá informar a su titular, en forma expresa, clara, precisa e inequívoca, sobre:

a) La finalidad del tratamiento y quiénes son o pueden ser sus destinatarios y la clase de destinatarios;

b) La existencia de archivos o bancos de datos, físico, electrónico, digital o de cualquier otro tipo y la identidad y domicilio del responsable;

c) El carácter obligatorio o facultativo de las respuestas al interrogatorio que le sea propuesto, en especial en cuanto a los datos sensibles.

d) Las consecuencias de la obtención de los datos, de la negativa a proporcionarlos o de la inexactitud de los mismos, y;

e) La posibilidad de ejercitar los derechos de acceso, rectificación, supresión, oposición y la acción de hàbeas data.

Art. 6.- (Consentimiento). El tratamiento de datos personales, se sujetará obligatoriamente a los siguientes requerimientos:

a. El consentimiento libre, expreso, informado e inequívoco del afectado, constará por escrito o por otro medio que lo equipare de acuerdo a las circunstancias, de no ser así adolece de ilicitud, salvo disposición en contrario.

b. El consentimiento podrá ser revocado de haber causa justificada para ello y no se le atribuyan efectos retroactivos.

c. Cuando no se requiera el consentimiento del afectado para el tratamiento de datos personales, y siempre que una ley no disponga lo contrario, podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal, en tal caso el responsable del fichero, archivo, registro, soporte, base o banco de datos los excluirá del tratamiento.

Art. 7.- (Excepciones) No se requerirá el consentimiento del interesado de los datos personales, cuando:

a. Se deriven de una relación contractual, científica o profesional y se requieran para su desarrollo o cumplimiento;

b. El tratamiento tenga como fin proteger un interés vital o superior del afectado, en los términos establecidos en esta Ley;

c. Se encuentren en soportes absolutamente de acceso público y sea necesario para la satisfacción del interés colectivo legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre y cuando no vulneren derechos, garantías y libertades establecidas en la Constitución de la República.

d. Se trate, de listados, registros, padrones, repertorios, inscripciones, asientos, archivos, protocolos, cuyos datos se limiten al nombre, número de documento de identidad, identificación tributaria o previsión y seguridad social, ocupación, fecha de nacimiento y domicilio, y;

e. Se refiera, a operaciones que realicen las entidades financieras y a las informaciones que reciban de sus clientes conforme a Ley.

Art. 8.- (Protección especial). Son objeto de protección especial los datos sensibles:

a. Ninguna persona está obligada a suministrar o proporcionar información sobre datos sensibles.

b. Podrán ser recolectados y tratados solamente cuando existan razones de interés general que permita la Ley o tenga finalidades estadísticas, científicas o históricas, siempre y cuando sus titulares no puedan ser identificados o el titular lo consienta de forma expresa.

c. Se prohíbe crear archivos o bancos de datos que contengan información que revelen datos sensibles en forma directa o indirecta, solo las organizaciones políticas y sindicales podrán hacerlo en forma general.

d. Los datos relativos a antecedentes penales podrán ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las disposiciones constitucionales, las leyes y reglamentos respectivos.

e. Podrán ser objeto de tratamiento, los datos personales que revelen ideología, filiación sindical o política, religión y creencias, mediante consentimiento expreso y por escrito del afectado.

Art. 9.- (Excepciones). Podrán tratarse datos sensibles, cuando sea necesario para la prevención, diagnóstico o tratamiento médico, la prestación de asistencia o gestión de servicios de salud, siempre que lo realice un profesional de la materia bajo las normas éticas y de secreto profesional o el tratamiento para salvaguardar la vida del afectado o de otra persona que esté incapacitada física o legalmente para dar su consentimiento.

Art. 10.- (Seguridad). Las personas responsables o usuarias del archivo, están obligadas a adoptar medidas tecnológicas y organizativas, para, garantizar la seguridad y confidencialidad de los datos personales, evitar adulteraciones, pérdidas, consulta o acceso y tratamiento no autorizado y que permitan descubrir las desviaciones intencionales o no de información, ya sea que los riesgos provengan de la acción humana o del medio tecnológico usado.

Está prohibido registrar datos personales en archivos o bancos de datos que no reúnan condiciones tecnológicas de integralidad y seguridad.

Art. 11.- (Automatización de bases de datos). En el caso de bases de datos que se mantiene en archivadores físicos se establecerá como tiempo máximo 7 años desde que esta ley entre en vigencia para que se automatice todas las bases de datos y se brinde la seguridad que establece el artículo anterior.

Art. 12.- (Secreto). La persona de la entidad pública que intervengan en cualquier estado del tratamiento de los datos personales están obligadas a mantener el secreto y a guardarlos fidedignamente; obligaciones que se mantendrán aun después de finalizar las relaciones con el titular, con el responsable del mismo. Se exime del deber de secreto, cuando medie orden judicial o haya razones fundadas relacionadas a la seguridad pública, la defensa nacional o la salud pública.

Art. 13.- (Cesión) Los datos personales objeto de tratamiento sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con el interés legítimo del cedente y del cesionario, con consentimiento previo de su titular, debiendo informárselo sobre la finalidad de la cesión e identificación del cesionario o las características que permitan hacerlo; el consentimiento para la cesión es revocable en cualquier momento. No se requerirá el consentimiento en los siguientes casos, cuando:

a. La ley así lo disponga.

b. Se trate de cesión entre dependencias de los órganos e instituciones del Estado en forma directa, en el ámbito de sus competencias.

c. Se trate de datos personales sobre salud y se requieran por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos o científicos, siempre y cuando se preserve la identidad de sus titulares mediante mecanismos de disociación adecuados;

d. Se hubiere aplicado un procedimiento de disociación de la información, de tal manera que los titulares de los datos sean inidentificables.

Art. 14.- (Transferencia internacional). Se prohíbe la transferencia de datos personales a países u organismos internacionales, que no ofrezcan seguridad y proporcionen niveles de protección adecuados.

Esta prohibición no tiene lugar cuando:

a) Se trate de asistencia judicial internacional;

b) Se refiera a intercambio de datos de naturaleza médica, de así requerir el tratamiento del paciente o por una investigación epidemiológica, de conformidad con las normas de la presente ley.

c) Se trate de transferencias bancarias o bursátiles y de las transacciones que de ellas se deriven, de acuerdo a las leyes aplicables;

d) Se hubiera acordado en el marco de tratados internacionales de los cuales la República del Ecuador sea parte;

e) Tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

No se considerará transferencia de datos el acceso de un tercero a los datos, cuando el mismo sea necesario, para la prestación de un servicio al responsable del tratamiento.

Art. 15.- (Tratamiento por terceros). El tratamiento por terceros debe constar en contrato escrito o en alguna otra forma que permita acreditar su celebración y contenido, se establecerá en forma expresa y clara que el encargado únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que, no aplicará o utilizará con fines distintos a los que constan en el contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato constarán las medidas de seguridad establecidas en esta Ley, que el encargado del tratamiento está obligado a implementar.

Cumplida las obligaciones contractuales, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento, al igual que el soporte o documento en que conste algún dato materia del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las cláusulas contractuales, será también responsable de las infracciones en que hubiera incurrido e incluso sanciones penales.

4.3.3 CAPÌTULO III

Derechos de los titulares de datos

Art. 16.- (Información). Toda persona podrá solicitar al organismo o institución pública información sobre la existencia de ficheros, archivos, registros,

soportes, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables, de constar en los mismos sus datos. El registro que se lleve para el efecto será de consulta pública y gratuita.

Art. 17.- (Acceso). El titular, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales que consten en los archivos o bancos de datos públicos o privados, en forma gratuita en intervalos no inferiores a seis meses, salvo justificación de un interés legítimo podrá hacerlo antes; en el caso de datos de personas fallecidas, corresponderá a sus herederos ejercer este derecho.

El responsable o usuario proporcionará la información en el término de diez días contados a partir de la fecha de haber sido requerido, vencido el cual, de no haberse cumplido o si consignado el informe, se considera insuficiente, queda expedita la acción de protección o de hábeas data prevista en la Constitución y la ley.

