SUSANA VALERIA IDROVO MOSQUERA

"LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ECUADOR"

Trabajo de Conclusión de Carrera presentado como requisito parcial para la obtención del título de Abogado de los Tribunales de Justicia de la República del Ecuador, con especialidad mayor en Derecho Empresarial y con especialidad menor en Derecho Internacional Comercial.

UNIVERSIDAD DEL PACIFICO

Cuenca, octubre 2011.

AGRADECIMIENTO

En primer lugar quiero agradecer a Dios, por guiar cada paso que doy y por darme la fortaleza y perseverancia para continuar con mis proyectos.

A mis padres por ser un pilar y apoyo fundamental en mi vida, por haberme enseñado a continuar a pesar de los tropiezos, por que sin su ayuda no hubiese podido culminar mi carrera, y sobre todo por ser esos maravillosos abuelitos con mi nena.

A Mark mi amado esposo, y mi hermosa hija Raphaela, por toda la comprensión, cariño, apoyo que me dan, por que sus palabras me motivaron a no rendirme y continuar, por haber sido mi fuente de inspiración y estimulación, ya que todos los esfuerzos y logros alcanzados son para nuestro bienestar, y sobre todo por el amor puro y desinteresado que me demuestra día a día.

A mis hermanos por el cariño y ayuda que me dieron en el momento preciso.

Al Doctor Juan Peña Aguirre, por su paciencia, apoyo y guía en el desarrollo de esta investigación, quiero agradecerle de todo corazón por las enseñanzas para ser una excelente profesional, y sobre todo por la amistad que me ha brindado.

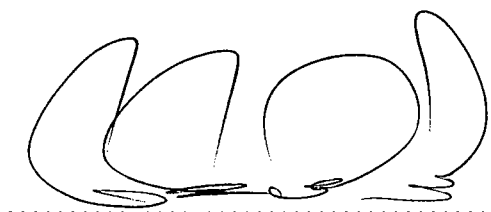
DEDICATORIA

Dedico esta Tesis a mis Padres Sr. José Idrovo y Sra. Bertha Mosquera, por su amor, paciencia y apoyo incondicional, papitos sé cuanto esperaron este momento.

Con muchísimo amor y esfuerzo dedico este triunfo a mi esposo Ing. Mark Gómez y mi hija Raphaela, por su infinito amor y apoyo.

CERTIFICACIÓN

Yo, Doctor Juan Antonio Peña Aguirre, como Director del Trabajo de Conclusión de Carrera, certifico que el presente trabajo fue desarrollado por Susana Valeria Idrovo Mosquera, bajo mi supervisión y que es el autor exclusivo del presente estudio.



.....

Doctor Juan Antonio Peña Aguirre

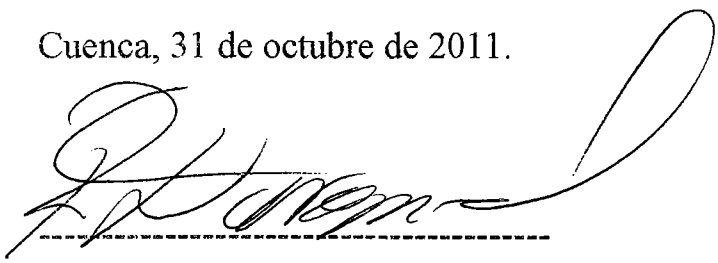
DOCUMENTO DE CONFIDENCIALIDAD

La Universidad Del Pacifico, se compromete a no difundir públicamente la información establecida en el presente Trabajo de Conclusión de Carrera "LA PROTECCIÓN DE DATOS DE CARÀCTER PERSONAL EN EL ECUADOR", de autoría de Susana Valeria Idrovo Mosquera.

Cinco copias digitales de este trabajo de conclusión de carrera quedan en custodia de la Universidad del Pacifico, las mismas que podrán ser utilizadas para fines académicos y de investigación.

Para constancia de este compromiso, suscribe

Cuenca, 31 de octubre de 2011.



Doctor Ricardo Darquea C.

CANCILLER DE LA UNIVERSIDAD DEL PACIFICO

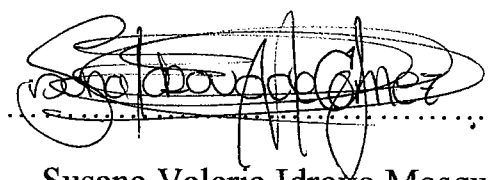
SEDE CUENCA

DECLARACION DE AUTORIA

Yo, Susana Valeria Idrovo Mosquera, declaro ser la autora de la presente tesis.

Todos los efectos académicos y legales que se desprendieren del mismo, son de mi responsabilidad.

Por medio del presente documento cedo mis derechos de autor a la Universidad del Pacífico – Escuela de Negocios– para que pueda hacer el uso del texto completo del Trabajo de Conclusión de Carrera denominado "LA PROTECCION DE DATOS DE CARÁCTER PERSONAL EN EL ECUADOR", con fines académicos y/o de investigación.



Susana Valeria Idrovo Mosquera

INDICE

INTRODUCCION.

Las personas, a lo largo de la vida, van dejando una enorme estela de datos que se encuentran dispersos, y que en la actualidad, con la aplicación de los modernos medios tecnológicos, es posible agrupar y tratar en forma conjunta, interrelacionándolos y analizando significados y actualizaciones conexas, creando o estudiando a voluntad aquellos aspectos de un perfil determinado del individuo que sea de interés controlar o conocer.

Por medio de la utilización de las técnicas informáticas y de la transmisión de datos entre ordenadores, con su capacidad de proceso, se puede ejercer un control social, sin que la persona llegue a percatarse, interferir en su vida.

Las sociedades desarrolladas, en la lucha a diario porque el individuo tenga mayores parcelas de libertad, ya están ofreciendo respuesta a este problema mediante el estudio de lo que se ha dado llamar el “derecho de las personas”, que tienen origen en la dignidad humana y que se encuentra recogido en las actuales constituciones

Por todo lo antes descrito vamos a desarrollar el estudio profundo de lo que supone la protección de datos de carácter personal y cual es su importancia.

CAPITULO I

CONTENIDO Y ALCANCE DEL DERECHO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

1.1.- REFERENCIA A LA REALIDAD ESPAÑOLA

#

Jurisprudencia del Tribunal Constitucional, relacionada con el artículo 18.4 de la Constitución Española.

En el año de 1999, el Tribunal Constitucional dictó tres sentencias, la 30/1999, de 8 de marzo y la 44/1999 y 45/1999, de 22 de marzo, que guardan relación con la Protección de Datos de Carácter Personal.

Estos tres fallos se refieren a la utilización por parte del empresario, de datos de la afiliación sindical de los trabajadores, para otros fines, pues los recurrentes, afiliados a un determinado sindicato, prestaban servicios para la empresa RENFE; siendo estos convocados por el Comité de Empresa a huelga en diversos días del mes de abril de 1994, en horarios que no coincidían con los horarios en que los trabajadores desarrollaban su actividad.

Pese a que los recurrentes no participaron en la huelga y así lo comunicaron a la Empresa, se les descontaron las retribuciones correspondientes en la nómina del mes de mayo de 1994, sin embargo, su reclamación de reintegro de la cantidad fue atendida en el mes de junio, afectando este descuento prácticamente a la totalidad de los empleados incluso a trabajadores sin opción sindical declarada.

Se debe mencionar que la empresa conoce el dato de la afiliación porque descuenta de los salarios la cuota sindical mediante diversas claves informáticas.

La sentencia configura el llamado derecho a la libertad informática o derecho a la autodeterminación informativa (según la doctrina alemana), al indicar que el derecho contemplado en el artículo 18.4 "*además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos*"[1]. Además indica que "*la garantía de la intimidad, latu sensu, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros*

[1]Estudio práctico sobre la protección de datos de carácter personal, Segunda Edición, Cristina Almuzara Almaida, Fanny Courdet, Editorial LEX NOVA S.A, pág. 270.

aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[2]

El Tribunal declaró que "*el artículo citado es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical, entendida ésta en el sentido que ha sido establecido por la doctrina de este Tribunal, porque es, en definitiva, el derecho que aquí se ha vulnerado como consecuencia de la detracción de salarios, decidida por la empresa al trabajador recurrente por su incorporación a determinado Sindicato*"[3]

Además indica que el artículo 18.4 "*no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica reguladora del Tratamiento Automatizado de Datos de Carácter Personal- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios*".

Con estos antecedentes, el Tribunal Constitucional consideró que la afiliación del trabajador a determinado Sindicato se facilitó por aquél con la exclusiva finalidad de que se le

[2]Estudio práctico sobre la protección de datos de carácter personal, Segunda Edición, Cristina Almuzara Almaida, Fanny Courdet, Editorial LEX NOVA S.A, pág. 271.

[3]Estudio práctico sobre la protección de datos de carácter personal, Segunda Edición, Cristina Almuzara Almaida, Fanny Courdet, Editorial LEX NOVA S.A, pág. 271.

descontara la cuota sindical para transferirla al Sindicato. Sin embargo, "*el dato fue objeto de tratamiento automatizado y se hizo uso de la correspondiente clave informática para un propósito radicalmente distinto: retener la parte proporcional del salario relativa al período de huelga*".

Así también, se consideró a esta conducta inconstitucional, ya que se presumió, que por el hecho de pertenecer a uno de los Sindicatos convocantes de la huelga, los trabajadores habían participado en la misma.

