UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

AREA SOCIOHUMANÍSTICA

TITULO DE MAGISTER EN DERECHO CIVIL Y PROCESAL CIVIL

El derecho a la protección de datos en procesos judiciales que involucran sistemas de telecomunicaciones

TRABAJO DE TITULACION.

AUTOR: Alulema Flores, Darwin Omar

DIRECTORA: Pacheco Montoya, Emma Patricia

CENTRO UNIVERSITARIO QUITO

2016

APROBACIÓN DE LA DIRECTORA DEL TRABAJO DE TITULACION

Doctora

Emma Patricia Pacheco Montoya

DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de titulación, denominado: El derecho a la protección de datos en procesos judiciales que involucran sistemas de telecomunicaciones, realizado por Alulema Flores Darwin Omar, ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, febrero de 2013

f)……..

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

" Yo Alulema Flores Darwin Omar declaro ser autor del presente trabajo de titulación: El derecho a la protección de datos en procesos judiciales que involucran sistemas de telecomunicaciones, de la Titulación Magister en Derecho Civil y Procesal Civil, siendo Emma Patricia Pacheco Montoya directora del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, concepto, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado o trabajos de titulación que se realicen con el apoyo financiero, académico o institucional (operativo) de la Universidad"

f. .....

Autor: Alulema Flores Darwin Omar

Cédula: 1002493334

AGRADECIMIENTOS

A Dios y a mis padres.

Darwin Alulema

DEDICATORIA

A Dios y a mis padres.

Darwin Alulema

ÍNDICE DE CONTENIDOS

RESUMEN

El debate actual sobre la publicidad de las actuaciones judiciales no está en quiénes tienen derecho de asistencia física a la vista ni en la cabida material del estrado, sino en la accesibilidad al contenido de los expedientes judiciales, su grado de visibilidad en los sistemas de telecomunicaciones. La cuestión es si esa accesibilidad debe articularse como un sistema cerrado con alcance sólo a las partes del procedimiento o a quienes tengan un interés legítimo en él, o por el contrario, como un sistema abierto al público en general. Aunque la Constitución del Ecuador regula los elementos concernientes al derecho a la intimidad, al honor, y a la libertad de información, el actual sistema de protección de datos en los procesos judiciales, no está refrendado en una ley orgánica, situación que afecta de manera intensa la confidencialidad de determinada información, por lo que es imprescindible la promulgación de una ley especial que establezca todos los parámetros jurídicos necesarios para que se garantice la protección a los derechos a la intimidad, honor y protección de datos en los procesos judiciales.

PALABRAS CLAVES: Protección de datos, actuaciones judiciales, sistema de telecomunicaciones

ABSTRACT

The current debate on the publicity of judicial proceedings is not about who has the right to physical assistance in sight or in material accommodate the dais, but in content accessibility court records, their degree of visibility in telecommunication systems . The question is whether that accessibility should be articulated as a closed scope only to the parties to the proceedings or who have a legitimate interest in it, or conversely, as open to the general public system. Although the Constitution of Ecuador regulates the elements concerning the right to privacy, honor, and freedom of information, the current system of data protection in judicial proceedings is not endorsed by an organic law, which affects intensely the confidentiality of certain information, which is essential to the enactment of a special law that establishes all the legal parameters necessary for the protection of the rights to privacy, honor and data protection in judicial proceedings is guaranteed.

KEYWORDS: Data protection, prosecution, telecommunications system

INTRODUCCIÓN

El principio de publicidad de las actuaciones judiciales es una manifestación del derecho a un proceso público. El desarrollo que este principio obtiene en la Constitución y Código de Procedimiento Civil es extraordinario, pues, por un lado, al mismo tiempo que el legislador consagra el principio de oralidad como garantía formal del proceso civil, establece la publicidad de las actuaciones orales, ya sea pruebas, vistas y comparecencias cuyo objeto sea oír a las partes antes de dictar una resolución y, por otro, se regula el acceso a la documentación de las actuaciones judiciales en procesos todavía en curso y a los libros, registros, archivos y sentencias de los procesos ya concluidos.

El estudio de esta segunda vertiente de la publicidad permaneció siempre arrinconado como un tema menor en los Manuales de Derecho Procesal Civil, dentro del capítulo más amplio relativo a la forma de los actos procesales, integrado en la Parte General del Derecho Procesal. Por publicidad de las actuaciones judiciales se ha entendido, tradicionalmente, la admisión del público en general, incluso de los medios de comunicación, dentro del propio escenario del juicio: un proceso de puertas abiertas, como medida disuasoria, impuesta en garantía de los ciudadanos, frente al riesgo de arbitrariedad judicial o de influencia gubernamental en el funcionamiento y composición de los órganos jurisdiccionales.

La publicidad absoluta de las actuaciones procesales, se concibió como una garantía procesal de inexcusable aplicación, sobre todo en el proceso penal. La publicidad en el sentido de acceso del público en general a la documentación judicial, mediante su consulta, no preocupó a los procesalistas como una posible cuestión también de interés público, sino sólo privado, exclusivo de las partes intervinientes en el proceso, bajo el prisma más amplio del derecho de defensa, aparte del interés científico por la investigación de los fondos documentales judiciales, ambiguamente regulado y confiado en la práctica al quehacer de archiveros y bibliotecarios.

El problema es que la documentación judicial incluye circunstancialmente anexada información claramente confidencial, datos personales aportados por las partes para describir los hechos alegados y establecer el objeto del proceso que, simplemente por su incorporación a los archivos judiciales, en la mayoría de los casos sin que medie el consentimiento de su titular, no se transforman automáticamente en información pública, ni pierden por tanto la protección especial que les asigna el ordenamiento jurídico por ser expresión del honor e intimidad de las personas.

Esta situación nos conllevó a establecernos como tema de investigación **EL DERECHO A LA PROTECCIÓN DE DATOS EN PROCESOS JUDICIALES QUE INVOLUCRAN SISTEMAS DE TELECOMUNICACIONES**, porque aunque Ecuador regula este tipo de protección a nivel Constitucional, no es suficiente, pues no se cuenta con una Ley Orgánica que desarrolle efectivamente esta salvaguardia. Por ello nos hemos trazado como objetivo general el de establecer los fundamentos jurídicos que intervienen en la protección de datos de carácter personal, como un obstáculo para la protección efectiva del derecho de Propiedad Intelectual, en los sistemas de telecomunicaciones, a partir de la distinción del principio de la exhibición de documentos, Habeas Data y los derechos a la intimidad, al honor y a la libertad de información, para su aplicación en la práctica forense.

A través del análisis de la legislación ecuatoriana, así como de los instrumentos regionales e internacionales de los que es parte, estableciendo la necesidad de normar la protección de datos en procesos judiciales relacionados con los sistemas de telecomunicaciones mediante una ley especial, pues la normativa interna que posee nuestro país, así como los instrumentos a los que se ha adherido en el entorno extranjero, no son suficientes para dar la seguridad necesaria en este tema, logros que a nuestra consideración no solo tributarán a una mayor y mejor seguridad de los datos personales en procesos judiciales, sino a que el ordenamiento jurídico patrio se perfeccione. Con este fin, hemos estructurado nuestra investigación en cinco capítulos, el primero dirigido a analizar las cuestiones esenciales de la exhibición de documentos, el habeas data y los derechos a la intimidad, el honor y a la libertad de expresión; el segundo el derecho a la protección de datos; y el cuarto al análisis de los resultados; y el quinto a las conclusiones y recomendaciones.

CAPÍTULO I

LA EXHIBICIÓN DE DOCUMENTOS, EL HABEAS DATA Y LOS DERECHOS A LA INTIMIDAD, AL HONOR Y A LA LIBERTAD DE INFORMACIÓN

1.1 Medios probatorios

En la doctrina (Parra Quijano, 2006, pág. 183), se han establecido diferentes clasificaciones de las pruebas, y se han agrupado en base a los criterios de pruebas por instrumentos; pruebas testificales o testimoniales; pruebas periciales; prueba por inspección ocular del juez; prueba de confesión; prueba por juramento y la presunción de prueba.

Los medios de prueba en un proceso civil, se refieren a los elementos de conocimiento por los cuales los jueces pueden realizar una apreciación de cómo sucedieron los acontecimientos, en una forma que se intente recrear la realidad de una manera lo más precisa posible; o como expone el profesor (García Falconí, 2013):

> (…) es un concepto jurídico y absolutamente procesal, que alude a la actividad necesaria para incorporar las fuentes de prueba al proceso, o sea son los instrumentos necesarios que deben utilizar los sujetos procesales para hacer valer en el proceso y acreditar los hechos alegados. (p. 1)

En este sentido se ha pronunciado también el profesor (Couture, 1993, págs. 490-491) quien expone que medio probatorio es "(…) toda cosa, hecho o acto que sirve por sí solo para demostrar la verdad o falsedad de una proposición formulada en juicio".

Aunque no existe consenso en la doctrina sobre la clasificación o tipos de medios de prueba, han sido muy importantes los aportes hechos por los estudiosos en el tema. El propio profesor (García Falconí, 2013), establece como medios de prueba la testifical, material, pericial y de confesión judicial. Por su parte (Bentham, 1971) expone que se distinguen en "(…) medios de prueba personales, cuyas fuentes de pruebas son las personas con sus conocimientos sobre hechos, y los medios probatorios reales, emanados de las fuentes consistentes en objetos del mundo exterior que registran información de acontecimientos" (p. 30).

En sentido general, intentando aunar todos los criterios doctrinales al respecto, somos del criterio de establecer como medios de prueba, la confesión; los documentos públicos; los documentos privados; los dictámenes periciales; el reconocimiento o inspección judicial; los testigos; las fotografías; las copias

fotostáticas; los registros dactiloscópicos; la fama pública, y las presunciones; aunque compartimos el criterio de que:

> Independiente del nombre que se les asigne a estos antecedentes (testimonio, documento e indicio (Carnelutti, 1955, pág. 89); o (persona, documento y cosa (Muños Sabaté, 1967, pág. 138); o (testimonio, cosas y documentos (Twining, 2006, pág. 193); o simplemente (testimonios y documentos (Denti, 1974, págs. 272-277)), inevitablemente siempre estaremos hablando de seres humanos y objetos del mundo exterior (Carnelutti F. , 1944, págs. 403-405)" (Meneses Pacheco, 2008, pág. 59).

Diversas han sido para la doctrina la diferenciación de las etapas de la fase probatoria. Para (Echandía, 2002) se estructura en:

> (…) la investigación de las evidencias; el aseguramiento, proposición y presentación de los medios; su admisión y ordenamiento y, por último, la recepción y práctica de los mismos" (p. 261). Para el insigne procesalista (Alcalá-Zamora y Castillo, 1964) "Cuatro momentos capitales se observan en la marcha de la prueba: proposición, admisión, ejecución y apreciación (p. 264).

A nuestra consideración, nos hemos adherido a la estructuración efectuada por (CEAAMER, 2015), (AIU, 2015) y por (IUSMX-UNAM, 2015), todos centros académicos de referencia internacional y en este sentido consideramos que la etapa probatoria se divide esencialmente en tres fases, la fase de ofrecimiento, en la que cada parte aporta los medios de prueba de que se valdrá para aseverar sus posiciones, en los escritos correspondientes, que son presentados al juez; la fase de admisión, en la que el tribunal, en correspondencia con el contenido de la legislación vigente, admite o rechaza las pruebas presentadas por las partes; y la fase de recepción o desahogo de las pruebas, en la que tiene lugar la diligenciación o rendición de las pruebas que presentaron cada una de las partes del proceso, que han sido admitidas.

Para (Echandía, 2002) la admisión de la prueba es "(…) el acto procesal por el cual el juez accede a que un medio de prueba determinado sea considerado como elemento de convicción en ese proceso y ordena agregarlo o practicarlo, según el caso" (p. 282). Para que las pruebas sean admitidas en un proceso civil, deben cumplir con una serie de requisitos de admisibilidad, la pertinencia; la oportunidad y la conducencia.

En cuanto a la pertinencia las pruebas que se aporten deben cumplir con este requisito, en la medida en que se deben corresponder con el hecho que se intenta demostrar, guardando estrecha relación con el asunto que se debate en el juicio. A consideración de (Picó I Junoy, 1996) es pertinente un medio probatorio cuando es "(…) adecuado por su naturaleza y objeto, al hecho que pretende probar" (p. 446).

En cuanto a la oportunidad, ha de ser cumplido puesto que si las pruebas no son presentadas en el término establecido, no serán admitidas en el proceso; mientras que la conducencia se refiere a que las pruebas deben estar adecuadamente conducidas, además de cumplir con los demás requisitos, para que sean admitidas, y de que sean analizados también todos aquellos requisitos específicos, atendiendo al proceso que se debate.

Igualmente, en la fase probatoria del proceso civil, han de ser cumplidos los principios de la actividad de la prueba. El principio de libertad de prueba pondera que todos los medios de prueba a presentar en un proceso, siempre que cumplan con los requisitos exigidos, pueden ser admitidos. Según el basamento de este principio, para probar un hecho se pueden utilizar los medios de prueba convencionales, así como todos aquellos, no convencionales, que no contengan el texto de la legislación vigente.

Por su parte el principio de pertinencia, es principio y requisito de admisibilidad, a la vez. Las pruebas que se aporten deben cumplir con el requisito de pertinencia, en la medida en que se deben corresponder con el hecho que se intenta demostrar, guardando estrecha relación con el asunto que se debate en el juicio. El principio de conducencia y utilidad se refiere que al momento de presentar una prueba, se debe cumplir con el principio de conducencia y utilidad, que guardan relación con el de pertenencia, pero se enfoca a que las pruebas que se presenten han de ser útiles para la resolución del caso, no incurrir en excesos de medios de prueba o en falencia en pos mismos.

En referencia a la utilidad (Jauchen, 2002) expone que "La utilidad de la prueba está directamente relacionada con la relevancia que el elemento tenga en relación con el objeto que debe probarse. Esto es, su importancia, idoneidad y eficacia para verificar

el mismo" (p. 25). Al respecto expone (Talavera Elguera, 2009) que "(…) un medio de prueba será útil si es relevante para resolver el caso particular y concreto" (p. 58).

Por su parte en cuanto al principio de legitimidad, este plantea que las pruebas presentadas deben estar comprendidas en el contenido legal posible de la legislación vigente. Es decir, no se podrán presentar medios de prueban que contravenga lo que está establecido en todas las normas de la legislación nacional, como pueden ser, por citar un ejemplo, elementos que afecten la dignidad o integridad de las personas, o medios de prueba, cuya obtención haya sido en forma ilícita.

El Código de Procedimiento Civil es exhaustivo en cuanto a los medios de prueba, que son regulados desde el artículo 122, hasta el artículo 268 de este cuerpo legal. Al respecto se regula en el artículo 121 cuáles son las pruebas que a los efectos del proceso civil ecuatoriano serán reconocidas legalmente, posibilitándose la admisión de otros medios probatorios que los tradicionales.

1.2 Exhibición documental entre las partes y por terceros

Varios han sido los autores que se han pronunciado sobre el deber de exhibición de documentos entre la partes. (Prieto-Castro, 1950, pág. 162) (Moreno Catena, 1985, págs. 538-539) Por su parte otros autores como (Cordón Moreno, 2001, pág. 1455) (De la Oliva Santos, 1997, pág. 367) ha tomado posiciones adversas a ese deber, negando así la existencia del mismo en base a la regla clásica *nemo tenetur edere contra se*, o sea, nadie está obligado a suministrar prueba a su adversario. En el proceso civil, a través de la exhibición de documentos se intenta permitir que los sujetos de derecho, obtengan la efectividad de sus derechos subjetivos frente a las conductas de otros que injustificadamente estancan el desarrollo adecuado del *íter procesalis*.

Pero esta cuestión no es pacífica en la doctrina, quizás porque se ha asentado con fuerza la posición de (Goldschmidt, 1936, pág. 100) quien ha introducido el concepto de carga procesal, diferenciándolo del concepto de deber. No obstante ello, ha estado tomando cierta importancia una institución en el derecho anglosajón,

establecidas esencialmente en las reglas 26 y siguientes de las Federal Rules of Civil Procedure, que imponen una obligación de las partes al inicio del proceso de revelar información, sin esperar una solicitud formal de la llamada discovery. En esta institución se puede observar un genuino y auténtico deber de colaboración. (Gilsanz Usunaga, 2010, pág. 96)

Parece ser que esta cuestión de obligación de proporcionarse o proveerse las partes y los terceros los elementos o medios de prueba que posean de forma tal que puedan favorecer o no el éxito de la pretensión particular, está, al decir de (Hunter Ampuero, 2008, pág. 151) muy estrechamente ligado a la buena fe, la que pudiera constituirse en uno de los fundamentos de este deber.