Art. 18.- (Contenido). La información debe ser proporcionada en forma amplia, clara, precisa detallada, sin codificaciones y acompañada de una explicación inteligible, en lenguaje sencillo accesible al conocimiento medio de la población, y versar sobre la totalidad del registro perteneciente al titular, aun cuando la petición se haga sobre un solo aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, a pesar de estar vinculados con el interesado. La información, a elección del titular, podrá entregarse por escrito, por medios electrónicos, digitales, telefónicos, de imagen, u otro idóneo.

Art. 19.- (Rectificación, actualización o supresión). Toda persona tiene derecho a que sus datos personales que estén incluidos en un archivo o banco de datos, sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad.

El responsable o usuario del banco de datos, procederá a la rectificación, supresión o actualización de los datos personales del afectado, en el plazo

máximo de cinco días hábiles de recibida la petición del titular o de advertido del error o falsedad. El incumplimiento de esta obligación, faculta plantear una queja al Departamento ecuatoriano de datos personales prevista en la presente ley para que se aplique la sanción correspondiente.

Los datos personales deben ser conservados durante el tiempo establecido en esta Ley o en las cláusulas contractuales.

Art. 20.- (Excepciones). Los responsables o usuarios de bancos de datos públicos podrán, mediante resolución motivada, negar el acceso, rectificación, actualización o la supresión cuando se trate de, proteger la defensa del país, el orden y la seguridad públicos, o los derechos e intereses de terceros; de igual manera, cuando puedan obstaculizar actuaciones judiciales o administrativas dirigidas a la investigación sobre incumplimiento de obligaciones tributarias o de aportes a la seguridad social, el desarrollo de funciones de control de la salud y de la naturaleza y el ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser motivada y notificada al afectado.

Sin perjuicio de lo establecido, se deberá brindar acceso a los registros indicados en caso de que el afectado lo requiera para ejercer el derecho a la defensa.

Art. 21.- (Gratuidad). No tendrá valor económico alguno para el interesado, el acceso, rectificación, actualización o supresión de datos personales inexactos o incompletos que se encuentren en registros públicos o privados.

Art. 22.- (Valoraciones). Las decisiones judiciales o los actos administrativos que contengan valoraciones de conductas humanas, contendrán datos personales que definan el perfil o la personalidad del interesado; los actos o decisiones contrarios serán absolutamente nulos.

Art. 23.- (Datos personales informatizados o digitalizados). En caso de terceras personas que por cuenta propia presten servicios de tratamiento de

datos personales, éstos no podrán utilizarse con un fin distinto al que conste en el contrato de servicios, ni cederlos a otras personas, ni aún para su conservación; cumplida la prestación contractual deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las medidas de seguridad por un período de hasta dos años.

Art. 24.- (Información crediticia). En cuanto a la información crediticia sólo pueden tratarse datos personales de carácter patrimonial, relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas y consentidas por el interesado; igualmente pueden tratarse los relativos al cumplimiento o incumplimiento de obligaciones patrimoniales, proporcionados por el acreedor o por quien actúe por su cuenta o interés.

El responsable o usuario del banco de datos, a petición del titular, comunicará las informaciones, evaluaciones y apreciaciones sobre sus datos que durante los últimos seis meses se hayan practicado y el nombre y domicilio del cesionario en caso de tratarse de datos obtenidos por cesión.

Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de algún modo extinga la obligación, debiendo hacerse constar dicho hecho.

La prestación de servicios de información crediticia no requerirá de consentimiento previo del titular de los datos a los efectos de su cesión, ni la posterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Art. 25.- (Datos para publicidad). En la recolección de información, respecto de direcciones domiciliarias, reparto de documentos, publicidad o venta directa

y otras actividades similares, se podrán tratar datos que permitan establecer perfiles con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido otorgados por los propios titulares u obtenidos bajo su consentimiento. En estos casos, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno, además podrá en cualquier momento solicitar el retiro o bloqueo de su nombre.

Art. 26.- (Datos procedentes de encuestas). La presente ley no se aplicará a las encuestas de opinión, mediciones y estadísticas, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades semejantes, siempre y cuando los datos recogidos no puedan atribuirse a una persona determinada o determinable. Si en la recolección de datos fuere posible mantener el anonimato, se utilizará una técnica de disgregación, de modo que no permita identificar a persona alguna.

Art. 27.- (Datos de menores de edad). Las niñas, niños y adolescentes son sujetos de protección integral de los derechos a la intimidad y a la privacidad, por tal motivo para precautelar su integridad de injerencias y violaciones arbitrarias e ilegales, se consideran datos sensibles a todos aquellos referidos a su persona. Se prohíbe expresamente la difusión de datos personales de la niñez y adolescencia por cualquier medio físico, electrónico o digital.

4.3.4 CAPÌTULO IV

Departamento ecuatoriano de datos personales:

Art. 28.- (Órgano de control) El departamento ecuatoriano de datos personales será el órgano de control encargado de vigilar a las entidades

Art. 29.- (Funciones y atribuciones). El órgano de control ejecutará las acciones necesarias para el cumplimiento de los objetivos y aplicación de las disposiciones de esta ley; en especial tendrá las siguientes funciones y atribuciones:

- Controlar a cada una de las entidades públicas en cuanto al registro lícito de datos personales.

- 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.
- Tutelar los derechos y garantías de las personas naturales.
- Sancionar a las entidades públicas que no están dando un tratamiento correcto a los datos personales.
- Autorizar las transferencias internacionales de datos, una vez que el Ecuador suscriba tratados con otros países argumentando que cuenta con una normativa sólida en el campo de protección de datos personales

Art. 30.- (Códigos de conducta). Las entidades públicas que estarán sujetas a esta ley están obligadas a elaborar códigos de conducta de práctica profesional, que establezcan regulaciones para el tratamiento de datos personales con el objeto de asegurar y mejorar las condiciones de operación de los sistemas de información.

Estos códigos se inscribirán en el registro que para el efecto llevará el órgano de control, se negará la inscripción cuando no se ajusten a las disposiciones legales y reglamentarias.

4.3.5 CAPÌTULO V

De las sanciones del órgano de control

Art. 31.- (Sanciones Pecuniarias) en el caso que las entidades públicas que no presentarán el informe del correcto manejo de los datos al Departamento ecuatoriano de protección de datos personales serán sancionados con multas desde seis mil a setenta mil dólares de los Estados Unidos de Norte América. En caso de reincidencia, el monto de la multa se duplicará. Si no se pudiera identificar al o los responsables del envío de correos electrónicos no deseados, la sanción económica recaerá en monto similares tanto a la entidad o servidor

de Internet de origen y a la empresa o servidor de Internet proveedora del cliente que haya recibido este tipo de comunicación.

Art. 32. (Sanciones penales) en el caso que las entidades públicas no cumplan con la presente ley y además realicen actividades que lesionen un bien jurídico protegido dentro de la materia de datos personales, el órgano de control emitirá un informe a la fiscalía para que se siga la causa y se realicen las investigaciones del caso.

Art. 33. (Procedimiento). El reglamento determinará las condiciones y procedimientos para la aplicación de las sanciones administrativas; deberán regularse, de acuerdo a la gravedad de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Art. 34.- (Ejecución). El departamento ecuatoriano de Protección de Datos Personales y en su caso las Delegaciones Regionales, serán las encargadas de la ejecución de las sanciones administrativas; el reglamento establecerá el destino de los dineros productos de las multas.

4.1.6 Disposiciones Generales

Primera: Las normas contenidas en esta ley son de aplicación obligatoria en todo el territorio nacional.

Segunda: El Ejecutivo reglamentará la presente ley y creará el órgano de control, dentro de los sesenta días de su promulgación e inmediatamente designará al Director Nacional del Departamento ecuatoriano de protección de datos personales.

Tercera: Las disposiciones de la presente Ley prevalecerán sobre otras normas del carácter que fueren que se opongan o que violaren a los derechos de protección de datos personales.