Dictamen 4/99: por el que se incluye el Derecho Fundamental a la Protección de Datos en el Catálogo Europeo de Derechos Fundamentales.

El Grupo de Trabajo sobre la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales, el 07 de septiembre de 1999, adoptó la siguiente recomendación:

El 04 de junio en Colonia, el Consejo Europeo decidió la elaboración de una Carta de Derechos Fundamentales de la Unión Europea, en su decisión, el Consejo declara lo siguiente:

"*La evolución actual de la Unión exige la redacción de una Carta de derechos fundamentales que permita poner de manifiesto ante los ciudadanos de la Unión la importancia sobresaliente de los derechos fundamentales y su alcance*".[4]

El grupo, que reúne a las autoridades encargadas de la Protección de Datos en los Estados miembros de la Unión Europea, aprueba la iniciativa del Consejo Europeo sobre la realización de una Carta Comunitaria de Derechos Fundamentales, observando que algunos países europeos han integrado un Derecho Fundamental a la Protección de Datos en su Constitución y en otros a través de la jurisprudencia.

En sus decisiones y sentencias, la Comisión Europea y el Tribunal Europeo de Derechos Humanos, han elaborado y definido un Derecho Fundamental, basándose en distintos Derechos Humanos vinculados a la Protección de Datos de Carácter Personal.

El nuevo artículo (286) del Tratado de la Unión Europea dispone que los actos comunitarios relativos a la protección de las personas físicas en lo que concierne al tratamiento de los datos personales son aplicables, a partir del 01 de enero de 1999, a todas las instituciones y órganos de la Unión Europea.

---

[4]La Carta de los Derechos Fundamentales de la Unión Europea Santiago Castellá Profesor de Derecho Internacional Público.

Con estos antecedentes, el grupo recomienda a la Comisión Europea, al Parlamento Europeo y al Consejo de la Unión Europea incluir el Derecho Fundamental a la Protección de los Datos de Carácter Personal en la Carta de Derechos Fundamentales.

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000.

Con fecha 4 de enero de 2001, se publicó la Sentencia 292 del Tribunal Constitucional de 30 de noviembre, dictada en relación con el recurso de inconstitucionalidad 1463/2000, promovido por el Defensor del Pueblo respecto de los artículos 21.1que hace referencia a la Comunicación de datos entre Administraciones Públicas y 24.1 y 2 que se refiere a Otras excepciones a los derechos de los afectados de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, la misma que considera que los incisos solicitados de los dos preceptos lesionan el contenido esencial de los derechos fundamentales del artículo 18.1, en relación con lo dispuesto en su apartado 4, y la reserva de ley del artículo 53.1 de la Constitución española.

Los mencionados incisos tienen el siguiente tenor literal:

Art. 21.1 LOPD en la parte que expresa " *o por disposición de superior rango que regule su uso* "; el art. 24.1, al referirse a: " *funciones de control y verificación de las administraciones públicas* " y " *persecución de infracciones ... administrativas* "; y el art. 24.2, primer párrafo, al establecer que " *Lo dispuesto en el artículo 15 [derecho de acceso a sus datos por los afectados] y en el apartado 1 del artículo 16 [derecho de rectificación y cancelación] 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 "[5]

Impugnación parcial del artículo 21.1 LOPD.

Se infringe lo que está dispuesto en el art. 53.1 CE, al permitir que una norma de rango inferior a la Ley autorice la cesión de datos entre Administraciones Públicas, sin el que haya consentimiento expreso del afectado e incluso utilizando cierta información para fines totalmente diferentes para los que fueron recogidos y automatizados. Toda vez que el artículo 20 de la misma Ley establece que la creación, modificación o supresión de ficheros de titularidad pública sólo podrá hacerse por medio de una disposición general que deberá ser publicada en el Boletín Oficial del Estado (BOE). Sin embargo dicha disposición general que establece que puede crear, modificar o suprimir el fichero de titularidad pública puede ser una norma de rango infralegal y en la práctica la mayoría de esas disposiciones son órdenes ministeriales y resoluciones administrativas que son dictadas de diferentes autoridades.

Por tanto, el art. 21.1 LOPD, contienen una excepción a la regla del art. 11 LOPD, por medio de la cual la cesión de datos sólo será posible si es que existiese el previo consentimiento del interesado, el mismo que puede ser excepcionado si la cesión viene dispuesta por una Ley. El art. 21.1 LOPD, admite la cesión de datos sin que exista el consentimiento de su titular, pero, siempre que esté autorizado en una norma reglamentaria, consecuentemente se impone una limitación al derecho fundamental a la autodeterminación informativa que es reconocida en

[5] Ley de Protección de Datos , Emilio del Peso Navarro, Ediciones Díaz de Santos S.A pág. 178

el art. 18.4 CE el mismo dispone que "*La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*, por lo que al permitir que se dé la cesión de datos personales sin que haya consentimiento del afectado, esta limitación que de forma muy restringida podría establecer una Ley. Por otra parte, la mencionada remisión al reglamento, lleva consigo una anomalía ya que autoriza al Ejecutivo para que establezca a su arbitrio límites, lo que es totalmente contrario a la reserva legal que establece el artículo art. 53.1 CE ¨ *Los derechos y libertades reconocidos en el capítulo segundo del presente título, vinculan a todos los poderes públicos. Sólo por Ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161.1.a)*[6]

El Defensor del Pueblo, indica que el permitir la cesión de datos personales es una garantía estrictamente necesaria del derecho a la intimidad de su titular, ya que si no existiese esa facultad se tornaría totalmente imposible controlar la circulación de la información que las administraciones tuvieren conocimiento de una persona, disminuyendo la protección de esos datos que garantiza la Carta Magna. Esto ocurriría en caso de que se autoriza a la administración a que divulgue y utilice los datos personales sin el conocimiento de los interesados.

El art. 11 de la Ley Orgánica de Protección de Datos, manifiesta de que sólo cabe la cesión de datos siempre que exista una finalidad que se relacione con las funciones para fines

[6] Estructura orgánica y derechos fundamentales de la Constitución Española de 1978, Mercedes Iglesias Bárez, pág. 148.

relacionados directamente con las funciones legítimas de cedente – cesionario, y cuando exista el consentimiento del afectado, este mismo artículo indica cuales son las excepciones al previo consentimiento del afectado, en la que se destaca en el caso de que hubiere una Ley que lo prevea.

Impugnación del art. 24.1 y 2 LOPD.

El Defensor del Pueblo argumenta en su impugnación que el inciso del apartado uno del artículo 24 exime a la Administración de cumplir con sus obligaciones de informar y advertir, ya que esto impide y dificulta las funciones de control y verificación de las Administraciones Públicas o en caso de que afectare al seguimiento de las infracciones administrativas. En el caso del primer párrafo del apartado dos de ese mismo precepto, se priva a los individuos de sus derechos de acceso a sus datos en poder de las Administraciones Públicas.

También hace referencia a los derechos de los titulares sobre ciertos datos que vulneran la esencia misma del derecho fundamental a la intimidad frente al uso de la informática, ya que impone restricciones injustificadas y desproporcionadas convirtiéndolo así en una materia impracticable y lo que es más grave aún, perdiendo la protección que requiere.

A la excepción a la que se refiere en el apartado uno del art. 24, la norma para determinar cuáles son los fines que justifican la limitación de aquellos derechos de acceso, rectificación y cancelación es tan genérica que cabe dentro de la actividad administrativa, de este modo los límites que de esta forma pueden imponerse a los derechos antes mencionados, lo que es fundamental en materia del derecho al honor y a la intimidad, manipulando el contenido,

poniendo trabas en el ejercicio de lo razonable y les despojan de la protección que es lo primordial.

Fundamentos Jurídicos.

El Defensor del Pueblo, manifiesta que entre los derechos de los afectados deben prevalecer el ser informados y la capacidad de consentimiento, así como los de acceso, rectificación y cancelación, integran el derecho fundamental de todos a controlar la finalidad para lo que fueron requeridos y el uso de los datos personales, es decir para que fueron facilitados dichos datos ya sea al Estado o a cualquier persona en particular.

En primer término, hay la posibilidad de que una norma reglamentaria autorice la cesión de datos entre Administraciones Públicas, para sean empleadas en el ejercicio de competencias o simplemente con una finalidad totalmente distinta a la que motivo su recogida sin que exista la necesidad del previo consentimiento del interesado, es decir que se le priva de una de sus mas firmes garantías.

En segundo lugar, la Administración Pública según lo dispuesto en el art. 24.1 y 2 LOPD puede decidir prudencialmente cuándo niega al interesado la información sobre la existencia de un fichero o tratamiento de datos de carácter personal, así como también sobre la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, las consecuencias de la obtención de los datos o de la negativa a suministrarlos, la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, sobre la identidad y dirección del responsable del tratamiento, en el apartado dos dispone también que en el caso de que se

utilicen ciertos cuestionarios o cualquier otro impreso para obtener información, se debe mencionar de forma clara y precisa todas las advertencias a que se refiere el apartado anterior, y para que también pueda decidir sobre cuándo denegar los derechos de acceso, rectificación y cancelación de esos datos personales.

