PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE JURISPUDENCIA

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

PROTECCIÓN LEGAL DE DATOS PERSONALES Y A LA RESERVA DE INFORMACIÓN PERSONAL, Y SU TRANSFERENCIA SIN CONSENTIMIENTO DE SU TITULAR

DIRECTOR: DR. SANTIAGO ACURIO DEL PINO

ANDREA PAOLA MERIZALDE REINOSO

QUITO 30 DE JUNIO DE 2014

Quito, 26 de junio de 2014

Señor Doctor
Santiago Guarderas
DECANO DE LA FACULTAD DE JURISPRUDENCIA
PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
Ciudad.-

De mi consideración:

Asunto: Informe de tesis Andrea Paola Merizalde Reinoso

1) **Resumen del contenido de la tesis.-**

La tesis "Protección legal de datos personales y la reserva de información personal, y su transferencia sin consentimiento del titular", constituye un análisis de las principales normas aplicables al manejo de datos tanto públicos como personales sensibles. El primer capítulo analiza los conceptos de dato e información y los principios que les aplican, en especial los relacionados con la obtención y protección de datos personales sensibles. En el segundo capítulo se analiza e derecho fundamental a la intimidad y se lo analiza en distintos cuerpos legales que contiene normas al respecto, además de referencias de derecho comparado sobre el tema. El capítulo 3, contiene referencias a situaciones relacionadas con la protección de datos públicos y personales. En el capítulo 4 se incluyen recomendaciones y no precisamente una propuesta. Finalmente se incluyen conclusiones y recomendaciones.

2) **Aspectos relevantes y positivos.-**

Debo destacar como aspectos positivos de la tesis los siguientes:

2.1. El tema es de mucha actualidad y además se evidencia que existe un vacío normativo (legal) que contenga reglas de protección de los datos personales.

2.2. Se ha hecho un destacable esfuerzo investigativo, que incluye el análisis de varias normas dispersas en el ordenamiento jurídico ecuatoriano.

3) Observaciones.-

Con relación a la Tesis objeto de este informe, tengo las siguientes observaciones:

3.1. El capítulo 2 debió ser el primero, pues se debería comenzar analizando el derecho fundamental a la intimidad como centro del análisis, para desembocar en el tema de la protección de los datos personales.

3.2. Se abordan y se analizan conjuntamente dos temas que merecen tratamientos claramente distintos: los datos públicos y los datos personales sensibles. El análisis debió concentrarse exclusivamente en la protección de datos personales.

3.3. He detectado algunas imprecisiones en citas como por ejemplo en las pags. 122, 136 y algunas conceptuales en las pags. 140, 141.

4) Calificación.-

Una vez analizada la Tesis presentada para informe y en base los aspectos relevantes y positivos y las observaciones que constan en este informe, otorgo la calificación de 8/10.

Atentamente,

Dr. Juan Francisco Palacios I.

B|B|A

Barzallo & Barzallo
ABOGADOS

Quito, 23 de junio de 2014

Dra.
Ivette Haboud
Secretaria de Facultad
Facultad de Jurisprudencia
Pontifica Universidad Católica del Ecuador.
Ciudad.

De mi consideración

En atención a su comunicación por la que se me solicita la revisión y calificación del trabajo previo a la disertación previa a la obtención del título de abogada de la señorita ANDREA PAOLA MERIZALDE REINOSO, cuyo título del trabajo es "**PROTECCIÓN LEGAL DE DATOS PERSONALES Y A LA RESERVA DE INFORMACIÓN PERSONAL, Y SU TRANSFERENCIA SIN CONSENTIMIENTO DE SU TITULAR**".

Respecto de los aspectos cualitativos del trabajo señalo que:

a). La temática de la investigación analiza aspectos que no han sido tomados en cuenta de la legislación vigente, por lo que parte adecuadamente del campo teórico.

El análisis legislativo abarca las normas relacionadas con la temática.

b). El trabajo cumple con las reglas metodológicas.

c). El trabajo no contiene suficiente investigación bibliográfica que respalde la investigación con diversidad de fuentes doctrinarias.

Por lo expuesto consigno la siguiente calificación:

8/10

Atentamente,

Dr. José Luis Barzallo

DEDICATORIA Y AGRADECIMIENTO

A mis padres

ABSTRACT

El presente trabajo de investigación tiene como propósito, demostrar la necesidad de la creación e instauración en el Ecuador, de una norma de carácter orgánico que regule el tratamiento de Datos Personales Sensibles, en todas sus etapas, desde la recolección de los mismos, hasta su uso posterior y mantenimiento.
Es importante también, que dentro de la norma sugerida se regule el consentimiento del titular de la información personal, como mecanismo primario de legitimidad en el uso de los datos personales sensibles por parte de terceros; mecanismo que requiere de una practicidad simple y accesible a todos los titulares, de tal manera que dispongan de información oportuna y veraz a cerca de la utilización de dicha información.

El análisis del Derecho Fundamental a la Intimidad y el Derecho Fundamental a la Protección de Datos Personales, fue fundamental en el desarrollo de la presente disertación, ya que pueden verse lesionados con el uso irrestricto de la información personal, y deben ser objeto de reparación según la Constitución y la ley.

La metodología de investigación empleada fue en su mayoría bibliográfica, en cuanto a doctrina de derecho, principales leyes vigentes pertinentes al tema de protección de datos personales, sentencias de la Unión Europea y españolas; y de campo en las visitas a las principales instituciones públicas de control.

El principal aporte del trabajo de investigación, es evidenciar el desconocimiento del tema de la Protección Jurídica de Datos Personales en el Ecuador, tanto de los ciudadanos como de muchos funcionarios públicos que tienen acceso a esta información, y correlativamente la obligación mantener en reserva estos datos por su naturaleza sensible para el titular de la misma, por lo que concluyo en la necesidad de la norma regule y permita que los procesos de tratamiento de datos personales sea legal, reservado y adecuado**.**

ÍNDICE

INTRODUCCIÓN

Vivimos en una época de gran desarrollo tecnológico, el tráfico de información se realiza rápidamente y en grandes cantidades gracias a la utilización de herramientas informáticas, y muchas veces la información transferida es accesible al público sin mayor restricción. Sin embargo, dentro de esta información pueden estar presentes datos personales, que merecen una mayor protección, en el sentido de que no deben ser accesibles al público ya que, el conocimiento de estos datos causaría un desmedro en la intimidad del titular o incluso materializarse en un perjuicio material.

Los datos personales, en muchos casos sensibles, se encuentran almacenados en distintas bases de datos, bajo la responsabilidad de instituciones públicas y privadas; y se utilizan o tratan con diferentes objetivos, como registro, censos o estadísticas, en la mayoría de los casos en el sector público; o con fines comerciales, de marketing o de crédito en el sector privado, no obstante, en nuestro medio estas instituciones tratantes de datos personales, no siempre guardan reserva de este tipo de información a pesar de que puede ser revelada o ser utilizada inapropiadamente.

Por esta fenomenología, el presente trabajo de investigación, pretende demostrar la necesidad de la incorporación de una ley orgánica, en nuestro ordenamiento jurídico, que regule la protección jurídica de los datos personales, ya que frecuentemente son entregados a instituciones públicas o privadas, a cambio de un servicio o sin el consentimiento informado de su titular.

Esta problemática trasciende cuando en estos intercambios o tratamiento de información, el titular o un tercero por desconocimiento entrega, o son obtenidos sin su consentimiento, datos personales sensibles que corresponden a la religión, filiación, política, ideología, vida sexual, ascendencia étnica o estado de salud, y que su mal uso puede ocasionar un daño legítimo en la privacidad e intimidad del titular de la información.

La hipótesis del presente trabajo de investigación se basa en que en el Ecuador no existe una adecuada protección jurídica de los datos personales que son tratados o almacenados en diferentes instituciones, por lo que es necesario que el derecho se adapte a estas innovaciones y regule de una mejor manera los procesos que permiten tratamiento de información, y más aún, que estos procesos coadyuven a

precautelar derechos como la intimidad o el buen nombre de los titulares de esta información personal.

El consentimiento del titular de la información personal, al momento de entregar sus datos personales, es el mecanismo práctico fundamental, que permite hacerle conocer al individuo sobre el uso que se le dará a su información, por cuanto tiempo, con que finalidad y de qué forma; mecanismo que esta instaurado en países como España, y que permite proteger la información, ya que de no cumplirse con las condiciones o parámetros con los cuales se recolectaron los datos, el titular puede exigir la reserva o anulación de esta información sensible por una vía jurídica.

No obstante, la entrega de este consentimiento no está regulada correctamente con ningún cuerpo legal en el Ecuador, por lo que es notoria la falta de protección jurídica de los datos personales de los ciudadanos en todos los momentos del tratamiento de su información.

Los objetivos trazados en la investigación fueron la verificación de la problemática en nuestro medio, así como comprobar la necesidad de la implantación de una regulación específica que revea todas las etapas del proceso de tratamiento de datos, desde la recolección hasta el almacenamiento de los mismos. Estos objetivos, fueron verificados a los largo de la investigación, pese a que no existió mayor conocimiento del tema en las instituciones de control relacionadas con el tema, lo que contribuyó a concluir la necesidad de la regulación y de que se brinde mayor conocimiento en el tema tanto a los responsables de la custodia de la información, y a los ciudadanos titulares de los datos.

Por esto, en los primeros capítulos de la disertación, se realiza un análisis doctrinal y legal del derecho fundamental de protección de datos personales, igualmente se hace referencia a legislaciones extranjeras que si regulan los procesos de tratamiento, y jurisprudencias españolas relevantes para entender la importancia de la creación de esta ley en el Ecuador.

De igual forma, en los dos capítulos finales, se realiza un análisis de la realidad nacional, en cuanto a la regulación existe y como esta regulación es vaga y no permite una correcta protección jurídica de la información personal sensible, así como el desconocimiento tanto de las instituciones públicas como de los ciudadanos en cuanto

a cómo se deben tratar los datos personales sensibles, los derechos que se pueden ejercer en este propósito y las medidas técnicas y administrativas que se deben tomar.

Los métodos utilizados para el desarrollo del presente trabajo de disertación fueron el método bibliográfico en su mayoría y de campo, ya que se visitaron instituciones públicas de control como la Superintendencia de la Información y Comunicación o la Dirección Nacional del Sistema de Registro de Datos Públicos, donde se constató el problema de la falta de cautela jurídica en la transferencia y tratamiento de los datos personales sensibles.

Después de realizar la investigación, concluyo que es necesaria la existencia de esta regulación especializada que debe estar contenida en una ley orgánica, que además de contener los principios del derecho fundamental a la protección de datos personales, de lugar a la creación de un órgano de control en el tema que esté a cargo de los procesos de recolección, tratamiento, almacenamiento y acceso de los datos personales sensibles, implementando medidas técnicas, jurídicas y de organización.

CAPÍTULO I

1. SITUACIÓN JURÍDICA DE LA INFORMACIÓN, BASES DE DATOS Y DATOS

Para el desarrollo del presente trabajo de investigación es necesario el análisis de ciertos conceptos jurídicos y derechos fundamentales que serán involucrados posteriormente, por ello estos conceptos se establecen en este primer capítulo.

1.1 LA INFORMACIÓN, BASES DE DATOS Y DATOS*:*

La información, es un concepto muy amplio y genérico, utilizado en todos los ámbitos de estudio, por lo que es necesario concretar lo que entendemos por ella para fines de esta investigación.

Primero, Etimológicamente, la palabra información tiene su origen en las raíces latinas "*in"* y "*forma"*, que significan, "*instruir hacia adentro*", es decir interiorizar una figura o forma que apreciamos de la realidad.

Philippe Breton en su obra *"Historia y crítica de la informática*", señala que:

> *La palabra "información" tiene un origen relacionado con la idea de forma. Informatio quiere decir en latín "acción de formar", "dar forma", y procede de forma, que sirve para designar la forma exterior de un objeto. Informar, en latín, es también educar, formar. La palabra tiene varios sentidos, pero todos se dirigen a la idea de construcción, elaboración*.[1]

Según el autor Idalberto Chiavenato:

> *La información consiste en un conjunto de datos que poseen un significado, de modo tal que reducen la incertidumbre y aumentan el conocimiento de quien se acerca a contemplarlos. Estos datos se encuentran disponibles para su uso inmediato y sirven para clarificar incertidumbres sobre determinados temas*.[2]

De estas definiciones de información infiero que es un conjunto de datos con una significación específica, que permite tener certeza acerca de un tópico, un objeto o una persona, que se encuentra en nuestro entorno.