4.1.7 Disposición Transitoria

Los archivos, registros, bases o bancos de datos existentes al momento de la vigencia de la presente ley y que contienen informes de carácter personal, deberán inscribirse en el registro que se establezca conforme a lo dispuesto en el artículo 26 y adecuarse a lo que dispone el presente régimen dentro del plazo que establézcase reglamento.

4.1.8 Disposición Derogatoria

En virtud de la vigencia de la presente Ley, quedan derogadas las normas y disposiciones que se opongan a la misma.

4.1.9 Disposición Final

La presente ley, entrará en vigencia, a partir de la fecha de su publicación en el Registro Oficial.

Bibliografía

Libros:

1. ACED FELÉZ, Emilio. Seguridad, privacidad y confidencialidad. El desafío de la protección de datos personales. Montevideo, editorial Trilce, 2004, pág. 21-25.
2. AMANGUE, Juan. Derecho a la Información y Hábeas Data e Internet. Buenos Aires. La roca, 2002, pág 54-57.
3. ANGULO MARCIAL, Noel. Manual de Tecnologías y Recursos de la información. México, editorial Tecnology, 2009, pág. 24.
4. BAZÁN, Víctor. El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. 1ª edición, México, Editorial Estudios constitucionales, 2009, pág. 131-140.
5. BENÍTEZ, LUIS. Análisis comparativo entre Hábeas data y acción de amparo. Paraguay, editorial Red Ius et Praxis, 2005, pág. 27-31.
6. CANIHUA FLORES, RUBEN. Elaboración de una medida tecnológica que permita garantizar y proteger el adecuado tratamiento de los datos personales en el Internet de tercera generación. Chile, editorial Campo verde, 2007, pág. 45.
7. CANTERA HERRERO, Francisco Javier. Influencia de la ley de protección de los datos en la gestión de Recursos Humanos en las empresas. Madrid, editorial Bosch, 2003, pág. 10
8. CONDE ORTÍZ, Concepción. La protección de datos personales, un derecho autónomo con base en conceptos de intimidad y privacidad. Madrid, editorial Dykinson, 2006, pág. 27- 38.
9. ESTEVA GALLICCHIO, Eduardo. El derecho a la protección de la vida privada y el derecho a la libertad de información en la doctrina y en la jurisprudencia. Uruguay, editorial Red Estudios Constitucionales, 2009, pág. 28.
10. FEIXAS GUTIÉRREZ, Gabriel. La protección de los datos de carácter personal. Barcelona, Bosch, 2001, pág. 342.

11. GARCIA BELAUDE, Domingo. Diferencias entre el Hábeas data y la acción de amparo o tutela constitucional. Perú, editorial Red Ius et Praxis, 2005, pág. 22-27.

12. GARRIGA DOMÍNGUEZ, Ana. Tratamiento de datos personales y derechos fundamentales. Madrid, editorial Dykinston, 2004, pág. 18-23.

13. GOIZÍNI, Oswaldo. El Hábeas Data y la protección de datos. México, editorial Estudios constitucionales, 2002, pág. 45.

14. HERRÁN ORTÍZ, Ana. El derecho a la intimidad en la nueva ley orgánica de protección de datos personales. Chile, editorial Dykinson, 2004, pág. 32-34.

15. MENDÉZ, Luis. El derecho de hábeas data. Uruguay, editorial Real, 2006, pág 102-107.

16. PESO NAVARRO, Emilio. Servicios de la Sociedad de la información, Madrid, Díaz de Santos editores, 2004, pág. 56-67.

17. PRADO HERRERA, Gerardo. Los derechos fundamentales y la aplicación en la justicia constitucional. Bolivia, editorial El Cid, 2009, pág. 12-18.

18. REYES KRAFFT, Alfredo. Las firmas electrónicas y las entidades de certificación. México, editorial Panamericana, 2009, pág. 45-46.

19. RUBIO NAVARRO, Antonio. Aspectos prácticos de la protección de datos de las personas físicas. Barcelona, editorial J.M. BOSCH, 2008, pág. 235-250.

20. RUIZ, Miguel. La configuración constitucional del derecho a la intimidad. Madrid, editorial Universidad Complutense, 2005, pág. 125-141.

21. SALAZAR, Miguel. El Derecho informático en la sociedad. Argentina, editorial Becerra, pág. 67-68.

22. SOSA FLORES, Miguel. El comercio electrónico. Bolivia, editorial El cid, 2005, pág. 21.

23. TÉLLEZ VADEZ, Julio. Manual de Derecho Informático. 3ª edición, México, editorial Instituto de Investigaciones jurídicas de la UNAM, 2001. Pág. 49.

24. VILLAR, José Manuel. Régimen Jurídico de la Informática en España.1ª edición, Madrid, editorial Complutense, 2005. Pág. 87-90.

25. ZUÑIGA URBINA, Francisco. El derecho a la intimidad y sus paradigmas. Chile, editorial Red ius praxis, 2005. Pág. 27-30.

Referencias Legales:

26. Constitución de la República del Ecuador. Registro Oficial 449, publicado el 20 de Octubre de 2008.

27. Constitución Política de la República del Ecuador. Registro Oficial 1, publicado el 11 de Agosto de 1998.

28. Ley 67(Ley de Comercio electrónico, firmas y mensajes de datos) Registro Oficial suplemento 557, publicado el 17 de abril del 2002.

29. Código de ética médica. Registro Oficial 300, publicado el 20 de Octubre de 1993.

30. Código Penal ecuatoriano. Registro Oficial 160, publicado el 29 de marzo de 2010 reformado.

ANEXOS

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 3 de 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 ellos o 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, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

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 fichero o 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 que se 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, a más 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 términos previstos por el Título VII de la presente Ley.

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

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

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

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

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

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

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

PROTECCIÓN DE DATOS PERSONALES

ENTREVISTA AL FISCAL DE DELITOS INFORMÁTICOS

DR. SANTIAGO ACURIO

1. **¿Por qué se busca proteger los datos personales?**

   El tema de datos personales se ha tratado hace 30 años en Europa, América y recientemente en nuestro país. Se busca proteger los datos de una persona por la seguridad de esta, además cada titular de los datos debe tener cuidado con la clase de datos que comparte, esto es tu como persona eliges que datos son públicos y que datos no. Y estar pendiente ya que si los datos fueron entregados para un fin no sean traspasados para otros esto es el tratamiento no autorizado de los datos.

   Y si existe un daño todo depende como se haya producido para resarcirlo, por el principio de subsidiaridad hay medidas civiles, administrativas, penales. Y se decide la acción a tomar puede irse por la vía constitucional como es una acción de protección, etc.

2. **¿Qué normas se aplica para la protección de Datos Personales?**

   - La constitución, en su art. 66
   - Ley de comercio electrónico
   - Normas administrativas
   - Código penal

3. **¿Cuáles son las sanciones que se puede aplicar a estas denuncias de casos?**

   Existe la sanción por la manipulación no autorizada de la información que se encuentra en el art. 202 del código penal.

4. **¿Piensa usted que se debería incrementar leyes que ayuden a este tema?**

   Sí podrían crearse más normas que ayuden a proteger este tema de los datos personales existen normas pero no son suficientes. Con el marco jurídico que existe en el Ecuador ahora la pregunta que debemos hacer ¿Es suficiente una medida civil o administrativa para la protección de datos personales? O que más necesito porque se debe brindar protección y satisfacción.

5. **¿Existe un control por medio del internet para que no se divulguen los datos personales?**

   Existen convenios internacionales para proteger que no se divulguen bases de datos por internet como es el convenio del cibercrimen en Europa trata en una parte del derecho a la intimidad de las personas el acceso ilegal a información pero precisamente esto es un reto ya que el internet es un medio de comunicación y lo que se coloca en internet ya no se puede borrar siempre va a existir un respaldo, por ejemplo las páginas web, lo que se denomina la web machine esto es el almacenamiento de las páginas web como google almacena todas las paginas que has buscado desde tu computador.

6. **¿Qué opina usted sobre las políticas de privacidad de las páginas web brindan realmente seguridad a las personas?**

   Existen políticas de privacidad que se tratan de justificar de toda responsabilidad entonces te pueden poner llamémoslo así cláusulas prohibitivas que se van en contra de los derechos al consumidor.