Por el contrario, para el Abogado del Estado los incisos recurridos de los mencionados preceptos legales no son contrarios a la Constitución porque no sólo respetan la reserva legal del art. 53.1 CE, sino que, además, asignan limitaciones razonables y proporcionadas al derecho fundamental a la intimidad y a la autodeterminación informativa, en su opinión respecto del art. 21.1 LOPD pues no impone ninguna restricción al derecho a consentir la cesión de datos, lo que sólo puede imputarse al apartado cuatro de dicho precepto, que no ha sido impugnado en el presente recurso de inconstitucionalidad, insiste el Abogado del Estado que se tratan de límites fijados por la Ley sino que afectan a los derechos fundamentales a la intimidad y a la autodeterminación informativa. Límites, manifiesta el Abogado del Estado, que únicamente responden a fines proporcionados y razonables, sin que el haber recurrido para su identificación a conceptos jurídicos genere disminución de los derechos legales o fundamentales en cuestión, ya que su empleo es fiscalizable jurisdiccionalmente.

El Convenio Internacional de 1981 y la Directiva 95/46/CE, se tomaran en cuenta serán tenidos en cuenta más adelante para corroborar el sentido y alcance del específico derecho fundamental que, a partir del contenido del derecho a la intimidad , ha reconocido la Constitución Española en orden a la protección de datos personales.

La informática ofrece amplias posibilidades tanto para recoger como para comunicar datos personales y por tanto éstas actividades entrañan indudables riesgos, toda vez que una persona puede ignorar cuáles son los datos que le conciernen que se encuentran recogidos en un fichero, sino peor aún si estos han sido trasladados a otro y con qué finalidad, por tanto, el derecho fundamental a la intimidad no aporta por sí sólo una protección suficiente frente a las nuevas modalidades de intercambio de información que viene derivado de un progreso tecnológico.

Ya con la inclusión del vigente art. 18.4 CE el constituyente realzó la importancia de proteger los datos de carácter personal, ya que era consciente de los riesgos que podría acarrear el uso de la informática y por facultó al legislador la garantía de ciertos derechos fundamentales, así como también del pleno ejercicio de los derechos de la persona. Para ello se debió incorporar un instituto de garantía, como una respuesta a las nuevas formas de amenaza concretamente contra la dignidad, y los derechos de la persona, que no deja de ser un derecho o libertad fundamental.

El Tribunal en algunas decisiones ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que se conoce como un derecho o libertad fundamental de que a lo largo de este estudio se hace mención, así como también el derecho a la libertad fundamental como respuesta a las potenciales agresiones a la dignidad que se desencadenan por el uso de “la informática” como la reconoce la Constitución.

La garantía de la vida privada de la persona y de su reputación son hoy positivos, ya que excede el ámbito propio del derecho fundamental a la intimidad el mismo que se traduce en un derecho de control sobre los datos que se refieren a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, la oposición del ciudadano a que ciertos datos personales sean utilizados para fines distintos con los que fueron obtenidos.

Este derecho esencial a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con el que si bien comparte el objetivo de ofrecer una real protección constitucional de la vida privada personal y familiar, da a su titular un sinnúmero de facultades, vale recalcar el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, ya sea desarrollando el derecho fundamental a la protección de datos, o bien regulando su ejercicio.

El derecho fundamental a la intimidad del art. 18.1 CE, tiene la función de proteger a la persona de cualquier intromisión que se pueda realizar en el ámbito de su vida personal y familiar y que ésta desea excluir del conocimiento ajeno y de las invasiones de personas desconocidas en contra de su voluntad. Mientras que el derecho fundamental a la protección de datos tiene como finalidad garantizar a la persona el poder de controlar sus datos personales, en lo que se refiere a su uso y destino, con el único fin de impedir que esos datos sean ventilados a terceras personas y esto llegare a afectar su dignidad.

Por lo tanto, existe una diferencia ya que el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, es decir, el poder de cuidar su vida privada de una publicidad que no ha requerido, mientras que el derecho a la protección de datos garantiza a los individuos el poder de disponer sobre sus datos.

De allí nace la gran diferencia entre el derecho a la protección de datos, ya que el objeto es más extenso que el del derecho a la intimidad, pues el derecho fundamental a la protección de datos amplía su garantía no sólo en lo que se refiere a la intimidad, sino a lo que en ocasiones el Tribunal ha definido en términos más amplios como “esfera de los bienes de la personalidad” que pertenece al ámbito estricto de la vida privada, sin poder dejar de mencionar el valor fundamental que tiene el respeto de la dignidad personal, tal como es el derecho al honor, y el pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que son relevantes sean o no relativos al honor, a la ideología política, preferencias sexuales, creencias religiosas y a cualquier otro dato que se considera confidencial.

Cabe mencionar que el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar, esta diferencia radica en su contenido, toda vez que da a la persona el poder jurídico de imponer a terceros el que se abstengan de entrometerse en la esfera íntima de la persona y más aun la prohibición de hacer uso de los mismos, esto es lo que no se contiene en el derecho fundamental a la intimidad, ya que este si bien garantiza a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo si se impone los mencionados deberes de hacer. Por lo tanto el derecho a que se requiera, con previo consentimiento la

obtención como el uso de los datos personales, y finalmente el derecho a acceder, rectificar y cancelar dichos datos, solo está establecido en el derecho de protección de datos de carácter personal.

En resumen de todo lo que se ha mencionado podríamos llegar a la conclusión que el contenido del derecho fundamental a la protección de datos consiste en la aptitud de disposición y de control sobre los datos personales que le permite a la persona decidir cuáles de sus datos pueden ser proporcionados a terceros, ya sea que es una persona en particular o el Estado, por lo tanto la persona en momento que así lo requiera sabrá quien tiene sus datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Por tanto, si a una persona se le priva de las facultades de disposición y control sobre sus datos personales, se lo estará también privando de su derecho fundamental a la protección de datos.

La Ley es quien fija los limites a un derecho fundamental, así lo establece la Constitución, por lo tanto los derechos fundamentales pueden ceder, ante bienes, e incluso intereses constitucionalmente relevantes, siempre sea respetuoso con el contenido esencial del derecho fundamental restringido.

Es así que si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, dichos límites no pueden ser distintos a los constitucionalmente previstos, es decir que el apoderamiento legal que permite a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, estaría justificado sólo si responde a la protección de otros derechos fundamentales. Por lo tanto, si dichas

operaciones con los datos personales de cualquier persona, no se realiza con la respectivo cuidado y en observancia de las normas que lo regulan, se violenta el derecho a la protección de datos.

Por ello, cuando la Constitución no contempla esta posibilidad de que un Poder Público distinto al Legislador fije y aplique los límites de un derecho fundamental y que esos límites sean diferentes a los que implícitamente se derivan de la existencia de los derechos y bienes que constitucionalmente se encuentran protegidos, pues es de total importancia que la Ley habilitante sujete a los Poderes Públicos en ese cometido a procedimientos y criterios todos los que fueren necesarios. Esa Ley habrá infringido el derecho fundamental, toda vez que no cumple con el mandato que contiene la Ley, ya que una vez que renuncia a regular la materia que se la ha encomendado y remite ese cometido a otro Poder Público, no se cumple con la principal garantía de los derechos fundamentales en el Estado democrático y social de Derecho.

Esta doctrina es aplicable al presente caso, puesto que las normas legales que se impugnan en los arts. 21.1 y 24.1 y 2 LOPD, establecen cuales son las facultades que reúne el contenido del derecho fundamental a la protección de datos personales. Es por ello, que en la medida en que este régimen legal haya establecido restricciones al ejercicio de este derecho y precisamente en este caso que será estudiado mas adelante, haya previsto supuestos en lo que se deja a la Administración Pública competente la facultad de conceder o denegar prudencialmente el ejercicio de estas facultades por las personas correspondidas, en esos casos se habría producido una vulneración de las garantías legales con las que la

Constitución ha querido garantizar el respeto por todo lo que concierne a los derechos fundamentales.

El motivo de la inconstitucionalidad del art. 21.1 LOPD es evidente, ya que el artículo53.1 CE, establece cuales son los límites del derecho de consentir la cesión de datos; la LOPD no ha fijado por sí misma cuales son los límites del derecho a consentir la transmisión de datos personales entre las Administraciones Publicas y con qué finalidad fueron recogidos, sino que se ha limitado a identificar la norma que puede hacerlo en su lugar, norma que bien puede ser reglamentaria, y con un arreglo al precepto impugnado será una norma de superior rango, y con mayor razón para el caso de que la modificación lo sea por una norma de similar rango, la que pueda autorizar esa cesión inconsentida de datos personales, por lo que es contrario a la Constitución.

En lo que tiene que ver con los incisos impugnados del art. 24.1 y 2 LOPD, vale indicar que la reserva de Ley prevista en el art. 53.1 CE respecto a la regulación de los límites de un derecho fundamental no sólo excluye apoderamientos a favor de las normas reglamentarias como el que antes hemos enjuiciado, sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites.

Además , teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley, éstas pueden vulnerar la Constitución si carecen de certeza y previsibilidad en los límites que imponen y su modo de aplicación, lesionando fundamentalmente el principio de seguridad jurídica, sino también la Ley estaría

lesionando el contenido esencial del derecho fundamental, puesto que la manera en la que se han fijado los limites lo hacen irreconocible e imposibilitan su ejercicio en la práctica.

De aquí se origina que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es idónea de generar una indeterminación sobre los casos a los que se aplica tal restricción, y en caso de que produzca este resultado, la Ley deja de cumplir la función de garantía del derecho fundamental, ya que deja que es su lugar se aplique la voluntad de quien ha de aplicarla, es decir , generando una merma de la eficacia del derecho fundamental como la de seguridad jurídica.