Nuestra Ley Sustantiva Civil establece principios de buena fe en varios de sus artículos. Lo expone en los preceptos 80 numeral 5; 94; 355; 662; 717; 721; 722; 944; 950; 953; 955; 1018; 1290; 1291; 1471; 1506; 1562; 1591; 1592; 1642 numeral 6; 1753; 1793; 1854 numeral 3; 1857; 1866; 1962; 1974; 1993; 2026; 2076; 2105; 2201; 2202; 2203; 2242; 2308; y 2410. En sentido general hacen alusión a cuestiones relacionadas con la buena fe, y en tal sentido exponen por ejemplo, lo referido a la restitución del demandado cesa si este actuó de buena fe, que el matrimonio declarado nulo surte efectos legales para el cónyuge que actuó de buena fe, que la restitución para dar alimentos cesa para el que obró de buena fe, el disfrute de los frutos de la cosa del poseedor podrá hacerlo si actuó de buena fe. Un artículo trascendental es el artículo 721 que expone lo que pudiera considerarse como buena al exponer que “La buena fe es la conciencia de haberse adquirido el dominio de la cosa por medios legítimos, exentos de fraude y de cualquier otro vicio”. (Ecuador, Código Civil, 2005)

Otro de los fundamentos en el que se puede fundar este deber de exhibir documentos se encuentra en el deber general de veracidad y de integridad dentro del proceso civil. (Picó i Junoy, 2003, pág. 80) Existen ordenamientos legales como el alemán o el austriaco en el que se regulan los llamados derechos de veracidad o completitud, o sea, plenitud. (Hunter Ampuero, 2008, pág. 154) Autores como Diez-Picazo y Ponce de León consideran que como una expresión de este principio de veracidad y plenitud que debe regir dentro del proceso civil, el ordenamiento jurídico exige un comportamiento de buena fe, como limitación a posibles conductas

deshonestas dentro del mismo, por lo que implican no engañar ni defraudar. (Díez-Picazo y Ponce de León, 1963, pág. 134)

No obstante, tampoco esta posición es pacífica en la doctrina pues, personalidades del proceso civil como Calamandrei o Scarselli consideran que dentro del proceso civil no existe realmente un verdadero y propio deber de veracidad. (Calamandrei, 1950, pág. 23) (Scarselli, 1998, pág. 112)

A pesar de unas y otras posiciones los llamados deberes de colaboración, entendidos como aquellos que implican "(…) acompañar al proceso todos los medios de prueba al alcance de la parte" (Hunter Ampuero, 2008, pág. 156), significa indudablemente un fundamento de la buena fe procesal, porque intentar esconder, negar o alterar cualquier medio probatorio, implicaría una conducta contraria a la buena fe, y al decir de (González Granda, 2007, pág. 66) "(…) se trataría de un comportamiento desleal".

Como medios de prueba documental, el Código de Procedimiento Civil ecuatoriano establece los documentos públicos y los documentos privados, en relación con el documento público, esta norma establece en su artículo 164 la definición de documento público o como también los denomina auténticos. Expone que son los autorizados con las formalidades legales imprescindibles establecidas por ley ante un funcionario competente para ello. Una cuestión importante es que igualmente le confiere la categoría de documento público a los mensajes de datos que hayan sido otorgados, conferidos, autorizados o expedido por y ante una autoridad competente y en el que conste la firma electrónica.

Para que un documento público pueda hacer fe, y por tanto constituir una prueba documental, debe estar debidamente autorizado por la autoridad competente en cada caso, y se puede realizar una clasificación o agrupación general de diferentes clases de documentos públicos, como son los diplomas, decretos, mandatos, edictos, provisiones, requisitos, exhortos, certificaciones, copias o testimonios de actuación de procedimientos gubernativos o judiciales, asientos de libros y otras actuaciones de funcionarios o servidores públicos; y asientos de libros y registros parroquiales.

Los instrumentos públicos que se intente que sean valorados como prueba, pueden igualmente ser autorizados en el extranjero, y en el Ecuador se procede a su autenticación o legalización, referidos en el Código de Procedimiento Civil, en sus artículos 188 y 190, cuando se expresa en sentido general que si un instrumento público ha sido autorizado en un estado extranjero, si hubieren sido autenticados pues tendrán la misma validez que como si hubiere sido expedido en el territorio nacional. En este sentido agrega que esta autenticación se realizará ante el funcionario consular ecuatoriano en el territorio en que se autorizó dicho instrumento.

En el caso de los instrumentos privados, el Código de Procedimiento Civil establece una clara definición, al exponer en su artículo 191 que “Instrumento privado es el escrito hecho por personas particulares, sin intervención de notario ni de otra persona legalmente autorizada, o por personas públicas en actos que no son de su oficio.” (Ecuador, Código de Procedimiento Civil, 2014)

Los instrumentos privados están establecidos de forma taxativa en el Código de Procedimiento Civil en su artículo 193, regulando que son los vales simples y las cartas; las partidas de entrada y las de gasto diario; los libros administrativos y los de caja; las cuentas extrajudiciales; los inventarios, tasaciones, presupuestos extrajudiciales y asientos privados; y los documentos a que se refieren los Arts. 192 y 194. (Ecuador, Constitución de la República, 2008)

Los documentos privados, o incluso solamente datos, pueden ser susceptibles de registro en archivos informáticos, y en consecuencia requieren de una especial protección y tutela jurídica, para evitar que el contenido de esos archivos sea usado de forma indebida, y por tanto se lesione el honor y la intimidad de los sujetos. Por tales razones, por ejemplo, la legislación prescribe el *habeas data*, como acción dirigida no solamente ante aquellas conductas que implican que no se le ha brindado determinada información a una persona, sino para cuando esa información ha sido incompleta, o ha sido utilizada sin el consentimiento de su titular para acciones diferentes para las cuales está destinada o de forma tal que a consideración de su titular le afectan.

La exhibición de documentos se realiza en un juicio independiente según establece la Ley Procesal Civil nacional en su artículo 821 referido al juicio de exhibición,

estipulando que “Si se solicita la exhibición de cosas muebles, o de documentos que deben exhibirse, para fundar una demanda o para contestarla, se dispondrá que dentro de tres días haga la exhibición la persona de quien se la pide.” (Ecuador, Código de Procedimiento Civil, 2014). Sin embargo, en la misma medida, de acuerdo a lo regulado en la propia norma, en su artículo 826 y 65, la exhibición de documentos puede presentarse como una diligencia preparatoria.

1.3 El habeas data

Entre los Derechos de Libertad recogidos en la Constitución de la República del Ecuador se establece en su artículo 66 numeral 7 “El derecho de toda persona agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario.” (Ecuador, Constitución de la República, 2008)

Nuestra Carta Magna, a partir del artículo 84, establece el conjunto de las garantías constitucionales, que se pueden clasificar como garantías normativas; políticas públicas, servicios públicos y participación ciudadana y garantías jurisdiccionales. Dentro de las garantías jurisdiccionales establecidas, encontramos las medidas cautelares; la acción de protección; el habeas data; la acción de habeas corpus; la acción de acceso a la información pública; la acción por incumplimiento; y la acción extraordinaria de protección.

Específicamente, el artículo 92 de nuestra Ley de Leyes establece que:

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

> persona afectada podrá demandar por los perjuicios ocasionados. (Ecuador, Constitución de la República, 2008)

Es decir, que todos los datos referidos al ámbito privado de un sujeto que consten en algún registro o archivo de entidades públicas o privadas, en un soporte material o electrónico, deben estar protegidos conforme a la ley, y el titular de esa información, tiene el derecho de acceder a esos datos. Toda la información contenida en esta clase de archivos o registro puede ser modificada, eliminada o anulada por su titular, según sea su designio, debido a que los datos que contiene son de clase privada, y por tanto puede involucrar los derechos personalísimos de su titular. En caso que esta información sea mal usada, publicada, variada, o se atente contra los derechos del titular, este puede ejercitar las acciones legales pertinentes, en ocasión de demandar a quien le haya causado alguna clase de perjuicio.

1.4 El derecho al honor y a la intimidad

Son diversos los conceptos de intimidad que se han esbozado en la doctrina, por ejemplo el caso de la definición brindada por los autores (Pierini & Lorences & Tornabene, 1999) exponen que:

> El poder o potestad de tener un domicilio particular, papeles privados, ejercer actividades, tener contactos personales y pensamientos que no trascienden a terceros, en virtud del interés personal de no hacerlos públicos cuando se trata de hechos privados o datos sensibles de las personas. (p. 237)

En un fallo de la Corte Constitucional Colombia se hace alusión a: “El derecho (…) de poder exigir el adecuado manejo de la información que el individuo decide exhibirá los otros, es una derivación directa del derecho a la intimidad, que se ha denominado derecho a la autodeterminación”. (Derecho a la autodeterminación-identidad, 1997)

La autora Mariana Sánchez, basada en el sistema anglosajón, plantea que:

> Para los juristas norteamericanos el derecho a la intimidad era definido como "El derecho a estar solo", es decir, el derecho a que las personas no conozcan, vean, escuchen lo referente a nuestra vida, pudiendo agregarse también "que nosotros no queremos que trascienda". (Torres Rodas, 2005)

Otros autores exponen que “La intimidad es sinónimo de conciencia de vida interior, por lo tanto este campo queda completamente fuera del ámbito jurídico, pues desde todo punto de vista es imposible penetrar auténticamente en la intimidad ajena” (Recasens Siches, 1978). Asimismo expone (Cárcamo Olivos, 2010) “Es el derecho que tiene todo ser humano de mantener exclusivamente para sí e intocada la esfera del resguardo personal y de extenderla y comunicarla, a quien crea o estime conveniente” (p. 97).

En la (Argentina, Ley 25.326 de Protección de los Datos Personales, 2000, pág. 4) de la República Argentina, el artículo 5 establece que:

> ARTÍCULO 5.- 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

La Corte Suprema de Argentina ha establecido que el derecho a la privacidad:

> Ampara la autonomía individual integrada por sentimientos, hábitos, costumbres, relaciones familiares, posición económica, creencias religiosas, salud mental y física y todos los hechos y datos que integran el estilo de vida de una persona, que la comunidad considera reservadas al individuo y cuyo conocimiento o divulgación significa un peligro para la intimidad. (Torres Rodas, 2005, págs. 30-31)

En nuestra Ley Suprema, en su artículo 66 numeral 20, se reconoce y garantiza a los sujetos un grupo de derechos, entre los que están el derecho a la intimidad personal y familiar. (Ecuador, Constitución de la República, 2008) La intimidad abarca el ámbito privado de un sujeto y su familia. La existencia de un sujeto debe acontecer libre de la injerencia de los demás, para que se desarrolle de forma libre, sujeto a sus decisiones.

En la Declaración Universal de los Derechos Humanos, proclamada en el año 1948 se estableció el derecho a la intimidad como una de las garantías fundamentales del ser humano. De la misma manera se lo menciona en el artículo 11 del Pacto de San José de Costa Rica 1984. Al respecto el Comité de Derechos Humanos ha expresado que:

> (…) Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no

> autorizadas por ley para recibirla, elaborarla y emplearla y porque nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación. (Comité de Derechos Humanos-ONU, 2008)

Según el profesor (García Falconí, 2015) el Derecho a la Intimidad presupone lo siguiente:

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

El propio autor plantea que el Derecho a la Intimidad se divide en intimidad física y psicológica, y por tal razón, cada una de estas clasificaciones abarca un ámbito determinado:

> 1. A la intimidad física; esto es:
> a) A la vida sexual;
> b) A las funciones fisiológicas de excreción, así como de hechos y actos relativos al propio cuerpo, que son tenidos por repugnantes o socialmente inaceptables;
> c) A defectos, anomalías o enfermedades físicas no ostensibles;
> d) A padecimientos físicos intensos; y,
> e) Al parto y a la agonía de un ser humano.
> 2. A la intimidad psicológica; esto es:
> a) Ideas y creencias religiosas, filosóficas, parapsicológicas y políticas, que el individuo debe sustraer al conocimiento de terceros;
> b) Aspectos concernientes a la vida relacional, amores, simpatías, afectos, etc.;
> c) Momentos penosos o de extremo abatimiento;
> d) Actos de fijación o modificación del estado civil;
> e) Condiciones en las relaciones paterno-filiales;
> f) La vida privada de un individuo no divulgada, en cuanto puede ser motivo de bochornos para éste;
> g) En general todo dato, hecho o actividad personal no conocidas por otros, cuya difusión produzca turbación moral o psíquica del afectado; y,
> h) Comunicaciones escritas u orales de tipo personal; esto es, dirigidas únicamente al conocimiento de varias personas determinadas; y, que tengan como contenido alguno de los puntos expuestos. (García Falconí, 2015)

A modo de conclusión se puede establecer que el existe una serie de presupuestos que se asocian con el derecho a la intimidad, o sea que este derecho implica la libertad de:

- no participar en la vida colectiva,
- aislarse de la comunidad de cierto modo y durante cierto tiempo,
- establecer una relación cero,
- disfrutar de un espacio para respirar,
- ejercer un derecho de anonimato,
- tener derecho a un círculo de vida exclusiva,
- no ser conocido en ciertos aspectos por los demás.

La protección brindada por el derecho a la intimidad abarca los sentimientos del sujeto, sus costumbres, sus relaciones de cualquier clase, sus creencias religiosas, su salud y sus decisiones y acciones.

El autor Gonzalo Zambrano Palacios en el prólogo que hiciera a la investigación de (Andrade Santander, 1998) plantea que: “Empero el derecho a la intimidad que comprende una garantía básica de la persona, no ha merecido el tratamiento conceptual que lo estructura debidamente. Se lo considera adscrito a las garantías esenciales del hombre”.

En la Constitución del a República del Ecuador, se protege el derecho al honor en varios artículos. Al respecto expone:

> Art. 11.- El ejercicio de los derechos se regirá por los siguientes principios: (…)
> Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte. (…)
> Derechos de libertad
> Art. 66.- Se reconoce y garantizará a las personas: (…)
> 18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona. (…) (Ecuador, Constitución de la República, 2008)

El derecho al honor, está protegido por la legislación penal y tipificada en el Código Orgánico Integral Penal las conductas que laceren este derecho, como el delito de injuria, garantizando la protección a los derechos personalísimos de los sujetos.

El derecho al honor, además de implicar el ámbito privado de una persona, ataca el ámbito colectivo, en tanto puede mancillar una imagen y crear una serie de consecuencias de tipo social que no solo implicarán al sujeto en cuestión, sino pueden llegar a determinado grupo de personas que lo rodee.

1.5 Acción de habeas data

La acción de habeas data inicialmente se establece a nivel constitucional mediante la regulación en su artículo 92 al exponer que:

> Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
> Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.
> La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados. (Ecuador, Constitución de la República, 2008)

Pero igualmente, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional establece en referencia a la Acción de Hábeas Data en su artículo 49 que su objetivo es garantizar a nivel jurisdiccional que toda persona tenga acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma o sus bienes, estén bajo el cuidado o custodia de personas públicas o privadas, así como personas naturales, en cualquier soporte. Igualmente establece que tendrá derecho a dominar el uso que se haga de la misma. Agrega además que ante la violación de esta normativa, pues procederá la reparación integral. (Ecuador, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009) Se trata pues de una reproducción casi literal de lo plasmado en la Constitución al respecto.

Más allá del objeto propiamente dicho de la Acción del Habeas Data, plasmado en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, es importante establecer los casos que se plantean taxativamente en esta norma, en relación con los supuestos en que procede dicha acción:

> Art. 50.- Ámbito de protección.- Se podrá interponer la acción de hábeas data en los siguientes casos:
> 1. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas.

> 2. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos.
> 3. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente. (Ecuador, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009)

La legitimación para interponer la acción de habeas data, es para todo el sujeto interesado en su información personal, o la persona que ostente la debida representación de este sujeto, en consonancia con el articulado de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional: "Art. 51.- Legitimación activa.- Toda persona, natural o jurídica, por sus propios derechos o como representante legitimado para el efecto, podrá interponer una acción de hábeas data." (Ecuador, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009)

En el caso de las personas jurídicas, la Acción del Habeas Data protege, más que el honor y la intimidad de las personas, la identidad; buena imagen; nombre comercial; valor del fondo de comercio; marca de los productos, y prestigio de la institución.

La legitimación pasiva de la Acción del Habeas Data, corresponde a los sujetos responsables de los registros donde se archiva la información. Para el caso de registros públicos, la legitimación pasiva corresponde al funcionario a cargo del registro de que se trate. En el caso de los registros privados, la legitimación pasiva recae sobre el sujeto que sea el representante legal de la institución u organización donde se archive la información.