   En el art. 4 de la ley de defensa al consumidor te habla de la obligación del proveedor de servicios de entregarte toda la información acerca del uso del bien cuando ha cumplido con esta obligación, el art. 5 dice que el consumidor habiendo recibido toda esta información y habiendo un medio objetivo en esta información tiene que actuar en consecuencia a

lo que se le ha dicho así se podría evitar mucho robo de información porque el factor humano tiene mucho que ver en esto.

7. **¿Existe alguna sentencia en Ecuador sobre la violación a los datos personales?**

   Aun no existe ninguna sentencia sobre este tema.

8. **¿De su experiencia como fiscal que recomendación podría dar usted a la ciudadanía para que prevengan sus datos personales ya que están expuestos diariamente?**

   Las personas deben tener precaución sobre sus datos, esto es deben saber que datos se deben proporcionar y mucho más cuando colocan en la red. Tenemos que poner seguridades como sistema de encriptación, claves en las computadoras en los teléfonos celulares, proteger la información esto es la seguridad física y la seguridad que brinda la normativa.

   En las redes sociales muchos no tiene la seguridad de sus perfiles y se encuentran datos que se los puede ver fácilmente.

   Esto es más grave aun cuando menores de edad usan estas redes sin la más mínima seguridad y han existido caso en otros países que pedófilos se aprovechan de estos perfiles para desencadenar en una serie de abusos como es el grooming (ciber acoso). Por este motivo en Canadá y ciertos países de Europa ha obligado cambiar la privacidad de redes sociales para que se controle el compartimiento de perfiles.

VIOLACION DE CLAVES O SISTEMAS DE SEGURIDAD PARA OBTENER INFORMACION ART. 202.1

PROVINCIAS	2008*	2009	2010	2011**
AZUAY	2	0	0	0
BOLIVAR	0	0	0	0
CAÑAR	0	0	1	0
CARCHI	0	0	1	0
COTOPAXI	2	1	1	0
CHIMBORAZO	0	0	0	0
EL ORO	0	0	0	0
ESMERALDAS	0	0	0	0
GUAYAS	12	3	7	5
IMBABURA	1	0	5	0
LOJA	1	0	1	0
LOS RIOS	1	1	0	0
MANABI	1	2	0	0
MORONA SANTIAGO	0	0	0	0
NAPO	0	0	0	0
PASTAZA	0	0	1	0
PICHINCHA	6	0	30	20
TUNGURAHUA	0	0	0	0
ZAMORA CHINCHIPE	0	0	0	0
GALAPAGOS	0	0	0	0
SUCUMBIOS	0	0	2	0
ORELLANA	0	0	0	0
SANTO DOMINGO DE LOS TSACHILAS	0	2	0	0
SANTA ELENA	0	0	2	2
TOTALES	**26**	**9**	**51**	**25**

* La información en el año 2008 es por capítulos (De los delitos contra la inviolabilidad del secreto) no por delitos.

** La información solo esta hasta abril

Política de privacidad de Facebook

Este documento consta de ocho secciones, y puedes ir directamente a cada una de ellas seleccionando los enlaces siguientes:

1. Introducción

Preguntas. Si tienes alguna pregunta o duda sobre nuestra política de privacidad, ponte en contacto con nuestro equipo de privacidad a través de esta página de ayuda. También puedes contactar con nosotros por correo ordinario en 1601 S. California Avenue, Palo Alto, CA 94304.

Programa TRUSTe. Facebook es titular de una licencia de certificación del programa de privacidad TRUSTe. Esto significa que nuestra política y nuestras prácticas han sido supervisadas por TRUSTe, una organización independiente dedicada a comprobar las políticas y prácticas de privacidad y seguridad para garantizar que cumplen los estrictos requisitos de su programa. Esta política de privacidad se aplica al sitio web www.facebook.com. El programa TRUSTe sólo incluye la información recopilada a través de este sitio web, y no comprende otros datos, como información que pudiera recopilarse a través de software descargado de Facebook.

Si tienes alguna queja sobre nuestra política o nuestras prácticas, infórmanos a través de esta página de ayuda. Si no te satisface nuestra respuesta, puedes ponerte en contacto con TRUSTe.

Safe Harbor. Facebook también participa en el marco Safe Harbor desarrollado por el Departamento de Comercio de Estados Unidos y la Unión Europea. Como parte de nuestra participación en Safe Harbor, nos comprometemos a resolver todos los posibles conflictos que puedan surgir en relación con nuestras políticas y prácticas a través de TRUSTe. Para ver nuestra certificación, entra en el sitio web del programa Safe Harbor del Departamento de Comercio de los Estados Unidos.

Ámbito. La presente política de privacidad incluye Facebook al completo. No obstante, no es aplicable a entidades que no sean propiedad o no se encuentren bajo el control de Facebook,

incluidos los sitios web y aplicaciones que utilicen la plataforma. Si utilizas o accedes a Facebook, estarás aceptando las prácticas de privacidad aquí definidas.

No se acepta información de niños menores de 13 años. Si tienes menos de 13 años, no intentes registrarte en Facebook ni nos facilites ningún dato personal. Si descubrimos que hemos recibido información de un niño menor de 13 años, borraremos esa información lo más rápido posible. Si crees que podría obrar en nuestro poder información procedente de un niño menor de 13 años, ponte en contacto con nosotros a través de esta página de ayuda.

Participación de los padres. Recomendamos encarecidamente que los menores de 13 años de edad o más pidan permiso a sus padres antes de enviar información sobre sí mismos a través de internet, y animamos a los padres a que enseñen a sus hijos prácticas seguras para el uso de internet. Encontrarás material de ayuda acerca de cómo los padres pueden hablar con sus hijos sobre un uso seguro de internet en esta página de ayuda.

2. Información que recibimos

Información que nos envías:

Información sobre ti. Cuando te registras en Facebook, nos facilitas tu nombre, correo electrónico, sexo y fecha de nacimiento. Durante el proceso de registro, te ofrecemos la posibilidad de conectarte a tus amigos, centros educativos y empleados. También podrás añadir una foto. En algunos casos podríamos pedirte información adicional por motivos de seguridad o para ofrecerte servicios específicos. Una vez registrado puedes proporcionar otra información sobre ti relacionada, por ejemplo, con tu ciudad de residencia, ciudad de origen, familia, relaciones, redes, actividades, intereses y lugares. También puedes proporcionar información personal sobre ti, como tus tendencias políticas y religiosas.

Contenido. Una de las finalidades principales del uso de Facebook es compartir contenido con los demás, por ejemplo, actualizar tu estado, cargar o hacer una foto, cargar o grabar un vídeo, compartir un enlace, crear un evento o un grupo, hacer un comentario, escribir algo en el muro de alguien, escribir una nota o enviar un mensaje. Si no deseas que guardemos los metadatos asociados al contenido que compartes en Facebook (como las fotografías) elimina los metadatos antes de cargar el contenido.

Información sobre transacciones. Podemos guardar los datos de las transacciones o pagos que realices a través de Facebook. Si no deseas que almacenemos el número de cuenta de origen de tu pago, puedes eliminarlo a través de la página de pagos.

Información sobre amigos. Te ofrecemos herramientas de importación de contactos para ayudarte a cargar las direcciones de tus amigos para que puedas encontrarles en Facebook e invitar a unirse a aquellos contactos que todavía no usen Facebook. Si no deseas que almacenemos esta información, entra en esta página de ayuda. Si nos das tu contraseña para

obtener estos contactos, no la guardaremos una vez cargada la información de los contactos.

Información que recopilamos cuando interactúas con Facebook:

Información sobre la actividad en el sitio web. Realizamos un seguimiento de las acciones que llevas a cabo en Facebook, como añadir conexiones (incluido unirte a un grupo o añadir un amigo), crear un álbum de fotos, enviar un regalo, dar un toque a otro usuario, indicar que "te gusta" una publicación, asistir a un evento o conectarte a una aplicación. En algunos casos, también estás llevando a cabo una acción cuando nos proporcionas información o contenido. Por ejemplo, si compartes un vídeo, además de almacenar el contenido real que has actualizado, podemos registrar el hecho de que lo hayas compartido.