En relación con el derecho fundamental a la intimidad, para que la Ley restrinja este derecho debe mencionar con precisión todos los presupuestos materiales de la medida limitadora.

Con respecto al derecho a la protección de datos personales cabe indicar que la legitimidad constitucional de la restricción de este derecho no está basada solo en la actividad de la Administración Pública, pues es el legislador quien debe determinar en qué caso concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y cuáles son las circunstancias en las que puede limitarse, sobre todo es él quien debe realizarlo por medio de ciertas reglas precisas que hagan previsible al interesado la imposición de dicha limitación y sus consecuencias.

En el caso presente, el empleo por la LOPD en su art. 24.1 de la expresión "funciones de control y verificación", deja un espacio de incertidumbre amplio, ya que permite a la Administración poner los limites a los derechos fundamentales, renunciando la LOPD a fijar los parámetros, dándole el poder a la Administración para hacerlo, de tal modo que permite

reconducir a las mismas a toda actividad administrativa que conlleve a entablar una relación jurídica con un administrado, que efectivamente se dará en todos los casos en los que la Administración así lo requiera, por lo que implícitamente le da la potestad para que la Administración pueda verificar, controlar y vigilar que el administrado haya actuado conforme al régimen jurídico administrativo.

De igual forma, el art. 24.2 emplea la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, dejando una incertidumbre amplia, basta manifestar en que toda actividad administrativa, tiene como finalidad la salvaguardia de intereses generales.

Las mismas tachas merecen también los otros dos casos de restricciones que han sido impugnados por el Defensor del Pueblo, la relativa a la persecución de infracciones administrativas (art. 24.1 LOPD) y la garantía de intereses de terceros más dignos de protección (art. 24.2 LOPD).

Por lo tanto existe la posibilidad de que, con arreglo al art. 24.1 LOPD, la Administración pueda sustraer al interesado información relativa al fichero y sus datos según dispone el art. 5.1 y 2 LOPD, mencionando los perjuicios que esa información pueda conducir a la persecución de una infracción administrativa, puesto que supone una grave restricción de los derechos a la intimidad y a la protección de datos que carece de todo fundamento constitucional. En este punto cabe destacar que se trata de una práctica que puede causar indefensión en el interesado, el mismo que se ve impedido en forma correcta su defensa frente a un posible expediente sancionador por la comisión de infracciones administrativas al

negarle la propia Administración acceso a los datos que sobre su persona pueda poseer y que puedan ser empleados en su contra sin posibilidad de defensa alguna.

Como en otra ocasión se ha aseverado ,que los motivos de limitación adolecen de tal grado de indeterminación, el mismo que deja un gran campo de maniobra a la discrecionalidad administrativa, la misma que no es compatible con las exigencias de la reserva legal en cuanto constituye una cesión en blanco. Además al no haber ninguna referencia a los presupuestos y condiciones de dicha restricción, por lo que resulta insuficiente determinar si la decisión administrativa es el fruto previsible de la razonable aplicación de lo dispuesto por el legislador. De manera tal que el mismo art. 24.2 LOPD impone al derecho fundamental a la protección de los datos personales, mas la circunstancia de que se trate de un límite cuya fijación y aplicación no viene precisada en la LOPD, sino que se abandona en la entera discreción de la Administración Pública, que a la vez es responsable del fichero en cuestión.

La tacha del Defensor del Pueblo se contrae al inciso "o por disposiciones de superior rango" del apartado 1 del art. 21, la declaración de inconstitucionalidad y nulidad se fundamenta, en que la LOPD puesto que no ha fijado por sí misma, como le impone el art. 53.1 CE, los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas con fines diferentes que motivaron su recogida, sino que sólo ha identificado la norma que puede hacerlo en su lugar. En relación con este fundamento no cabe circunscribir dicha declaración sólo al referido inciso sino al más amplio que incluye tanto las disposiciones de creación del fichero como el contenido literal del impugnado, extendiendo la inconstitucionalidad y nulidad a su totalidad, esto es cuando la comunicación hubiere sido

prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso.

Fallo.

Estimar el presente recurso de inconstitucionalidad y, en consecuencia:

- Declarar contrario a la Constitución y nulo el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o" del apartado 1 del art. 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Declarar contrarios a la Constitución y nulos los incisos "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas" y "o administrativas" del apartado 1 del art. 24, y todo su apartado 2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Luego de analizar la Sentencia 292/2000, de 30 de noviembre, se puede ver con claridad que el Tribunal Constitucional, al declarar la inconstitucionalidad de algunos incisos de la LOPD, permite enmarcar a la Protección de Datos de Carácter Personal, dentro de los Derechos Fundamentales, ya que, en el articulado de la Constitución Española no consta dentro de esta categoría de derechos, para esto, la mencionada sentencia, se apoya en otros derechos fundamentales como el de la Intimidad, pero dejando claramente establecido, que se trata de un derecho autónomo y distinto al de la Intimidad.

En la sentencia se pueden diferenciar claramente tres fases:

La primera, que reconoce el Derecho a la Protección de Datos,

La segunda, que lo distingue del Derecho a la Intimidad, y

La tercera, que indica el contenido del derecho.

Por tanto para concluir este análisis debo mencionar que el derecho a la protección de datos de carácter personal, es aquel que tiene todo ciudadano para disponer libremente de sus datos, desvinculándolo del derecho a la intimidad y configurándolo como un derecho fundamental independiente.

1.2.- CONCEPTO DEL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS:

A la protección de datos debemos entenderla 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 los límites de su intimidad ¨.[7]

[7]Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2002. Davara&Davara. Asesores Jurídicos. Director: Pr. Dr. D. Miguel Ángel Davara Rodríguez

Se trata por tanto, de una protección a la persona ante el manejo o manipulación, no autorizada o no permitida por la Ley, de sus datos de carácter personal. Es, consecuentemente, una protección jurídica ante la potencial agresividad de la informática.

Protección, que se encuentra prevista en legislaciones como la española, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Y tal como se manifestó en la sentencia 292/2000, esta protección es un Derecho Fundamental, que hoy es indispensable para el desarrollo de la sociedad.

1.3.- DEFINICIONES RECOGIDAS EN LA LEY ORGÁNICAESPAÑOLA 15/1999.

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

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

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 d datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

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.

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

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

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.

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.

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

Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tiene 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.

1.4.- DESARROLLO DE LOS PRINCIPIOS ESTABLECIDOS EN LA LEY ESPAÑOLA:

Una vez conocidas las definiciones recogidas en la Ley española, se detallará un breve análisis de los Principios de la Protección de Datos.

Calidad de los Datos.

Daremos inicio al análisis de este principio indicando que los datos de carácter personal sólo se podrán recoger para su tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido.

Es así, que el responsable del tratamiento aun teniendo la autorización del interesado, no puede incluir mas datos que los estrictamente necesarios, para que de esta manera se atienda

a la finalidad autorizada en el momento del consentimiento inicial, es por ello que claramente se ha venido manifestando que debe existir una correlación entre la obtención del dato y la finalidad para la que obtuvo la información.

Por lo que, no pueden ser utilizados para fines incompatibles con aquellas para las que los datos hubieran sido recogidos. Sin embargo, vale indicar que la legislación española, no considera incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Así también, en materia de protección de datos uno de los principios esenciales, es que los datos sean reales es decir, que los datos sean exactos y estén al día, de tal manera que respondan con veracidad a la situación actual del afectado, ya que si los datos de carácter personal fueran inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados[8], en el plazo de diez días[9].

El término *situación actual* es acogido en la Ley española actual, ya que en la Ley Orgánica 5/1992, se hablaba de *situación real,*[10] *siendo modificado tanto el artículo 4.3, como el 29.4*

[8] Sentencia de la Audiencia Nacional, Sala de lo Contencioso Administrativo, Sección Primera. Recurso Número: 1883/2001, de 03 de diciembre de 2003.

[9] LOPD. Artículo 16. 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 ¨.

[10] LORTAD. Artículo 4.3. ¨ Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado ¨.

de la LOPD. (Reforma muy importante para evitar el mantenimiento de la anotación llamada saldo cero en los ficheros de solvencia).

Así también, el responsable del tratamiento tiene la obligación de cancelar los datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron registrados, salvo que éstos tengan un valor histórico, estadístico o científico.

Por último debemos mencionar que la Ley Orgánica 15/1999, prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Derecho de Información.

Este principio hace referencia a todas las personas a quienes se les solicita sus datos de carácter personal, deben ser informadas de la existencia de un fichero, y sobre todo de cual es la finalidad de la recogida de los datos, de los destinatarios de la información, así como también del carácter obligatorio o facultativo de su respuesta a las preguntas planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En todos los medios que suelen usarse para la recogida de datos, tales como cuestionarios u otros impresos, deben establecerse de forma claramente legible, todas estas situaciones que permitan cumplir con el principio de información.

En caso de que el interesado no fue quien entregó sus datos de carácter personal al responsable del tratamiento, éste último, tiene la obligación de comunicarle dentro de los tres meses siguientes al momento del registro de los datos, de su procedencia, identidad del responsable y derechos que le asisten. Sin embargo hay ciertas excepciones tales como, que el tratamiento tenga fines históricos, estadísticos o científicos, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, así como también cuando los datos provengan de fuentes accesibles al público y se destinen a la publicidad, teniendo en ese caso que informar al interesado en cada comunicación que se le dirija.

Consentimiento.