Cuando se realiza el mal uso de los datos, o no se adoptan las medidas de seguridad necesarias para la protección de estos, se puede realizar una demanda civil por daños y perjuicios contra el responsable de la protección de esa información. Cuando se incumple con la garantía jurisdiccional de habeas data, es posible invocar la garantía de incumplimiento ante la Corte Constitucional, prevista en el artículo 164 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

1.6 Límites del derecho de libertad de información

El derecho a la libertad de información, está consagrado en varios documentos jurídicos de carácter internacional. La Convención Americana sobre Derechos Humanos, en su artículo 13 expone que toda persona tiene la libertad de buscar, recibir y difundir por cualquier vía informaciones e ideas de toda índole. Agrega además que no debe este derecho estar sometido a cesura, a menos que la Ley así lo disponga y siempre que atente contra los derechos o reputación de los demás, o la seguridad nacional, el orden público o salud y moral de la personas. (Convención Americana sobre Derechos Humanos, 1969)

Por su parte la Declaración Universal de Derechos Humanos, en su artículo 19 expone que:

> Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. (Declaración Universal de Derecho Humanos, 1948)

Otro de los importantes instrumentos a nivel internacional relacionados es el Pacto Internacional de Derechos Civiles y Políticos, desarrollado en el marco del Sistema de Protección de Derechos Humanos de las Naciones Unidas. En su artículo 19 expone que ningún ser humano puede ser molestado por razón de sus opiniones, reconociendo que todos tienen derecho a la libertad de expresión que implica buscar, recibir y difundir informaciones e ideas de toda índole. En este sentido reproduce literalmente en sus acápites segundo y tercero lo expuesto por el artículo 13 de la Convención Americana sobre Derechos Humanos. (Pacto Internacional de Derechos Civiles y Políticos, 1966)

En cuanto a la Declaración de Chapultepec, adoptada en la Conferencia Hemisférica sobre Libertad de Expresión, establece una serie de principios relacionados con la libertad de información en sentido general. En este sentido estipula que no existen personas ni sociedades libres sin que posean libertad de expresión y prensa, definiéndolo como un derecho inalienable del ser humano. Agrega que cualquier sujeto posee el derecho de buscar y recibir informaciones así como expresar opiniones y divulgarlas sin restricción alguna. Obliga al sector público a poner a

disposición de la ciudadanía la información que se generare dentro de sus competencias. Establece una serie de conductas delictivas e ilegales que atentan contra la libertad de expresión y de prensa. En este sentido expone que una de las violaciones graves a la libertad de prensa es la creación de obstáculos al libre flujo informativo. Aunque una declaración corta, establece una serie de principios relacionados con la libertad de información muy importantes y de obligada consulta. (Declaración de Chapultepec, 1994)

La Constitución de la República del Ecuador establece la Acción de Acceso a la Información Pública en su artículo 91 cuando expresa que tendrá por objeto dicha acción, garantizar el acceso a la misma cuando haya sido negada de forma expresa o tácita por autoridad competente o cuando no haya sido ofrecida con la certeza en la cantidad suficiente, determinando la improcedencia de cuando el argumento sea la secretividad, reserva o confidencialidad de la misma. (Ecuador, Constitución de la República, 2008)

Las características de la Acción de Acceso a la Información Pública a consideración de (Navas Alvear, 2008) son que:

> Posee un carácter sumario del procedimiento. Teóricamente y si pese a lo confuso de los incisos donde se establecen los diversos tiempos, no debería demorar más de 5 días la resolución y 10 días en la entrega de la información por parte del recurrido. Este procedimiento no tiene el carácter de excluyente frente a la acción de amparo. Así lo precisa el primer inciso del artículo 22 de la Ley. Sin embargo, es declarativo a diferencia de la antes mencionada acción. Es decir, establece el derecho del peticionario sobre la información. Tiene una importante función de control democrático al permitir una revisión en "sede judicial" de la información clasificada como reservada. En estos casos los efectos de la resolución superan el contexto "inter partes".

La petición de esta acción debe contener los siguientes elementos:

- Identificación del recurrente
- Fundamentos de hecho y de derecho
- Señalamiento de la autoridad de la entidad sujeta a esta Ley, que denegó la información
- La pretensión jurídica.

Según la Ley Orgánica de Transparencia y Acceso a la Información Pública, en su artículo 22, la legitimación para interponer esta acción corre a cargo de toda persona

a quien s ele hubiere negado de alguna forma cualquier tipo de información o le haya sido dada de forma incompleta por alguna de las posibilidades, o sea por alteración de la misma o falsedad, argumentándosele en su carácter de reservado, confidencial o secreto. (Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública, 2012)

Las causales para interponer una Acción de Acceso a la Información Pública, se encuentran establecidas taxativamente en el Reglamento a la Ley Orgánica de Transparencia y Acceso a la Información Pública, estableciendo como fundamento lo siguiente:

> Art. 16.- a) La autoridad ante la que se hubiere presentado la solicitud de acceso se hubiera negado a recibirla o hubiere negado el acceso físico a la información; y,
> b) La información sea considerada incompleta, alterada o supuestamente falsa, e incluso si la negativa se hubiera fundamentado en el carácter reservado o confidencial de la misma. (Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública, 2012)

Cuando se ejercita el derecho a la libertad de la información, se puede incidir en la violación o interrupción de otros derechos protegidos constitucionalmente como pueden ser el derecho a la intimidad, al honor, a la propia imagen, entre otros. Cuando se presenta esta superposición jurídica del ámbito de protección de derechos diferentes que se colisionan, es preciso analizar cuál de estos derechos es prioritario, y cómo garantizar que no se lesione su ámbito de protección.

Cuando se presenta esta clase de disquisición, es establecer la calidad del hecho comunicado, es decir, la trascendencia pública y el interés general de la información presentada. Así como la incidencia en la imagen pública del sujeto del que se comunica el acto o la imagen. Pero realmente un elemento esencial en estos casos, es la comprobación de la veracidad de la información que se publica.

Los límites del derecho a la información pueden ser internos o externos. Los límites internos se relacionan con la comprobación de la veracidad del hecho publicado, como un aspecto objetivo que debe ser identificado. Pero como un límite interno de carácter subjetivo, se desarrolla la actitud del informador hacia la verdad. Los límites externos, se relacionan con los derechos personalísimos, o bienes jurídicos de igual jerarquía.

En este caso se puede concluir que el ordenamiento jurídico ecuatoriano no garantiza la protección a:

- La información falsa.
- La información veraz, pero que puede lesionar bien jurídico protegido, sin que exista una causa de justificación.

Los profesionales de la información, pueden tener a las fuentes de la información sin limitaciones, como un derecho de los ciudadanos y como un deber de los profesionales que informan las fuentes de comunicación.

.

CAPÍTULO II

EL DERECHO A LA PROTECCIÓN DE DATOS

2.1 Los datos personales

Está claro que en esta materia, los datos no es lo que importa proteger, o sea, que los datos en sí, no necesitan protección alguna, pero si, esos datos ya están relacionados de manera alguna a una persona, se trata de cuestión diferente, pues ya en este momento no estamos intentando dar protección al dato en sí, sino al titular del mismo, a la persona, por cuanto ya no sería dato meramente, sino dato personal, o sea, información personal. Y es que al decir de (F. de Marcos, 2010) "El valor de los datos personales es absolutamente innegable. De un lado, en términos de derecho de la personalidad, del individuo, y, de otro, aunque no nos guste excesivamente el planteamiento, en claros términos económicos" (p. 78).

Los datos personales se erigen como aquella "(…) información de cualquier tipo concerniente a personas físicas identificadas o identificables" (Universidad Autónoma Ciudad Juárez, 2012). Por su parte la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de Ecuador, establece en su Disposición General Novena que se entenderá que "Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley". (Ecuador, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002)

El autor (Torres Espinoza, 2010) conceptualiza la protección de datos de la forma siguiente:

> El concepto de protección de datos nació como una mera contraposición a la interferencia en la vida privada de las personas facilitada por el avance tecnológico. Sin embargo, con el transcurso del tiempo, esa concepción fue evolucionando hasta llegar al momento actual en el que la doctrina internacional lo entiende como la protección jurídica de las personas en lo concerniente al tratamiento de sus datos personales, tanto en forma manual como automatizada.
> (…) ha evolucionado la concepción del derecho a la vida privada, pues ha dejado de concebirse como la libertad negativa de rechazar u oponerse al uso de la información personal para convertirse en la libertad positiva de supervisar su uso. (p. 9)

En el Diccionario de conceptos sobre protección de datos de Argentina, se establece que:

> Archivos, registros, bases o bancos de datos: Conjunto organizado de datos personales objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
> Datos Personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

> Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos personales sean objeto de tratamiento por parte de terceros. (Argentina, Diccionario de conceptos sobre Protección de Datos, 2012)

Los titulares de los datos personales, ostentan los siguientes derechos:

Derecho de oposición. Para la Agencia Española de Protección de Datos consiste en que los ciudadanos puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario. (España, Agencia española de Protección de Datos, 2014)

Derecho de información. Implica que toda persona posee derecho a ser informado en forma detallada, sencilla y de manera previa a la recopilación de sus datos sobre la finalidad para la que sus datos personales serán tratados; la existencia del banco de datos en que se almacenarán; la identidad y domicilio del titular del banco de datos que recaba los datos personales, y en su caso del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo de conservación de sus datos personales; cómo ejercitar los derechos que la ley le concede y los medios previstos para ello. (Perú, Autoridad Nacional de Protección de Datos Personales, 2014, pág. 8)

Derecho de acceso. Acceso. Se refiere a que toda persona tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos. (Perú, Autoridad Nacional de Protección de Datos Personales, 2014, pág. 12)

Derecho de rectificación, cancelación o supresión. La rectificación (Actualización, Inclusión): Es el derecho del titular de datos personales que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos o falsos. Cancelación (Supresión): El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados; hubiere vencido el plazo establecido para su tratamiento; se ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al reglamento. (Perú, Autoridad Nacional de Protección de Datos Personales, 2014, pág. 11)

Derecho de tutela. Este derecho tiene por finalidad garantizar el ejercicio efectivo por parte del ciudadano de los derechos de acceso, rectificación, cancelación y oposición. El ciudadano al que le haya sido denegado el ejercicio de los derechos de acceso, rectificación, cancelación y oposición puede ponerlo en conocimiento de la autoridad pertinente, para que ésta constate la procedencia o improcedencia de la denegación. (España, Agencia española de Protección de Datos, 2014, pág. 26)

La impugnación de valoraciones. Este derecho permite al interesado impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. El interesado podrá impugnar actos jurídicos o decisiones privadas que impliquen una valoración de su comportamiento basado únicamente en un tratamiento de datos personales que ofrezca una definición de su personalidad. (España, Universidad de Alcalá, 2015)

Derecho de consulta. Cualquier persona podrá conocer de forma gratuita la existencia de tratamientos de datos de carácter personal (ficheros), sus finalidades y la identidad del responsable del fichero mediante consulta al Registro de Datos Personales correspondiente. La información existente y objeto de consulta se refiere a determinadas características de los ficheros, tales como, identificación, quién es el responsable del mismo, dónde se ubican, el tipo de datos que tratan, órgano ante el cual ejercitar los derechos de acceso, rectificación, cancelación y oposición, y los colectivos de los que se recabaron los datos, entre otras. En definitiva, estos

Registros no recogen el contenido de los ficheros, sino las características de los mismos. (España, Universidad de Alcalá, 2015)

La Constitución de la República del Ecuador establece en su artículo 66 que:

> 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 ley. (Ecuador, Constitución de la República, 2008)

2.2 Principios de la protección de datos

Los principios que rigen la protección de los datos son:

Pertinencia. Se refiere a que para cumplir una finalidad determinada sólo se deben manipular los datos estrictamente pertinentes, de forma tal que "(…) en el ejercicio de la manipulación de datos con una finalidad determinada se cause el menor daño posible al citado derecho fundamental" (España, Agencia española de Protección de Datos, 2014) y es este sentido el "(…) responsable del fichero no podrá recabar ni tratar más datos de los estrictamente necesarios para alcanzar el fin que se propone". (Rebollo Delgado, 2005, pág. 146)

Finalidad. Se refiere a los motivos en que se fundamenta la utilización de los datos por parte del que será el responsable del fichero, a la actividad a la que dirige dicho responsable de la manipulación de la información. (Aparicio Salom, 2000, pág. 81)

Utilización no abusiva. A consideración de (Del Peso Navarro, 2000, pág. 18), este principio forma parte del principio de finalidad. Se refiere esencialmente a que los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Al respecto expone (Solorio Pérez, 2009) que:

> Los datos de carácter personal solo podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido (p. 22).

Exactitud. Se refiere a que los datos que se vayan a tratar para la consecución de cualquier finalidad sean exactos, actualizados y completos. En este sentido el datos es exacto cuando "(…) refleja lo que el emisor del mismo quiere reflejar y es reconocido por el receptor de la misma manera" (Ruiz Carrillo, 2005, pág. 20). Por su parte completo se refiere a que cuando se desea reflejar una realidad, no es necesario aportar todos los matices sobre la misma, sino que es suficiente que la información que se aporta sea suficiente para reconocer e identificar dicha realidad. (Aberasturi Gorriño, 2011, pág. 236). En este sentido actualizados hacen referencia a que se "(…) refieran al tiempo en el que se tratan, y no al pasado" (Aberasturi Gorriño, 2011, pág. 236).

Derecho al olvido. Este derecho se encuentra vinculado con el principio de exactitud o como le ha llamado (Correa et al, 1994, pág. 260) principio de limitación en el tiempo. Este derecho hace alusión a que los datos personales deben desaparecer del archivo o base de datos una vez que hayan cumplido con el fin para el cual fueron recabados. Al respecto expresa (Solorio Pérez, 2009, pág. 25) que:

> Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Legalidad. Se refiere a que el procesamiento de los datos personales debe ser legal y legítimo. Este principio ha sido llamado también como principio de limitación de la recolección (Correa et al, 1994, pág. 258) se refiere a que procedimiento de recogida de datos no debe ser realizado en forma ilícita o desleal. Un ejemplo expuesto de métodos ilegales aquellas investigaciones privadas realizadas por detectives, el uso de instrumentos de grabación o escucha de conversaciones privadas, la violación de correspondencia o papeles privados.

Publicidad. Este principio hace referencia a que toda base de datos ya sea de carácter pública o privada destinada a proporcionar informes debe inscribirse en el registro correspondiente, posibilitando que a través de su consulta los sujetos puedan tomar conocimiento de los archivos en los cuales se encuentran sus datos, para poder ejercer la defensa adecuada.

Control. Este principio se refiere a que es necesario que exista un órgano de control que se responsabilice por el cumplimiento real de los principios contenidos en la legislación en materia de protección de datos personales. Estas instituciones han adoptado diferentes formas, mientras unas se han independizado del poder ejecutivo, otras se han constituido como parte integrante del mismo. (Del Peso Navarro, 2000, pág. 89) A pesar de las consideraciones de uno u otro tipo, si consideramos pertinente que estas instituciones cuenten con la independencia y potestades suficientes para poder supervisar, sin limitaciones que el general funcionamiento de las bases de datos, sea acorde a la Ley. (Correa et al, 1994, pág. 254)

Seguridad. Es uno de los principios más importantes, por cuanto los asuntos relacionados con el tratamiento de los datos personales, desde el momento de su recolección, tratamiento y cesión a terceros, acarrea innumerables problemas. Para ello se hace necesario que las bases de datos se encuentren en plataformas de óptimas condiciones técnicas de integridad y seguridad.

Defensa de los datos sensibles. Para el (Argentina, Centro de Protección de Datos Personales, 2015) datos sensibles serán:

> Aquellos datos personales que revelen origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o a cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos.

Por su parte el (Colombia, Consejo para la Transparencia, 2011) expone que:

> Los datos sensibles corresponden a aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. (p. 13)

Consentimiento. El consentimiento reconoce la posibilidad que posee el titular de una información de datos, de autorizar o no un determinado tratamiento de los mismos, y al decir de (Cantero Martínez, 2005, pág. 259), “Precisamente esa facultad de disponer de lo que corresponde a cada uno no es otra cosa que el reconocimiento del principio de autonomía. Sin duda alguna el consentimiento es

expresión de este principio". Por su parte (Messia de la Cerda Ballesteros, 2003) expone que "El consentimiento informado constituye el principal exponente de la autodeterminación de las personas respecto a sus datos" (p. 219).

2.3 Normativa vigente

Existen una serie de artículos en la Constitución de la República del Ecuador, que hacen alusión al ámbito de protección de los datos, como es el caso de:

> Art. 40.-Se reconoce a las personas el derecho a migrar. No se identificará ni se considerará a ningún ser humano como ilegal por su condición migratoria.
> El Estado, a través de las entidades correspondientes, desarrollará entre otras las siguientes acciones para el ejercicio de los derechos de las personas ecuatorianas en el exterior, cualquiera sea su condición migratoria: (…)
> 5. Mantendrá la confidencialidad de los datos de carácter personal que se encuentren en los archivos de las instituciones del Ecuador en el exterior. (…)
> Art. 45.-Las niñas, niños y adolescentes gozarán de los derechos comunes del ser humano, además de los específicos de su edad. El Estado reconocerá y garantizará la vida, incluido el cuidado y protección desde la concepción.
> Las niñas, niños y adolescentes tienen derecho a la integridad física y psíquica; a su identidad, nombre y ciudadanía; a la salud integral y nutrición; a la educación y cultura, al deporte y recreación; a la seguridad social; a tener una familia y disfrutar de la convivencia familiar y comunitaria; a la participación social; al respeto de su libertad y dignidad; a ser consultados en los asuntos que les afecten; a educarse de manera prioritaria en su idioma y en los contextos culturales propios de sus pueblos y nacionalidades; y a recibir información acerca de sus progenitores o familiares ausentes, salvo que fuera perjudicial para su bienestar.
> Art. 66.-Se reconoce y garantizará a las personas:
> 11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica.
> Art. 92.-Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
> Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.
> La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.
> Art. 362.-La atención de salud como servicio público se prestará a través de las entidades estatales, privadas, autónomas, comunitarias y aquellas que ejerzan las

> medicinas ancestrales alternativas y complementarias. Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes.
> Los servicios públicos estatales de salud serán universales y gratuitos en todos los niveles de atención y comprenderán los procedimientos de diagnóstico, tratamiento, medicamentos y rehabilitación necesarios. (Ecuador, Constitución de la República, 2008)

El numeral 5 es uno de los preceptos importantes en relación a ello, al establecer la confidencialidad de los datos de carácter personal ubicadas en los archivos ecuatorianos que se ubiquen en el exterior. No obsta esta regulación no hace una alusión con suficiencia a la protección de estos datos con carácter constitucional. Por su parte el artículo 45 reconoce una serie de derechos a las niñas, niños y adolescentes, en los que no se estipula de manera literal este derecho a la protección de datos.