Acceso a la información del dispositivo y del navegador. Cuando accedes a Facebook desde un ordenador, teléfono móvil u otro dispositivo, podemos obtener información de dicho dispositivo sobre tu tipo de navegador, ubicación y dirección IP, así como las páginas que visitas.

Información sobre cookies. Utilizamos "cookies" (datos que almacenamos en tu ordenador, teléfono móvil u otro dispositivo durante un período de tiempo prolongado) para que Facebook sea más fácil de usar, para que nuestra publicidad sea mejor y para proteger tanto a ti como a Facebook. Por ejemplo, las empleamos para guardar tu nombre de usuario (pero nunca tu contraseña) de modo que te resulte más sencillo iniciar sesión cada vez que quieras entrar en Facebook. También utilizamos las cookies para confirmar que estás conectado a Facebook, y para saber cuándo estás interactuando con aplicaciones y sitios web de la plataforma Facebook, nuestros widgets, botones de compartir y nuestros anuncios. Puedes eliminar o bloquear las cookies mediante la configuración de tu navegador, pero en algunos casos puede influir en tu capacidad de uso de Facebook.

Información que recibimos de terceros:

Plataforma de Facebook. No poseemos ni operamos las aplicaciones o sitios web que utilizas a través de la plataforma de Facebook (como juegos y otros programas). Cuando te conectes a un sitio web o una aplicación de la plataforma, nos suministrarán información, incluida la información acerca de las acciones que realizas. En algunos casos, es posible que recibamos una cantidad limitada de información antes de que te conectes a la aplicación o sitio web para poder personalizar el proceso de conexión.

Información procedente de otros sitios web. Podemos establecer programas con socios publicitarios y otros sitios web en los que éstos comparten información con nosotros:

- Podemos solicitar a los anunciantes que nos indiquen cómo nuestros usuarios han respondido a los anuncios que les mostramos (y, con fines comparativos, cómo han actuado en su página otros usuarios que no habían visto los anuncios). Esta compartición de datos,

denominada comúnmente "seguimiento de conversión" nos ayuda a medir la efectividad de nuestra publicidad y a mejorar la calidad de los anuncios que ves.

- Podemos recibir información sobre si has visto o no, o si has interactuado con determinados anuncios de otros sitios, para medir la efectividad de dichos anuncios.

Si en cualquiera de estos casos recibimos datos que todavía no tenemos, les otorgaremos el carácter de "anónimos" en un plazo de 180 días, lo cual significa que no asociaremos la información con ningún usuario en particular. Si establecemos dichos programas, sólo haremos uso de la información según se explica en la sección "Cómo utilizamos tu información" expuesta a continuación.

Información procedente de otros usuarios. Podemos recopilar información acerca de ti a partir de otros usuarios de Facebook (como cuando un amigo te etiqueta en una foto, un vídeo o un lugar, proporciona detalles de vuestra amistad o indica su relación contigo).

3. Compartir información en Facebook.

En esta sección se explica cómo funciona la configuración de privacidad y cómo se comparte tu información en Facebook. Antes de compartir información en Facebook debes tener en cuenta tu configuración de privacidad.

Nombre y fotografía de perfil. Facebook ha sido diseñado para que te resulte sencillo encontrar y conectarte a otros. Por este motivo, tu nombre y fotografía de perfil carecen de configuración de privacidad. Si no quieres compartir tu fotografía de perfil, debes eliminarla (o no añadir ninguna). También puedes controlar quién puede encontrarte al buscar en Facebook o en motores de búsqueda públicos utilizando la configuración de búsqueda.

Información de contacto. La configuración de tu información de contacto controla quién puede ponerse en contacto contigo en Facebook y quién puede ver tu información de contacto (por ejemplo, tu dirección de correo electrónico y número de teléfono). Recuerda que esta información no es obligatoria (excepto la dirección de correo electrónico) y no tienes por qué compartir tu dirección de correo electrónico con nadie.

Información personal. La configuración de tu información personal controla quién puede ver tu información personal (por ejemplo, tus tendencias políticas y religiosas) si decides añadirla. Recomendamos compartir esta información utilizando la opción "amigos de mis amigos".

Mis publicaciones. Puedes seleccionar una configuración de privacidad para cada publicación que realices usando el editor de nuestro sitio. Tanto si vas a cargar una foto como a publicar una actualización de estado, puedes controlar exactamente quién puede verla en el momento de crearlo. Cada vez que compartas algo, busca el icono del candado. Si haces clic en el candado se mostrará un menú que te permite elegir quién podrá ver tu publicación. Si decides no seleccionar tu configuración en el momento de publicar el contenido, dicho contenido se compartirá en consonancia con la configuración de privacidad de Mis publicaciones.

Conexiones. Facebook permite conectarte prácticamente a cualquier persona o cosa que desees, desde amigos y familiares hasta la ciudad donde resides o los restaurantes que te gusta visitar y tus grupos y películas preferidos. Puesto que hacen falta dos para conectarse, tu configuración de privacidad sólo controla quién puede ver la conexión en tu página de perfil. Si te incomoda que tu conexión esté disponible públicamente, deberías eliminarla (o no crearla).

Sexo y fecha de nacimiento. Además del nombre y la dirección de correo electrónico, requerimos que nos facilites tu sexo y fecha de nacimiento durante el proceso de registro. Te pedimos la fecha de nacimiento para comprobar que eres mayor de 13 años y, así, poder limitar mejor el acceso a contenidos y anuncios que no sean adecuados para ciertas edades. Puesto que tu fecha de nacimiento y sexo son obligatorios, no puedes eliminarlos. Sin embargo, puedes editar tu perfil para ocultar todo (o parte) de dichos campos para que no los vean otros usuarios.

Otros. Otras indicaciones que debes recordar:

- Parte del contenido que compartes y de las acciones que llevas a cabo se mostrarán en las páginas de inicio de tus amigos y en otras páginas que visiten.

- Si otro usuario te etiqueta en una foto, vídeo o lugar, puedes eliminar la etiqueta. También puedes limitar quién puede ver que has sido etiquetado en tu perfil desde la configuración de privacidad.

- Incluso después de eliminar información de tu perfil o eliminar tu cuenta, pueden permanecer copias de dicha información visible en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de privacidad, o haya sido copiada o almacenada por otros usuarios.

-Debes entender que la información puede ser compartida a su vez o copiada por otros usuarios.

-Algunos tipos de comunicaciones que envías a otros usuarios no pueden eliminarse, como por ejemplo los mensajes.

- Cuando publicas información en el perfil de otro usuario o realizas un comentario en la publicación de otro usuario, dicha información queda sujeta a la configuración de privacidad del otro usuario.

-Si utilizas una fuente externa para publicar información en Facebook (como una aplicación móvil o un sitio web de Connect) debes comprobar la configuración de privacidad de dicha publicación, puesto que la establece la fuente externa.

Información de "Todos". La información configurada como "todos" está disponible públicamente, como tu nombre, foto de perfil y conexiones. Dicha información permanece

accesible y visible para todo aquel que entre en Internet (incluidas las personas no registradas en Facebook), queda sujeta a indexación por parte de motores de búsqueda de terceros y puede ser importada, exportada, distribuida y redistribuida por nosotros y otros sin limitaciones de privacidad. Dicha información puede asociarse contigo, incluido tu nombre y fotografía de perfil, incluso fuera de Facebook, por ejemplo, en motores de búsqueda públicos y cuando visites otros sitios de Internet. La configuración de privacidad predeterminada para ciertos tipos de información que publicas en Facebook está establecida en “todos”. Puedes revisar y modificar la configuración predeterminada en tu configuración de privacidad. Si eliminas el contenido compartido con "todos" previamente publicado en Facebook, lo borraremos de tu perfil de Facebook, pero no podemos controlar su uso fuera de Facebook.

Menores. Nos reservamos el derecho de aplicar métodos de protección especial para menores (como proporcionarles un contenido adecuado a su edad) y aplicar restricciones a la capacidad que tienen los adultos para compartir y conectarse a menores, reconociendo que esto puede suponer para los menores una experiencia más limitada en Facebook.