El consentimiento es uno de los principales principios de la Protección de Datos, lo podemos resumir al indicar que el afectado es el único que decide en que momento, en que lugar, y en que tiempo se podrán exponer sus datos a terceros, es decir que el ciudadano debe otorgar su consentimiento y después de este se podrá dar inicio a cualquier tratamiento automatizado de sus datos.

Sin embargo, éste principio tiene sus excepciones y los casos en los que la Ley española no exige el consentimiento son:

- Cuando se recojan los datos de carácter personal 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.

- 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.

Debemos mencionar también que dentro de las facultades que tiene el afectado están, la de revocar el consentimiento cuando exista causa justificada y la de oponerse a un tratamiento automatizado en los casos en que no sea necesario el consentimiento.

Datos Especialmente Protegidos.

Se consideran datos sensibles o especialmente protegidos aquellos que hacen referencia al origen racial, a la salud, a la vida sexual, a la ideología, a la afiliación sindical, a la religión y a las creencias. Para el tratamiento de estos datos, siempre debe existir el consentimiento del afectado por escrito y se le comunicará debidamente acerca de su derecho a no prestarlo.

Estos datos podrán ser tratados y cedidos cuando una ley así lo disponga, cuando el afectado lo consienta expresamente, cuando el tratamiento resulte necesario para la prevención o para diagnósticos médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, realizado por un profesional sanitario sujeto al secreto profesional o por cualquier otra persona , pero que esté sujeta a una obligación equivalente de secreto, o cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el caso de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Finalmente, se debe mencionar que los datos 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.

Seguridad.

Para referirme a este principio me remitiré al Reglamento de Medidas de Seguridad de los Ficheros Automatizados de la legislación española, que en su artículo 4 establece tres niveles de seguridad:

1.- Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2.- Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento

se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

3.- Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

Estas medidas de seguridad deberán ser adoptadas por el responsable del fichero, y, en su caso, por el encargado del tratamiento a fin de evitar la alteración, pérdida, tratamiento o acceso no autorizado, de los datos.

Deber de Secreto.

La Ley Orgánica 15/1999, establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento automatizado 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.[11]

[11] LOPD. Artículo 10. ¨ 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 ¨.

Para asegurar el cumplimiento de este principio, pues se deberá incluir en los contratos de todo el personal que vaya a tener acceso a los datos de carácter personal, cláusulas de confidencialidad.

Cesión de Datos.

Este principio es uno de los mas conflictivos, toda vez, que los datos de carácter personal sólo podrán ser cedidos 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, salvo que la cesión está autorizada en una ley, que se trate de datos recogidos de fuentes accesibles al público, que 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, que 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, cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos o 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.

Para que el consentimiento sea valido, es necesario que la información que se facilite al interesado, 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.

Comunicación de datos entre Administraciones Públicas.

Como regla general se entiende que, los datos de carácter personal que una Administración Pública recoja o elabore con destino a otra, podrán ser objeto de cesión, pero los datos no podrán ser cedidos a otras administraciones para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo que la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
Cabe recalcar que la Ley Orgánica 15/1999, establece como excepción al artículo 11.2.b), que, los datos recogidos de fuentes accesibles al público por las Administraciones Públicas, no pueden comunicarse a ficheros de titularidad privada, sin que medie el consentimiento del interesado.[12]

De la misma manera debemos mencionar en este punto, que la Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre, declaró contrario a la Constitución y nulo el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o" del apartado 1 del art. 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Acceso de datos por Cuenta de Terceros.

[12] LOPD. Artículo 11.2.b) ¨ Cuando se trate de datos recogidos de fuentes accesibles al público ¨.

Del mismo modo que la Ley da inicio al desarrollo de este principio, comenzaré diciendo que, 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.[13]

Del anterior acápite se desprende claramente que en este tipo de tratamientos no se requiere el consentimiento del afectado, pero si bien éste no es necesario, por el contrario lo es, la elaboración de un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido, que lo regule.

En el contrato se debe establecer que el encargado del tratamiento únicamente trate los datos conforme a las instrucciones del responsable del tratamiento, y no sean utilizados con fines diferentes al que figure en dicho contrato, así como también constarán las medidas de seguridad que deben implantarse.

Terminada la prestación contractual, los datos de carácter personal deben ser destruidos o devueltos al responsable del tratamiento.

[13] LOPD. Artículo 12.1 ¨ 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 ¨.

CAPITULO II

DISPOSICIONES LEGALES EN EL ECUADOR Y SU APLICACIÓN

2.1.-EL DERECHO A LA INTIMIDAD O DERECHO DE AUTODETERMINACIÓN INFORMATIVA

Previo a conocer las disposiciones legales ecuatorianas, referentes a la Protección de Datos, es preciso realizar una breve referencia al Derecho a la Intimidad, (actualmente denominado Derecho de Autodeterminación Informativa, en esta época de difusión del fenómeno telemático, que se caracteriza por la captación de gran cantidad de datos).

Derecho a la Intimidad es un Derecho reciente, ya que se lo considera autónomo al Derecho al Honor, su punto de referencia inicial más aceptado está en 1890 con la obra THE RIGHT TO BE ALONE, publicada en la Harvard Law Review y traducida al español como el derecho a estar solo, es decir el derecho a que las personas no conozcan, sepan, vean, lo que se refiere a nuestra vida.

Esta obra responde a la inquietud de un prestigioso abogado estadounidense, Samuel Dennis Warren, casado con la hija de un Senador muy conocido (Boyard) con quien tuvo muchos problemas, ya que la prensa sensacionalista no lo dejaba en paz, ya que lo seguía a todo momento, publicando sus infidelidades.

Este prestigioso abogado estuvo siempre acompañado por su colega, el jurista Louis Dembitz Brandeis, con quien elaboró la obra denominada "DERECHO A LA INTIMIDAD."

En esta obra se observa el cambio de contenido de los derechos antiguos y se constata el nacimiento de nuevos Derechos:

Por ejemplo el derecho a la vida que en un inicio servía para proteger a las personas frente a las formas variadas de agresión violenta, hoy en día es un derecho que nos permite también disfrutar de la vida y es el derecho que tenemos de no ser molestados.

El Derecho a no ser molestado, pretende en este caso:

1.-Protegerse contra el sensacionalismo de la prensa amarillista, que contaba con medios para invadir la esfera privada de los individuos.

2.- Separar el Derecho a la Intimidad, del Derecho al Honor.

El Derecho al Honor tiene su raíz en la idea de pertenencia a la persona, es decir el honor se refiere directamente al trato dado y recibido por los demás y protege los perjuicios causados en la reputación de una persona, siempre derivados de su relación con otras y Derecho a la Intimidad se refiere a la ofensa a la propia estima y sentimientos de una persona.

Para Warren y Brandeis el Common Law garantiza a las personas el derecho a decidir hasta que punto puedo comunicar a otros mis sentimientos, mis pensamientos y emociones, siendo esto idéntico a la definición dada por el Tribunal Alemán en la sentencia sobre la Ley del Censo de 1983, que se refiere a la Autodeterminación Informativa, que dice: ¨*Una persona decide cuando y dentro de que límite revela situaciones referentes a su propia vida* ¨.

3.-Vincular a la intimidad con el Derecho Moral y no con el Patrimonial, ya que teste derecho lo tiene todo autor sobre la publicación de su obra, es decir que solo él puede decidir si publica o no su obra, es consecuencia del Derecho a la Intimidad.

4.-Warren y Brandeis pusieron de relieve el carácter no absoluto que tiene el Derecho a la Intimidad, mencionando las siguientes limitaciones:

- No se impedirán publicaciones de los asuntos de interés público (se deriva de la libertad de información).
- Los asuntos de interés de la Justicia o de otras autoridades públicas.
- Publicación de los hechos por parte del propio afectado o con su consentimiento. (Actual principio del consentimiento para tratar los datos personales de un individuo.)

- Publicación hecha oralmente y sin causar daño, porque no está en juego el Honor sino la Intimidad.

De lo dicho se colige que las características del Derecho a la Intimidad son:

- Inicialmente este derecho responde a las minorías (élite social), para posteriormente preocuparse de las capas más extensas de la sociedad, la intimidad es un elemento esencial de la personalidad humana.

- Pese a su autonomización, este derecho no se ha separado completamente de otros derechos fundamentales, ya que en algunos casos si se lo vulnera, este no es el fin, sino el medio para atacar otros Derechos Fundamentales, el derecho a la intimidad tiene una conexión inescindible con la dignidad humana.

- Existe una vinculación entre la necesidad de salvaguardar la intimidad y las nuevas posibilidades invasivas que se dan por el desarrollo de la tecnología, el derecho a la intimidad es inalienable, intransferible, irrenunciable e inembargable.

2.2.-DE LA CONSTITUCION DEL AÑO 1998, DEL PROYECTO DE CONSTITUCION PRESENTADO POR EL CONSEJO NACIONAL DE EDUCACION SUPERIOR Y LA CONSTITUCION DE 2008

Como resultado del avance tecnológico nuestras libertades se han visto afectadas, razón por la cual a continuación nos referiremos a un tema que se encuentra regulado en nuestra Constitución, el mismo que hace referencia al Protección de Datos de Carácter Personal y que se encasilla dentro del capítulo correspondiente a los Derechos de Libertad.

Como antecedente merece la pena mencionarse que la Constitución del año 1998, en el capítulo 2, de los derechos civiles, artículo 23, numeral 8 se hace referencia solamente y en términos generales el derecho que tenemos las personas a la honra, buena reputación y a la intimidad personal y familiar, indicando que la ley protegerá el nombre, la imagen y la voz de la persona.