Por su parte el artículo 66 si hace una clara alusión a este derecho, en lo que a nuestra consideración se refiere es a los datos personales declarados sensibles, aunque así no los llama el artículo, por lo que implica una definición restrictiva al no ser suficientemente clara en su conceptualización. El artículo 92 hace mención específicamente a estos aspectos. No obstante ello, no consideramos acertado el dar la posibilidad de que se pueda realizar cualquier tipo de acción con referencia a los datos personales mediante la institución de la representación, por cuanto se tratan de derechos de carácter personalísimos, por lo que cualquier posibilidad de que sea otra persona la que pueda realizar acciones con estos, desnaturaliza la institución.

2.4 Datos protegidos

Los datos especialmente protegidos contienen elementos relacionados con la ideología, la afiliación sindical, la religión y las creencias de un sujeto. Por tanto, solo pueden ser tratados dichos datos, cuando sea consentido por el sujeto, de forma expresa y mediante un escrito. Pero además se pueden analizar como datos con especial protección aquellos que se refieren al origen racial, a la salud y a la vida sexual de las personas.

El Convenio Europeo para la Protección de los Derechos de las Personas con respecto al tratamiento automatizado de datos de carácter personal, se firmó en

Estrasburgo, en fecha 28 de enero del año 1981, planteando que el tratamiento indebido de los datos de carácter personal, además de lesionar el derecho fundamental a la protección de datos, podría dañar otros derechos fundamentales.

A tenor de lo dispuesto en la Ley del Sistema Nacional del Registro de Datos Públicos, se creó el Sistema Nacional de Registro de Datos Públicos para proteger y garantizar los derechos que se constituyen, modifican o extinguen, y coordinar el intercambio de información de los registros de datos:

> Art. 28. - Creación, finalidades y objetivos del Sistema Nacional de Registro de Datos Públicos. - Créase el Sistema Nacional de Registro de Datos Públicos con la finalidad de proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten por efectos de la inscripción de los hechos, actos y/o contratos determinados por la presente Ley y las leyes y normas de registros; y con el objeto de coordinar el intercambio de información de los registros de datos públicos. En el caso de que entidades privadas posean información que por su naturaleza sea pública, serán incorporadas a este sistema. (Ecuador, Ley del Sistema Nacional de Registro de Datos Públicos, 2010)

Existe una serie de instituciones que integran el Sistema Nacional de Registro de Datos Públicos, principalmente los diferentes registros, que aportan sus datos a este sistema centralizado:

> Art. 29. - Conformación. - El Sistema Nacional de Registro de Datos Públicos estará conformado por los registros: civil, de la propiedad, mercantil, societario, datos de conectividad electrónica, vehicular, de naves y aeronaves, patentes, de propiedad intelectual y todos los registros de datos de las instituciones públicas y privadas que mantuvieren y administren por disposición legal información registral de carácter público.
> Será presidido por la Directora o Director Nacional de Registro de Datos Públicos, con las facultades que se determinan en la presente Ley y su respectivo reglamento. (Ecuador, Ley del Sistema Nacional de Registro de Datos Públicos, 2010)

2.5 Análisis del juicio de exhibición previsto en el Código de Procedimiento Civil ecuatoriano

Dentro de las cuestiones importantes que entran en contradicción con el Derecho Fundamental de protección de datos personales en nuestro país, está lo estipulado en la Sección Vigésima Segunda Del juicio de exhibición, del Título II De la sustanciación de los juicios del Código de Procedimiento Civil ecuatoriano. El artículo 821 establece esencialmente la posibilidad de solicitar la exhibición de

documentos para promover una demanda o contestarla, estableciendo el término de tres días para que la persona a quien se le pide que exhiba, lo haga. En este sentido cabe destacar que no se restringe únicamente a los litigantes dentro del proceso civil, sino que de la interpretación de la norma se admite que la petición podrá establecerse contra una tercera persona.

Por su parte el artículo 822 establece una obligación legal de mostrar los mismos si el propio tenedor confiesa que el objeto de dicha prueba está en su poder. El artículo 823 obliga igualmente a aquella persona o institución que posea dichos documentos a exhibirlos o expedir copia o compulsa de ellos. Los artículos siguientes, desde el 824 y hasta el 827, se refieren fundamentalmente a la oposición de exhibir los mismos por causas justificadas o no justificadas, así como a la petición dentro del término de prueba y a la consecuencia de incumplir con la petición del juez de exhibir los documentos solicitados.

Es totalmente contraproducente que la Constitución de nuestro país reconozca la protección de los datos personales, y que mediante este articulado se viole tan flagrantemente este derecho fundamental y de una forma tan directa, dentro del proceso civil.

Este articulado estipula la obligación de que el sujeto natural o jurídico en quien se establezca que posee documentos que deben ser mostrados, sin más análisis el juez lo ordenará, violando por ende el Derecho a la Protección de Datos Personales. Estos documentos pueden ser de las más disímiles formas y contener los más sensibles datos referidos a las partes procesales o a terceros implicados, y por ende, con este carácter de delicado debe ser tratado.

La normativa del Código de Procedimiento Civil no establece la obligatoriedad de que el juez realice un análisis profundo sobre la pertinencia de exponer dichos documentos y la información contenida en ella. Simplemente el juez puede compeler a que se muestren, sencillamente a petición de parte interesada, sin que la norma lo obligue a que la parte que realizó la petición, le demuestre al órgano jurisdiccional, la necesidad de que dichos datos, de que la información contenida en los mismos, sea imprescindible para la demostración de hechos y su vinculación con la pretensión.

Y aunque la norma establece el Derecho de Oposición, queda a competencia del juez dictar la resolución definiendo la procedencia o no de la exhibición. Y puede acontecer que la exhibición se ordene a una institución o archivo donde se concentren datos personales, en la práctica el funcionario no tendría objeción, ante la petición de un juez, de brindar información en cuya custodia se encuentra, pero que no le pertenece y por ende su sensación de confidencialidad es relativo, por cuanto no es su información sensible.

En este sentido debe establecerse un procedimiento para que, si la información se le pide a una institución sobre un sujeto que no se encuentra presente en el proceso, se le dé cuenta para que pueda oponerse, si lo estimare, a la exhibición de dicha información. Se trata pues de respetar a ultranza este derecho constitucionalmente regulado.

Otra cuestión criticable es que se deja a consideración del juez qué entender por datos personales contenidos en este documento, pues no es sino la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la que define qué entender por datos personales y datos sensibles, sin que este ente esté obligado a hacerse de estos conceptos de otra norma para aplicarlos al procedimiento civil, pues este ha sido insuficiente al tratar este tema tan importante. Es pues la consideración del juez, en base a los argumentos que le de cada parte, la que se tiene en cuenta para definir si, la información contenida en el documento que se pide exhibirse, es sensible o no, provocando incertidumbre al respeto, porque lo que puede ser sensible para un sujeto o institución, no necesariamente lo debe ser para el que juzga.

2.6 Estudio comparado de la Protección de Datos

Para realizar un estudio serio sobre cualquier tema, es necesario analizar el entorno internacional de la figura a investigar. Ello posibilita tener un alcance mayor sobre el tema. La protección de Datos a nivel internacional ha tenido un tratamiento diferenciado en cada país. En algunos países el tratamiento que se le ha hecho ha sido fuerte y dirigido a proteger los datos personales a ultranza, por lo que en dichos sistemas legales la utilización de estos datos derivados de sistemas de telecomunicaciones en procesos judiciales se minimiza al máximo.

Por su parte, en otros sistemas legales, la protección no es tan radical, pues el bien común o interés público lo ubican por encima del derecho a la protección de datos personales derivados de sistemas de telecomunicaciones. Se trata de una postura que defiende la protección de los citados datos, pero que ante situaciones del imperio necesario de la justicia, se hace imprescindible la utilización de los mismos en procesos establecidos. Ante esta situación, analizaremos las posiciones de Colombia y Argentina, quienes consideramos poseen legislaciones importantes en este tema.

2.6.1 Colombia

El Decreto número 1377 del año 2013, modifica la Ley de Protección de Datos, Habeas Data, de Colombia. Este Decreto establece instituciones de tipo muy actual, como es el *spam*, o para aquellos sujetos que utilicen de forma inadecuada datos de los ciudadanos. La sanción en estos casos corresponde a una multa de hasta 2.000 salarios mínimos vigentes, correspondiente a $1180 millones.

La Superintendencia de Industria y Comercio, en sus siglas SIC, obliga, mediante el Decreto 1377, a que las empresas que quieran usar datos personales recogidos antes de la entrada en vigor de este decreto, deben solicitar la autorización de los ciudadanos por los medios pertinentes que son utilizados de forma habitual.

A modo de crítica al Decreto 1377, se expuso que:

> A menos de una semana de haber emitido el decreto 1377 del 2013 que reglamenta la ley de protección de datos, ya se anunciaron algunas demandas.
> Según los argumentos de los demandantes de la norma, es ilegal que a las personas se les notifique por avisos de prensa la solicitud de autorización del uso de sus datos, dado que no todos tendrán la oportunidad de ver ese mensaje.
> De igual forma consideran que violan los derechos de los ciudadanos, las autorizaciones tácitas. Estas se darán cuando los colombianos no respondan, en un período de 30 días, los correos que piden la autorización para el uso de la información.
> Sin embargo, la Superintendencia de Industria y Comercio, dice que la norma es legal y que cualquier inquietud y queja de la ciudadanía se puede hacer a través de la página web de la entidad. (Redacción de El País y Colprensa, 2013)

El Decreto 1377, de fecha 27 de junio del 2013, establece un conjunto de obligaciones particulares:

1). El anuncio como tal (y a los cinco días siguientes de la comunicación, enviar carta comunicándole al respecto a la Superintendencia de Industria y Comercio).
2). Formato de autorización para que si lo desean lo diligencien los titulares de datos recolectados previamente.
3). Determinación de canal electrónico y físico para recibir las autorizaciones.
4). Política de tratamiento de la información personal (pues esta se debe indicar en el anuncio).
5). Conducto regular y canales físicos y electrónicos definidos para que el titular ejerza sus derechos de acceso, rectificación y supresión. (Colombia, Decreto 1377, 2013)

Los datos que son recolectados a partir de la entrada en vigor del Decreto 1377, cumplen con los siguientes requisitos:

1). Aviso de Privacidad (que se puede hacer estratégicamente en el mismo formato de autorización de la captura).
2). Definir o crear un área o sujeto responsable de la protección de la información personal, según el tamaño empresarial del cliente (es decir aquí opera el criterio de responsabilidad demostrada consagrado en los arts. 26 y 27 del Decreto 1377).
3). Establecer cláusulas para transmisiones y transferencias de datos (si estas aplican).
4). Definir o conocer cuáles son los grupos de interés del cliente.
5). Definir las finalidades y los tratamientos genéricos en cada grupo de interés, pues esto se debe indicar en la política de tratamiento y en el formato de autorización. (Colombia, Decreto 1377, 2013)

2.6.2 Argentina

En el año 2003, se creó en Argentina la Dirección Nacional de Protección de Datos Personales, en sus siglas PDP, como órgano de control para la efectiva protección de los datos personales. A este se subordina el Registro Nacional de las Bases de Datos, que a su vez controla bases de datos que circulan en el país, en consonancia con el Ministerio de Justicia, Seguridad y Derechos Humanos.

La Dirección Nacional de Protección de Datos Personales tiene conocimiento de:

- La existencia de una base de datos.
- Objeto de la recolección de datos y su finalidad.
- Nombre y domicilio del responsable de la base de datos.

La Ley 25.326, establece como infracciones de su regulación las siguientes:

> Supresión de datos personales de registros de bases de datos en caso de comprobarse el hecho denunciado.
> Rectificación de datos personales de registros de bases de datos.
> Acceso a la información.
> Actualización de datos personales.
> Confidencialidad en el tratamiento de datos. (Argentina, Ley 25.326 de Protección de los Datos Personales, 2000)

Además de controlar las infracciones, la Dirección Nacional de Protección de Datos Personales, puede ejercitar las siguientes funciones:

> Acción Judicial de Habeas Data. Esta acción procede para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquellos. En caso de falsedad o discriminación solicitará la supresión, rectificación, confidencialidad o actualización de sus datos.
> Aprobación de Consentimientos Informados.
> Aprobación de Transferencias Internacionales de bases de datos.
> Control de las bases de datos a través del Registro Nacional de bases de Datos privadas y públicas.
> Inspecciones en empresas y organismos.

El Registro Nacional de Bases de Datos, subordinado a la Dirección Nacional de Protección de Datos Personales refiere que:

> Es el medio que la ley otorga para conocer y controlar a los registros, archivos, bases o bancos de datos que traten datos personales. El acceso para consultar el registro es público y gratuito. Por medio de él todas las personas podrán conocer qué tipo de información es la que maneja cada base de datos y quién es el responsable de la misma. Los particulares podrán acudir a la DNPDP a efectos de conocer qué bases de datos pueden tener sus datos, quién es el responsable, y luego acudir a dichos registros, archivos, bases o bancos de datos para corregir, suprimir o rectificar el asiento. (Argentina, Registro Nacional de Bases de Datos, 2015)

2.7 Proyecto de Ley de Protección de Datos Personales en Ecuador

Con el constante auge de las nuevas tecnologías en la vida pública y privada de los sujetos, se presenta la necesidad de valorar la sanción del enriquecimiento desproporcionado e ilegal, y de las malas prácticas, en relación con los espacios de intercambio de datos. Con este espíritu se promulgó un Proyecto de Ley de Protección de Datos Personales en nuestro país, el que no llegó a dar sus frutos.

No obstante ello, es necesario el análisis, del Proyecto de Ley de Protección de Datos Personales (Torres Espinoza, 2010), que establece elementos muy importantes para garantizar la protección de los derechos de los ciudadanos. Por

ejemplo, en este proyecto se plantean los requisitos de identificación y validación de la identidad, para el acceso a servicios y prestaciones públicas.

Por tanto se precisa un breve análisis de este proyecto de ley, que como elemento esencial establece las infracciones, en relación con las sanciones a imponer, como forma de garantizar la protección de los datos, exponiendo a tal efecto lo siguiente:

> INFRACCIONES Y SANCIONES
> Art. 38.-Responsables.-Los responsables de los sujetos al régimen sancionador esta trate de archivos de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y y demás normas aplicables a la materia.
> Legitimación activa y pasiva.-
> La acción de protección de los datos personales podrá ser ejercitada por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de Cuando la acción sea ejercida por personas jurídicas, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.
> En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.
> La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes. (Ecuador, Proyecto de Ley de Protección de Datos, 2015)

El Proyecto de Ley de Protección de Datos Personales, delimita las clases de sanciones que se imponen, en relación con la gravedad del acto que sea cometido por el infractor:

> Art. 39.-Tipos de infracciones.
> Las infracciones se calificarán como leves, graves o muy graves.
> Son infracciones leves:
> a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
> b) No proporcionar la información que solicite de Datos, en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de dato
> c) No solicitar la inscripción del Registro del Instituto Nacional de Protección de Datos constitutivo de infracción grave.
> d) Proceder a la recolección afectados sin proporcionarles la información que señala la presente Ley.
> Son infracciones graves:
> a) Proceder a la creación de recolección de datos de carácter personal para los mismos, sin autorización la ley.
> b) Proceder a la creación de recolección de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
> c) Proceder a la recolección consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
> d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal, cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

> e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Datos.
> f) Tratar los datos de carácter personal de forma ilegítima o con principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
> g) La vulneración del deber de guardar secreto sobre los datos de carácter personal, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
> h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
> i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero. (Ecuador, Proyecto de Ley de Protección de Datos, 2015)

Además este Proyecto de Ley hace mención a las clases de sanciones que se imponen de acuerdo a la gravedad del hecho cometido, bien sea leve, grave, o muy grave:

> Art. 40.- Tipo de sanciones.
> 1. Las infracciones leves serán sancionadas con multa de 100 a 1000 dólares.
> 2. Las infracciones graves serán sancionadas con multa de 1.000 a 5.000 dólares.
> 3. Las infracciones muy graves serán sancionadas con multa de 5.000 a 20.000 dólares.
> La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que se antijuridicidad y de culpabilidad presentes en la concreta actuación infractora. (Ecuador, Proyecto de Ley de Protección de Datos, 2015)

No obstante elementos importantes relacionados con este proyecto el mismo se archivó por la Asamblea Nacional en base a considerar que varios de los preceptos propuestos en la misma ya encuentran respaldo en varias normas existentes ya, tanto en la Constitución como en la legislación secundaria, como la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional; y la Ley de Transparencia y Acceso a la Información Pública. Igualmente se consideró que "(…) el proyecto no tiene la condición ni alcance jerárquico de Ley Orgánica" (Ecuador, Agencia Pública de Noticias del Ecuador y Suramérica (ANDES), 2012). Igualmente se consideró que existen errores en el modo de establecerse los medios de protección de datos personales, así como la innecesaria creación de un organismo con competencia nacional dirigido a regular la actividad.