---

[1] BRETTON, Philippe. *Historia y Critica de la Informática,* Editorial Cátedra, Madrid, Año 1989, p. 22.
[2] CHIAVENATO, Idalberto, *Concepto de Información*, http://definicion.de/informacion/#ixzz2bEdZfpWy, Acceso: seis de agosto de 2013 a las 18h37.

La información en nuestros días cobra una importancia relevante por cuanto nos permite tener conocimiento de diversos temas, al igual que difundir ese conocimiento y explotar las posibilidades que nos brinda este mundo tecnológico. Por lo que es bastante entendible la importancia de tener un control en el manejo de esta información porque al igual que es una herramienta de desarrollo puede también ocasionar ciertos perjuicios morales o económicos a personas o grupos de personas, como la discriminación, daño moral, perjuicios laborales, competencia desleal, entre muchos otros. Sin embargo para motivos de esta investigación me centrare en analizar la protección jurídica que se le debe dar a la información de carácter personal.

1.1.1 DERECHO A LA INFORMACIÓN

Esta definición de información se relaciona con el área jurídica, propia de nuestro estudio, de la siguiente forma:

En primer lugar debemos entender que en actualmente vivimos una revolución tecnológica donde, el conocimiento, la información y las comunicaciones, tienen una importancia preponderante en las relaciones humanas, tanto privadas como públicas, por lo que se vuelve una necesidad que el derecho regule estos los procesos dinámicos de creación, acceso y transferencia de información.

Según RODOLFO DANIEL UICICH, en su obra Los Bancos de Datos y el Derecho a la Intimidad, "*El derecho a la información o acceso a la información, parece que abarca la gama de derechos y libertades que se refieren a la expresión*",[3] ya que como sabemos, es característico del ser humano desde siempre, ser soberanos en nuestros pensamientos, ideas y sentimientos, por lo que somos dueños de nuestra libertad de pensar, sin embargo la forma de transmitir esos pensamientos e incluso información de algún hecho presenciado, aprendido o de conocimiento empírico o situacional, es una dificultad ya que puede afectar los derechos e intereses de los demás.

Si bien, históricamente existen casos como los autoritarismos, en los que se restringe el acceso del hombre a la información, es claro que la tendencia que ha predominado, es la libertad de información; la razón clara es el desarrollo de medios de comunicación y electrónicos, que aportan a la sociedad en la que nos

[3] UICICH, Rodolfo Daniel, *Los Bancos de Datos y el Derecho a la Intimidad*, editorial AD-HOC, Buenos Aires, Argentina, primera edición, julio 1999, p.19.

desenvolvemos, donde el acceso inmediato y masivo a la información se ha convertido en una herramienta poderosa e indispensable. Por estos motivos acceso a la información se ha convertido en un tema necesario de regular normativamente.

Según el Doctor José C. García Falconí, Ex Ministro Juez de la Ex Corte Superior de Justica de Quito, en su "*Manual de Practica Procesal Constitucional*", "*La información, constituye en todas sus modalidades, núcleo fundamental del Estado de Derecho, de convivencia ciudadana y de desarrollo democrático de las sociedades*".[4]

El acceso, transferencia y transparencia de la información, permite que el ciudadano cree opinión pública, que exista participación ciudadana, ejercicio de derechos como los políticos, desarrollo social entre otras acciones indispensables para el progreso social y para el buen desenvolvimiento del Estado.

El derecho a la información es inherente al ser humano, sin embargo gracias al desarrollo de la capacidad tecnológica y lo barato que resultan las comunicaciones, se forja un poder social que debe ser regulado, además de ser equitativo y transparente.

Según, Daniel Uicich:

> *En la conferencia reunida en Paris en la Vigésima Conferencia General de la UNESCO, en 1979, se promulgo un nuevo orden mundial de la información y comunicación, mas junto y equilibrado, destacando que el derecho a comunicar es un proceso bidireccional cuyas participantes mantendrán un dialogo democrático y equilibrado, con posibilidades de acceso y participación*.[5]

Como podemos ver en la citas anterior, en las convenciones, normativa y resoluciones de carácter internacional, el derecho a la información es acogido como un derecho fundamental de todas las personas que debe ser garantizado por los diferentes estados y con ciertas características como que debe ser regulado en la medida que no limite derechos de terceros, y que va de la mano con otros derechos como el de acceso, opinión, expresión, comunicación y además la capacidad tecnológica y los medios existentes para su transferencia.

El derecho a la información, dadas las circunstancias actuales, consiste en dar y recibir información particular u oficial, y puede relacionarse con la libertad de expresión

[4] GARCIA FALCONÍ, José C. *Manual de Practica Procesal Constitucional*, editorial Librería Jurídica Cevallos, Quito, Ecuador, Año 2000, p. 30.
[5] Op. Cit. 3. p. 23.

o de opinión, por lo que para definir el derecho a la información, enuncio las libertades fundamentales que lo comprenden:

- Libertad de investigar
- Libertad de difundir
- Libertad de recibir informaciones y opiniones
- Libertad de acceder a la información publica
- Derecho a no recibir información distorsionada
- Derecho a no ser objeto de información falsa o abusiva

En las redacciones normativas en las que consta este derecho, estas libertades no resultan absolutas por lo que se reconoce el sentido relativo de las mismas.

El Doctor José C. García Falconí menciona que el Derecho a la Información abarca lo siguiente:

- *El Derecho individual de quien emite o difunde sus ideas*
- *El Derecho Colectivo de quienes tienen derecho a recibir la información*
- *El Derecho vinculado con la actividad económica de la prensa*

Es decir, este derecho está constituido por un doble conjunto de situaciones: significa la posibilidad de expresar ideas sobre cualquier materia y también el poder comunicarlas; así como comprende la libertad de información y de investigación[6]

Por todo lo dicho, el derecho a informar y ser informado de una forma correcta, prevé libertades que contribuyen a las relaciones sociales a grande escala y permite el ejercicio de muchos otros derechos, es un pilar de la democracia y del desarrollo estatal, en este sentido se debe velar por la información que se difunde o que por otro lado debe ser confidencial.

El derecho a la información, en cuanto a no recibir información distorsionada o ser objeto de información falsa o abusiva, anteriormente era muy difícil de controlar, quizás por ello era considerado como un "*lujo para países ricos*", al referirse a las leyes de Protección de Datos, sin embargo en nuestros días es una "*necesidad de toda comunidad organizada*"[7].

[6] Op. Cit. 4. p. 107.
[7] Op. Cit. 3. p. 25.

Entonces, el derecho a la información puede ser exigible en cuanto a su acceso, como también en cuanto a procurar, como sujeto pasivo de la información, que no se distorsione la información o que ésta sea revelada, y así, no afectar la intimidad, el buen nombre, orden público, ni seguridad del estado.

Por esto, el tema de la Información, su acceso, difusión y transferencia están reconocidos como un Derecho Fundamental en nuestra Constitución, en su sección tercera, cuyo contenido pertinente para el presente trabajo cito a continuación:

> *Artículo 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:*
>
> *2. El acceso universal a las tecnologías de información y comunicación.*
>
> *Artículo. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:*
>
> 1. *Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.*
>
> 2. *2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.*[8]

La constitución vigente, prevé como derecho fundamental, todas las formas de ejercicio del derecho a la información, igualmente al acceso a las tecnologías que son generalmente la herramienta de transferencia y difusión de la información, e incluso los espectros radioeléctricos y la libertad de comunicación en general.

Es importante anotar que también se nos garantiza la calidad de la información y la participación social en el intercambio de la misma; y, el Estado se compromete, por decirlo así, a brindar libre acceso a la información pública y a tutelar el ejercicio de este derecho, que se debe entender dentro de sus límites de ejercicio y derechos de terceros, objeto de esta tesis.

Igualmente, según la carta magna, todos tenemos la garantía de que exista reserva en el secreto profesional y cláusula de conciencia a toda persona, ya que esta información, por su naturaleza, de ser revelada puede lesionar derechos. Y, el Estado

[8] REGISTRO OFICIAL 449 de 20 de octubre de 2008, *Constitución de la República del Ecuador*, Art. 16 y Art 18.

como ente tutelar, se ve en la obligación jurídica de precautelar esta información, como también precautelar los datos de carácter personal de sus administrados como lo analizaremos posteriormente.

El Derecho a la Información se recoge igualmente en algunos cuerpos legales como por ejemplo:

Ley Orgánica de Comunicación:

Esta ley pretende cumplir tanto con los derechos fundamentales reconocidos y garantizados en la Constitución, como el derecho a la información en especial, ya que es un derecho inherente a la persona humana por su naturaleza racional, y es deber del Estado velar el ejercicio de estos derechos.

Nuestra convivencia y desarrollo corresponde a una interacción social, por lo que es necesaria la expresión de nuestro ser, así como el acceso a la información expresada, sea esta histórica o empírica.

La ley de Orgánica de Comunicación establece:

> *Artículo. 29.- Libertad de información.- Todas las personas tienen derecho a recibir, buscar, producir y difundir información por cualquier medio o canal y a seleccionar libremente los medios o canales por los que acceden a información y contenidos de cualquier tipo.*
> *Esta libertad solo puede limitarse fundadamente mediante el establecimiento previo y explícito de causas contempladas en la ley, la Constitución o un instrumento internacional de derechos humanos, y solo en la medida que esto sea indispensable para el ejercicio de otros derechos fundamentales o el mantenimiento del orden constituido.*
>
> *Toda conducta que constituya una restricción ilegal a la libertad de información, será sancionada administrativamente de la misma manera que esta Ley lo hace en los casos de censura previa por autoridades públicas y en los medios de comunicación, sin perjuicio de las otras acciones legales a las que haya lugar.*[9]

Transmitir información es un quehacer diario dentro de nuestras relaciones personales, por lo que es necesario proteger la libertad de producir, transferir y recibir información, sin esto seriamos aislados del medio social y no podríamos interactuar con los demás. Esta es la justificación de la existencia de este derecho, además de

[9] REGISTRO OFICIAL, Suplemento 22 de 25 de junio de 2013, *Ley Orgánica de Comunicación* Art. 29.

motivos históricos que nos han dejado una gran lección, como autoritarismos o desmanes por parte de grupos privilegiados poseedores exclusivos de la información.

Por ello el papel importante del legislador cuando elabora las normas regulatorias de derechos fundamentales, ya que siempre debe obedecer al objetivo de precautelar el interés social y bien común.

En conclusión, al igual que otros derechos fundamentales, debe existir la garantía del ejercicio del derecho a la información, regularlo con sus excepciones en nombre del bien común y sancionar a los que no permitan su ejercicio, sea un particular u órgano estatal.

Ley del Sistema Nacional de Registro de Datos Públicos:

Esta ley también ampara al Derecho Fundamental a la Información desde la perspectiva de su acceso, ya que, acceder a la información pública y privada, o la tecnología que la posee, es una garantía de todos los ciudadanos.

Es necesario que el individuo esté informado de lo que sucede en la actividad pública y social. Éste hecho ciertamente coadyuva a que el ciudadano esté al tanto de las políticas públicas y con suerte conozca acerca de los medios jurídicos de los que dispone para hacer efectivos sus derechos.

En nuestro caso particular, es necesario que el ciudadano conozca los procedimientos de acceso a la información registral establecidos en la ley, hecho bastante utópico, pero que se podría poner en marcha con miras a que la protección de datos personales en el Ecuador sea más efectiva.

El espíritu de esta ley también viene dado en el sentido de que el acceso a la información registral sea libre y que exista la protección jurídica de los datos de carácter personal, existentes en los registros públicos

Esto por varias razones. Primero, porque con esta garantía, se abre la esfera de protección de otros derechos fundamentales como la identidad, intimidad, buen nombre, entre otros; y además porque permite que el ciudadano tenga conocimiento de los datos personales que son conocidos y que están siendo procesados por el Estado u otras instituciones.

En segundo lugar, porque con esta protección jurídica de los datos personales, se busca que el ciudadano tenga la libertad de decidir y disponer sobre su información personal; y, en tercer lugar, porque permite tener esta garantía, reflejada en una norma disponiendo que esos datos sean manejados con el debido cuidado, e impidiendo que se divulguen a terceras personas.

Gracias a esto el titular de los datos personales tendrá la seguridad de que su información es debidamente tratada y que no se le causará perjuicios de ningún tipo.

De igual forma, esta ley trata el tema del derecho a la información en su artículo cuarto, donde se establece la responsabilidad de la integridad de la información; esto quiere decir que básicamente las instituciones públicas o privadas, o personas naturales, quienes tengan a cargo información de carácter personal, deben velar por su integridad, protección y control.