En el proyecto presentado por la Comisión de Juristas del CONESUP (Consejo Nacional de Educación Superior), en el capítulo 2, De los derechos civiles, artículo 24, numerales 10 y 11 se establece que el Estado reconoce y garantiza a las personas los siguientes derechos:

> ***10.*** *A la honra, la buena reputación y la intimidad personal y familiar. La Ley protegerá el buen nombre, la imagen y la voz de la persona.*
>
> ***10.1.*** *La Ley regulará el uso del tratamiento automatizado de la información para garantizar el pleno ejercicio de esos derechos;*

> ***10.2.*** *El patrimonio genético de una persona no puede ser analizado, registrado o publicado si no es con el consentimiento del sujeto o sobre la base de una prescripción legal.*
>
> ***10.3.*** *Solo en los casos de necesidad médica se utilizará información referente a la salud y vida sexual.*
>
> ***10.4.*** *Sin el consentimiento de la persona, no se utilizará información personal sobre creencias religiosas, orientación sexual, filiación política, situación laboral y económica, que, sin constar en registros públicos se refiera a la esfera de su intimidad.*
>
> ***11.*** *A acceder a la información que sobre si mismas o sobre sus bienes tengan entidades o personas públicas o privadas y a conocer el uso que se haga de ella.*

Además en la Sección tercera, Del habeas data, artículo 111, numeral 1 del mencionado proyecto se indica que:

> *Para proteger los derechos consagrados en el Art. 24, números 10 y 11 de esta Constitución, toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre si misma o sobre sus bienes consten en entidades públicas o privadas.*

De lo que se menciona en líneas precedentes se deduce que existe un gran avance en materia de Protección de Datos de Carácter Personal entre lo establecido en la Constitución de 1998 y lo mencionado en el Proyecto del CONESUP, sin embargo a criterio personal, si bien hay un avance y evolución en el mencionado proyecto, pero el mismo carece de independencia, es decir, no existe una separación entre Derecho a la Intimidad y Derecho a la Protección de Datos de Carácter Personal, pues tal como cita Miguel Ángel Davara Rodríguez [14]:

> ***a)*** *se trata de un derecho fundamental – el derecho fundamental a la protección de datos*
>
> ***b)*** *que es independiente y autónomo del derecho a la intimidad y*
>
> ***c)*** *que no se reduce a los datos íntimos de la persona sino a cualquier tipo de dato personal sea o no íntimo, garantizando al titular de los datos un poder de disposición sobre los mismos asociado al poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos.*

Pues dentro del numeral 10 se hace referencia a la honra, la reputación, la intimidad personal y familiar y a continuación se menciona que la Ley regulará el tratamiento automatizado de información que garantice el ejercicio de estos derechos, es decir lo relativo a la utilización de las nuevas tecnologías, para posteriormente referirse al patrimonio genético de una persona y

[14]Miguel Ángel Davara Rodríguez, La Transposición de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, Fundación Vodafone, Universidad Pontifica Comillas Madrid. Madrid, 2004.

los datos especialmente protegidos (nominados así en legislaciones como la española [15]) esto es; los que hacen referencia a la salud, vida sexual, creencias religiosas, orientación sexual, filiación política, situación laboral y económica, indicando finalmente que para su uso es necesario el consentimiento, el mismo que forma parte de los Principios de la Protección de Datos ¨ *El Consentimiento del Afectado* ¨ como lo menciona Julio Tellez Valdés [16].

Por todo lo mencionado es necesario separar a estos dos derechos, para lo cual sugerimos el siguiente texto:

10.- A la honra, la buena reputación y la intimidad personal y familiar. La Ley protegerá el buen nombre, la imagen y la voz de la persona.

11.- A la protección de sus datos de carácter personal.

11.1.-La Ley regulará el ejercicio de este derecho sobre la base del consentimiento de la persona titular del mismo.

Además en la Sección tercera, Del habeas data, artículo 111, numeral 1 del mencionado proyecto debería decir:

---

[15]Ley Orgánica de Protección de Datos de Carácter Personal, 13 de diciembre de 1999. España.

[16] Julio Téllez Valdés, Derecho Informático 3ra Edición. Mc Graw Hill/ Interamericana Editores, S.A. DE C.V, México D.F, 2003.

Para proteger el derecho consagrado en el Art. 24, números 10, 11 y 12 de esta Constitución del 1998, toda persona tendría derecho a acceder a los documentos, bancos de datos e informes que sobre si misma o sobre sus bienes consten en entidades públicas o privadas, a más de los dispuesto en la ley.

Este es un claro ejemplo de lo que sucedía en nuestra legislación respecto de la Protección de Datos de Carácter Personal, pues como lo hemos visto durante todo este análisis, existía una confusión con el Derecho a la Intimidad, la misma que nacía de nuestra propia Constitución y posteriormente en las normas que pretenden aplicarla, ni siquiera se tiene claro el bien que se protege.

Con estos antecedentes debo concluir manifestando que la Asamblea Nacional Constituyente elaboró nuestra nueva Carta Magna, en donde se ha incluido a la Protección de Datos de Carácter Personal como un Derecho Fundamental independiente al Derecho a la Intimidad, con el siguiente contenido:

Art. 66.- numeral 19.- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Ahora bien es importante que posteriormente debe desarrollarse una Ley de Protección de Datos de Carácter Personal, que además de permitir una adecuada protección, se desarrolle

acorde a nuestra realidad nacional, más no en lo que se ha hecho hasta el momento, esto es; introducir artículos en otros cuerpos legales, los mismos que al contrario de dar una salida a los posibles problemas que pueden surgir en este campo, más bien complican el panorama, tal como sucede en las escasas disposiciones que sobre la materia se incluyen dentro de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

2.3.- REFERENCIA A LA LEY DE COMERCIO ELECTRÓNICA, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

Dentro de la Ley No. 67. RO/ Sup 557, de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, de 17 de Abril del 2002, se hace referencia a los siguientes artículos:

Art. 9.- 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.

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.

En capítulo V, se tipifican las Infracciones Informáticas, mediante reformas al Código Penal, que incluyen a continuación del artículo 202, el siguiente artículo innumerado

Art...- *Obtención y utilización no autorizada de información.- 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, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".*

Dentro del Glosario de Términos que consta en la Disposición General Novena, se hace referencia a lo siguiente:

Intimidad: *El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.*

Datos personales: *Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.*

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.*

De las disposiciones legales a las que se hacen referencia en líneas precedentes, se desprende que dentro de nuestra legislación, concretamente dentro de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, todavía existe confusión entre el Derecho a la Intimidad y Derecho a la Protección de Datos de Carácter Personal.

Además se hace una escasa referencia a sus principios fundamentalmente, pues se menciona solamente al consentimiento, que si bien es el principio fundamental de este derecho, para su aplicación efectiva es necesario el conocimiento y entendimiento del resto de principios que se han detallado a lo largo del presente estudio.

Dentro de las reformas al Código Penal se establece una sanción a las personas que obtengan información sobre datos personales y posteriormente la cedan, publiquen, utilicen o transfieran sin la autorización del titular; sin embargo dentro de la misma Ley, en el Glosario de Términos, no se especifica de manera clara lo que debemos entender por Protección de Datos, pues se menciona que son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley, por tanto esta situación hace que este artículo se vuelva inaplicable.

Para concluir debemos mencionar que dentro del artículo 9 de la Ley, se establece como excepción del consentimiento, los datos personales que se obtengan de fuentes accesibles al público, sin embargo no se indica que debe entenderse como fuentes accesibles al público, dejando abierta la posibilidad de evadir responsabilidades al amparo de que los datos sean obtenidos de fuentes accesibles al público.

2.4.-APLICACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ECUADOR.

Del texto de la Ley se desprende que dentro de nuestra legislación, no es posible proteger de manera plena el Derecho a la Protección de Datos de Carácter Persona, derecho que actualmente es considerado como un Derecho Fundamental, tal como se lo ha concebido en otros países, que han comprendido su alcance y por ende su importancia.

Dentro de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, se pretende sancionar a las personas que utilicen los datos personales, sin el consentimiento del afectado, sin embargo dentro de la misma ley, en el Glosario de Términos se dice que serán considerados Datos Personales, aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de la ley, sin que se especifique claramente que datos deben ser considerados personales y por tanto esta situación vuelve inaplicable al artículo innumerado antes mencionado.

CAPITULO III

IMPORTANCIA DE LA PROTECCION DE DATOS DE CARÁCTER PERSONAL, EN LAS RELACIONES COMERCIALES.

3.1. Generalidades

Hoy en día con las facilidades que nos brinda la tecnología en temas de transmisión de datos, la recolección de los mismos se torna tan fácil e imperceptible que no podemos explicarnos como ciertas entidades u organismos mantienen en sus ficheros nuestros datos personales.

Sin desconocer las ventajas de la tecnología de la información y comunicación, debemos hacer hincapié en las desventajas, que afectan nuestros derechos fundamentales, como por ejemplo la “intimidad”, al procesar los datos electrónicamente.

Como venimos analizando a lo largo de este estudio, pues vivimos en un mundo globalizado de permanente evolución en todos los aspectos, pero por sobre todo la globalización incrementa los niveles de interrelación entre los países que forman el globo, abarcando una gran variedad de aspectos tales como los económicos, políticos, jurídicos, ideológicos, sociales y culturales.