No obstante estas consideraciones, creemos totalmente desacertado la no admisión y aprobación del citado proyecto. No obstante las falencias que en el orden práctico haya podido tener, lo cierto es que Ecuador no necesita que en otras leyes secundarias, cuya finalidad y objeto es otro bien diferente a la protección de datos personales, existan normas por las cuales se le pueda dar tratamiento y protección a los datos de carácter personal. Estas leyes, no fueron promulgadas con esa finalidad, por lo que no podemos dejar a que en varias normas, se regule de forma aislada, alguna que otra institución que de cierto grado de protección a este tipo de datos. No es suficiente que determinadas instituciones de aseguramiento puedan estar en estas legislaciones.

La práctica indica que es imprescindible la creación de una norma específica que con suficiencia de respuesta a los problemas y dificultades que hoy enfrenta la protección de datos personales en el ámbito nacional. Una norma, cuyo objetivo único y exclusivo sea el de regular con capacidad, todas las instituciones relacionadas con los datos personales, de forma tal que por sí sola, sin tener que ir a otras normas secundarias, sea capaz de revelar con eficacia, la savia del problema. No es justificación lo expuesto por la Asamblea Nacional sobre la creación de un ente administrativo para dirigir y controlar dicha institución. Son justificaciones que más que representar el criterio unánime de la Sociedad de la Información ecuatoriana, es una postura arcaica, retrógrada y que representa opiniones políticas parcializadas, pues fácilmente esta función se le puede imponer a un organismo competente sin la necesidad de crear uno nuevo.

Lo que intentamos exponer con el análisis, es que las legislaciones expuestas y que supuestamente dan protección a los datos personales en Ecuador, no son suficientes para enfrentar la amplia gama de manifestaciones relacionadas con la protección de datos personales en nuestro país. Solo una norma especial que regule esta cuestión, daría respaldo lógico a las conductas que en este momento se están materializando con mayor fuerza en el ámbito nacional.

2.8 Protección de Datos Personales y Propiedad Intelectual

A simple vista y mediante un análisis superficial podríamos entender que la Propiedad Intelectual no posee vinculación alguna con los datos personales, o la

protección de estos en Sistemas de Telecomunicaciones cuando se encuentren en debate en determinado proceso judicial. Pero la realidad no es esa. La integralidad en la que tienen lugar los procesos en la actualidad, donde la mayoría de ellos posee un respaldo mediante los Sistemas de Telecomunicaciones, hace que los datos personales y los Derechos de Propiedad Intelectual, encuentren una vinculación sensible.

La realidad estriba en que los Derechos de Propiedad Intelectual, ya fueres los Derechos de Autor o de Propiedad Industrial, pueden verse sometidos a litigios en determinado proceso judicial por cualquiera de las violaciones establecidas en la legislación y que constituyen el contenido de estos derechos. El quebrantamiento, por ejemplo, del derecho a ser nombrado, cuando una obra es publicada, constituye una violación de datos personales, que pudiera implicar una demanda para la restitución de la situación con la consiguiente reparación de daños o indemnización de perjuicios.

Esta infracción se pudo dar mediante la utilización de Sistemas de Telecomunicaciones, pues una obra que haya sido publicada en Internet, sin hacer mención a su autor; o la simple alteración de la misma, implica violaciones del Derecho de Autor, que se manifestó mediante estos sistemas informáticos, y que provoca acción legal. Peor no obsta ello, en la Litis que pudiera tener lugar ante los Tribunales, estos derechos no están absolutamente protegidos, pues se pueden debatir cuestiones privadas o confidenciales sobre obras en las que el autor aun no haya publicado y cuya originalidad o novedad pueda quedar en un estado dudo ante cualquier petición de partes procesales para que se enseñen.

Lo que queremos dejar sentado es, que en determinado proceso judicial por violación de cualquier derecho de Propiedad Intelectual, podría lograrse la divulgación dentro de dicho proceso, de datos referidos a obras inéditas que pudieran perjudicar a la parte obligada. Teniendo como base ello es que consideramos existe un gran riesgo de transgresión de los datos personales en estos procesos.

Es indudable que los datos de carácter personal están estrechamente ligados con los llamados Derechos de Propiedad Intelectual. Tal y como ha sido definida por la

Organización Internacional de la Propiedad Intelectual (OMPI) al referir que son aquellas:

> (…) creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizadas en el comercio. La propiedad intelectual se divide en dos categorías: propiedad industrial y derecho de autor. (Organización Mundial de la Propiedad Intelectual, 2010, pág. 2)

Los derechos de propiedad intelectual tienen la misma esencia que el resto de los derechos de propiedad, pues permiten al creador o al titular de una patente, marca o derecho de autor, beneficiarse en el uso, disfrute y abuso de la obra que han creado.

La protección del derecho de autor comprende un grupo amplio de creaciones artísticas del ámbito literario, artístico y científico, sin importar su forma de expresión, soporte o medio. (Convenio de Berna para la Protección de las Obras Literarias y Artísticas, 1886)

Existen diversas clases o tipos de derechos que protege el derecho de autor. En primer lugar los llamados derechos patrimoniales que son los que permiten de exclusivamente la explotación de la obra, pero solo hasta el plazo que determine la ley nacional del país de la obra, contado a partir de la muerte del último de los autores. Al transcurrir dicho término, esta pasa a ser de dominio público y cualquier persona puede explotar la obra.

Los derechos patrimoniales protegidos son el derecho de reproducción o copia; derecho de comunicación pública; derecho de distribución y derecho de transformación.

Otra de las clases de derechos que protege el derecho de autor son los derechos morales, que se refiere a aquellos derechos que posee el autor de manera permanente, y serán irrenunciables e imprescriptibles. Los derechos morales que protege el derecho de autor son el derecho de divulgación; derecho de paternidad; derecho de integridad; derecho de modificación o variación; derecho al retiro de la obra del comercio; y derecho de acceso.

Y existen otras clases de derechos como los derechos conexos, que protegen a personas que si bien no son autores de la obra, tiene de igual manera un conjunto

de derechos sobre ella, por ejemplo los artistas, intérpretes, traductores, editores, productores; los derechos de reproducción, mediante el cual el autor de la obra puede impedir a terceros que efectúen copias o reproducciones de sus obras; el derecho de comunicación pública, por la que el autor o cualquier otro titular de los derechos sobre la obra, puede autorizar una representación o ejecución viva, o en directo, de su obra, como es el caso de la representación de una pieza teatral o la ejecución de una sinfonía por una orquesta para una sala de concierto; y los derechos de traducción que permiten reproducir y publicar una obra traducida, pero con el permiso del titular de la obra en el idioma original.

Es menester entonces delimitar si los derechos de Propiedad Intelectual constituyen o pueden constituir Datos Personales. Como hemos expuesto los datos personales constituyen toda aquella información asociada a una persona y que permite diferenciarla de otros sujetos integrantes de la sociedad, mediante su documento de identidad, lugar de nacimiento, estado civil, edad, lugar, lugar de residencia, trayectoria académica, laboral, profesional, estado de salud, características físicas, ideología política, vida sexual, entre otras cuestiones. (Colombia, Superintendencia Industria y Comercio, 2015)

El principal problema que se da entre datos personales y derechos de propiedad intelectual, tiene lugar en las redes sociales. La cuestión fundamental es en muchas ocasiones los propios sujetos ofrecen o ceden en las llamadas redes sociales sus datos personales, por diferentes cuestiones, de forma consciente o inconsciente, para dar respuesta a las necesidades diarias de mantenimiento o realización de acciones personales mediante la utilización de internet. En muchas ocasiones cuando accedemos a un sitio web, donde publicaremos determinada obra en la que indudablemente constan nuestros datos personales, no nos percatamos de las advertencias que en la misma se hacen relacionadas con los avisos legales y políticas de privacidad, aunque generalmente se encuentran en sitios de difícil acceso o localización y para la mayoría no son comprensibles.

No obstante ello, se hace necesario que los sujetos que utilicen estos medios y vayan a realizar una actividad de publicación de sus datos personales por cualquier razón, observe estos ítems que aparecen generalmente en la parte inferior de la página web en la que realizan su actividad, porque se establecen con la finalidad de

que se conozca el tratamiento que dicha página web hará de sus datos personales y las implicaciones que conlleva su tratamiento por la misma.

La personas publican creaciones propias en las redes sociales, bajo su titularidad, pero con la rapidez con que fluye la información en este medio, tanto su obra como sus datos pueden ser mal utilizados por personas inescrupulosas en la remisión de correos electrónicos llamadas spam; la realización de estafas en línea, o simplemente el plagio de la obra o alteración de los datos de su titular. Son enormes las cantidades de personas que en las diferentes plataformas de internet publican junto con sus datos personales, una obra musical o fotográfica con el objetivo de promocionarla, y es cuando surgen las diferentes situaciones problémica relacionadas con violación de los Derechos de Autor y alteraciones de los datos personales.

Este es solo uno de los ámbitos en que pueden verse afectados los llamados Datos Personales y los Derechos de Propiedad Intelectual. Hemos demostrado que indudablemente existe una interrelación casi natural entre ambas instituciones, pues una obra creada procede inexcusablemente de un sujeto que posee datos que lo hacen autor de dicha creación, por lo que donde quiera que vaya la obra irá el autor no en físico sino como persona que ha creado y cuya creación se encuentra presente, por lo que cualquier alteración de la obra, repercutirá en los elementos identificativos de su inventor.

Otro de los fenómenos que atenta no solo contra los derechos de Propiedad Intelectual sino contra los datos personales, es la piratería, que:

> (…) abarca la reproducción y distribución de copias de obras protegidas por el derecho de autor, así como su transmisión al público o su puesta a disposición en redes de comunicación en línea, sin la autorización de los propietarios legítimos, cuando dicha autorización resulte necesaria legalmente. La piratería afecta a obras de distintos tipos, como la música, la literatura, el cine, los programas informáticos, los videojuegos, los programas y las señales audiovisuales. (UNESCO, 2015)

En nuestro país, este fenómeno se relaciona con la debilidad de las normas y legislaciones vigentes, y se vincula igualmente con el costo desleal de los productos, puesto que las copias ilegales de CD de música y películas se venden hasta precios de un dólar, e incluso menos cantidad, por solo citar un ejemplo. Es muy común que

en el desarrollo de la realización de una copia de cualquier de estas obras, se cambie de autor, o se alteren los datos del mismo, por lo que de forma directa está afectando los datos personales.

CAPÍTULO III

SISTEMAS DE TELECOMUNICACIONES Y PROCESOS JUDICIALES

3.1 Sistema de Telecomunicaciones

Los Sistemas de Telecomunicaciones, son:

> (…) infraestructura física a través de las cuales se transporta información (…) con base en esa infraestructura se ofrece a los usuarios servicios de telecomunicaciones (…) Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, y puede utilizar diferentes redes de transporte, y, por tanto, el usuario requiere de distintos equipos terminales. (EcuRed, 2016)

Los Sistemas de Telecomunicaciones se pueden clasificar en los siguientes:

- Redes conmutadas. Consisten en una sucesión alternante de nodos y canales de comunicación (…) Existen dos tipos de conmutación en este tipo de redes: conmutación de paquetes y conmutación de circuitos. La conmutación de paquetes, el mensaje se divide en pequeños paquetes independientes, a cada uno se le agrega información de control, y los paquetes circulan de nodo en nodo. Al llegar al nodo al que está conectado el usuario destino, se reensambla el mensaje y se le entrega. La conmutación de circuitos busca y reserva una trayectoria entre los usuarios, se establece la comunicación y se mantiene esta trayectoria durante todo el tiempo que se esté transmitiendo información.
- Redes de difusión.- Disponen de un canal al cual están conectados todos los usuarios, y todos ellos pueden recibir todos los mensajes, pero solamente extraen del canal los mensajes en los que identifican su dirección como destinatarios. (EcuRed, 2016)

3.2 Sistema Informático

Un sistema informático es:

(…) un sistema de información que basa la parte fundamental de su procesamiento, en el empleo de la computación (…) que emplea un sistema que usa dispositivos que se usan para programar y almacenar programas y datos. Si además de la información, es capaz de almacenar y difundir los conocimientos que se generan sobre cierta temática, tanto dentro, como en el entorno de la entidad, entonces está en presencia de un sistema de gestión de información y conocimientos. (EcuRed, 2016)

Los Sistemas de Informáticos se pueden clasificar en los siguientes:

- Sistemas de procesamiento básico de la información. Son aquellos en que las computadoras se limitan a realizar las operaciones de procesamiento físico de la información.
- Sistemas de apoyo a la toma de decisiones. Se apoyan en los Sistemas de información para la dirección (MIS), los que crean y actualizan las bases de datos, que los primeros utilizan. Los DSS se destinan a la toma de decisiones, están

hechos para apoyar el trabajo individual o para las decisiones en grupo, apoyan mucho en la llamada investigación de operaciones o los métodos cuantitativo de la toma de decisiones, técnicas matemáticas para apoyar el trabajo del ser humano en las llamadas decisiones bien estructuradas, débilmente estructuradas y no estructuradas, las cuales por su complejidad pueden tener errores al ser analizadas por el ser humano con métodos tradicionales (intuición, experiencia).

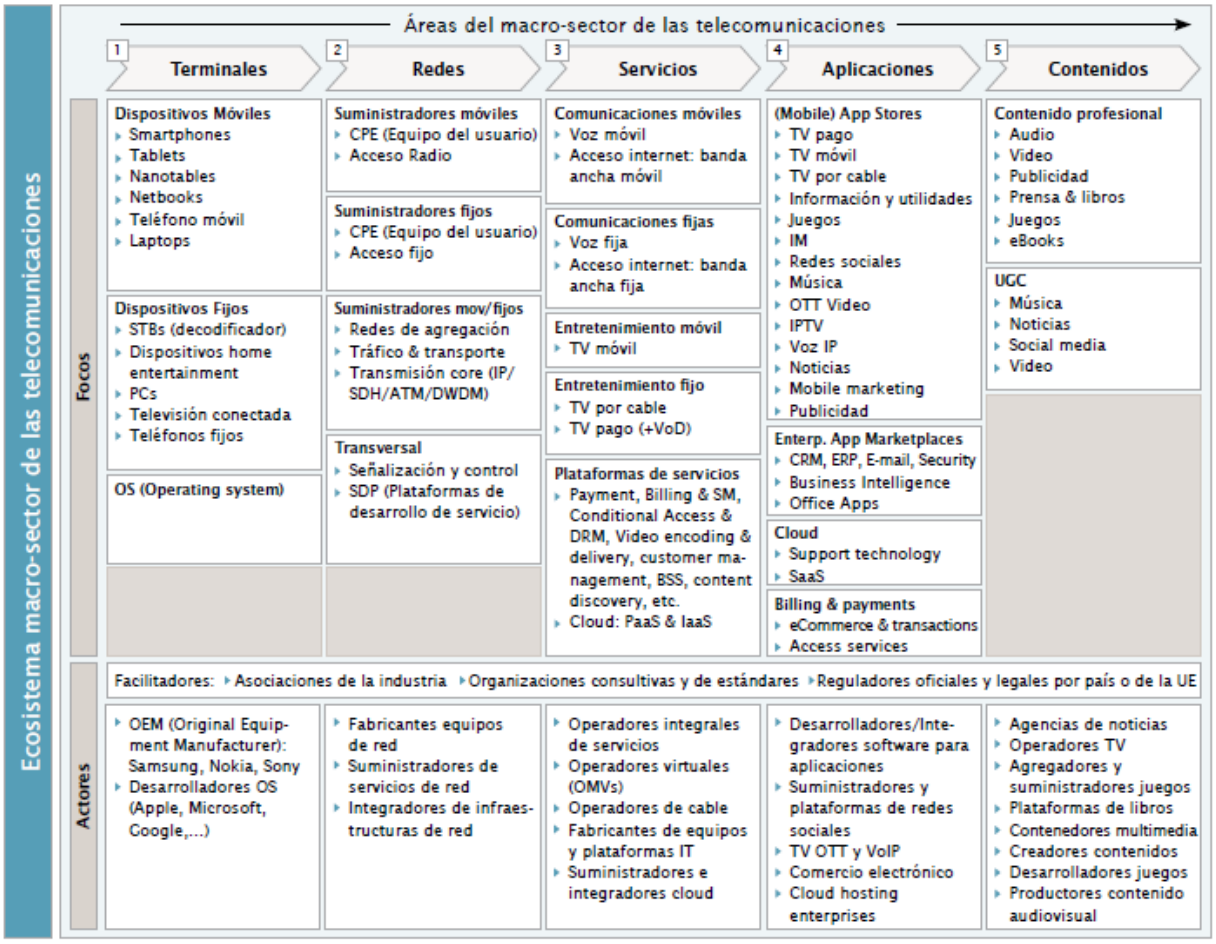
- Sistemas basados en la inteligencia artificial. Los sistemas de expertos, como comúnmente se les conoce, tiene una base de datos especial donde se almacenan los conocimientos de los expertos humanos. Esta se llama base de conocimientos, su confección y llenado se apoya en una tecnología llamada ingeniería del conocimiento, a medio camino entre la informática y la tecnología. Además estos sistemas cuentan con programas especializados en inteligencia artificial conocidos como motores de inferencia, mediante los cuales revisan las bases de conocimientos y ejecutan las operaciones "inteligentes" para solucionar los problemas que se les plantea.
- Sistemas basados en técnicas WEB. Los sistemas basados en la WEB, pueden ser también de uso externo, o sea, para comunicar información al entorno de la entidad (clientes, suministradores, niveles superiores, agencias gubernamentales, público en general y otras entidades políticas o administrativas de control). En estos casos la información que aparecerá en el sitio WEB estará acorde con la misión y los objetivos de la entidad.
- Sistemas de gestión del conocimiento. Los sistemas de gestión de relaciones son sistemas muy asociados a los SIM y a la gestión comercial, pues se utilizan para propiciar una adecuada relación con los clientes de la entidad. Se utilizan prácticamente en todo el ciclo de relaciones con el cliente. Pueden emplearse para definir: provisiones de ventas, registros de visitas de gestión al cliente, contactos realizados en ferias y congresos, volúmenes de compras anteriores, intenciones de compra anterior o satisfechas, comportamiento de pago, bancos con los que trabaja, oportunidades de negocio, acciones directas de marketing que ha recibido. (EcuRed, 2016)