El derecho a la información procura su calidad en los procedimientos de manejo y acceso; demandando mayor eficiencia y transparencia en el desempeño de estos procesos, por parte de quienes manejan la información. Solo de esta manera el Estado puede cumplir con la garantía consagrada en la Constitución y la ley.

La ley del Sistema Nacional de Registro de Datos Públicos, pretende regular un procedimiento específico para el ejercicio del derecho de acceso a la información existente en los registros públicos, facultad propia del derecho a la información. Éste procedimiento permite que los ciudadanos conozcan y dispongan de los datos que se encuentren en el registro público de las instituciones estatales.

En este caso, nos estamos refiriendo a datos públicos, que indudablemente forman parte de la información que el ciudadano tiene derecho a acceder si es su voluntad o necesidad.

El derecho a acceder a información registral, es una forma de ejercitar el derecho a la información ciertamente, sin embargo, considero que este ejercicio cabe siempre que no se afecte derechos de terceros, por ello este acceso es permitido en datos cuya naturaleza es publica, es decir datos identificación o registrales. No obstante, la ley ha procurado una ficha como herramienta de consulta de los datos personales reservados que están incorporados en registros.

La información personal reservada, es accesible solo por el interesado, ya que se entiende que solo su titular, tiene interés sobre ella. Es claro que el Estado realiza procesos y maneja datos de sus administrados, pero se entiende que es por fines de orden público, por lo que se presupone que no se vulnerará derechos con esto, y que se brinda un correcto manejo de los datos sean estos públicos o no.

Ley Orgánica de Defensa al Consumidor:

La Ley de defensa al consumidor también tiene presente al Derecho a la Información, en el sentido de que los consumidores, tienen derecho a estar informados acerca de los productos o servicios que reciben; en cuanto la calidad de ellos, elaboración, utilidad, riesgos etc.,

Esto gracias a que es deber del Estado garantizar el derecho a disponer de bienes y servicios públicos y privados, de óptima calidad; a elegirlos con libertad, así como a recibir información adecuada y veraz sobre su contenido y características; y además al Estado le corresponde proteger los derechos de los consumidores sancionando la información fraudulenta, la publicidad engañosa, la adulteración de los productos, la alteración de pesos y medidas, y el incumplimiento de las normas de calidad.[10]

Conclusión del Análisis al Derecho a la Información:

Las condiciones actuales de la tecnología nos permiten el manejo de grandes cantidades de información, entre ellas datos personales, que a su vez se agrupan en bases de datos, que deben ser reconocidos, rectificados o incluso excluidos de estas bases. Lo que evidencia lo relativo del derecho a la información y la afectación de otros derechos fundamentales como el derecho a la intimidad o buen nombre, que podría suceder si no se protegen estos datos de manipulaciones o de intereses de terceros.

Es por esto que se necesita distinguir que las personas tenemos derecho a la información autentica, pero del mismo modo tenemos derecho a la intimidad y a que nuestra información personal sea privada, no manipulada ni de conocimiento público,

[10] Cfr. REGISTRO OFICIAL, Suplemento 116, Fecha de publicación 10 de julio del 2000, Ultima reforma 13 de octubre 2011, *Ley Orgánica de Defensa al Consumidor*.

por lo que es claro que el derecho a la información se encuentra limitado a nuestro derecho fundamental a la intimidad.

El Derecho a la Información, también tiene límites, de los cuales el Doctor José C. García Falconí, dice:

> *La Información es un derecho, no puede apartarse de los hechos, así no se trata de una libertad absoluta y arbitraria, sino reglada y determinada por hechos reales e interpretados en forma imparcial; de este modo el derecho a la información no es ilimitado ni arbitrario, o sea que los medios de comunicación deben ceñirse a los hechos reales y su interpretación no debe salirse de la verdad contenida en los mismos que pueden ser verificados pues el público tiene derecho a recibir información veraz e imparcial, o sea que las informaciones no deben basarse en hechos falsos sino que debe ser una información veraz.*[11]

Se puede inferir entonces que uno de los límites a este derecho es la veracidad que debe contenerlo, ya que no transferible a los ciudadanos aquella información que no sea verdadera. Es un derecho colectivo el derecho a ser informado de manera oportuna y sobretodo veraz, no manipulada ni arreglada.

Otro de los límites de este derecho es que no debe sobrepasar la honra o buen nombre de una persona natural o jurídica, derechos también garantizados en la Constitución y la Ley. Ciertamente la información se puede utilizar como una herramienta para vulnerar derechos o satisfacer intereses, prácticas que deben ser evitadas.

Los derechos parten de una garantía de dignidad humana que debe ser respetada, tanto para el que informa como para quien recibe la información y sobre todo para el que es titular o parte de la misma. Los derechos fundamentales a la Información y a la Protección de Datos Personales deben coexistir, por ello incluso se prevén mecanismos como la rectificación, habeas data, fe de erratas, entre otras para guardar el honor de las personas en el caso de un exceso, equivocación o difusión de información falsa; mecanismos que además deben ser gratuitos, inmediatos y obligatorios.

La conclusión entonces es que tanto el derecho a la información como a la intimidad y a la protección de información personal, con sus respectivos limites, van de la mano y la única función de los mismo es el bienestar y desarrollo de los ciudadanos.

[11] Op. Cit. 4. p 30.

1.1.2 DATOS

La información que se maneja está compuesta, en su mayoría de datos, y "*el conjunto de datos va configurando el perfil de una persona, que puede brindar información que el titular no desea brindar*"[12]

Por este motivo la relevancia de hacer énfasis en el análisis de los datos personales, que son los que se deben proteger para que no existan abusos ni vulneración de derechos.

Como lo mencioné, la noción sobre la que se basa el concepto de información es el dato o conjunto de datos que tienen un significado. Por ello definiremos "dato" como aquel hecho o valor a partir del cual se puede inferir una conclusión o, como se define por la Real Academia de la Lengua Española, será el antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho.

Según RODOLFO DANIEL UICICH, "*el dato es tan solo el impulso electrónico que queda grabado en un programa o sistema que puede ser recuperado, es decir vuelto a la pantalla siguiendo determinado procedimiento*"[13]

Según el autor, José C. García Falconí, "*el dato hace referencia a cualquier conjunto de letras, números, o signos que tiene un significado*"[14]

Con estas definiciones podemos comprender que el dato es la mínima expresión que forma parte de una información, y que en muchos casos puede ser personal o incluso sensible, como el objeto de investigación del presente trabajo, por ello la importancia de su análisis, ya que con estos datos se pude lesionar derechos fundamentales.

1.1.3 BASES DE DATOS

Generalmente los datos de los ciudadanos son accesibles por Estado hasta su muerte, muchas veces por motivos identificación, registro, censos, e incluso para la

[12] Op. Cit. 3. p. 46.
[13] Id. 12.
[14] Op. Cit. 4. p. 258.

toma de decisiones acerca de políticas públicas económicas y sociales. Por ello se manejan expedientes o formularios entre otros documentos, donde se encuentra información personal de los ciudadanos o extranjeros, información que ciertamente puede afectar su vida jurídica y social.

Esta información ha existido desde siempre, sólo que en papel, sin embargo en la actualidad las herramientas tecnológicas e informáticas, mejoran las posibilidades de sistematizar esta información, que es recogida en archivos informáticos llamados "bases de datos", que sustituyen a los antiguos ficheros de papel.

Respecto a esto José C. Garcia Falconi, define: "*Un Banco de Datos, es un conjunto de datos estructurados organizados y reagrupados por conjuntos homogéneos, mientras que por información se entiende el resumen de datos (DATA)"*[15], este autor también dice que la doctrina entiende a las bases de datos como:

- *Es un conjunto de archivos interrelacionados, que es creado y manejado por un sistema de gestión o de administrar la base de datos*

- *Es Cualquier conjunto de datos almacenados electrónicamente o de manera manual*[16]

Podemos concluir entonces que las bases de datos son un archivo de datos que se encuentran almacenados ya sea un archivo físico o en lo que es objeto de esta tesis, una computadora o en la nube de información, que se puede acceder por vía telemática. En estas últimas bases de datos, almacenadas en medios electrónicos, se desprende el dato electrónico, mediante un *"proceso automatizado de búsqueda*" [17]

Existen bases de datos de diversos tópicos como de antecedentes penales, incumplimientos comerciales, demandas, de información patrimonial, entre otras, pero en conclusión son un depósito de información que contiene datos sobre individuos que pueden ser sensibles, por ello la importancia del fin para el cual se utilice la información, su modo de recolección y la veracidad de la base de datos.

José C García Falconí, en su obra "*Manual de Practica Procesal Constitucional*" nos dice que el legislador utiliza el termino *base de datos* con el objetivo de describir los registros públicos en general, sin realizar mayor especificación.

[15] Ibid. 14. p. 177.
[16] Ibid. 15. p. 255.
[17] Op. cit. 3. p.46.

Otros autores como Carlos Alberto Villalba en su obra *"La Protección Intelectual de los Bancos de Datos sobre sus propios Datos"*[18] explica, que las bases de datos implican organización, y un sistema de manejo donde el usuario pueda tener acceso y administración de estos datos, por ello la necesidad de implantar un software para estos fines, incluso con el objetivo de transparentar el acceso y manejo de la información. Por ello creo la creación en nuestro País de la Ley del Sistema Nacional de Registro Datos Públicos con su ente principal la Dirección Nacional del Sistema de Datos Públicos, órgano público que realiza esta regulación y esta organización de los datos registrados y registrables.

Las bases de datos tienen las siguientes características:

1. "*El tratamiento de la información*
2. *El medio electrónico de este tratamiento (hardware y software).*
3. *La conjunción de esos datos con una finalidad o motivo propio*"[19]

Los Bancos o Bases de datos pueden ser públicos o privados, los privados son aquellos que están contenidos en archivos o almacenamientos privados, no están destinados al uso público. En nuestra legislación solo se hace referencia a los bancos de datos de uso público o registrable, por ello la peligrosidad de que existan bases de datos particulares que contengan datos personales de terceros y que sean utilizados con fines ilícitos.

En nuestro país, las bases de datos y su utilización se encuentran recogidas en leyes como por ejemplo:

Ley del Sistema Nacional de Registro de Datos Públicos.

Este cuerpo legal bastante pertinente es este tema, por cuanto precisamente su objeto de regulación con la registrabilidad de los datos de acceso público y que el Estado tiene de sus administrados, por esto es claro que hace referencia a las bases de datos.

---

[18] VILLALBA, Carlos Alberto, *La Protección Intelectual de los Bancos de Datos sobre sus propios Datos,* http://www.infojus.gov.ar/doctrina/daca880172-villalba-propiedad_intelectual_bancos_datos.htm;jsessionid=13agclmrfsa377s9ij4g5ew0q?0&bsrc=ci*, acceso: 24 de julio de 2013, a las 16h00.*

[19] Op. Cit. 3. p. 46.

Entonces, se justifica la existencia de la ley por la necesidad de regulación del manejo de la información, contenida muchas veces en las bases de datos, que son manejadas por las instituciones públicas, y donde pueden también contenerse datos personales sujetos de protección jurídica.

El Estado, tiene por obligación poner en conocimiento de los ciudadanos la existencia y contenido de registros o bases de datos de personas y bienes, con el objetivo de que al tener este conocimiento impugnen los registros, en caso de afectar a sus derechos.

Se debe entender que la Ley del Sistema Nacional de Registro de Datos Públicos, regula datos o bases de datos de los usuarios de registros públicos y que esos datos son públicos, que si bien merecen un manejo correcto no siempre es reservado por cuanto no siempre son sensibles ni pueden vulnerar derechos. Y en el caso de que existan vulneraciones, la naturaleza de público permite que se puedan reclamar, y probar la veracidad de ellos.

Los registros de datos públicos son:

- Registro Civil
- Registro de la Propiedad
- Registro Mercantil, Societario, Vehicular, de naves y aeronaves,
- Registros de patentes, de propiedad intelectual
- Registros de datos crediticios
- los que determine la Dirección Nacional de Registro de Datos Públicos

Establecer cuales con las entidades registrales nos permite tener una visión de cuáles son las instituciones públicas que administran bases de datos de las personas, para dirigir nuestras impugnaciones y reclamos si es que ese fuere el caso.

Los registros de datos públicos son los que están determinados en la ley, por lo que solo ellos son competentes y responsables del manejo de la información registral, y de igual forma, es nuestro derecho reclamar inoperatividad o falta de cuidado de su parte.