Sin embargo, debemos indicar que en lo que se refiere a Protección de Datos de Carácter Personal en el mundo, se divide en tres grandes grupos, aquellos países donde existe legislación en la materia; aquellos donde existen iniciativas regulatorias concretas a ser implementadas a corto o mediano plazo; y finalmente aquellos países donde no existe regulación ni iniciativas a desarrollarse.

El Continente Europeo es el que mayor regulación tiene en lo que se refiere a la Protección de Datos, sin embargo, en el Continente Americano se están realizando una gran cantidad de intentos regulatorios, no llegando todavía a una total protección, debiendo manifestar que Argentina es el único país de Latinoamérica que ha sido reconocida por la Unión Europea, por tener dentro de su legislación, una norma que regule dicha materia.

En nuestro país se han presentado algunos proyectos de Ley, con el propósito de mantener un acercamiento al tema, es el caso de la Asociación Ecuatoriana de Derecho Informático y Telecomunicaciones (AEDIT), quienes elaboraron un proyecto de Ley Orgánica de Protección de Datos Personales, la misma que presenta como objetivo principal " garantizar y proteger los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, tanto públicos como privados, para garantizar el Derecho de Honor y a la Intimidad de las personas, así como también el acceso a la información que sobre

las mismas se registre, de conformidad a lo establecido en la Constitución Política de la República del Ecuador"[17]

3.2.-IMPORTANCIA DE LA PROTECCION DE DATOS DE CARACTER PERSONAL EN LAS RELACIONES COMERCIALES.

La Protección de Datos desde sus considerandos destaca la importancia de los flujos transfronterizos de datos personales para el desarrollo del Comercio Internacional y las relaciones comerciales entre diferentes países, los mismo que se han tornado como una necesidad en el mundo globalizado que habitamos, a pesar de que el planeta es gigante, con la tecnología y todos los avances que tenemos hoy en día, el planeta esta en nuestras manos, ya que podemos obtener cualquier tipo de información solo sentándonos frente a un ordenador y digitando el titulo de cualquier tema que requerimos, y con solo presionar una tecla obtenemos gran cantidad de información sobre los contenidos de nuestro interés.

Dado el avance tecnológico, diariamente entran en vigencia nuevos métodos para la recogida de datos de los ciudadanos, por ello se ha tornado necesario que exista una regulación en esta materia.

[17] Proyecto de Ley Orgánica de Protección de Datos Personales (AEDIT). Archivo Pdf.

La Protección de Datos, se puede entender como la protección jurídica de los individuos con relación al tratamiento automatizado de los datos de carácter personal, este reforzamiento se ha hecho necesario por la creciente utilización de la informática para fines administrativos, ya que los ficheros automatizados tienen una mayor capacidad de almacenamiento en comparación con los ficheros manuales y razón por la cual permiten realizar con gran velocidad un mayor numero de operaciones.

El régimen protección de los datos personales, permite a los ciudadanos ejercer su legitimo poder de disposición y control en lo respecta a sus datos personales, los mismos que reposan en diferentes registros, como bases de datos, cuestionarios, etc.

Los poderes a los que se hace mención, el mismo que le faculta al ciudadano a restringir el acceso a sus datos, comienza desde el momento que se va a obtener la información, es decir desde la recogida de datos, la obtención y el acceso a los datos, su posterior almacenamiento y tratamiento, así como el uso de posibles terceras personas ya sea el Estado o un particular que pudiesen tener acceso a su información.

Por lo que la importancia a la protección de datos de carácter personal es realmente amplia, y no trata de proteger solo a la Intimidad ya que como lo estudiamos anteriormente, son dos derechos totalmente diferentes, puesto que en la protección de datos se trata de dar una protección mas profunda, en el derecho anglosajón se lo conoce como “privacy”, en español se traduce a “privacidad”, lo que busca es proteger aspectos de la personalidad que individualmente no tienen mayor trascendencia pero que, al unirse con otros, pueden

configurar un perfil determinado de las personas, es por ello que surge el derecho de sus titulares a exigir que los datos permanezcan en el ámbito de su privacidad.

La informática entendida como un medio, constituye un poder, ya que elimina cualquier barrera de tiempo y espacio, permitiendo de tal modo el uso de todo tipo de información, en las sociedades informatizadas el poder ya no representa la fuerza física que se puede aplicar, sino a la facilidad de obtener cualquier tipo de información, la misma que permite controlar e influir en la conducta de los ciudadanos, sin que sea necesario recurrir a medios de coerción.

Ahora bien, con todo el avance tecnológico que soportamos, se abren nuevos mercados por conquistar y nuevas inversiones para realizar, como lo manifestamos en líneas precedentes las distancias geográficas no interfieren en la realización de las transacciones comerciales.

3.3.-QUE SUPONE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

La protección de datos busca garantizar la intimidad de las personas, el resguardo o protección a su intimidad, fundamentalmente la capacidad de disponer, controlar y saber cual es la finalidad para la cual se destina la información recogida y que se refiere a sus datos, de esta manera se evita la transmisión y utilización ilegal de su información.

El derecho a la protección de datos, en términos históricos es relativamente nuevo, toda vez que siempre se le ha dado un tratamiento dentro del derecho a la intimidad, siendo esto totalmente errado, ya que si bien puede ser objeto de confusión la intimidad, con los datos personales, debemos tener presente la diferencia que existe entre estos ya que el ámbito de protección de datos va mas allá de la intimidad, pues se protege los derechos y libertades en general, frente al abuso de la informática.

Por lo tanto los datos personales se han definido de una forma amplia, ya que todos pueden ser potencialmente peligrosos, es decir no existen datos inocuos.

La mayoría de las Leyes protectoras, dan definiciones generales que indican simplemente que es un dato persona es el que se refiere o afecta a una persona determinada o determinable.

Para ellos debemos mencionar que no todos los datos merecen de idéntica protección, por ello debemos distinguir los datos que necesitan una protección ordinaria, por ejemplo aquellos datos que se los denomina como “datos públicos de mera identificación” y que fácilmente los podemos encontrar en una guía telefónica, directorios profesionales, estos no deben tener la misma protección y por lo tanto no podemos someterlos a exageradas disposiciones generales de las leyes de protección de datos, en este caso no se puede exigir el consentimiento expreso o tácito del afectado para el empleo con otros fines, en este caso la *publicidad*, ya que siendo de otro modo afectaría y seria incompatible con las necesidades de datos que tienen las empresas, para de esta manera desarrollar su actividad.

Pero por otro lado tenemos los datos que necesitan de mayor protección que la ordinaria, y a los que se les denomina *datos sensibles,* y estos están reconocidos en la legislación, como es el caso del tipo de origen étnico, tendencias políticas, convicciones religiosas, preferencias sexuales, enfermedades, entre otros de esta índole.

Los países que tienen dentro de su sistema legislativo una norma que haga referencia a la protección de datos, pues deben hacer mención a los ficheros automatizados, manuales y convencionales, ya que estos tres tipos de ficheros contienen información personal, entre ellos la diferencia que existe es la capacidad de almacenamiento. Sin embargo, los ficheros automatizados generan cierta peligrosidad ya que facilitan enormemente la explotación de los datos que en ellos se hayan contenidos.

El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos, es decir existe una vinculación entre la necesidad de salvaguardar los datos personales de las nuevas posibilidades invasivas que abren tecnologías cada vez mas sofisticadas.

3.4.-LAS EMPRESAS DEBEN TENER ACCESO A LOS DATOS DE CARÁCTER PERSONAL.

Es un tema que en nuestro país no se encuentra totalmente desarrollado, ya que las mayoría de empresas ecuatorianas no consideran o por decirlo de otra manera no prestan atención a

las TIC (Tecnologías de la Información y Comunicación) como una alternativa para ser mas competitivos, se puede afirmar que entre las posibles causas se encontrarían la falta de conocimiento, falta de recursos y sobre todo falta de asesoramiento para romper paradigmas e ingresar su empresa al mundo de comercio y negocios electrónicos, se las denominada e-commerce y e-business, estos se consideran en la actualidad como una herramienta empresarial fundamental que deberían ser integradas a los sistemas de gestión. El solo tenerlas no conlleva al éxito , sin embargo, se ha demostrado que no tenerlas implica un fracaso de negocio, ya que si se desea competir en la Nueva Economía, las relaciones comerciales internacionales a través de La Internet, de la información, y la globalización.

Por ello podemos decir que las TIC, se consideran como instrumentos necesarios para las grandes, medianas y pequeñas empresas, ya que por medio de estas se puede optimizar recursos mejorar los recursos y mejorar la eficiencia de los distintos procesos empresariales, producción, ventas y administración de tal manera que se reduzcan costos y a la vez que se eleva su competitividad.

Ahora bien debemos indicar que en el ámbito legal una empresa es una persona jurídica, lo que se convierte en un limitante para aplicar la protección de datos de carácter personal, ya que la persona jurídica no goza de carácter personal, es decir no es sujeto de protección, ya que un sujeto de protección y derechos es toda aquella persona física que tenga derechos y obligaciones, por lo que las personas jurídicas están excluidas de está protección.

Pues bien, en el caso de que se divulgue información de las empresas a terceras personas cabe mencionar que estas pueden recurrir a los tribunales y exigir daños y perjuicios haciendo valer sus derechos, pero deberán plantear cualquier reclamo amparándose por el uso indebido de los datos o informaciones relacionados con ellas, pero no así como una violación a su intimidad y del derecho a la protección de datos, sino como consecuencia una violación o porque se a incumplido un contrato.