4. Información que compartes con terceros.

Plataforma de Facebook. Como ya hemos mencionado, no operamos los sitios web y aplicaciones que utilizan la plataforma de Facebook ni somos sus propietarios. Esto significa que al utilizar estas aplicaciones y sitios web, tu información de Facebook no está sólo disponible para Facebook. Antes de permitir el acceso a cualquier información sobre ti, les requerimos que acepten una serie de condiciones que limitan su uso de tu información (puedes consultar estas condiciones en la sección 9 de nuestra Declaración de derechos y responsabilidades) y ponemos en práctica medidas técnicas para garantizar que sólo obtienen información autorizada. Para obtener más información sobre la plataforma, visita la página Acerca de la plataforma.

Conexión a una aplicación o sitio web. Cuando te conectas a una aplicación o sitio web, éstos tendrán acceso a Información general sobre ti. El término Información general incluye tu nombre y los nombres de tus amigos, fotografías de perfil, sexo, identificador de usuario, conexiones y cualquier contenido compartido usando la configuración de privacidad “Todos”. Para ayudar a estos sitios web y aplicaciones a poner en práctica medidas de seguridad y controlar la distribución de contenido apropiado a usuarios de diferentes edades, podemos poner a su disposición información sobre la localización de tu equipo informático o dispositivo de acceso, así como tu edad. Si la aplicación o el sitio web desea acceder a otros datos, tendrá que pedirte permiso.

Te proporcionamos herramientas para controlar cómo compartir tu información con aplicaciones y sitios web que utilicen la plataforma. Por ejemplo, puedes bloquear el acceso de aplicaciones específicas a tu información en la configuración de las aplicaciones o en la página “Acerca de” de la aplicación. También puedes utilizar tu configuración de privacidad para limitar qué parte de tu información está disponible para “todos”.

Aconsejamos que leas siempre las políticas de los sitios web y las aplicaciones de terceros

para cerciorarte de que estás de acuerdo con el modo en el que usan la información que compartes con ellos. Facebook no puede garantizar que estos sitios web o aplicaciones cumplirán nuestras normas. Si encuentras alguna aplicación o sitio web que infringe nuestras normas, infórmanos de este incumplimiento en esta página de ayuda y tomaremos las medidas oportunas.

Cuando tus amigos utilizan la plataforma. Si tu amigo se conecta a una aplicación o sitio web, éstos podrán acceder a tu nombre, fotografía de perfil, sexo, ID de usuario y aquella información que hayas compartido con "todos". También podrán acceder a tus conexiones, pero no podrán acceder a tu lista de amigos. Si ya te has conectado a ese sitio web o aplicación (o dispones de otra cuenta en estos lugares), es posible que éstos también puedan conectarse con tu amigo a través de ese sitio web o aplicación. Si la aplicación o el sitio web desean acceder a cualquier otro contenido o información tuya (incluida tu lista de amigos), tendrá que obtener permiso específico de tu amigo. Si tu amigo concede permiso a la aplicación o al sitio web, sólo podrán acceder a contenido e información sobre ti a la que tu amigo pueda acceder. Además, sólo podrán utilizar dicho contenido y dicha información en conexión con ese amigo. Por ejemplo, si un amigo facilita a una aplicación acceso a una fotografía que sólo compartes con tus amigos, dicha aplicación puede permitir a tu amigo ver o imprimir la fotografía, pero no puede mostrársela a nadie más.

Te proporcionamos una serie de herramientas para controlar cómo se comparte tu información cuando tu amigo se conecta a una aplicación o sitio web. Por ejemplo, puedes utilizar tu configuración de privacidad de las aplicaciones para limitar qué información pueden poner tus amigos a disposición de las aplicaciones y los sitios web. También puedes bloquear aplicaciones o sitios web particulares para que no accedan a tu información. Puedes utilizar tu configuración de privacidad para limitar los amigos que pueden acceder a tu información o limitar qué parte de tu información está disponible para "todos". También puedes desconectarte de un amigo si no estás de acuerdo con el modo en que utiliza tu información.

Sitios web y aplicaciones de terceros aprobados previamente. Para proporcionarte experiencias sociales útiles fuera de Facebook, en ocasiones necesitamos proporcionar Información general sobre ti a sitios web y aplicaciones de terceros aprobados previamente que utilicen la plataforma cuando los visites (si aún tienes una sesión iniciada en Facebook). Del mismo modo, cuando uno de tus amigos visita un sitio web o aplicación aprobados previamente, recibirá información general sobre ti para que podáis conectaros también a través de ese sitio web (si también dispones de una cuenta en dicho sitio web). En estos casos, requerimos que estos sitios web y estas aplicaciones se sometan a un proceso de aprobación y participen en diferentes acuerdos con el objetivo de proteger tu privacidad. Por ejemplo, estos acuerdos incluyen disposiciones relativas al acceso y eliminación de tu Información general, así como la posibilidad de rechazar la participación en la experiencia ofrecida. También puedes eliminar cualquier sitio web o aplicación aprobados previamente que hayas visitado aquí, o bloquear todos los sitios web y aplicaciones aprobados previamente para que no obtengan información general sobre ti cuando los visites aquí. Además, si cierras la sesión de Facebook antes de visitar un sitio web o aplicación aprobados previamente, éstos no podrán acceder a tu información. Puedes ver una lista completa de sitios web aprobados previamente en nuestra página Acerca de la Plataforma.

Exportación de información. Puedes (al igual que todos aquellos a cuya disposición has

puesto tu información) utilizar herramientas como fuentes RSS, aplicaciones de libretas de direcciones del teléfono móvil o funciones de copiar y pegar para obtener y exportar (y en algunos casos importar) información de Facebook, incluida tu propia información y todos los datos sobre tu persona. Por ejemplo, si compartes tu número de teléfono con tus amigos, éstos pueden utilizar aplicaciones de terceros para sincronizar dicha información con la libreta de direcciones de sus teléfonos móviles.

Publicidad. En ocasiones, los anunciantes que presentan publicidad en Facebook emplean métodos tecnológicos para medir la efectividad de sus anuncios y personalizar el contenido publicitario. Puedes renunciar a la fijación de cookies de numerosos anunciantes haciendo clic aquí. También puedes usar la configuración de cookies de tu navegador para limitar o evitar la fijación de cookies por parte de redes publicitarias.

Enlaces. Al hacer clic en algunos enlaces de Facebook, es posible que te lleven fuera de nuestro sitio web. No nos hacemos responsables de las políticas de privacidad de otros sitios web, y te animamos a que leas sus normas de privacidad.

5. Cómo utilizamos tu información

Utilizamos la información que recopilamos para tratar de ofrecerte una experiencia segura, eficaz y personalizada. A continuación, incluimos algunos datos sobre cómo lo hacemos:

Para gestionar el servicio. Utilizamos la información que recopilamos para ofrecerte nuestros servicios y funciones, evaluarlos y mejorarlos y prestarte servicio técnico. Empleamos la información para impedir actividades que podrían ser ilegales y aplicar nuestra Declaración de derechos y responsabilidades. También utilizamos una serie de sistemas tecnológicos para detectar y ocuparnos de actividades y contenido en pantalla anómalos con el fin de evitar abusos como el correo basura. Estos esfuerzos pueden provocar, en ocasiones, el fin o la suspensión temporal o permanente de algunas funciones para algunos usuarios.

Para ponernos en contacto contigo. Ocasionalmente, podemos ponernos en contacto contigo para informarte de anuncios relativos a servicios. Puedes optar por no recibir ninguna comunicación salvo actualizaciones esenciales en la página de notificaciones de la cuenta>. En los mensajes de correo electrónico que te enviemos, podemos incluir contenido que veas en Facebook.