De igual manera en la **Ley de Propiedad Intelectual**, también existen artículos que hablan de las bases de datos como los que a continuación cito:

Sección II
Objeto del derecho de autor

Art. 8.- La protección del derecho de autor recae sobre todas las obras del ingenio, en el ámbito literario o artístico, cualquiera que sea su género, forma de expresión, mérito o finalidad. Los derechos reconocidos por el presente Título son independientes de la propiedad del objeto material en el cual está incorporada la obra y su goce o ejercicio no están supeditados al requisito del registro o al cumplimiento de cualquier otra formalidad.

Las obras protegidas comprenden, entre otras, las siguientes:

b) Colecciones de obras, tales como antologías o compilaciones y bases de datos de toda clase, que por la selección o disposición de las materias constituyan creaciones intelectuales, sin perjuicio de los derechos de autor que subsistan sobre los materiales o datos;[20]

Podemos ver en este caso, que en otro ámbito del derecho las bases de datos también son objeto de protección ya que en algunos casos pueden constituirse como obras de ingenio o mérito, ya que el autor puede pasar meses compilando información para constituirles en fuente de consulta. Además porque pueden ser bases de datos electrónicas, y también hay derechos en juego, como los del creador del software o del medio tecnológico que permite su acceso, como podemos apreciar en el artículo de la Ley de Propiedad Intelectual que cito a continuación:

Art. 22.- Se entiende por comunicación pública todo acto en virtud del cual una pluralidad de personas, reunidas o no en un mismo lugar y, en el momento en que individualmente decidan, puedan tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas, como en los siguientes casos:

h) El acceso público a bases de datos de ordenador por medio de telecomunicación, cuando éstas incorporen o constituyan obras protegidas;[21]

De igual manera existen definiciones de bases de datos, en cuerpos normativos internacionales como por ejemplo en **Argentina, donde en el decreto 164/94 del 3 de febrero de 1994 en su artículo 1 inciso b),** define, por primera vez en la legislación argentina, a las bases de satos, de la siguiente manera:

[20] REGISTRO OFICIAL 320, de 19 mayo 1998, *Ley de Propiedad Intelectual*, Art 8
[21] Idid. 20. Art. 22

b) Se entenderá por obras de base de datos, incluidas en la categoría de obras literarias, a las producciones constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos.[22]

En este caso ya se entiende a las bases de datos como producciones constituidas por un conjunto de datos, con el objetivo que se procesen, uniendo conceptos como que se produce con un fin y que guarda información que debe ser procesada o almacenada. Considero que para el fin de esta investigación es una definición bastante acertada y que sintetiza los pasos de tratamiento de información, que muchas veces puede contener datos personales sensibles.

Igualmente en **Francia, la ley No. 78-17 del 6 de enero de 1978**, relativa a la informática, los ficheros y las libertades, al referirse a las bases de datos se habla acerca del tratamiento de su información y establece:

Se denomina tratamiento automatizado e informaciones nominativas en el sentido de la presente ley, a todo conjunto de operaciones realizadas por medios automáticos, relativas a la recolección, registro, elaboración, modificación y destrucción de informaciones nominativas, así como todo conjunto de operaciones de la misma naturaleza relacionado con la explotación de archivos o bases de datos, especialmente las interconexiones o vinculaciones, consultas o comunicaciones de informaciones nominativas. [23]

Esta definición de tratamiento de la información es clave para el desarrollo de la presente disertación por cuanto, se entiende de qué forma se procesa la información o datos, desde la recolección hasta la destrucción, de tal forma que sea automatizado y que de esta forma se pueda explotar o sacar provecho a estas bases de datos, como consultas, registros, estadísticas, estudios entre otros. Es claro que esta definición solo es para los fines de esa ley, sin embargo es una buena manera de entender cuál es el trato que se le da a la información y como debe ser.

La Resolución del Consejo de Ministros de la Organización de Cooperación y Desarrollo Económico (OCDE) europea[24], del 23 de septiembre de 1980, también define a las bases de datos, en el artículo primero de su directiva:

[22] Decreto 164/94, de 3 de febrero de 1994, Argentina, Art. 1 inc. b
[23] La ley No. 78-17, de 6 de enero de 1978, Francia,
[24] N.B. Organización para la Cooperación y Desarrollo Económicos, Fundada en 1961, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) agrupa a 34 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo.

Toda colección de obras, o materiales ordenados, almacenados y accesibles mediante medios electrónicos, así como el material electrónico necesario para el funcionamiento de la misma, por ejemplo: su diccionario, índice o sistema de interrogación o presentación de información, no quedaran comprendidos en la definición de los programas de ordenador utilizados en la realización o el funcionamiento de las bases de datos.[25]

En esta resolución también encontramos una definición bastante completa de lo que es y de lo que puede contener una base de datos, ya que por su naturaleza puede contener múltiples tipos de datos. Se infiere entonces que las bases de datos al ser una colección deben tener un orden o con índice y presentación, facilitando el acceso a la información que existe en ella.

1.1.4 CLASIFICACIÓN DE LOS DATOS

Existen variadas clasificaciones de los datos según los autores, así que citare algunas de ellas para tener una visión amplia acerca de esta división.

RODOLFO DANIEL UICICH, clasifica a los datos de la siguiente manera:

a) **Dato anónimo:** Llamamos así al dato estadístico o general que no personaliza ni permite la personalización.

b) **Dato nominativo**: Es aquel que está referido a una persona determinada. Lo dividimos de acuerdo a como sea la forma de acceso a la identificación de la persona en:

- **Directos:** cuando lo identifica sin necesidad de proceso alguno

- **Indirectos:** cuando permite la identificación, pero no lo identifica en forma directa, sino agrupando datos.

A su vez el Dato nominativo se puede clasificar en:

- **Dato nominativo sensible:** Aquel que afecta o puede afectar la intimidad

[25] Op. Cit. 3. p. 47

- **Dato nominativo no sensible:** es aquel que si bien es personal, es destinado a ser público, por ejemplo número de documento de identidad, y que su difusión suele no ser traumática

El Dato nominativo sensible, es el protagonista de esta investigación, ya que son los datos personales que son propios de la intimidad de la persona y se entiende que por su naturaleza deben ser reservados y por esto para su recolección y manejo se necesita una regulación proteccionista.

1.1.5 DATOS PERSONALES SENSIBLES

Debemos tener en cuenta que el uso de herramientas informáticas o TICS[26], transforma las relaciones humanas y por supuesto, las relaciones jurídicas, por lo que las vulneraciones al derecho a la intimidad no son nuevos pero si han aumentado por el uso masivo de medios electrónicos.

Cualquier ciudadano se encuentra registrado de una u otra forma, en varias bases de datos, como en los de la función judicial, registro civil, policía, bancos, tarjetas de crédito, unidades educativas, etc. Por ello surge la necesidad de proteger los datos personales sensibles que estén en las diferentes bases de datos, para que no se realice un uso indiscriminado o arbitrario de ellos, y que además para que éste uso sea con autorización expresa del titular y que no exista afectación a ningún derecho.

Los Datos Personales que son sujetos a especial protección son aquellos que se entienden por sensibles, ya que con la revelación de ellos la invasión a la intimidad sería más severa y lesiva. Por ello el derecho con el afán de proteger estos datos, no prevé normas que obliguen a los administrados a facilitar datos de esta índole, ya que sería inconstitucional, por lo que más bien se intenta que estos datos sean entregados con el debido consentimiento el titular de la información, y procurando que los procesos de tratamiento sean lícitos y adecuados.

Daniel Santos García, en su obra "*Nociones Generales sobre la Ley Orgánica de Protección de Datos*"[27] en su análisis de la ley Orgánica sobre este tema vigente en

[26] N.B. Las tecnologías de la información y la comunicación
[27] GARCIA SANTOS, Daniel, *Nociones Generales de la Ley Orgánica de Protección de Datos,* editorial Tecnos, Madrid, España, Año 2005, p.72

España, explica que los datos personales sensibles son de la ideología, religión, creencias, origen racial, vida e inclinación sexual, estado de salud y se refiere a ellos de la siguiente manera:

Ideología: Son los datos son el conjunto de ideas que tiene el individuo respecto a la realidad o al sistema, y tiene que ver por ejemplo con la inclinación política o filiaciones sindicales por ejemplo**.**

Religión: la convicción religiosa, viene dada por la libertad de culto y claramente nadie debe ser privado de sus prácticas religiosas y tampoco divulgar sus creencias y cultos si no lo cree necesario.

Creencias: tiene relación con las convicciones del individuo que pueden varias de las de los demás, pero no dejan de ser información personal que no se puede divulgar son consentimiento del afectado.

Origen racial: son relativos a la pertenencia de una persona a un pueblo o nación y los datos culturales, sociales y físicos que definan a un grupo social con relación a la persona.

Este tipo de datos son delicados por el tema de posible discriminación o segregación racial que se ha vivido en muchas sociedades a lo largo de la historia, por ello la protección a esta información. Debemos tener en cuenta que actualmente se considera una sola raza humana con diferentes grupos étnicos, y los datos del origen racial pueden incluso atentar contra la igualdad de las personas y las libertades colectivas.

Vida o inclinación sexual: los datos acerca de la vida sexual son bastante variados, pero entendemos que la sexualidad es la el ámbito más profundo de la intimidad por lo que incluye datos acerca de la actividad sexual, la ausencia de dicha actividad, preferencias sexuales y toda la información de este acerca de este tema.

Salud: Estos datos hacen referencia no solo a las enfermedades que padezca el individuo sino también a diagnósticos y tratamientos, el autor nos aclara que incluso un informe médico psicotécnico que contenga la categoría “apto” o “no apto” se considera un dato de salud. Son los datos que se refieran al estado de salud pasada,

presente o futura, y de la salud física o mental, y deben extenderse a adicciones como la drogadicción o alcoholismo.

Estos datos deben ser protegidos particularmente ya que pueden ser obtenidos por terceros y pueden cobrar gran importancia en datos administrativos o fiscales relacionados con la salud. Y puede generar valoraciones diversas en situaciones como préstamos o empleos.

1.2 PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES SENSIBLES

Como se analizó los datos personales sensibles, deben ser objeto de protección por parte del Estado y las leyes de forma obligatoria. E Igualmente en una situación ideal debe existir esta preocupación por la reserva de información personal de los consumidores o usuarios, en las entidades (públicas o privadas), sin embargo no siempre se cumple, por lo que es necesario que exista una regulación con el objeto de la protección legal de datos personales sensibles en el Ecuador.

Una situación que acontece a menudo es que las empresas, manejan datos informáticos, es que estos datos constituyen uno de los valores más importantes para ellos por la facilidad que les brinda a la hora de comercializar su producto, debido a la generalización en el uso de los instrumentos informáticos como herramientas para de producción y de consumo; y. generalmente se maneja la información de los usuarios sin que exista de por medio un consentimiento expreso del titular, ni políticas de custodia de los datos, además sin órganos de control ni sanciones para quienes vulneran derechos divulgando información personal reservada.

Dada esta problemática, muchos países ya se han preocupado ya por este tema, ya hace mucho tiempo, como enuncio a continuación:

- Alemania, en su ley *Land Hesse* de 1970. En la entonces Alemania occidental.
- Suecia, en 1973 dicta la primera ley orgánica sobre el tema que se modificó en 1982.
- Estados Unidos de Norte América, en 1974 *distan Privacy Act*, para dictar con carácter más específico el *Right to Financial Privacy Act* de 1978 y la *Privacy Protection act* de 1980
- Austria, Dinamarca, Noruega en 1978
- Gran Bretaña en 1984 se dicta la *Data Protection Acta*

- Francia el 6 de enero 1978 con la ley No 78-17 sobre la Informática, Ficheros y Libertades
- Convenio para la Protección de Personas con respecto al tratamiento Automatizado de Datos de carácter Personal suscripto en Estrasburgo en 28 de enero de 1981
- Ley del 19 de junio de 1992 distada por la Asamblea Federal de la Confederación de Suiza sobre la Protección de los Datos
- Argentina, el decreto 164/94 del 3 de febrero de 1994 y la Resolución del Consejo de Ministros de la Organización de Cooperación y Desarrollo Económico (OCDE) europea, del 23 de septiembre de 1980
- España, la Ley Orgánica de mayo de 1995 de Regulación al Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)

Acerca de la Protección Jurídica de los Datos Personales, como todo en todo ámbito jurídico, se han desarrollado principios para su correcto ejercicio, por lo que he realizado un análisis de ellos a continuación.