3.3 Sector de las Telecomunicaciones

La Empresa de Consultoría Europea ALTRAN, en su Informe de Evolución del macro-sector de las Telecomunicaciones en España 2014-2017, plantea un "(…) ecosistema del macro-sector de las Telecomunicaciones en el que se han identificado 5 grandes áreas industriales (terminales, redes, servicios, aplicaciones y contenidos) con sus correspondientes sub-áreas y componentes" (ALTRAN, 2014).

En este sentido el propio Informe determina una serie de actores que pueden intevenir en cada uno de os componentes establecidos, de forma tal que pueden influir en ellos, ya fuere en las terminales, las redes, los servicios, las aplicaciones o los contenidos en ellos. La figura que en dicho informe se agrega, la presentamos a continuación.

Figura 1. Áreas del macro sector de las telecomunicaciones.



Fuente: (ALTRAN, 2014)

En cada una de estas áreas existe información de usuarios que son administradas por los operadores:

- Terminales. En el caso de los terminales en el 2014 en Ecuador se empezó a realizar un registro de los terminales, asociando los códigos IMEI que son únicos para cada dispositivo a los propietarios.
- Redes. En el caso de las Redes protocolo IP es utilizado para el enrutamiento de información ya que estos son etiquetas que se asignan a cada nodo usuario de la red.
- Servicios. En el caso de servicios, como los de telefonía o televisión, estos están asociados a un suscriptor.
- Aplicaciones. En el caso de aplicaciones como Facebook, Instagram, Skype, Gmail, cada usuario se registra con un perfil accediendo a los servicios de la aplicación de forma ubicua.
- Contenidos. En el caso de contenidos, como Netfilx, Yotube, FoxPlay a más de los datos de los usuarios registran perfiles de comportamiento. (ALTRAN, 2014)

En todos estos casos la información debe ser manejada adecuadamente por los operadores, ahora bien muchos de ellos no se encuentran en el país, lo que dificulta determinar la norma legal con la que se rigen.

3.3 Delitos de Telecomunicaciones e Informáticos

No existe en la doctrina tradicional o reciente, menciones especiales a qué entender por Delitos de Telecomunicaciones. Tanto la teoría como la jurisprudencia se ha encargado de tratar los llamados Delitos Informáticos, y dentro de las conductas típicas del mismo, aquellas que afectan las telecomunicaciones. Ello justifica l ausencia de una doctrina nacional o foránea sobre este último.

No obstante, nosotros somos partidarios de distinguirlos a efectos de nuestra investigación. Es claro que no todo medio de telecomunicaciones es un medio informático, y viceversa. Esos medios electrónicos, son, en potencia, herramientas que en dependencia del uso y abuso, podrían ser mecanismo de telecomunicaciones o informáticos. Ello dependerá también del destino y uso que se le dé al medio. Una simple computadora, por ejemplo, es un medio informático, pero no necesariamente es un medio de telecomunicaciones. Solo si se incorporan a su sistema, los programas que permitan establecer relaciones por conducto de ella, mediante la telecomunicación, se convertirá entonces en un medio de este tipo.

Por Delitos Informáticos se pueden entender aquellas "(…) actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje". (Criminalística.mx, 2015)

Los Delitos de Telecomunicaciones incorporados en el Título XIII de la Ley Orgánica de Telecomunicaciones, se detallan a continuación:
En el Capítulo Primero trata sobre infracciones, citando los artículos:

- Art. 116.- Ámbito subjetivo y definición de la responsabilidad.
- Art. 117.- Infracciones de primera clase.
- Art. 118.- Infracciones de segunda clase.
- Art. 119.- Infracciones de tercera clase.
- Art. 120.- Infracciones cuarta clase. (Ecuador, Ley Orgánica de Telecomunicaciones, 2015)

Según Davara Rodríguez, un delito Informático es "(…) la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" (Davara Rodríguez, 1990, pág. 26).

Los Delitos Informáticos incorporados en el Código Orgánico Integral Penal (COIP), están en el Capítulo Segundo que trata sobre Delitos contra los Derechos de Libertad, en su Sección Sexta que menciona Delitos contra el Derecho a la Intimidad Personal y Familiar:

- Art. 178.- Violación a la intimidad.
- Art. 179.- Revelación de secreto. (Ecuador, Código Orgánico Integral Penal, 2014)

Dentro de este mismo Capítulo en su Sección Novena menciona, Delitos contra el Derecho a la Propiedad:

- Art. 186.- Estafa.
- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 191.- Reprogramación o modificación de información de equipos terminales móviles.
- Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.
- Art. 193.- Reemplazo de identificación de terminales móviles.
- Art. 194.- Comercialización ilícita de terminales móviles.
- Art. 195.- Infraestructura ilícita. (Ecuador, Código Orgánico Integral Penal, 2014)

También en este mismo capítulo en su Sección Segunda menciona, Delitos contra el Derecho a la Identidad:

- Art. 212.- Suplantación de identidad. (Ecuador, Código Orgánico Integral Penal, 2014)

En el Capítulo Tercero que trata sobre Delitos contra los Derechos del Buen Vivir, en su Sección Tercera, menciona Delitos contra la Seguridad de los Activos de los Sistemas de Información y Comunicación, citando los artículos:

- Art. 229.- Revelación ilegal de base de datos.
- Art. 230.- Interceptación ilegal de datos.
- Art. 231.- Transferencia electrónica de activo patrimonial.
- Art. 232.- Ataque a la integridad de sistemas informáticos.
- Art. 233.- Delitos contra la información pública reservada legalmente.
- Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. (Ecuador, Código Orgánico Integral Penal, 2014)

En el Capítulo Sexto trata sobre Delitos contra la Estructura del Estado Constitucional, en su Sección Única menciona Delitos contra la Seguridad Pública, citando el artículo:

- Art. 354.- Espionaje. (Ecuador, Código Orgánico Integral Penal, 2014)

En el Capítulo Séptimo trata sobre Terrorismo y su financiación, en su Sección Única menciona Delitos contra la Seguridad Pública, citando el artículo:

- Art. 366.- Terrorismo. (Ecuador, Código Orgánico Integral Penal, 2014)

3.3 Jurisprudencia

1.- En el trámite de la tutela administrativa presentada por una parte de los causahabientes de Oswaldo Guayasamín en contra de Talleres Guayasamín, por la presunta violación del derecho de autor a través de la utilización de los diseños del pintor, se dictó una resolución que, en lo principal, dispuso la suspensión de toda actividad de utilización, explotación, venta, oferta en venta, exportación o reproducción de los diseños de autoría del maestro. (OMPI/JPI-JDA/GDL/04/2 EC, 2004)

Para este caso como en muchos el internet permite el acceso a contenidos que poseen derechos de autor, debido a que mediante sistemas de almacenamiento de datos estos son copiados y distribuidos.

2.- Para el caso de Gigatribe que es una red peer-to-peer para intercambio de archivos, desarrollada en Francia. En el 2010, un juez federal de Estados Unidos dictaminó que la expectativa razonable de privacidad no se extiende al intercambio de archivos en GigaTribe. En el proceso, un informante le dio a la policía acceso a los archivos de sus amigos en GigaTribe, y se descubrió pornografía infantil. 31 En noviembre del 2011 se descubrió una cuenta de Gigatribe que contenía 300 gigabytes de pornografía infantil. La denuncia de dicha cuenta comenzó en Australia, donde la policía, en su investigación, dio a conocer que la direcciones IP's de donde se habían subido dichas imágenes provenían de Ecuador. Indicado este hecho y siendo éste un delito transnacional, la organización que se hizo cargo del caso fue la Interpol.

> Es por ello que los documentos investigados en Australia fueron remitidos a la Interpol de Melbourne (en dicho país), para su posterior envío a la Interpol de Lyon en Francia, luego a la de Londres en Reino Unido, a la de Buenos Aires en Argentina y finalmente a la Interpol de Quito en Ecuador. Una vez que los documentos se encontraron en Ecuador, la Fiscalía General del Estado junto a Interpol, DGI y Policía Judicial prosiguieron con las investigaciones que dieron como resultado final la localización de los autores del ilícito, quienes se encontraban en la ciudad de Guayaquil. (Cuenca Espinosa, 2012, pág. 20)
>
> En Ecuador, en cuanto a Delitos Informáticos, se realiza la denuncia a través del Ministerio Público, es decir, a través de la Fiscalía General del Estado, quien cuenta con la cooperación internacional de la Interpol (por el problema de una o más jurisdicciones), y de manera local con el Servicio de Inteligencia de la Policía Judicial y Contrainteligencia, para las debidas capturas y seguimientos. (Cuenca Espinosa, 2012, pág. 22)

El proceso se observa que a partir de las direcciones IP asociadas a un usuario se accede a información que es de custodia de los operadores de acceso a Internet, las cuales son utilizadas antes de que empiece un proceso judicial.

3.- En cuanto al confrontamiento del Presidente Rafael Correa, y el creador de la página CRUDO ECUADOR, por:

> (…) un comentario "meme" en el cual se observa al Presidente de compras en un centro comercial de Europa, el Presidente Correa, públicamente expresó lo siguiente: "Somos 10000 más, así que le vamos a responder y también vamos a identificar a ésta persona". Por supuesto, la admonición del mandatario trajo como consecuencia la contestación del creador de CRUDO ECUADOR, que respondió lo siguiente: "Este pleito de un presidente contra un ciudadano que hace memes lo está ridiculizando. Querer mostrar mi identidad no solo vulnera mi derecho al anonimato, sino que lo haría responsable de cualquier cosa que pueda pasarme a mí y a mi familia. Esta página es manejada por una persona, pero miles de ecuatorianos son los que se expresan a través de ella; la gente me manda material. Si hay algo que me tiene todavía dudando de botar la toalla es el apoyo de la gente; muchas veces me llega a cansar esto, si no gano nada, nadie me paga".
> Por su parte el Presidente también anunció que se ha creado la página Somos +, para enfrentar lo que denominó una campaña sistemática de desprestigio en las redes sociales, y dijo: "Vamos a identificar a éstas personas para ver si es tan jocosa cuando todo el mundo sepa quién es, sin descartar que se pueda iniciar procesos judiciales". Terminó el mandatario manifestando que si hay que recurrir a la parte legal, lo haremos, eso se llama Estado de Derecho. (Observatorio de Derechos y Justicia, 2015)

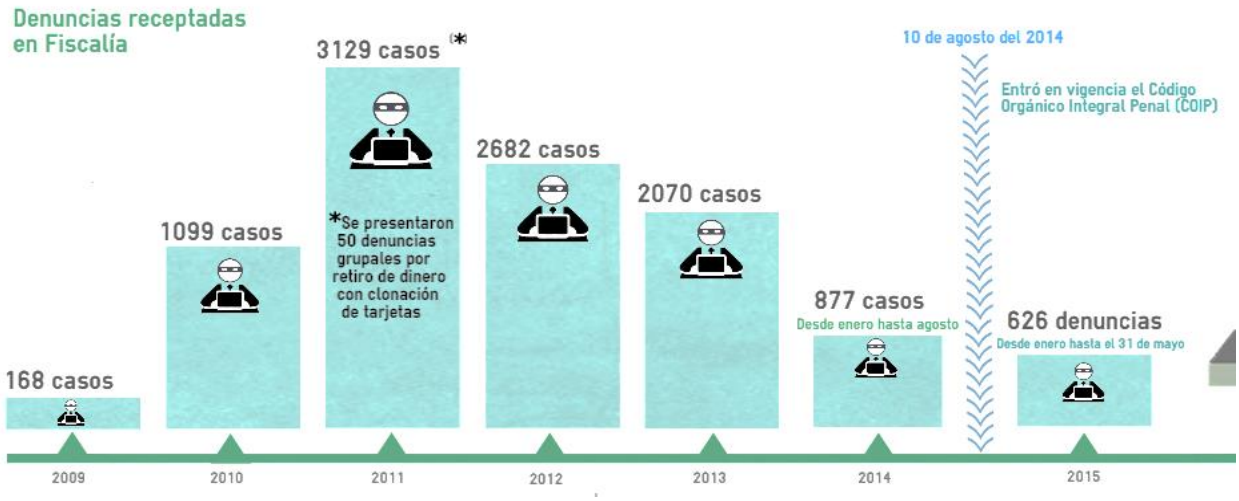
En este caso se llegó a determinar quién era el administrador de la página de CRUDO ECUADOR, de tal manera que recibió notas en su lugar de residencia, por lo que es claro que por medio de acceso a información que es almacenada por los proveedores de internet y asociada al usuario como es el caso de las lista de Direcciones IP, se identificó al creador de la página, lo cual deja de manifiesto que de alguna forma se accedió a información que solo debería accederse dentro de un proceso judicial y con autorización de un juez.

3.3.1 Casos de delitos Informáticos

Los presentes gráficos, aunque no guardan relación directa con la violación de datos personales relacionados con sistemas de telecomunicaciones en procesos judiciales, sí da una idea del fenómeno de los delitos informáticos en el Ecuador en el pasado reciente, lo que sin duda pone en atención a todos, porque se puede utilizar estos medios informáticos para lograr acceder a las bases de datos, incluso del Consejo

de la Judicatura, y lograr obtener acceso a los datos personales de los implicados en determinado proceso, para realizar acciones ilegítimas con los mismos.

Figura 2. Denuncias recepcionadas por la Fiscalía por posibles comisiones de Delitos Informáticos.



Fuente: Fiscalía General del Estado, Ecuador; 2015.

Estos son algunas descripciones de casos prácticos que han tenido lugar en nuestro entorno nacional, sobre la violación de la seguridad electrónica, mediante la sustracción de los datos personales de individuos. Aunque no guardan estrecha relación con nuestro tema, consideramos pertinente agregarlos, para tomar nota sobre las manifestaciones en este orden.

Caso 1.

Diana (nombre protegido) ingresó sus datos para realizar una compra por Internet, porque se ofrecían descuentos en productos de belleza. Por medio electrónico una persona usó su información, le endeudó en 2.500 dólares, a través de débitos de su tarjeta. (Ecuador, Boletín Fiscalía General del Estado, 2015)

Posibles causas:

- No cerró su sesión debidamente al terminar la transacción.
- Fue negligente con el uso de sus datos al permitir quizás que otros accedieran a los mismos sin ella percatarse.
- No revisar periódicamente su estado de cuenta.

Caso 2.

Mauricio E., de 21 años. Bloquearon su cuenta en Facebook y luego vio que alguien publicaba comentarios ofensivos y subía fotos en su nombre. El joven tuvo que enviar mensajes de texto, llamar por teléfono y redactar correos a sus contactos explicando que no era el autor de insultos a otras personas en la red. (Ecuador, Boletín Fiscalía General del Estado, 2015)

Posibles causas:

- No cerró su sesión debidamente al terminar la transacción.
- Fue negligente con el uso de sus datos al permitir quizás que otros accedieran a los mismos sin el percatarse.