En caso de que se trate del empresario individual o inclusive de un profesional, se debe indicar que no les ampara la protección de datos personales, toda vez que va mas allá de las actividades que conciernen a la intimidad y familia.

La Agencia de Protección de Datos española indica que no se aplica dicha protección a las empresas, ya sean que se hayan constituido como personas jurídicas, o que sea un empresario individual, ya que si la protección de datos hace referencia a la intimidad personal y familiar, las empresas no gozan de intimidad personal y familiar, por ello no puede ser aplicado.

Sin embargo, los datos del profesional o empresario individual, cuando realice actividades siempre que no se vinculen con el área mercantil, gozaran de protección.

3.5.- IMPORTANCIA Y UTILIDAD DE LOS DATOS PERSONALES EN LAS RELACIONES COMERCIALES.

Resulta fundamental e importante el rol que cumple la protección de datos personales en el ámbito de la sociedad de la información y las crecientes relaciones comerciales entre los países del globo terráqueo.

Es por ello que en la mayor parte de países desarrollados y otros en vías de crecimiento han incorporado cuerpos legales a su legislación, para por medio de ellas regulas las practicas concernientes a la utilización de datos personales. Ahora bien, todos sabemos que para que se den practicas de negociación debe existir el intercambio de información, y mas aun cuando se realizan transacciones con países que geográficamente se encuentran distantes, como manifestamos en líneas precedentes estas practicas pueden desarrollarse en el ámbito privado, como particular.

En el primer caso, debemos identificar a las partes que van a intervenir en la negociación para que una vez identificados se puedan diferencias de los datos personales.

Es un tema que no se ha dado la merecida importancia, toda vez que se acostumbra a intercambiar la información sin necesidad de que haya el consentimiento del ciudadano, y resulta familiar que recibamos llamadas telefónicas por ejemplo, de entidades financieras, cadenas de almacenes, etc., con la intensión de vendernos diferentes productos o servicios, es en donde se forma una incógnita y nos preguntamos de donde obtuvieron dicha información, sin embargo, queda en una simple inquietud mas no entablamos ninguna acción legal.

Es por ello que se visto la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos, entre todos los

ciudadanos del mundo, para que se cree una conciencia de respeto, en el caso de intercambio de información personal y mas aun en la transmisión de datos de carácter personal.

Para que exista transparencia en la divulgación de los datos personales, la legislación debe garantizar la protección de las libertades y derechos fundamentales de las personas físicas, y a su vez evitar las restricciones a la libre circulación de datos personales, imprescindibles para el desarrollo del comercio internacional.

Como vemos los peligros que conlleva el uso de las nuevas tecnologías de la información son evidentes , e indudablemente es necesario tomar medidas al respecto y esperar a que mas países vayan adoptando e incorporando a sus leyes una especial para garantizar la protección de datos personales, ya que los problemas globales exigen soluciones globales.

CONCLUSIONES.

De lo mencionado durante toda la investigación se desprende que la protección de datos de carácter personal ha recorrido un extendido camino a lo largo de legislaciones de varios países y de manera especial en el Ecuador, pues inicialmente se encontraba confundida con el derecho a la intimidad y posteriormente se fue independizando hasta alcanzar su autonomía como derecho fundamental en la actual constitución de 2008, la misma que se consagra en el numeral 19 del artículo 66 del mencionado cuerpo legal.

Si bien es importante para el desarrollo de este derecho fundamental el hecho de que se encuentre plasmado dentro de nuestra norma suprema, sin embargo es necesario, por no decir fundamental que se dicte una norma que viabilice su aplicación.

Las normas contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, realizan una referencia a este derecho e inclusive pretenden viabilizar su aplicación, sin embargo en la práctica se vuelve imposible aplicarlas por la falta de desarrollo normativo.

Es importante que dentro de nuestra constitución se encuentre plasmado este derecho fundamental, el mismo que se encuentra acorde a la realidad garantista en la que nos encontramos viviendo y que permite un desenvolvimiento armónico de los seres humanos dentro de una sociedad, pues a través de una adecuada protección de los derechos fundamentales garantizaríamos el tan anhelado buen vivir.

RECOMENDACIONES.

Consideramos de vital importancia un desarrollo normativo que permita una adecuada aplicación de este derecho fundamental, denominado Protección de Datos de Carácter Personal.

Las iniciativas deben venir no solamente de instituciones vinculadas con la tecnología, que en nuestro caso ha sido la Asociación Ecuatoriana de Derecho Informático y Telecomunicaciones, pues consideramos importante un aporte de los centros universitario, que en sus aulas cuentan con profesionales capacitados en las diferentes áreas del conocimiento.

Es hora que los centros de educación superior retomen el rol protagonista en nuestra sociedad y la iniciativa legislativa es una de ellas.

Los centros de acopio de información, como los registros de la propiedad o mercantiles deben considerar cuando menos las escasas normas que sobre la protección de datos de carácter personal se encuentran en nuestra legislación, al momento de utilizar y manejar de los datos personales.

En la actualidad existe la Dirección Nacional de Registro de Datos Públicos, a nuestro parecer este organismo también puede aportar con iniciativas para el desarrollo legislativo, pues en sus manos se encuentra el manejo de datos públicos.

Otro aspecto fundamental es la capacitación a profesionales del derecho, razón por la cual nuevamente la universidad juega un papel importante, para la capacitación tanto en pregrado cuanto en postgrado, en donde se puede llegar inclusive a los funcionarios judiciales, en cuyas manos se encuentra la resolución de conflictos suscitados por la mala utilización de los datos que forman parte de este derecho fundamental.

BIBLIOGRAFÍA

1. ALONSO MARTINEZ, Carlos. ¨ Protección de Datos de Carácter Personal. El Consentimiento en Entidades Financieras ¨. ASNEF. Madrid, 2002.

2. Constitución Política de la República del Ecuador. Asamblea Constituyente. 1998

3. Constitución de la República del Ecuador. Asamblea Constituyente. 2008
4. DAVARA RODRÍGUEZ, Miguel Ángel. ¨ La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) ¨. Encuentros sobre Informática y Derecho 1992 - 1993. Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE). Editorial Aranzadi, Pamplona, 1993.

5. Davara&Davara. Asesores Jurídicos y Microsoft Central 2001. ¨ Factbook. Comercio Electrónico ¨. Editorial Aranzadi. A Thomson Company.

6. Davara&Davara. Asesores Jurídicos. ¨ Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2002 ¨.

7. DAVARA RODRIGUEZ, Miguel Ángel. ¨ La Protección de Datos Personales en el Sector de las Comunicaciones Electrónicas ¨. Universidad Pontificia de Comillas. Madrid, 2003.

8. DAVARA RODRIGUEZ, Miguel Ángel. ¨ La Transposición de la Directiva sobre Privacidad y las Comunicaciones Electrónicas. Universidad Pontifica de Comillas. Madrid, 2004.

9. FERNÁNDEZ SALMERON, Manuel ¨ . La Protección de los Datos Personales en las Administraciones Públicas ¨. Prólogo de Antonio Troncoso Reigada. Thomson Civitas.

10. GARCIA MEXIA, Pablo y otros. ¨ Principios de Derecho de Internet. Edita: Tirant Lo Blanch. Valencia, 2002.

11. ¨ La Protección de Datos en Europa. Principios, Derechos y Procedimiento ¨. Grupo ASNEF EQUIFAX. Madrid, 1998

12. ¨ La Protección de los Datos Personales en el Derecho Español ¨. Editorial Dykinson. Madrid, 1999.

13. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal ¨. (BOE 298/1999 de 14-12-1999, pág. 43088).

14. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. R.O. Abril 2002.

15. Memoria de la Agencia Española de Protección de Datos ¨. Año 1999.

16. Memoria de la Agencia Española de Protección de Datos ¨. Año 2000.

17. Memoria de la Agencia Española de Protección de Datos ¨. Año 2001.

18. Memoria de la Agencia Española de Protección de Datos ¨. Año 2002.

19. PEREZ LUÑO, Antonio Enrique: ¨ Intimidad y Protección de Datos Personales: del Habeas Corpus al Habeas Data ¨. Un Estudio sobre el Derecho a la Intimidad. Luis García San Miguel Rodríguez-Arango (editor). Edit. Tecnos, Madrid, 1992.

20. PESO NAVARRO, Emilio del. ¨ Manual de Outsorcing Informático. Análisis y Contratación ¨. Editorial Díaz de Santos, S.A. Madrid, 2000.

21. PESO NAVARRO, Emilio del ¨ Ley de Protección de Datos. La nueva LORTAD ¨. Editorial Díaz de Santos, S.A. Madrid, 2000.

22. Sentencia del Tribunal Constitucional 292, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1463/2000. (BOE 04–01–2001).

23. Sentencia de la Audiencia Nacional, Sala de lo Contencioso Administrativo, Sección Primera. Recurso Número: 1883/2001, de 03 de diciembre de 2003.

24. SUÑE LLINAS, Emilio. ¨ Tratado de Derecho Informático ¨. Volumen 1. Introducción y Protección de Datos Personales. Servicio de Publicaciones Facultad de Derecho Universidad Complutense de Madrid. Instituto Español de Informática y Derecho. Madrid, 2002.

25. ¨ XVII Encuentros Sobre Informática y Derecho 2002 - 2003 ¨. Universidad Pontificia de Comillas. Madrid, 2003.