1.2.1 PRINCIPIO DE LA LIMITACIÓN DE LA RECOLECCIÓN DE DATOS:

Consiste en la obligación legal, de que toda recolección de datos sea realizada por medios lícitos y legítimos, y cuando sea necesario, es decir el caso de datos personales sensibles como ideas políticas, religiosas o morales, costumbres sexuales, raza, uso de estupefacientes etc., esta recolección debe ser con el conocimiento y consentimiento del titular de la información.[28]

Es importante la fase de obtención o recolección de datos, puesto que aquí se pude perder la calidad de la información o se puede obtener con medios ilícitos o sin autorización del titular de los datos, por ello se debe siempre propender a que los datos sean correcta y legalmente obtenidos.

Como lo explica Daniel Santos García en "*Nociones Generales de la Ley Orgánica de Datos Personales*", la recolección de los datos debe cumplir ciertas características ya sea para fines de registro o en general al momento de solicitar datos personales a un individuo; estas características son:

[28] Cfr. Op. Cit. 3. p. 49.

La adecuación: es la obligación asegurar al titular de los datos que estos se apegan a estrictas necesidades que persigue el recolector, que debe estar delimitada lo mejor posible, es decir se debe enunciar cual es el fin para el cual se pide los datos y que uso y tratamiento se les va a dar. Esto se aplica de igual forma para personas naturales o jurídicas que se den a la tarea de recolectar datos de índole personal.

La pertinencia: es la obligación de que los datos van a ser utilizado solamente en los fines o usos para el cual fueron recogidos, para ninguna otra actividad.
La recolección siempre debe estar ligada al tema de finalidad y tratamiento de la información ya que el ser información sensible no puede utilizarse para otros fines diferentes por los cuales se solicitó la información.

Datos no Excesivos: los datos recolectados, no podrán ser usados para finalidades diferentes, para las que fueron recogidos. Solo se puede utilizar los datos para la finalidad requerida y que solo se deben solicitar los datos que sean útiles para este objeto, ningún otro dato sensible diferente a estos se puede divulgar.

También se establece que en los casos que se requiera datos personales ara algún propósito laboral, de negocio o administrativo, solo se les debe dar uso dentro del ámbito contractual, no cumplir con este requisito es violar el principio de calidad de los datos; en el caso se requieran los datos para otros fines, debe existir consentimiento para este tratamiento por parte del titular de la información.

1.2.2 PRINCIPIO DE BUENA FE:

Este principio está justificado en este ámbito del derecho, ya que en general se necesita que exista una justificación social y por ende buena fe, en todos los procesos que tengan que ver con manejo y tratamiento de información personal, por su propia naturaleza que muchas veces puede ser reservada y que se pueden lesionar derechos en el caso de filtraciones o mal uso de esos.

No es posible especificar las situaciones en las que se debe aplicar el principio en los casos de los datos personales, ya que las situaciones son indefinidas sin embargo se debe aplicar la sana critica el modo en que los datos, especialmente personales fueron manejados.

1.2.3 PRINCIPIO DE LA CALIDAD DE LOS DATOS:

Del mismo modo, pueden suscitarse vulneraciones de derechos, cuando los datos no son veraces, se debe procurar entonces la calidad de estos datos personales ya que por su antigüedad o mala calidad pueden resultar falso y alejados de la realidad, por lo que Daniel Uicich, en su obra Los Bancos de Datos y el Derecho a la Intimidad, aclara que "*El dato personal debe ser exacto, completo y actualizado y estos caracteres en conjunto protegen al individuo*"[29]**.**

Solo de esta manera se entiende que la información personal responderá a las condiciones del titular de los datos y por ende se podrá dar un tratamiento correcto y obtener así el resultado deseado.

La calidad del dato garantiza también la seguridad jurídica del interesado, ya que al tener esa certeza no se podrán cometer errores en el procesamiento de la información y no se lesionara a la postre ningún derecho fundamental.

Es lógico pensar entonces que cuando exista algún error o falsedad en la información personal el interesado podrá acudir al responsable del tratamiento de los datos, para que se realicen rectificaciones o anulaciones del dato incorrecto ya sea a petición de parte o de oficio, ya que es un derecho del titular de esos datos, en la medida que tiene la disposición de sus datos.

1.2.4 PRINCIPIO DE ESPECIFICACIÓN DEL FIN:

"*Los datos no podrán ser recolectados sin tener un fin precisado, obviamente licito y dado a conocer al titular del dato*."[30]

Como lo explique en el principio de recolección de Datos la finalidad que se le dé a la información de carácter personal es gravitante, ya que solo se puede disponer de ella cuando el titular de la información autorice esto, para una actividad específica sea esto con un fin social, contractual o cualquiera que esta sea; ya que si existe esta aclaración la información recolectada puede ser utilizada con fines ilícitos, lucrativos o se puede difundir sin control, de tal manera que se vulneraria directamente el derecho a la intimidad del titular.

[29] Ibid. 28 p. 50
[30] Ibid. 29. p. 51

La recolección y procesamiento de los datos personales, tienen un fin específico, que generalmente no varía durante el tratamiento de esta información y el papel del titular, quien debe conocer que se está haciendo con su información y con qué objeto, solo de esta forma se mantendrá una relación entre quien le corresponde disponer de los datos, como el responsable de darle tratamiento.

1.2.5 PRINCIPIO DE RESTRICCIÓN DEL USO:

Es complemento lógico del principio de especificación del fin; ya que el dato debe ser utilizado o revelado solo para aquel propósito para el cual fue requerido, a menos que una ley diga lo contrario o que se pida consentimiento expreso del titular de dicha información.

En la ley española, por ejemplo, se ha considerado que se pueda utilizar la información para fines compatibles a los requeridos, como históricas, estadísticas o científicas, ya que solicitar el consentimiento cada vez que se requiera hacer uso de la información sería poco práctico, pero debe entenderse que cuando existen fines no compatibles o totalmente diferentes si de sebe informar al titular y solicitar el consentimiento[31].

1.2.6 PRINCIPIO DE LA JUSTIFICACIÓN SOCIAL:

"*El dato requerido debe ser necesario y lógico para la sociedad al momento de su recolección*." [32]

Este principio responde a la necesidad que impedir que la recolección de información personal, sea utilizada para fines ilícitos, contrarios a los valores de la sociedad, orden público y moral. Además porque se entiende que la recolección y procesamiento de los datos, tiene objetivos de registrabilidad, archivo, documentación que en general procuran un progreso más no un perjuicio para los titulares de estos datos.

No se puede utilizar información personal sin que sea para procurar un beneficio, ya que si no existe este resultado, tendría una reacción social negativa y

[31] N.B. Ley Orgánica de Protección de Datos Personales de España, Art. 4 numeral 2
[32] Op. cit. 3. p.51

que no permitiría el resultado deseado. Además que no sería lícito y lo más probable se sancionaría.

1.2.7 PRINCIPIO DE CONFIDENCIALIDAD:

> *El secreto del dato personal es protegido cuando se limita la recolección, se exige su exactitud y actualidad, y se limita su uso a la buena fe y al fin especificado. Pero el carácter de secreto del dato personal es de su propia esencia.*[33]

Este principio responde a la característica esencial de los Datos Personales Sensibles, ya que son reservados y solo se puede disponer de ellos a voluntad del titular de ellos, exige un secreto u una condición de no divulgación. La buena fe, el fin y el tiempo de disposición también son importantes para entender que el uso que se le dé a esta clase de datos no puede romper esta condición de confidencialidad.

En aplicación de este principio, es necesario el consentimiento del afectado, ya que solo él puede disponer de esta información sensible, o que la ley lo presuma para que se utilice un dato personal para un propósito "*estructuralmente necesario y definido previamente*"[34] como es el caso de registros, estadísticas o políticas de salud entre otras actividades estatales que son plenamente justificadas sociablemente, y siempre llevando calidad en el tratamiento de los datos obtenidos.

Por su naturaleza de confidencial, el dato personal sensible no puede ser vendido, ni cedido, más bien se procura su protección para que no sea de conocimiento de terceras personas y por lo tanto no afecte derechos como la intimidad, buen nombre o privacidad del interesado.

Los datos personales, están provistos de reserva o confidencialidad, solo los titulares puedes administrar esta información y además porque el Estado garantiza la esta confidencialidad, no se puede por ello difundir los datos o procesarlos de cualquier manera sino que se debe tener reserva y autorización del titular.

La autorización de uso, por parte del titular de la información es fundamental para anclar la confidencialidad ya que solo puede existir transferencia de datos personales con el consentimiento del interesado, de esta manera se protege la información pero también se permite su procesamiento cuando sea necesaria.

---

[33] Ibid. 32. p.52.
[34] Id. 33.

La confidencialidad de los Datos personales, es una de sus principales características y puede tener diversas aspectos como la reserva que debe tener un profesional, sea este médico, sicólogo, abogado, periodista, ya que por el ejercicio de sus funciones puede tener acceso a información confidencial de sus clientes o pacientes, y ellos están en la obligación de mantener reservada esa información.

1.2.8 PRINCIPIO DE GARANTÍA DE SEGURIDAD:

> "*Los responsables de los bancos de datos deben procurar que los datos no lleguen a personas no autorizadas. Son responsables por la pérdida o difusión no autorizada del dato*"[35]

Este principio nos aclara a responsabilidad que tiene el Estado, y por ello sus empleados y funcionarios de precautelar los datos personales sensibles y darles un correcto tratamiento, se entiende que es una garantía y que no se produzcan perdidas, alteraciones, filtraciones o modificaciones de la información personal que se encuentra en los registros o bases de datos públicos, tanto que si no se cumple con los requisitos de calidad o de seguridad, no se deben almacenar. Todo esto con el único objetivo de brindar seguridad al momento de manejar información, difundirla y con esto lograr que no se lesionen derechos fundamentales de los titulares de esta información.

El tratamiento de los datos personales sensibles es indispensable para que exista una seguridad adecuada, por ello deben existir una serie de medidas, que aseguren el cumplimiento de los derechos de Protección de Datos.

Considero adecuado acotar en este punto que la LOPD[36] española, prevé que exista una cesión de Datos entre Administraciones Publicas, en este caso basta con que las competencias de los entes versen sobre las mismas materias, para que se pueda ceder la información. Sin embargo en el caso de que sea con fines históricos de estadísticos o científicos, se necesita autorización del interesado porque el fin de la utilización de los datos varia, y en el caso de que el interesado solicite alguno de estos datos personales o información respecto de ellos deben ser informados de modo expreso, preciso e inequívoco de sus derechos.

---

[35] Ibid. 34. p. 53.
[36] N.B. Ley Orgánica de Protección de datos Personales de España

Daniel Santos García, en su obra, "*Nociones Generales de la Ley Orgánica de Protección de Datos",* admite la posibilidad que el Estado pueda subcontratar a terceros o a empresas particulares para que den tratamiento a la información personal sensible, pero se aclara que tendrán igual responsabilidad porque actual actuarían a nombre y representación de la entidad pública, y que de todas formas deben ceñirse a las medidas de seguridad que procuran la integridad de los datos.

1.2.9 PRINCIPIO DE LIMITACIÓN EN EL TIEMPO:

> **"***Cada dato es recolectado con un fin determinado, por ende no puede ser conservado más allá del tiempo necesario para este fin***"**[37]

Es claro que cuando se alarga el tiempo de conservación del dato, se podría entender que no está bien definido el propósito para el cual se lo utilizaría, o en su defecto se lo ha de ocupar en otro fin, caso en el que se podría estar atentando contra el derecho a la intimidad.

También este principio está dado por la calidad de la información, ya que el dato puede estar desactualizado y por ello puede que no sea veraz, por lo que el responsable del tratamiento de la información tiene la obligación de mantener la información exacta, esto quiere decir que debe estar actualizada y además que no se deben adivinar modificaciones no hacer deducciones. El mecanismo jurídico para reclamar esta exactitud por parte de los es el derecho de rectificación, en el Ecuador es o el habeas data.

Todos los procesos advierten plazos de tiempo en los que se debe tratar la información y que información debe ser tratada, limitando de esta forma a los procesos, de tal forma que el tratamiento sea eficaz y muy exacto en cuanto al resultado y a la seguridad en el manejo de los datos.

1.2.10 PRINCIPIO DE TRANSPARENCIA:

> *La transparencia en el manejo de los datos y en el desenvolvimiento de los bancos de datos es un elemento clave en la cuestión. Debe resultar de fácil acceso, el conocimiento sobre la existencia de bancos de datos, sus responsables y domicilio donde desarrollan sus actividades.*

[37] Op Cit. 3. p.53.