Caso 3.

Lorena A., de 31 años. La quiteña en febrero del 2015 tras recibir un correo expresándole que tenía que actualizar su estado de cuenta, ella sin percatarse actualizó su información. Pero luego se dio cuenta de que alguien había consumido 1.200 dólares de su tarjeta de crédito. (Ecuador, Boletín Fiscalía General del Estado, 2015)

Posibles causas:

- No cerró su sesión debidamente al terminar alguna transacción.
- Fue negligente con el uso de sus datos al permitir quizás que otros accedieran a los mismos sin el percatarse.
- No comunicarse telefónicamente antes de actualizar sus datos con la sucursal correspondiente para verificar la veracidad del correo

Caso 4.

Carmen (nombre protegido) no salía del asombro tras observar el estado de cuenta de su tarjeta de crédito, puesto que debía cancelar 913 dólares por una compra que jamás realizó. En el documento, que le llegó a finales de julio de 2014, constaba que ella había adquirido un tour aéreo para asistir al Mundial de Fútbol de Brasil por 900 dólares y un pago adicional por una recarga telefónica por 13 dólares. La mujer de 30 años, que ahora afronta una situación angustiosa por esas deudas no contraídas, jamás salió del país, ni hizo transacciones comerciales por Internet.

Su indignación es evidente porque este hecho causó problemas en su economía familiar. (Boletín Fiscalía General del Estado Ecuador, 2014)

Posibles causas:

- No cerró su sesión debidamente al terminar la transacción.
- Fue negligente con el uso de sus datos al permitir quizás que otros accedieran a los mismos sin ella percatarse.
- No revisar periódicamente su estado de cuenta.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- La Constitución de la República del Ecuador regula en forma adecuada los elementos concernientes al derecho a la intimidad, al honor, y a la libertad de información.

- La Constitución de la República del Ecuador establece como garantías jurisdiccionales la Acción de Habeas Data, y el Código de Procedimiento Civil, establece el Juicio de Exhibición de Documentos.

- El Derecho a la Protección de Datos está estrechamente ligada a los Derechos de Propiedad Intelectual, por lo que la violación de estos indudablemente afectan de forma directa los datos personales, siendo insuficiente en Ecuador, desde la legislación sobre propiedad intelectual, el campo de protección hacia los derechos de los autores de las creaciones y con ello de sus datos personales.

- En Ecuador, aunque han existido intentos de promulgar una Ley Orgánica de Protección de Datos Personales, no se ha consumado debido a opiniones negativas sobre los proyectos que han sido considerados por la Asamblea Nacional, existiendo un vacío legal especial para la protección de estos datos.

- El Código de Procedimiento Civil ecuatoriano establece dentro de sus procesos el llamado Juicio de Exhibición de Documentos, el que de la forma que se encuera redactada, obvia cualquier tipo de protección que pudiera existir de los datos personales relacionados con sistemas de telecomunicaciones, no estableciendo desde la perspectiva del Derecho Procesal Civil, límites en este sentido.

- El actual sistema de protección de datos personales encuentra respaldo constitucional, pero no está refrendado en una ley orgánica, situación de inmediata necesidad para lograr que una ley especial establezca todos los parámetros jurídicos necesarios para que se garantice la protección a los derechos a la intimidad, el honor y la protección de datos.

4.2 Recomendaciones

- Aprobar el Proyecto de Ley Orgánica de Protección de Datos Personales, que establezca todos los parámetros jurídicos necesarios para que se garantice la protección a los derechos a la intimidad, el honor y la protección de datos.

- Aprobar una Ley Reformatoria al Código de Procedimiento Civil ecuatoriano en lo referente al Juicio de Exhibición de Documentos, mediante el cual se establezcan limitaciones a esta acción.

- Que esta investigación constituya un material de estudio actualizado sobre la protección de datos en el Ecuador y las falencias que posee la misma en el orden legislativo, formando parte del material bibliográfico de la Universidad Técnica Particular de Loja para su consulta general.

CAPÍTULO V

LA PROPUESTA

5. Datos informativos

Finalmente la propuesta se aplicaría a toda la población residente en el Ecuador. Los beneficiarios de cualquier proyecto son aquellas personas a quienes se dirige la propuesta en cuestión, y que obviamente recibirán un beneficio con dicho proyecto. Los beneficiarios directos son aquellas personas que participarán directamente en el proyecto, y se benefician con su puesta en marcha. Pueden ser las personas que se emplearán en el proyecto, quienes obtendrán bienes y servicios de él, o que usarán de alguna manera el producto que se derive de la propuesta.

En el caso de la presente propuesta, se considera beneficiario directo inicialmente al sistema de protección de datos personales en el Ecuador. En el caso de la propuesta que se presenta, los beneficiarios indirectos serán todas las personas que habitan el Ecuador, en tanto se logre establecer y dar un adecuado tratamiento en los procesos civiles a los datos personales.

Los datos personales constituyen en la actualidad un conjunto de derechos fundamentales refrendados por la Carta Magna. Ello implica la necesidad imperiosa de que sean establecidas de forma clara, directa y urgente, los mecanismos efectivos para su protección dentro de los procesos judiciales. La realidad al respecto es muy diferente. Es claro que aunque la Constitución refrenda tal derecho, el Código de Procedimiento Civil obvia la trascendencia constitucional de tales preceptos, esencialmente en los Juicios de Exhibición de Documentos, situación que se grava con la ausencia de una ley especial que trate el tema.

La importancia de proponer no solo una reforma al Código de Procedimiento Civil ecuatoriano, sino la promulgación de una Ley Orgánica de Protección de Datos Personales, se asocia con el espíritu supremo no solo de garantizar el efecto inmediato y vinculante de la norma constitucional, sino de la necesidad de enfrentar situaciones de violación de estos derechos con normativas eficientes y suficientes.

5.1 Justificación

Se precisa que al momento de evaluar cualquier acción legislativa al respecto, se tomen en cuenta los urgentes y cada vez más acelerados cambios que enfrenta en

la actualidad la sociedad de la información, donde los sistemas de telecomunicaciones no ofrecen una plataforma lo suficientemente segura de protección de datos personales. Si unido a ello le sumamos la insuficiencia legislativa en el ámbito nacional para afrontar las disímiles situaciones que en torno a ello pueden originarse, entonces podemos concluir que se encuentra evidenciado la necesidad de adoptar medidas al respecto.

Los beneficiarios de la propuesta que se pretende serán el sistema legal ecuatoriano y la seguridad que provea a la protección de datos. También se benefician de forma general todos los habitantes del Ecuador, al contar con un orden legislativo suficiente que dé respuesta a las constantes violaciones de los datos personales que propicia el vacío legal existente así como la exigua regulación al respeto que se hace en la Ley Adjetiva Civil ecuatoriana.

El Ecuador, es uno de los países que cuenta con una Constitución que se preocupó por regular la protección de los datos personales, pero ha realizado poco el ente legislativo para desarrollar como es lógico, mediante una norma especial, la protección que implica el reconocimiento fundamental de este derecho.

5.2 Objetivo

Establecer la protección de datos personales a través de la reforma al Código de Procedimiento Civil y mediante la promulgación de una Ley Orgánica de Protección de Datos Personales en Ecuador, que permita otorgar una protección efectiva a los mismos tal y como se deriva de lo estipulado en la Constitución nacional.

5.2.1 Resultados esperados

La propuesta elaborada es de tipo legislativo, y versa sobre las modificaciones que deberían realizarse al Código de Procedimiento Civil ecuatoriano, referentes a las limitaciones que deben establecerse en el Juicio de Exhibición de Documentos, como límites ante la protección de datos personales. Igualmente se establecerán las bases fundamentales sobre las que se debe dirigir un futuro proyecto de Ley Orgánica de Protección de Datos Personales en nuestro país.

Esta reforma y proyecto legislativo será factible para lograr una mayor seguridad jurídica en la protección de datos personales relacionados con los procesos civiles y en sentido general, así como lograr la eficacia de una norma constitucional que hasta el momento no ha tenido un desarrollo legislativo suficiente. De igual forma el proyecto tendrá factibilidad externa, en tanto abarcará todo el país, una vez que se hagan efectivas las propuestas de reforma legislativa formuladas en este trabajo investigativo.

El impacto será el efecto que cause el proyecto en aquellos a quienes se dirige, y puede ser social, o económico. El impacto social es un cambio como resultado de un proceso, serán los efectos que se produzcan a nivel social por las ideas definidas en el proceso de investigación. En el caso de esta propuesta de reforma, va a tener un gran impacto social, toda vez que se dirige a lograr que se cumpla con la protección de los derechos de protección de datos personales en el Ecuador.

El impacto económico es uno de los impactos más importantes, debido a que permite conocer cómo afectará económicamente a los que participarán en la investigación, y si de hecho esta es o no factible. El presente proyecto tiene un impacto económico importante, puesto que con la propuesta de reforma legislativa se busca lograr que se protejan loa datos personales relacionados con la propiedad intelectual, derechos estos últimos que poseen un gran contenido económico.

5.3 Desarrollo de la propuesta

5.3.1 Reforma al Código de Procedimiento Civil de la República de Ecuador

Este proyecto de reforma tiene como objetivo modificar el articulado del Código de Procedimiento Civil vigente, en materia de Protección de Datos Personales de la forma siguiente:

PROYECTO DE LEY REFORMATORIA AL CÓDIGO DE PROCEDIMIENTO CIVIL

República del Ecuador

ASAMBLEA NACIONAL

EXPOSICIÓN DE MOTIVOS

Que Ecuador es uno de los países que ha refrendado con carácter constitucional el Derecho a la Protección de Datos Personales.

Que en base a las diferentes manifestaciones que están teniendo en la cotidianidad sobre las violaciones de los Datos Personales, los gobiernos adoptan todas las medidas tendentes a garantizar la seguridad de los mismos.

Que el Código de Procedimiento Civil ecuatoriano, dentro de sus procesos regula el Juicio de Exhibición de Documentos, en la que existe una clara vinculación con los Datos Personales, no estableciendo límites para la protección de los mismos en los diferentes procesos judiciales.

República del Ecuador
ASAMBLEA NACIONAL

CONSIDERANDO:

Que el artículo 1 de la Constitución de la República del Ecuador establece que El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada.

Que el numeral 8 del artículo 375 de la Constitución de la República del Ecuador establece que es deber del Estado Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción.

Que el numeral 9 del artículo 11 de la Constitución de la República del Ecuador establece como principio que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución.

Que el artículo 82 de la Constitución de la República del Ecuador establece el derecho a la seguridad jurídica que se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

Que el artículo 84 de la Constitución de la República del Ecuador dice que la Asamblea Nacional y todo órgano con potestad normativa tendrán la obligación de

adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales.

En uso de sus atribuciones constitucionales y legales expide la siguiente:

LEY REFORMATORIA AL CÓDIGO DE PROCEDIMIENTO CIVIL DE LA REPÚBLICA DEL ECUADOR

Artículo 1.- Incorpórese en el artículo 821:

Art. 821.- Si las cosas muebles o documentos que se pretende que se exhiban, poseen datos personales de cualquier índole, a los efectos de determinar su naturaleza y alcance, el juez convocará en el término de dos días a una audiencia, en la que se definirá, previa escucha de ambas partes, sobre la pertinencia y real necesidad de que dicha información sea conocida y traída a juicio. El juez valorará la conveniencia de difundir en el proceso dicha información, y su decisión estará regida por el principio de protección de Datos Personales establecidas en la Constitución y demás leyes, por lo que la utilización de los Datos personales contenidos en dichos bienes muebles o documentos, solo tendrá un carácter excepcional.

5.3.2 Propuesta de bases legales sobre las que debe fundarse una futura Ley Orgánica de Protección de Datos Personales en el Ecuador.

Esta segunda propuesta estará dirigida a la Asamblea Nacional con la finalidad de que establezca o tome en consideración las cuestiones esenciales que no deben faltar en el análisis y aprobación de una futura Ley Orgánica de Protección de Datos Personales en el Ecuador, sin que sea nuestra intención, establecer todos los institutos que debe contener la misma.

Los institutos que proponemos lo hacemos en base a las leyes que hemos analizado en el Derecho Comparado, logrando extraer lo que a nuestra consideración es lo mejor de cada una, para que de esa forma la conformación de la nueva norma jurídica, no falten cuestiones esenciales que hacen perfectible la citada Legislación. La norma debería abarcar como mínimo los siguientes contenidos:

- Objeto de la Ley.
- Definiciones de términos básicos.
- Ámbito de aplicación.
- Principios rectores
  . Legalidad.
  . Licitud.
  . Proporcionalidad.
  . Calidad.
  . Seguridad.
  . Transparencia.
  . Acceso y circulación restringida.
  . Consentimiento.
  . Finalidad.
  . Temporalidad.
  . Disposición de Recurso.
  . Nivel de protección adecuado.
  . Libertad.
  . Confidencialidad.
  . Disponibilidad.
- Valor de los principios.
- Alcance sobre tratamiento de datos personales.
- Limitaciones al consentimiento para el tratamiento de datos personales.
- Datos sensibles.
- Flujo transfronterizo de datos personales.
- Derechos de los niños, niñas y adolescentes.
- Medidas de seguridad en el tratamiento de datos personales.
  . Seguridad física.
  . Seguridad lógica.
  . Seguridad de desarrollo y aplicaciones.
  . Seguridad de cifrado.
  . Seguridad de comunicaciones y redes.
- Niveles de seguridad.
  . Básico.
  . Medio.
  . Alto.

- Confidencialidad de datos personales.
- Derechos del Titular de datos personales.
  . Derecho de información del titular de datos personales.
  . Derecho de acceso del titular de datos personales.
  . Derecho de actualización, inclusión, rectificación y supresión.
  . Derecho a impedir el suministro.
  . Derecho de oposición.
  . Derecho al tratamiento objetivo.
  . Derecho a la tutela.
  . Derecho a ser indemnizado.
  . Contraprestación.
  . Limitaciones.
- Procedimiento para ejercer los derechos del titular.
- Casos en que no es necesaria la autorización del titular.
- Impugnación de decisiones.
- Obligaciones del titular y del encargado del banco de datos personales.
- Banco de datos personales.
  . Creación, modificación o cancelación de bancos de datos personales.
  . Prestación de servicios de tratamiento de datos personales.
  . Códigos de conducta.
- Órgano competente de Protección de Datos Personales.
  . Órgano competente y régimen jurídico.
  . Funciones del Órgano competente de Protección de Datos Personales.
  . Registro Nacional de Protección de Datos Personales.
  . Confidencialidad.
  . Recursos del Órgano competente de Protección de Datos Personales.
- Infracciones y sanciones administrativas.
  . Procedimiento sancionador.
  . Infracciones leves, graves y muy graves.
  . Sanciones administrativas.
  . Multas coercitivas.

5.4.3 Conclusiones y recomendaciones de la propuesta

De acuerdo a los análisis que hemos realizado en nuestra investigación, la sociedad ecuatoriana no encuentra un adecuado respaldo legal en materia de protección de datos personales. En la propuesta elaborada se cumple con los requisitos de evaluación de un proyecto, toda vez que los objetivos de este se relacionan directamente con las necesidades e intereses de la población en base a la legislación ecuatoriana vigente.

También se cumple con la condición de eficacia, pues se espera cumplir con los objetivos propuestos, en la correcta actuación del Estado ecuatoriano, para velar por los derechos de la ciudadanía a la protección de sus datos personales, esencialmente en los procesos judiciales pero en un universo general. La propuesta además es eficiente, puesto que la correcta aplicación normativa relativa a los datos personales, redundará en el beneficio social y económico del sistema de derecho, Estado y la sociedad ecuatoriana.

La propuesta elaborada, una vez que se desarrolle y sea legislada, tendrá un importante impacto social y económico en la nación ecuatoriana, contribuyendo a cumplir con el derecho constitucionalmente reconocido de protección de datos personales.

BIBLIOGRAFÍA

Aberasturi Gorriño, U. (2011). *Los principios de la Protección de Datos aplicados en la sanidad.* Bilbao: Universidad del País Vasco.

Acurio del Pino, D. S. (s.f.). Definición y el concepto de Delitos Informáticos. En *Delitos Informáticos* (págs. 10-11).

Acurio del Pino, S. (s.f.). Sujetos del delito informático. En *Delitos Informaticos* (págs. 15-20).

Aguirre, V. (17 de junio de 2013). *Tutela Judicial Efectiva*. Obtenido de http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/funcionjudicial/2013/06/17/tutela-judicial-efectiva.

Alcalá-Zamora y Castillo, N. (1964). Introducción al estudio de la prueba. *Revista de Derecho y Ciencias Sociales*, 233.

ALEGSA.COM.AR. (s.f.). *DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA*. (ALEGSA.COM.AR) Recuperado el 14 de Agosto de 2015, de http://www.alegsa.com.ar/Dic/control%20de%20acceso.php.

ALTRAN. (2014). *Evolución del macro-sector de las Telecomunicaciones en España 2014-2017. La perspectiva de sus propios actores.* Barcelona: ALTRAN.