Para ofrecerte anuncios personalizados. No compartimos información tuya con anunciantes sin tu consentimiento. (Un ejemplo de consentimiento sería que nos pidieses que suministrásemos tu dirección de envío a un anunciante para recibir una muestra gratuita.) Permitimos a los anunciantes elegir las características de los usuarios que verán sus anuncios y podemos utilizar cualquiera de los atributos que hayamos recabado que no te identifiquen personalmente (como información que puedas haber decidido no mostrar a otros usuarios, por ejemplo, el año de nacimiento) para seleccionar el público apropiado para dichos anuncios. Por ejemplo, podríamos utilizar tu interés por el fútbol para mostrarte anuncios de equipamiento de fútbol, pero no le decimos a la empresa que vende el equipamiento quién eres. Puedes consultar los criterios que pueden seleccionar los anunciantes visitando nuestra página de

publicidad. Aunque no compartimos tu información con anunciantes sin tu consentimiento, cuando hagas clic en un anuncio o interactúes de otro modo con éste, existe la posibilidad de que el anunciante pueda colocar una cookie en tu navegador y tomar nota de que cumple los criterios que ha seleccionado.

Para ofrecer anuncios sociales. En ocasiones, emparejamos los anuncios que ofrecemos con información pertinente que poseemos sobre ti y sobre tus amigos para que los anuncios resulten más interesantes y se adapten mejor a ti y a tus amigos. Por ejemplo, si te conectas a la página de tu grupo de música favorito, podemos mostrar tu nombre y la foto de tu perfil al lado de un anuncio de dicha página que verán tus amigos. Sólo compartimos la información personal visible en el anuncio social con el amigo que puede ver el anuncio. Puedes optar por que tu información no sea utilizada en anuncios sociales en esta página de ayuda.

Para complementar tu perfil. Podemos utilizar información acerca de ti que recabemos de otros usuarios de Facebook para completar tu perfil (por ejemplo, cuando se te etiqueta en una foto o se te menciona en una actualización de estado). En tales casos, generalmente te permitimos eliminar el contenido (por ejemplo, permitiéndote eliminar la etiqueta de una foto tuya) o limitar la visibilidad de tu perfil.

Para hacer sugerencias. Utilizamos la información de tu perfil, las direcciones que importas a través de las herramientas de importación de contactos y otra información pertinente para ayudarte a conectar con tus amigos, lo que incluye hacerte sugerencias a ti y a otros usuarios con los que conectes en Facebook. Por ejemplo, si otro usuario importa la misma dirección de correo electrónico que tú, podemos sugerir que os conectéis entre vosotros. Si quieres limitar tu visibilidad en las sugerencias que realizamos a otras personas, puedes ajustar la configuración de privacidad de visibilidad de búsqueda, ya que sólo estarás visible en nuestras sugerencias en la medida en que elijas estarlo en el resultado público de la búsqueda. También puedes bloquear a usuarios específicos para que no se te realicen sugerencias de ellos o para que no se les realicen sugerencias tuyas a ellos.

Para ayudar a tus amigos a encontrarte. Permitimos a otros usuarios utilizar información de contacto que tengan sobre ti (como tu dirección de correo electrónico) para encontrarte, incluso a través de herramientas de importación y búsqueda de contactos. Puedes impedir que otros usuarios utilicen tu dirección de correo electrónico para encontrarte usando tu configuración de búsqueda.

Software descargable. Algunas aplicaciones de software descargables y applets que ofrecemos, como las barras de herramientas del navegador y las herramientas para cargar fotos, nos transmiten datos. Podemos no realizar ninguna declaración formal si creemos que la recopilación y uso de información por nuestra parte es el fin obvio de la aplicación, por ejemplo, el hecho de recibir fotografías cuando se utiliza la herramienta para cargar fotos. Si creemos que no resulta obvio que estemos recopilando o utilizando dicha información, te avisaremos la primera vez que nos facilites la información, de tal manera que puedas decidir si deseas utilizar esa función.

Cuentas in memoriam. Si se nos notifica que un usuario ha fallecido, podemos convertir su cuenta en una cuenta in memoriam. En tales casos, restringimos el acceso al perfil a los

amigos confirmados y permitimos a éstos y a los familiares que escriban en el muro del usuario en recuerdo suyo. Podemos cerrar una cuenta si recibimos una solicitud formal de un pariente del usuario u otra solicitud legal pertinente para hacerlo.

6. Cómo compartimos información

Facebook se basa en compartir información con otros (amigos y miembros de tus redes) al tiempo que te ofrece una configuración de privacidad que puedes utilizar para restringir el acceso de otros usuarios a tu información. Compartimos tu información con terceros cuando creemos que dicha acción está permitida por ti, que es razonablemente necesaria para ofrecer nuestros servicios o cuando se nos exige legalmente que lo hagamos. Por ejemplo:

Cuando realizas un pago. Cuando realices transacciones con otras personas o efectúes pagos en Facebook, sólo compartiremos la información de la transacción con los terceros que sean necesarios para completar la transacción. Requeriremos que los terceros acuerden respetar la privacidad de la información.

Cuando invitas a un amigo a que se una a Facebook. Cuando nos pides que invitemos a un amigo a que se una a Facebook, le enviaremos un mensaje de tu parte, usando tu nombre. La invitación también puede contener información sobre otros usuarios que tu amigo pueda conocer. También le enviamos hasta dos recordatorios en tu nombre. Puedes ver quién ha aceptado tus invitaciones, enviar recordatorios y eliminar las direcciones de correo electrónico de tus amigos en la página del historial de invitaciones. Si tu amigo no quiere que conservemos su información, la eliminaremos a petición suya en esta página de ayuda.

Cuando eliges compartir tu información con comerciantes. Puedes elegir compartir información con comerciantes o proveedores de comercio electrónico no asociados con Facebook a través de ofertas en el sitio web. Esto será a tu entera discreción y no les suministraremos información tuya a dichos comerciantes sin tu consentimiento.

Para ayudar a tus amigos a encontrarte. De forma predeterminada, incluimos cierta información que has colocado en tu perfil en los resultados de búsqueda de Facebook para ayudar a tus amigos a encontrarte. Sin embargo, puedes controlar quién puede ver dicha información, así como quién puede encontrarte en búsquedas, a través de la configuración de privacidad. También colaboramos con proveedores de mensajería instantánea y correo electrónico para ayudar a sus usuarios a identificar cuáles de sus contactos son usuarios de Facebook, de forma que podamos promocionar Facebook a dichos usuarios.

Para dar a los motores de búsqueda acceso a información públicamente disponible. En general, restringimos el acceso de los motores de búsqueda a nuestro sitio web. Podemos permitirles acceder a información configurada con la opción “todos” (junto con tu nombre y fotografía de perfil) y a la información de tu perfil que sea visible para todos. Puedes cambiar la visibilidad de parte de tu información de perfil usando tu configuración de privacidad. También puedes impedir que los motores de búsqueda sometan a indexado tu perfil usando tu configuración de búsqueda.

Para ayudar a mejorar o promocionar nuestro servicio. A veces compartimos datos agregados con terceros para ayudar a mejorar o promocionar nuestro servicio. Sin embargo, sólo lo hacemos de tal manera que no se pueda identificar a ningún usuario en particular ni vincularse a éste con ninguna información o acción específica.

Para prestarte servicios. Podemos ofrecer información a proveedores de servicios que nos ayudan a facilitarte los servicios que ofrecemos. Por ejemplo, podemos utilizar a terceros para alojar nuestro sitio web, enviar actualizaciones por correo electrónico acerca de Facebook, eliminar información repetitiva de nuestras listas de usuarios, procesar pagos u ofrecer enlaces o resultados de búsqueda (lo que incluye enlaces promocionados). Estos proveedores de servicios pueden tener acceso a tu información personal para utilizarla durante un período de tiempo limitado, pero cuando esto ocurre, implantamos sistemas de protección técnicos y contractuales razonables para restringir su uso de dicha información a la ayuda que nos prestan para ofrecer el servicio.

Para publicitar nuestros servicios. Podemos pedir a anunciantes ajenos a Facebook que muestren anuncios para promocionar nuestros servicios. Podemos pedirles que entreguen dichos anuncios basándose en la presencia de una cookie, pero al hacerlo, no se compartirá ninguna otra información con el anunciante.