Asimismo debe conocerse la existencia de y característica de los datos personales recolectados, así como la finalidad de su recolección[38]

Las actividades estatales deben ser transparentes como regla general, más aun cuando de información sensible se trata, entonces, debe existir una protección en todas las etapas de su tratamiento, para que haya filtraciones, ni se de una mala interpretación de ella. Tal como expresa Rodolfo Daniel Uicich, en su obra Los Bancos de Datos y el Derecho a la Intimidad: "*Partiendo del criterio de que no hay nada que ocultar, la actitud de los responsables de los bancos de datos no deben dar lugar a interpretación errónea, ni suspicaz*"[39]

El conocimiento sobre la existencia de las bases de datos y sus características en el tratamiento de la información, da a lugar a mayor confianza en los procesos, e incluso los hace aceptados a nivel social, con lo que se consigue colaboración por parte de todos los que intervienen en su manejo.

1.2.11 PRINCIPIO DE PARTICIPACIÓN DEL INDIVIDUO:

El dato personal tiene un titular, y él es esencial desde el punto de vista jurídico, ya que solo él puede ejercer los derechos relacionados con la protección de sus datos, es decir realizar rectificaciones o solicitar su información, dar su consentimiento para la transferencia de esta información etc., por lo que no solo debemos dejar la responsabilidad al Estado de aquella protección, se debe propender a que en nuestra sociedad, el ciudadano este informado sobre sus derechos y la lesividad de la difusión de información sensible.

La única forma de que un ciudadano haga valer sus derechos es teniendo conciencia de ellos.

La participación del titular se manifiesta desde el consentimiento para la utilización de los datos personales sensibles, tema que analizare posteriormente, y en el ejercicio de los derechos.

El derecho de Protección de Datos da algunas herramientas para exigir el cumplimiento de los derechos de los ciudadanos en esta materia, se trata de

[38] Ibid. 37. p. 54.
[39] Id. 38.

mecanismos que operan después de que se le solicito la información al titular, e introducidos en un sistema o base de datos.

En Países como España, existen entes estatales competentes en la materia, como la Agencia Española de Protección de Datos, hace exigible estos derechos y cualquier incumplimiento da paso a la actuación de la tutela administrativa en este sentido. Por ello hare un análisis de los mecanismos que tienen los ciudadanos en este país para la protección de sus datos.

1.2.11.1 DERECHO DE CONSULTA:

> **"***Todos los ciudadanos tienen el derecho de consultar los Registros de Datos, a la entidad competente, de carácter público o privado*"[40]

Se entiende entonces, que la entidad pública competente tiene la misión de dar a conocer la ubicación oficina o dependencia de los ficheros o registros de datos personales existentes, para que posteriormente el afectado ejercite sus derechos de acceso, rectificación, oposición, cancelación o impugnación de valoraciones de la información según corresponda. Los responsables del tratamiento de la información no pueden negarse ni entorpecer esta consulta, ya que puede ser sancionado.

En caso de las Instituciones públicas, los responsables del manejo de la información personal sensible, deben respetar los derecho de los titulares o afectados, y no obstaculizar su ejercicio.

Del derecho de consulta de información personal, en nuestro país, podemos decir primero, que la constitución alberga la posibilidad de que se puede ejercitar este derecho a cualquier institución pública, y e incluso se delega esta competencia a la Procuraduría General del Estado, en el caso de que no exista un órganos especializado en el tema requerido, sin embargo, se trata de cualquier consulta, no necesariamente de información personal que se esté procesando en algún órganos estatal. Como vemos, a pesar de que no se determina al derecho de consulta en materia de datos personales, como una figura sólida, se puede accionar de alguna con las herramientas jurídicas que expongo, por lo que hago énfasis en la necesidad de crear procedimientos claros para que el administrado tenga como hacer cumplir su derecho de forma satisfactoria.

[40] Op Cit. 4. p. 96.

1.2.11.2 IMPUGNACIÓN DE VALORACIONES EN LOS TRATAMIENTOS DE LOS DATOS PERSONALES:

En el momento en que los datos personales son tratados, en muchos casos, sometidos a una valoración automática de características y comportamientos, a través medios informáticos. Un ejemplo de estos con las técnicas *SCORING*[41], son valoraciones automáticas que permiten adecuar requisitos de la empresa con los consumidores. El derecho en su labor de protección, establece mecanismos para que los ciudadanos se protejan de decisiones automáticas que otros realicen sobre sus datos personales, como la Impugnación de los actos que impliquen valoraciones de comportamientos del consumidor o titular de la información, ya que esta valoración es obtenida de los datos personales y se puede elaborar un perfil del individuo.

Daniel Santos García, en su obra Nociones Generales de la Ley Protección de Datos dice "*La decisión susceptible de ser impugnada ha de basarse únicamente en un tratamiento de datos destinado a evaluar determinados aspectos de la personalidad del individuo*".

Estas valoraciones pueden revelar estilo de vida, nivel de consumo, ingresos, residencia entre otros y segmentan a los individuos para ofrecer productos. Esto da lugar a que la información ya valorada se comercialice y muchas empresas utilicen esta información valorada.

Este mecanismo de impugnación del titular de los datos, puede ser activado cuando:

- Se requieren que el uso de las valoraciones tengan efectos jurídicos, es decir que se afecten derechos fundamentales

- Debe existir una afectación significativa en la oferta personalizada de algún producto

Es lógico que los que solicitan información personal, lo hacen son la finalidad de valorar esos datos, por lo que es permitido realizar esta actividad, pero el interesado se reserva el derecho a impugnarla en el caso de que se vea afectado algún bien jurídico.

[41] Id. 40.

1.2.11.3 DERECHO DE ACCESO:

Es el derecho exclusivo del titular de conocer toda la información que contenga datos de carácter personal que sean objeto de tratamiento a la persona que esté a cargo de aquella información.

El dueño de los datos, los puede requerir ya que es su derecho conocer que información se está utilizando y de qué forma, cual es la finalidad, el origen, las transferencias, resultado de cualquier proceso etc.

Este derecho también tiene aplicación en datos que sean identificativos o nominativos, ya que el titular es dueño igualmente de esa información y puede conocer el manejo de ella.

Se entiende que este derecho al igual que el anterior debería ser gratuito y debe ser dirigida al responsable de la información en tratamiento, y solo el titular de la información puede ejercitar este derecho, acreditando su legitimidad, para garantizar el derecho a la intimidad y por supuesto la protección de sus datos. El responsable que entregara lo solicitado.

Al poner a disposición la información personal al afectado, legitimado activo, se le brinda seguridad del trato que se le esté dando a sus datos, y permite que exista transparencia en los procesos, además que brinda una visión general de la base de datos que se está procesando y la forma.

En legislaciones como la española existen límites a este derecho, como que solo se lo puede solicitar una vez al año, para evitar gastos administrativos; y se debe acreditar un interés legítimo sobre los datos tratados, como por ejemplo que se esté utilizando los datos para otros fines no comunicados.

El tema de demostrar legítimo interés, es un argumento, bastante usado por la administración en el caso de datos públicos, que están siendo tratados pero no necesariamente significan un perjuicio a sus titulares, sin perjuicio de otros derechos.
A diferencia de en lacos de las bases de datos públicas, en las bases de datos privadas, se entiende que el titular de los datos, siempre podrá ejercitar este derecho incluso varias veces al año, por cuanto el afectado está en libertad de conocer el

destino de la información que se está procesando y nunca puede constituir un obstáculo su naturaleza privada.

Puede denegarse el derecho de acceso en el caso de bases de datos de Fuerzas Armadas y de Seguridad Publica, ya que se entiende que pueden estar en juego intereses estatales o libertades de terceros, por lo que este tipo de información tiene un tratamiento especial y en todo caso que el derecho de acceso que entorpezca la actividad pública u orden social.

En nuestro país, el mecanismo más adecuado para el acceso a la información personal que se encuentra en ficheros o registros públicos es el Habeas data, que analizare más adelante.

En el caso ya de los datos personales sensibles, como los datos referentes a la salud, como diagnósticos, tratamientos y estado físico, por lo que si hablamos de que debe existir protección jurídica para esta información, debe existir la correcta confidencialidad de la información del paciente y acceso a ella, y que debe ser de cumplimiento general.

En las instituciones públicas, la mayoría de información personal que se maneja es información pública, y por ende este derecho al acceso a la información se trata de aquella registral, sin embargo es pertinente para este análisis por cuanto en esa información registral pueden estar presentes datos personales sensibles como el caso de afiliaciones políticas, información racial o de culto.

Estos entes públicos realizan actividades de tratamiento de datos, por lo que según la ley, deben mantener un correcto manejo de la misma y permitir que se realice un ejercicio correcto del derecho a la información y además mantener políticas de manejo eficaces y responsables con la información de los ciudadanos, acogiendo el principio de calidad de la información.

Los servidores o funcionarios públicos que tendrán sanciones y no deberán obstaculizar este ejercicio.

En cuanto al derecho de protección de los datos personales, es importante garantizar este derecho ya que en muchos casos el acceso a esta información advierte al titular el tratamiento de sus datos y permite, en el caso de existir errores o que los

datos no sean precisos, rectificarlos y así mantener transparencia en los procesos de manejo de información.

Lo importante es clasificar correctamente la información dentro de estos cuatro grupos y utilizar el mecanismo jurídicamente correcto para acceder a ella.

En conclusión el Derecho a Acceder a Datos Personales, por parte de su titular es una de las facultades de las que se ve provisto el ciudadanos para ejercer eficazmente su derecho fundamental, solo de esta forma llega al conocimiento de que datos están siendo tratados y bajo de modalidad por lo que se trata de uno de los ejercicios más claros de disposición de su información.

1.2.11.4 DERECHO DE RECTIFICACIÓN:

Es el derecho que tiene el titular de la información personal, de solicitar al responsable de la bases de datos para que mantenga una exactitud de los mismos, por lo que se deberá rectificar la información en el caso de que exista un error, o los dato sean inexactos, inadecuados, o excesivos[42]

Todo esto cumpliendo con los principios que estamos analizando y según la regulación que exista al respecto, por lo que en la ley debe existir un procedimiento establecido y además un plazo de tiempo en el que se debe ejercitar el derecho y la administración debe dar el cumplimiento debido.

Dentro de nuestra legislación el mecanismo legal pertinente es el Habeas Data, en el caso de que el titular de la información desee rectificar o modificar información personal constante en un registro o fichero públicos, también existe la posibilidad de que se demande por los daños ocasionados, en el caso de que esta información incorrecta cause algún daño a su titular o se vulnere algún otro derecho fundamental, que se llevara por cuerda separada y se entiende que también se exigirá mediante órganos jurisdiccional.

Según el artículo 21 de la Ley del Sistema Nacional de Datos Públicos, se puede modificar o rectificar alguna información constante en las bases de datos públicos, siempre que el solicitante sea su titular, y cuando no se viole disposición legal u orden judicial o administrativa y además nunca podrá violentar derechos de

[42] Ibid. 41. p. 97.

terceros; sin embargo existe esa prerrogativa del titular de la información para que se rectifique cualquier dato que este errado, inexacto o desactualizado.

Esta posibilidad de rectificar información no veraz, logra mayor seguridad para los dueños de los datos, como para los que los manejan en instituciones públicas, y más aún en los entes registrales donde pueden existir más casos de presencia de datos personales sensibles en sus archivos, además de mejorar el sistema de protección de datos siendo que se garantiza la calidad de los mismos y calidad en su tratamiento.

1.2.11.5 DERECHO DE CANCELACIÓN:

Es la facultad que tiene el afectado para solicitar que se cancelen datos excesivos, inexactos, inadecuados, o erróneos de bases de datos en tratamiento.
Al igual que los otros derechos debe estar establecido en la ley y requiere que se dé cumplimiento en un plazo de tiempo. En el caso de que la información personal este cedida a otra administración o entidad se debe dar noticia de esta cesión al interesado para que pueda accionar su derecho en la entidad adecuada, este derecho garantiza el derecho a la intimidad, entre otros fundamentales.

Cuando se realiza una cancelación de datos, estos no pueden ser sometidos a tratamiento y tampoco pueden ser difundidos, simplemente se eliminan de la base de datos y los respaldos que existan de estos datos; supone el fin de la relación jurídica entre el titular de la información y la entidad responsable del tratamiento de la misma.
Si se desea volver a procesar los datos, la entidad deberá volver a solicitarlos de la manera establecida en los principios y en la ley siempre respetando los derechos fundamentales.

1.2.11.6 DERECHO DE INDEMNIZACIÓN:

Los titulares de los datos personales, pueden reclamar indemnización en el caso de que se haya ocasionado algún daño o lesión a derechos fundamentales, en la materia o falta de protección en general, siempre que se justifique el daño, que haya una relación jurídica y que el perjuicio sea significativo.