Andrade Santander, D. (1998). *El derecho a la intimidad.* Quito: Quito: Andino.

Aparicio Salom, J. (2000). *Estudios sobre la Ley Orgánica de Protección de Datos de Carácter Personal.* Navarra: Editorial Arazandi.

Argentina, Centro de Protección de Datos Personales. (10 de 12 de 2015). *Preguntas Frecuentes.* Obtenido de http://www.cpdp.gob.ar/index.php?view=items&cid=1%3Afcat_cpdp&id=7%3Afac_Qu%C3%A9+son+los+datos+sensibles&option=com_quickfaq&Itemid=7.

Argentina, Diccionario de conceptos sobre Protección de Datos. (2012). *Diccionario de conceptos sobre Protección de Datos.* Buenos Aires: http://www.protecciondedatos.com.ar.

Argentina, Ley 25.326 de Protección de los Datos Personales. (30 de 10 de 2000). Ley 25.326 de Protección de los Datos Personales. Buenos Aires, Buenos Aires, Argentina: Senado y Cámara de Diputados Argentina.

Argentina, Registro Nacional de Bases de Datos. (2015). *http://www.jus.gob.ar/*.

Bentham, J. (1971). *Tratado de las pruebas judiciales.* Buenos Aires: Editorial EJEA.

Boletín Fiscalía General del Estado Ecuador. (2014). *El COIP contempla una pena de tres a cinco años de prisión por robos de cuentas bancarias.* Quito: FGE.

Carnelutti, F. (1944). *Sistema de Derecho procesal civil.* Buenos Aires: Editorial Uteha.

Carnelutti, F. (1955). *La prueba civil.* Buenos Aires: Ediciones Acay.

CEAAMER. (1 de 12 de 2015). *Centro de Estudios Avanzados de las Américas.* Obtenido de http://www.ceaamer.edu.mx/new/der3/tgp/modulo8.pdf.

Colombia, Consejo para la Transparencia. (2011). *Protección de Datos Personales.* Santiago: Consejo para la Transparencia.

Colombia, Decreto 1377. (27 de junio de 2013). Colombia.

Colombia, Superintendencia Industria y Comercio. (22 de 12 de 2015). *Sobre la Protección de datos personales.* Obtenido de http://www.sic.gov.co/drupal/sobre-la-proteccion-de-datos-personales.

Comité de Derechos Humanos-ONU. (2008). *Examen de los informes presentados por los Estados partes de conformidad con el artículo 40 del Pacto.* Ginebra: ONU.

Convención Americana sobre Derechos Humanos. (1969). *Pacto de San José.* Washington D.C.: OEA.

Convenio de Berna para la Protección de las Obras Literarias y Artísticas. (9 de 9 de 1886). *http://www.wipo.int/.*

Convenio de París para la Protección de la Propiedad Industrial. (20 de 3 de 1883). *http://cemprende.unapec.edu.do.*

Cordón Moreno, F. (2001). Comentario a los artículos 328 y 329 LEC. En F. Cordón Moreno, *Comentarios a la Ley de Enjuiciamiento Civil* (pág. 1455). Pamplona: Arazandi.

Correa et al, C. M. (1994). *Derecho Informático.* Buenos Aires: Editorial DePalma.

Couture, E. J. (1993). *Vocabulario jurídico: con referencia especial al Derecho Procesal positivo vigente uruguayo.* Buenos Aires: Editorial Depalma.

Criminalística.mx. (2015). *Delitos informáticos*. Recuperado el 2 de Septiembre de 2015, de http://www.criminalistica.com.mx/areas-forenses/seguridad-publica/548-delitos-informcos

Cuenca Espinosa, A. (2012). *El Delito Informático en el Ecuador "Una nueva tendencia criminal del Siglo XXI". Su evolución, punibilidad y proceso penal.* Obtenido de http://www.egov.ufsc.br/portal/sites/default/files/el_delito_informatico_en_el_ecuador_una_tendencia_criminal_del_siglo_xxi-alexander_cuenca.pdf.

Davara Rodríguez, M. Á. (1990). Análisis de la Ley de Fraude Informático. *Revista de Derecho UNAM*, 26.

De la Oliva Santos, A. (1997). *Derecho Procesal Civil.* Madrid: Centro de Estudios Ramón Areces (CERA).

Decisión 486 Régimen Común sobre Propiedad Industrial. (1 de 12 de 2000). *http://www.wipo.int.*

Declaración de Chapultepec. (1994). *Libertad de Expresión.* México D.F.: Conferencia Hemisférica sobre Libertad de Expresión.

Declaración Universal de Derecho Humanos. (1948). *Herramientas para la Defensa y Promoción de los Derechos Humanos.* New York: Fundación Acción Pro Derechos Humanos.

Declaración Universal de los Derechos Humanos. (2008). Santiago de Chile: Oficina Regional de Educación para América Latina y el Caribe-UNESCO.

Del Campo Changuin, R. (2013). *La legitimidad de la información en el Derecho Constitucional ecuatoriano.* Obtenido de http://www.uees.edu.ec/servicios/biblioteca/publicaciones/pdf/37.pdf.

Del Peso Navarro, E. (2000). *Ley de Protección de Datos. La nueva LORTAD.* Madrid: Editorial Díaz de Santos.

Denti, V. (1974). Cientificidad de la prueba y libre valoración del juez. En M. &. Sentís, *Estudios de Derecho probatorio* (págs. 272-277). Buenos Aires: Editorial Ejea.

Derecho a la autodeterminación-identidad, Sentencia T-552/1997 (Corte Constitucional Colombia 30 de 10 de 1997).

Diario EL COMERCIO. (20 de Julio de 2015). *Quien intercepte mensajes puede ser sancionado con 5 años de prisión*. Recuperado el 2 de Diciembre de 2015, de http://www.elcomercio.com/actualidad/interceptar-mensajes-presion-hackeo-ecuador.html.

Echandía, H. D. (2002). *Teoría general de la prueba judicial.* Bogotá: Editorial Temis.

Ecuador, Agencia Pública de Noticias del Ecuador y Suramérica (ANDES). (4 de 10 de 2012). *ANDES.* Obtenido de http://www.andes.info.ec/es/pol%C3%ADtica/7277.html.

Ecuador, Boletín Fiscalía General del Estado. (2015). *Los delitos informáticos van desde el fraude hasta el espionaje.* Quito: FGE.

Ecuador, Código Civil. (10 de 5 de 2005). *Código Civil ecuatoriano.* Obtenido de http://www.cortenacional.gob.ec/cnj/images/pdf/leyes/codigo_civil.pdf

Ecuador, Código de Procedimiento Civil. (2014). Código de Procedimiento Civil. Registro Oficial Suplemento 58 de 12-jul.-2005.

Ecuador, Código Orgánico Integral Penal. (24 de 4 de 2014). Código Orgánico Integral Penal de Ecuador. Quito, Pichincha, Ecuador: Ministerio de Justicia, Derechos Humanos y Cultos.

Ecuador, Constitución de la República. (2008). http://biblioteca.espe.edu.ec/.

Ecuador, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (10 de 4 de 2002). San Francisco de Quito, Pichincha, Ecuador: Congreso Nacional.

Ecuador, Ley del Sistema Nacional de Registro de Datos Públicos. (31 de marzo de 2010). Ley del Sistema Nacional de Registro de Datos Públicos. Ecuador: Suplemento del Registro Oficial 162, 31-III-2010.

Ecuador, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. (2009). Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Registro Oficial Suplemento 52 de 22-oct-2009.

Ecuador, Ley Orgánica de Telecomunicaciones. (18 de 2 de 2015). Obtenido de https://www.grupotvcable.com/wp-content/uploads/2015/07/ley_organica_de_telecomunicaciones.pdf.

Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública. (2012). Ley Orgánica de Transparencia y Acceso a la Información Pública. www.ecuadorestrategicoep.gob.ec/ley-transparencia.

Ecuador, Proyecto de Ley de Protección de Datos. (2015). *Asamblea Nacional.* Obtenido de http://documentacion.asambleanacional.gob.ec/

EcuRed. (2016). *Sistema de Telecomunicaciones*. Obtenido de http://www.ecured.cu/Sistema_de_telecomunicaciones.

EcuRed. (2016). *Sistema Informático*. Obtenido de http://www.ecured.cu/Sistema_inform%C3%A1tico.

España, Agencia española de Protección de Datos. (21 de 12 de 2014). *Derecho de Oposición.* Obtenido de https://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/oposicion-ides-idphp.php.

F. de Marcos, I. D. (2010). Protección de datos de carácter personal en México: problemática jurídica y estatus normativo actual. En S. Charvel Orozco, *Protección de datos personales. Compendio de lecturas y legislación* (pág. 78). Guadalupe: D.R. Tiro Corto Editores.

Fiscalia General del Estado del Ecuador. (13 de junio de 2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Recuperado el 2 de

Diciembre de 2015, de Los delitos informáticos van desde el fraude hasta el espionaje: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

García Falconí, J. (2013). ¿Qué es la Prueba? *Revista Judicial derechoecuador.com*, 1.

García Falconí, J. (2015). Derecho a la intimidad personal y familiar. *Revista Judicial derechoecuador.com*, 1.

Gilsanz Usunaga, J. (2010). *El Proceso Civil Estadounidense: La Tutela Judicial Cautelar.* Navarra: Editorial Arazandi.

Goldschmidt, J. (1936). *Teoría General del Proceso.* Barcelona: Editorial Ciencias Jurídicas.

Hacker, Cracker, Lammer, Newbie. (15 de Noviembre de 2009). Recuperado el 21 de Agosto de 2015, de http://planethacked.blogspot.com/2009/11/hacker-cracker-lammer-newbie.html.

Hunter Ampuero, I. (2008). No hay Buena Fe sin Interés: La Buena Fe Procesal y los Deberes de Veracidad, Completitud y Colaboración. *Revista de Derecho*, 151 y ss.

Informático, D. d. (s.f.). *Definición de Delito Informático*. Recuperado el 7 de Agosto de 2015, de http://www.delitosinformaticos.info/delitos_informaticos/definicion.html.

Iturralde, F. (2012). *Teoría de la prueba.* Loja: Universidad Técnica Particular de Loja.

IUSMX-UNAM. (20 de 10 de 2015). *Universidad Nacional Autónoma de México.* Obtenido de http://www.iusmx.com/index.php?option=com_wrapper&view=wrapper&Itemid=103.

Jauchen, E. (2002). *Tratado de la prueba en materia penal.* Buenos Aires: Rubinzal-Culzoni Editores.

Lerna, E. (2011). *Aspectos legales de la seguridad informática.* Barcelona: Universitat Oberta de Catalunya.

Llangarí, A. (2016). *Análisis de los Delitos Informáticos y de Telecomunicaciones en el Ecuador bajo las nuevas normas juridicas.* Quito: Universidad de las Fuerzas Armadas.

Meneses Pacheco, C. (2008). Fuentes de prueba y medios de prueba en el proceso civil. *Revista Ius Et Praxis*, 59.

Messia de la Cerda Ballesteros, J. A. (2003). *La Cesión o Comunicación de Datos de Carácter Personal.* Madrid: Editorial Thomson-Civitas.

Meza Ayala, M. J. (2008). Fraude en Roming, Robo de líneas Telefónicas. En *Fraude en Telecomunicaciones* (pág. 18. 20). Quito: Publiasesores.

Meza Ayala, M. J. (2008). *Fraudes en Telecomunicaciones.* Quito: Publiasesores.

Moreno Catena, V. (1985). Comentarios al artículo 603. En V. Cortés Domínguez, *Comentarios a la reforma de la Ley de Enjuiciamiento Civil* (págs. 538-539). Madrid: Eitorial Tecnos.

Muños Sabaté, L. (1967). *Técnica probatoria. Estudios sobre las dificultades de la prueba en el proceso.* Barcelona: Editorial Praxis.

Navas Alvear, M. (2008). El Recurso Constitucional de acceso a la información pública. *Revista Judicial derechoecuador.com*.

Observatorio de Derechos y Justicia. (2015). *Reporte Caso Crudo Ecuador. Reporte Mensual del mes de Enero.* Obtenido de http://www.derechosyjusticia.org/internacionales/reporte-caso-crudo-ecuador/.

Ochoa, K. (27 de 10 de 2015). Ecuador fue incluido en "lista negra" de piratería de Estados Unidos. *Metro.ecuador.com.ec*, pág. 1.

OMPI/JPI-JDA/GDL/04/2 EC. (24 de 2 de 2004). *Situación actual de Derecho de Autor en Ecuador.* Obtenido de http://www.wipo.int/edocs/mdocs/lac/es/.../ompi_jpi_jda_gdl_04_2_ec.doc.

Organización Mundial de la Propiedad Intelectual. (2010). *Qué es la Propiedad Intelectual?* Suiza: OMPI.

Pacto Internacional de Derechos Civiles y Políticos. (1966). *Herramientas para la Defensa y Promoción de los Derechos Humanos.* New York: Fundación Acción Pro Derechos Humanos.

Parra Quijano, J. (2006). *Manual de Derecho Probatorio.* Bogotá: Librería Ediciones del Profesional LTDA.

Perú, Autoridad Nacional de Protección de Datos Personales. (2014). *El Derecho Fundamental a la Protección de Datos Personales. Guía para el Ciudadano.* Lima: Ministerio de Justicia y Derechos Humanos.

Picó I Junoy, J. (1996). *El derecho a la prueba en el proceso civil.* Barcelona: José María Bosch Editor S.A.

Picó i Junoy, J. (2003). *El Principio de la Buena Fe Procesal.* Barcelona: Editorial J.M. Bosch Editor S.A.

Pierini & Lorences & Tornabene, A. &. (1999). *Habeas Data. Derecho a la Intimidad.* Buenos Aires: Editorial Universidad.

Pino, S. A. (s.f.). Tipos de Delitos Informáticos. En *Delitos Informáticos* (págs. 22-29).

Prieto-Castro, L. (1950). *Estudios y Comentarios para la Teoría y la Práctica PÑrocesal Civil.* Madrid: Editorial Reus.

Rebollo Delgado, L. (2005). *El Derecho Fundamental a la Intimidad.* Madrid: Editorial Dykinson.

Recasens Siches, L. (1978). *Tratado General de filosofía del Derecho.* México: Editorial Porrua.

Redacción de El País y Colprensa. (5 de 8 de 2013). *http://www.elpais.com.co*.

Roldán, C. S. (s.f.). *Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?* (Codejobs) Recuperado el 12 de Agosto de 2015, de https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.aB6Ne245.dpbs.

Ruiz Carrillo, A. (2005). *Manual Práctico de Protección de Datos.* Barcelona: Editorial Bosch.

Sarasola, I. (s.f.). *Que es cracker informatico*. Recuperado el 21 de Agosto de 2015, de http://cracker88.galeon.com/.

Scarselli, O. (1998). Lealtá e Probitá nel compimento degli Atti Processuali. *Rivista Trimestrale di Diritto e Procedura Civile*, 112 y ss.

Seguridad Informatica. (29 de Octubre de 2011). Recuperado el 15 de Agosto de 2015, de http://lyzzy-seguridadinformatica.blogspot.com/2011/10/unidad-3-control-de-acceso.html.

Solorio Pérez, O. J. (2009). *Habeas Data y supuesto de reserva de Información Pública.* México: Universidad de Colima.

Supertel. (2011). Clonación de teléfonos celulares, Call back o llamada revertida, By pass, Fraude Tercer País. *Delitos en telecomunicaciones 2011*, 4-6, 12-16.

Talavera Elguera, P. (2009). *La prueba en el nuevo proceso penal.* Lima: Academia de la Magistratura-AMAG.

Torres Espinoza, B. (2010). *Proyecto de Ley Orgánica de Protección de Datos Personales.* Cuenca: Universidad de Cuenca.

Torres Rodas, T. (2005). *El derecho a la intimidad y la garantía constitucional del hábeas data en el derecho tributario.* Quito: Universidad Andina Simón Bolívar.

Twining, W. (2006). What is the law of evidence? En W. Twining, *Rethinking Evidence. Exploratory Essays* (pág. 193). Cambridge: Cambridge University Press.

UNESCO. (10 de 12 de 2015). *Observatorio Mundial de Lucha contra la Piratería.* Obtenido de http://portal.unesco.org/culture/es/ev.php-URL_ID=39397&URL_DO=DO_TOPIC&URL_SECTION=201.html.

Universidad Autónoma Ciudad Juárez. (2012). *Conceptos básicos de Protección de Datos Personales.* México: Unidad de Transparencia.

Wikepedia. (s.f.). *Hacker (seguridad informática)*. (Wikepedia) Recuperado el 20 de Agosto de 2015, de https://es.wikipedia.org/wiki/Hacker_(seguridad_inform%C3%A1tica)#Pandillas_criminales_organizadas.

YADERSY. (31 de Julio de 2014). *Fases o Etapas de un ataque informático*. Recuperado el 28 de Agosto de 2015, de https://yadersy.wordpress.com/2014/07/31/fases-o-etapas-de-un-ataque-informatico/.