Para ofrecer servicios conjuntos. Podemos prestar servicios de forma conjunta con otras empresas, como se el caso del servicio de clasificados del Marketplace de Facebook. Si utilizas estos servicios, podemos compartir tu información para facilitar dicho servicio. Sin embargo, identificaremos al socio y te presentaremos la política de privacidad del proveedor de servicios conjuntos antes de que utilices dicho servicio.

Para responder a requerimientos legales y evitar daños. Podemos revelar información con arreglo a citaciones, órdenes judiciales u otros requerimientos (incluidos asuntos civiles y penales) si creemos de buena fe que la ley exige dicha respuesta. Esto puede incluir respetar requerimientos de jurisdicciones ajenas a los Estados Unidos cuando creamos de buena fe que las leyes locales de tal jurisdicción exigen dicha respuesta, son aplicables a usuarios de dichas jurisdicción y resultan coherentes con estándares internacionales generalmente aceptados. También podemos compartir información si creemos de buena fe que resulta necesario para impedir un fraude u otra actividad ilegal, evitar un daño físico inminente o protegernos tanto a nosotros como al usuario de personas que infrinjan nuestra Declaración de derechos y responsabilidades. Esto puede incluir compartir información con otras empresas, abogados, tribunales u otras entidades gubernamentales.

Transferencia en caso de venta o cambio de control. Si la propiedad de toda o prácticamente toda nuestra empresa cambia, podemos transferir tu información al nuevo propietario para que el servicio pueda seguir operativo. En tal caso, tu información seguiría estando sujeta a los compromisos asumidos en la Política de privacidad preexistente.

7. Cómo puedes cambiar o eliminar información

Edición de tu perfil. Puedes cambiar o eliminar la información de tu perfil en cualquier momento yendo a la página de tu perfil y haciendo clic en “Editar mi perfil”. La información se actualizará de inmediato.

Eliminar los contactos cargados. Si utilizas nuestra herramienta para importar contactos con el fin de cargar direcciones, después puedes eliminar la lista en esta página de ayuda. Puedes eliminar las direcciones de correo electrónico de amigos que hayas invitado a unirse a Facebook en tu página del historial de invitaciones

Desactivación o eliminación de la cuenta. Si quieres dejar de utilizar tu cuenta, puedes desactivarla o eliminarla. Cuando desactivas una cuenta, ningún usuario podrá verla, pero no será eliminada. Guardamos la información de tu perfil (conexiones, fotos, etc.) por si más tarde decides volver a activarla. Muchos usuarios desactivan sus cuentas por motivos temporales y al hacerlo, nos piden que mantengamos su información hasta que vuelvan a Facebook. Seguirás pudiendo reactivar la cuenta y restaurar tu perfil en su totalidad. Cuando eliminas una cuenta, se borra de forma permanente de Facebook. Sólo deberías eliminar tu cuenta si estás seguro de que nunca querrás reactivarla. Puedes desactivar la cuenta en la página de configuración de la cuenta o eliminar tu cuenta en esta página de ayuda.

Limitaciones sobre la eliminación. Incluso después de eliminar información de tu perfil o eliminar tu cuenta, pueden permanecer copias de dicha información visible en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de privacidad, o haya sido copiada o almacenada por otros usuarios. Sin embargo, tu nombre dejará de estar asociado con dicha información en Facebook. (Por ejemplo, si publicas algo en el perfil de otro usuario y después eliminas tu cuenta, dicha publicación podría permanecer, pero atribuirse a un “Usuario de Facebook anónimo”.) Asimismo, podemos conservar cierta información para evitar el robo de identidades y otras conductas inadecuadas, incluso si se ha solicitado la eliminación. Si has facilitado a aplicaciones o sitios web de terceros acceso a tu información, éstos pueden conservar tu información hasta el límite permitido por sus términos de servicio o políticas de privacidad. Sin embargo, después de desconectarte de ellos, ya no podrán acceder a la información a través de nuestra plataforma.

Copias de seguridad. La información eliminada y borrada puede permanecer en copias de seguridad hasta un máximo de 90 días, pero no estará disponible para los demás.

Información de contacto de no usuarios. Si un usuario nos facilita tu dirección de correo electrónico pero no eres usuario de Facebook y quieres que la eliminemos, puedes hacerlo en esta página de ayuda. Sin embargo, esa solicitud sólo se aplicará a las direcciones que tengamos en el momento de la solicitud y no a ninguna dirección que los usuarios nos faciliten posteriormente.

8. Cómo protegemos la información

Hacemos todo lo posible para mantener a salvo tu información, pero necesitamos tu ayuda. Para obtener información más pormenorizada sobre cómo mantener la seguridad en Facebook, visita la página de seguridad (Facebook Security) de Facebook.

Medidas que tomamos para mantener a salvo tu información. Mantenemos la información de tu cuenta en un servidor protegido con un firewall. Cuando introduces información confidencial (por ejemplo, contraseñas y números de tarjeta de crédito), la ciframos usando tecnología de capa de socket seguro (SSL). También utilizamos medidas sociales y automatizadas para aumentar la seguridad (como el análisis de la actividad de la cuenta por si hubiera algún comportamiento fraudulento o anómalo de otro tipo), podemos limitar el uso de funciones del sitio web en respuesta a posibles signos de abuso, podemos eliminar contenido inadecuado o enlaces a contenido ilegal, y podemos suspender o desactivar cuentas por si hubiera violaciones de nuestra Declaración de derechos y responsabilidades.

Riesgos inherentes a compartir información. Aunque te permitimos definir opciones de privacidad que limiten el acceso a tu información, ten en cuenta que ninguna medida de seguridad es perfecta ni impenetrable. No podemos controlar las acciones de otros usuarios con los que compartas información. No podemos garantizar que sólo vean tu información personas autorizadas. No podemos garantizar que la información que compartas en Facebook no pase a estar disponible públicamente. No somos responsables de que ningún tercero burle cualquier configuración de privacidad o medidas de seguridad en Facebook. Puedes reducir estos riesgos utilizando hábitos de seguridad de sentido común como elegir una contraseña segura, utilizar contraseñas diferentes para servicios diferentes y emplear software antivirus actualizado.

Informar de incumplimientos. Deberías informarnos de cualquier incumplimiento de la seguridad en esta página de ayuda.

9. Otros términos

Cambios. Podemos cambiar esta Política de privacidad conforme a los procedimientos señalados en la Declaración de derechos y responsabilidades de Facebook. Salvo indicación en contrario, nuestra política de privacidad en vigor se aplica a toda la información que tenemos sobre ti y tu cuenta. Si realizamos cambios en esta Política de privacidad, te lo notificaremos publicándolo aquí y en la página Facebook Site Governance. Puedes asegurarte de que recibes notificación directamente haciéndote fan de la página Facebook Site Governance.

Consentimiento para la recopilación y procesamiento en Estados Unidos. Al utilizar Facebook, das tu consentimiento para que tus datos personales sean transferidos y procesados en Estados Unidos.

Términos definidos. "Nos", "nosotros", "nuestro", "Plataforma" y "Facebook" significan lo mismo que en la Declaración de derechos y responsabilidades. “Información” y “contenido” se

utilizan de forma más general e intercambiable aquí que en la Declaración de derechos y responsabilidades, salvo que el contexto lo limite de otro modo.

Enlaces útiles

Declaración de derechos y responsabilidades
Página Facebook Site Governance
Configuración de aplicaciones
Configuración de privacidad
Página de notificaciones de la cuenta
Página de ayuda para quejas sobre nuestras prácticas y políticas de privacidad
Página de ayuda para informar sobre el uso por parte de un menor de 13 años
Página de ayuda con información para ayudar a los padres a hablar con sus hijos sobre el uso Seguro de Internet
Cómo eliminar una cuenta
Fallecimiento de un usuario
Cómo denunciar a un impostor
Cómo denunciar contenido abusivo
Cómo denunciar una cuenta que está comprometida
Cómo solicitar la eliminación de datos de personas que no son usuarios de Facebook
Cómo eliminar contactos del buscador de amigos
Cómo denunciar o bloquear aplicaciones de terceros
Explicación general sobre las aplicaciones de terceros y cómo acceden a los datos