Todos estos derechos son propios de la Protección de Datos, y los he tomado como ejemplo de la legislación española, estos derechos son derechos

personalísimos, es decir que solo pueden ejercerse por su titular y pueden presentar excepciones en el caso de derechos de terceros y son en general derechos gratuitos y fundamentales.

Se establece entonces la responsabilidad de quien maneja o tiene a cargo información personal, con el objetivo de que no se divulgue y además que se mantenga la calidad de esta información, por lo que en el tercer inciso de este artículo encontramos el derecho de solicitar una indemnización en que caso de que la información que reposa en las instituciones públicas no sea veraz o sea imprecisa o sea divulgada; ya que bajo estos supuestos pueden ocasionarse perjuicios desde patrimoniales como morales.

1.2.12 PRINCIPIO DE CONSENTIMIENTO DEL AFECTADO:

En materia de Protección de Datos Personales, este principio es uno de los principales, ya que supone el poder de disposición que tiene el interesado en su información de carácter personal

El consentimiento es "*la manifestación de voluntad libre inequívoca específica e informada*"[43] donde:

Libre: se trata de la libertad con la cual se manifestó la voluntad sin que exista coacción o vicios.

Inequívoca: es necesario que exista una acción que indique el consentimiento.

Especifica: se entiende que es para un fin establecido.

Informada: la persona que esté dando el consentimiento tiene que conocer el motivo por el cual se le solicita la información y, el fin que va a tener.

El consentimiento debe ser solicitado por la persona o entidad responsable del proceso de tratamiento que se le vaya a dar a la información, y por lo mismo debe brindar los medios necesarios para hacer conocer al dueño de los datos personales, el motivo por el cual se recaban, el trato que se les va a dar y el resultado final.

[43] Ibid. 42. pp. 62, 63.

En el mejor de los casos el consentimiento debe ser expreso o por escrito, sin embargo no es siempre es práctico, por lo que el España por ejemplo, se puede, utilizar además medios electrónicos o grabaciones de voz, de esta manera el responsable de la recolección de datos podrá probar el consentimiento, en caso de existir un desacuerdo o Litis en ese sentido.[44]

La persona que da el consentimiento sobre sus datos personales, debe tener la capacidad general para suscribir actos y contratos, en el caso de interdictos el representante deberá ser quien otorgue el consentimiento necesario para ceder estos datos. En el caso de personas menores de edad se entendería que por no ser capaces relativos, no pueden otorgar este consentimiento, aunque la AGENCIA Española de Protección de datos en el año 2000, manifestó en un estudio que las personas mayores de catorce años pueden expresar el consentimiento a cerca de la transferencia de datos personales. Aunque es un precedente no es obligatorio para las demás legislaciones, yo considero que debe los únicos que pueden otorgar consentimiento son las personas mayores de edad y totalmente capaces.

Al establecer que el consentimiento es la manifestación de voluntad inequívoca, se entiende que debe existir una acción por medio de la cual se da este consentimiento; por lo que concluimos también que existen formas de expresar el consentimiento, que pueden ser tacitas o expresas. El consentimiento tácito corresponde a la falta de actividad o silencio, pero este tipo de consentimiento no es el ideal en tema de transferencia de datos personales sensibles, por la protección jurídica que debe existir en este tipo de información.

El consentimiento expreso por el contrario se entiende como el que se otorga mediante una acción inequívoca, como por escrito; este consentimiento es necesario en la transferencia de datos personales sensibles como los de origen racial o de vida sexual por ejemplo, ya que por la naturaleza de reserva de aquellos datos no se puede prescindir de la autorización del titular para que se someta a tratamiento o difusión.

En el caso de datos personales sensibles, es necesaria limitar el acceso a esa información, ya que se puede vulnerar derechos con la divulgación de dichos datos por lo que pueden presentarse varios casos en los que el consentimiento se presenta, estas son:

[44] Ibid 43. pp. 64, 65

1. El titular, otorga su consentimiento en cuyo caso se podrá disponer del dato y someterlo a tratamiento, cumpliendo con los principios enunciados y con lo que dispone la constitución y las leyes, que es el caso que analice anteriormente.

2. Cuando el interés público prima sobre el derecho a mantener en secreto algún dato personal y una ley así lo dispone, en cuyo caso se entiende el consentimiento tácito del titular de los datos.

3. Cuando los datos personales se recogen de fuentes accesibles al público; cuando se recojan para el ejercicio de las funciones propias de las Administraciones Publicas en el ámbito de sus competencias, en cuyo caso en consentimiento expreso es necesario cuando la finalidad del uso de los datos cambie o verse sobre otro tema.

Debemos hacer énfasis en que los datos no deben cederse varias veces entre instituciones, sino cada vez que se sino cada vez que el titular entregue sus datos y su consentimiento, y la cesión se permite cuando los fines y necesidades de las instituciones cesionarias sean similares a las de la institución cedente

Un ejemplo claro de cómo se maneja el tema del consentimiento en la transferencia y tratamiento de la información es España, legislación en la que se prevé excepciones para el consentimiento o incluso modos de oponerse al mismo.

En este país en especial, para datos referentes a la salud, y vida sexual y origen racial se necesitara el consentimiento sin necesidad que sea por escrito, y en el caso de los datos referentes a ideología, creencias, además de expreso deberá ser protegido, por cuanto estos últimos son datos que en la Ley Orgánica de Protección de Datos personales denomina Datos especialmente protegidos.

También en España, existen figuras como la excepción, revocación y oposición al consentimiento, que analizare brevemente a continuación para tener una idea de los procedimientos que se desprenden del consentimiento en otras legislaciones y además para entender la importancia de este acto en materia de Protección de Datos Personales por cuanto la difusión o transferencia de la información personal sin autorización del interesado da pie a conductas atentatorias de derechos.

Conclusión del Primer Capítulo

La importancia de esta capitulo, es entender los conceptos de datos y bases de datos, derecho a la información y su alcance, establecidos en la doctrina y la ley, permitiendo así que se entienda la problemática que causaría el mal uso de esta de datos personales sensibles que conforman una base de datos a cargo de una institución pública o privada.

Igualmente se realiza una análisis de los principios el derecho a la protección de información personal, ya que es necesario que se precisen, en la media que su aplicación garantiza el efectivo ejercicio el derecho y además da luces en cuanto al proceso de creación normativa por la que debemos atravesar en el Ecuador.

También el análisis de este capítulo nos permite verificar la realidad de otros ordenamientos jurídicos, donde si está regulado este derecho de manera adecuada, es decir, teniendo en cuenta sus principios, órgano regulador, y los procesos de tratamiento de los datos, el responsable de los mismos y sobre todo el consentimiento del titular de los datos, facilitando la participación del interesado en el tratamiento y permitiéndole disponer de su información.

CAPÍTULO II

2. EL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

2.1. DERECHO FUNDAMENTAL A LA INTIMIDAD ENFOCADA A LA PROTECCIÓN DE DATOS PERSONALES

La convivencia social, propia de la naturaleza humana permite apreciar la dimensión de lo social desde dos puntos de vista, lo individual y lo colectivo. Estas dos aristas dentro de la realidad del hombre solo llegan a una armonía cuando se encuentran en perfecto equilibro, esto quiere decir que el medio, la sociedad, las conjuga, es decir, permite una realización del individuo en todos los aspectos y a la par brinda un orden social y bien común entre sus integrantes.

La vida en comunidad como en ciudades, y a grande escala en países, disminuye en cierto sentido la intimidad de la vida del individuo, por lo que el Estado cumple un papel regulador que ya no se limita a ser un mero observador sino que interviene para garantizar y de este modo brindar protección jurídica a la intimidad de las personas.[45]

El Diccionario de la Real Academia de la Lengua Española respecto a la intimidad dice: "*Es la parte personalísima comúnmente reservada, de los asuntos, designios o afecciones de un sujeto o de una familia*"[46].

Otra de las conceptualizaciones del derecho a la intimidad que me pareció oportuna es:

> *El juez de la Suprema Corte de los Estados Unidos Cooley, señaló que el derecho a la intimidad, es el derecho a ser dejado en la soledad de su espíritu, al manifestar "THE RIGHT TO BE ALONE", o sea el derecho a estar solo, a que las personas no conozcan, sepan, vean, escuchen, lo referente a nuestra vida, y que nosotros no queremos que trascienda; de tal modo que es una consecuencia o derivación del hecho a la dignidad del ser humano*[47]

---

[45] Cfr. FERREIRA RUBIO, Delia M, *El derecho a la Intimidad*, Buenos Aires Argentina, Editorial Universidad SRL, Año 1982, pp. 32 y 33.

[46] REAL ACADEMIA DE LA LENGUA ESPAÑOLA. *El Diccionario de la Lengua Española (DRAE)*. Madrid, La edición actual 22.ª, publicada en 2001

[47] HONORABLE CÁMARA DE DIPUTADOS DE MÉXICO. *Compendio de Protección de Datos.* Ciudad de México, Tiro Corto editores, 2013, http://inicio.ifai.org.mx/Publicaciones/CompendioProteccionde Datos8.pdf, Ingresado el 20 de agosto de 2013 a las 16h10

Según esta reflexión se infiere que es un derecho oponible a terceros por lo cual es un terreno que no puede ser invadido por particulares ni el Estado, y responde a una necesidad del ser humano para mantener su dignidad y su estilo de vida.

Dentro de este derecho fundamental encontramos entonces, varios ámbitos y actividades de la vida del individuo por lo que la esfera de protección es amplia, ya que responde a decisiones personales, hábitos e incluso preferencias que nacen de la individualidad y diversidad de las personas que conforman el aglomerado social, propias de un buen vivir.

Este derecho tiene como característica que debe ser impenetrable para terceros y que además el individuo es quien decide si extender esta información o guardarla para un campo privado, ya que este conjunto de aspectos que conforman la vida privada, queda totalmente excluido del ámbito social de los ciudadanos, es una propiedad personal.

Derecho Fundamental de la Intimidad, que se reconoce en nuestra constitución, cúspide de la pirámide jurídica, como también en tratados internacionales, como en la Declaración Universal de Derechos Humanos.

La intimidad se reconoce apenas desde el siglo XX, y es acogida en el catálogo de los Derechos Humanos en 1944, en el artículo 12 de la Declaración Universal de Derechos Humanos que dice: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."* [48]

Con esto podemos inferir que el derecho a la intimidad se refiere a las intrusiones de terceras personas en la vida personal del individuo, que sean injustificadas. Es decir la facultad de excluir a los demás de hechos, pensamientos, creencias, actividades y demás factores de la vida personal, imagen, buen nombre o datos personales que por ser reservados y personales no se desea que sean accesibles ni públicos.

A la intimidad se la debe concebir como un tema inherente a las personas, por su propia necesidad de reservar algo para sí o para sus seres cercanos; por ello es

[48] *Declaración Universal de los Derechos Humanos*, Resolución 217 A (III), el 10 de diciembre de 1948 en París Francia.

propio de una sociedad tolerante respetar la intimidad de sus integrantes, por la misma diversidad que existe, que generan diversas opiniones, puntos de vista, que podrían a su vez generar reacciones negativas al ser o incluso atentatorias de derechos o libertades.

La idea de reserva, está motivada por la repercusión social que podría tener la difusión de estos datos, ya que el afectado podría tener una sanción social por parte del grupo humano al que pertenece. Esto nos ayuda a entender que la intimidad tiene una dimensión más bien relativa y no universal, por cuanto cada sociedad tiene sus puntos de vista, creencias y culturas, y con este bagaje pueden juzgar y tener diferentes reacciones.

El individuo no podría controlar a la sociedad para hacer respetar su intimidad o las opiniones que se vierten acerca de ella, por lo que es necesaria la intervención del Estado para que establezca controles o sanciones los que se entrometan con temas sensibles y reservados de algún ciudadano.

El derecho a la intimidad lo que pretende precautelar es la vida privada de las personas, que son precisamente estos hechos o conductas que salen de la esfera social y que pertenecen a la individualidad de las personas.

Según la doctrina, este derecho fundamental, se apoya en una concepción humanista, por la esencia social del hombre que permite estas relaciones individuo-comunidad, que dejan inalienable ciertos aspectos de la vida de este individuo, fuera del conocimiento público, con el objetivo de que la dignidad de la persona humana no se vea involucrada.

La doctrina dice con razón, que la persona no puede estar sujeta de modo permanente a la observación y a la injerencia de sus congéneres, inclusive tiene derecho a reclamar de sus propios familiares, aún de los más allegados, el respeto a su soledad en ciertos momentos, la inviolabilidad de sus documentos personales y de su correspondencia, así como la mínima consideración respecto de problemas y circunstancias que deseen mantener en reserva.

El derecho a la intimidad es un derecho constitucional fundamental, autónomo, forma parte del catálogo de los derechos de la personalidad y que protege la dignidad de la persona., y dentro de este se halla la posibilidad de la realización personal y la

decisión de como el individuo desea llevar su vida, por lo que lo ideas seria que esta información no conste en ninguna base de datos y peor que sea accesible por un particular.

Existe entonces, en determinados casos un conflicto cuando estos aspectos deben constar en cuestiones públicas, ya que puede ser inevitable en algunos casos para el desarrollo de ciertas actividades estatales, por lo que en estos casos la única forma de respetar el derecho a la intimidad es manteniendo procedimientos exactos, no maliciosos y actualizados y con esto se consigue la aprobación del titular de esta información y también precautelar derechos como la integridad personal y buen nombre.

Este derecho supone la protección jurídica de la Vida Privada del ciudadano y de su familia, y responde a la necesidad del individuo a mantener estos aspectos libres de la injerencia pública y así lograr cierta tranquilidad en el desarrollo de su personalidad y estilo de vida.

El Estado tiene el deber jurídico y político de hacerlo respetar y garantizar con instrumentos efectivos su cumplimiento y solo podrá vulnerarlo cuando estén en juego derechos colectivos como el orden público, y aun en ese caso se deben poner en marcha medidas de seguridad al titular de esta información.

La diversidad de la personalidad humana, puede presentar fenomenologías variadas, sin embargo el deber del Estado y de las personas que conformamos la sociedad es permitir que esta diversidad aflore, para aprender de nuestros semejantes y permitir además lineamientos básicos de vida, con el objetivo de realizar nuestro proyecto de vida y afrontar según nuestra voluntad las libertades que nos son brindadas en nuestro desenvolvimiento social y personal.

Por nuestra naturaleza diversa, el forjar nuestra personalidad, puede ser desaprobado por el resto de personas que conviven a nuestro alrededor, así que este derecho permite la libertad de elección sin que tengamos que ser impuestos por los demás, es decir el derecho a vivir en consecuencia a lo que creemos sin tener que justificar nuestras decisiones. Claramente dentro del ámbito de las actividades licitas y que no atenten contra los derechos fundamentales de terceros.

La intimidad del individuo es está presente en muchas circunstancias de su vida personal, y por ello es derecho a la protección de esta intimidad. Últimamente, con el desarrollo de la tecnología y de la informática, la intimidad puede verse más comprometida, por la forma de masiva de transferencia de información actualmente ya que esto supondría intromisiones en la vida privada de las personas; por lo que el derecho a la intimidad, protege lo siguiente:

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.[49]

Como lo vemos la esfera en que se desarrollan las facetas singularmente reservadas en la vida de la persona, es bastante amplia, y la protección de este derecho se extiende a varias actividades y aspectos del desenvolvimiento personal del individuo pero, como consta en la cita anterior el derecho a la intimidad protege Información relacionada con la vida sexual, estado de salud, ideas creencias religiosas y políticas, que son precisamente los datos personales sensibles, objeto de

[49] GARCÍA FALCONÍ, José. *Derecho a la Intimidad Personal y Familiar*, http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechocivil/2011/02/02/derecho-a-la-intimidad-personal-y-familiar, Acceso: 1 de septiembre de 2013 a las 17h00

la presente investigación, y susceptibles de protección jurídica por medio del derecho y mecanismos jurídicos efectivos.

El análisis del Derecho Fundamental a la Intimidad, nos permite determinar cuál es el ámbito de la vida del individuo, que se vería lesionada en el caso de que se transfiera o divulgue información personal sensible, sin el consentimiento o conocimiento de su titular. El derecho de protección de datos, es un derecho que protege indirectamente la intimidad del individuo, y colabora con el hecho de que el titular solo entregue información que desee y bajo un marco de requisitos que garanticen que si vida personal no será violada.

El Derecho a la intimidad consiste en la libertad que tenemos las personas a excluir a otras del conocimiento acerca de sentimientos, emociones, conductas, información personal e imagen personal. También se puede interpretar como la medida en la que estos aspectos pueden comunicarse a terceras personas. Se puede derivar entonces, que la intimidad está dada por el individuo, el control que tiene sobre esta información y aspectos de su vida personal que se concretarían en sus datos personales, ya que la divulgación, no autorizada de esta información personal sensible, daría pasó a la vulneración directa del derecho a la intimidad.

Las regulaciones jurídicas que han evolucionado alrededor de este tema, buscan en general mantener una protección legal de la información personal, de terceros, que eventualmente podrían lesionar el derecho a la intimidad o buen nombre del titular. La información potencialmente dañosa son los ámbitos que ocupan la vida privada del individuo como son creencias políticas o religiosas, decisiones de vida sexual o ascendencia racial, estos datos son clasificados como sensibles y no pueden ser accesibles al público; por lo el objeto de la regularización es la fuente de acceso, que en muchos casos se trata de herramientas informáticas.

En los procesos de recolección y tratamiento de datos, es donde los datos personales son más vulnerables, ya que pueden ser filtrados o difundidos sin el consentimiento del titular, y estos procesos generalmente se realizan con herramientas electrónicas, ya que facilitan estos procesos, por lo cual es derecho no puede estar alejado de esto y se genera una necesidad valida de regulaciones jurídicas de estos procesos.

Las medidas de seguridad técnicas como disposiciones para los responsables del tratamiento de la información de carácter personal permiten que exista información de calidad y que esta no se utilice para otros fines que los propuestos, y en la mayoría de casos estos fines son de materia social, es decir que el Estado, solo puede manejar información personal con fines de orden público y para sus actividades de desarrollo público, e incluso en estas actividades se debe manejar la protección de los datos personales de los ciudadanos los brindan.

2.2. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LA CONSTITUCIÓN

El objeto jurídico de investigación de esta disertación, es la Protección de Datos Personales, y la vulneración que se pueden producir al derecho a la intimidad, buen nombre, a la honra y con relación a los derechos de autor, precisamente por la inexistencia de esta protección.

El derecho a la intimidad puede ser vulnerado de muchas formas, no obstante algunas se pueden ocasionar por el mal uso de las TIC´S[50] o cuando no existe la adecuada custodia de la información o datos personales de particulares, recogidas o no en bases de datos, por la misma naturaleza de la información personal que en muchos casos puede ser sensible como estado de salud, ideología, inclinación sexual, inclinación política entre otras. Todo esto dentro del contexto actual de desarrollo electrónico donde las nuevas tecnologías pueden aportar para la filtración y mal uso de los datos personales, ya que en el diario vivir de la sociedad, las tecnologías son utilizadas para la mayoría de nuestras actividades académicas, explicando de esta manera la dependencia tecnológica que tenemos.

Por lo mismo la Constitución de la República, vigente desde el 20 de octubre de 2008, se refiere a este derecho con relación a la protección de datos personales en los siguientes términos.

Primero, en relación a la garantía de acceso a las TIC´S:

> "*Artículo 16: Todas las personas, en forma individual o colectiva, tiene derecho a:*
>
> *2: El acceso universal a las tecnologías de información y comunicación*"[51]

[50] N.B. Tecnologías de la Información y Comunicación
[51] Op. Cit. 8. Art 16.

En este numeral del artículo 16 de la Constitución del Ecuador se garantiza el acceso a las tecnologías de la información y comunicación, la justificación para esta garantía es que estas herramientas tecnológicas propenden al progreso de la sociedad al facilitar la transferencia de información y conocimiento. Además podría eventualmente contribuir a sistematizar servicios públicos o privados, brindar facilidades técnicas para la producción y comercialización de productos y un sinfín de avances y mejoras sociales. Por ello esta garantía es muy positiva, sin embargo estas herramientas electrónicas pueden de igual forma mal utilizarse cuando se accede a información confidencial o personal de alguna persona, que no está dando su autorización expresa para que se acceda o divulgue aquellos datos para un fin específico. Por este motivo, en la Constitución también existen normas que garantizan la Protección del Derecho a la Intimidad con relación la protección de datos personales correcta, tal como se cita a continuación.

> *Artículo 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*[52]

En este numeral se garantiza que el ciudadano se reserve datos personales sensibles, lo crucial en este artículo es que no se podrá obligar ni exigir que se de autorización para el uso de esta información ni a que se declare sobre ella, sea esta personal o de terceros salvo necesidad médica.

Estos derechos tienen directa relación con los principios de Protección de datos personales que analice en el primer capítulo:

- Con el Principio de Restricción de Uso
- Con el Principio de Confidencialidad
- Con el Principio de Garantía de seguridad por parte del Estado
- Con el Principio de consentimiento del afectado

[52] id. 51.

En el mismo artículo 66 de la Constitución, numeral 19**,** se garantiza concretamente el derecho a la protección de los datos de carácter personal como cito a continuación:

> *El derecho a la Protección de Datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley*.[53]

Este es el texto legal en el que se recoge el objeto de la presente disertación, en el sentido que prevé la protección del acceso, recolección y difusión de los datos personales, sin autorización del titular de la información, es decir la intromisión de terceras personas, en la vida privada del individuo, por lo que aquí se encuentra la relación directa que existe entre la intimidad que se ve relevada al momento de manipular o difundir los datos personales sensibles del ciudadano, y una vez más se justifica la protección que el derecho se le debe brindar a la información sensible en los procesos de tratamiento de la misma en instituciones públicas y privadas sea cual sea el fin.

Es importante de este numeral, la protección, generalmente en estos procesos de recolección es donde se puede filtrar la información personal ya sea de medios electrónicos o gracias a ellos y que el acceso a esta información debe ser restringido y tutelado por el Estado.

Igualmente se protege la difusión y transferencia de esta información en el sentido que solo se utilice para un fin autorizado por el titular. No se pude jugar con la condición religiosa, ideológica o sexual de una personal por lo que se debe cuidar de que solo se utilice los datos para fines progresistas más no discriminatorios, con fines de lucro o vulneratorios. En este sentido La constitución al ser garantista, en este sentido, propende a una correcta custodia de la información personal e igualmente ampara los principios de protección de datos de la siguiente manera:

- Con el principio de limitación de recolección de datos.
- Con el principio de buena fe.
- Con el principio de confidencialidad.
- Con el principio Participación del individuo.

[53] Id. 52.

Igualmente en el numeral 20 del artículo 66 de la Constitución, garantiza: el derecho a la intimidad personal y familiar.

En este numeral se garantiza el derecho a la intimidad, objeto igualmente de la presente investigación, preponderante ya que si los datos personales son filtrados el derecho que principalmente se ve vulnerado es el de la Intimidad de la persona y que debe exigir una reparación inmediata de este derecho fundamental.

> *Artículo 66, Numeral 22: El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; esta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación*[54]

El supuesto que establece la norma, podría eventualmente transferir datos personales, por lo que en general se busca un respeto al derecho a la intimidad, y entre ello, una protección de la información personal, que si es difundida puede poner en evidencia aspectos propios de la vida privada de las personas, por lo que se intenta garantizar este derecho bajo diversos supuestos.

Estas normas en relación al correcto manejo de y protección de Datos Personales, que es el elemento esencial, mediante el cual se puede lesionar el derecho y dar paso a una sanción o reparación oportuna del derecho lesionado.

2.2.1. HABEAS DATA

En la constitución, encontramos también mecanismos para la defensa jurídica del derecho a la protección de los datos personales, uno de ellos es la garantía constitucional del Habeas Data, que se encuentra establecido en el artículo 92 que dice:

> *Artículo 92: Acción de hábeas data. Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.*

[54] Id.53.

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[55]

En este artículo se establece una garantía de los administrados en cuanto a accesibilidad, actualización y manejo de la información personal por parte de sus titulares, con la respectiva autorización y de una manera, con la idea de que se garantiza estos procesos por parte del Estado, y que son transparentes, sin embargo en la práctica se cumple mucho estos postulados.

La garantía Jurisdiccional del Habeas Data, cumple con varios de los principios de protección a los datos personales sensibles, como son garantizar la calidad de los datos, la confidencialidad de los mismos, el consentimiento para su uso, entre otros, por lo que se entiende que es la garantía más precisa ara ejercitar los derechos que posee el ciudadano en cuestión del tratamiento de su información.

La protección de los datos personales, no solo abarca el hecho de que no sean publicados, sino también que en los procedimientos en los que se utilice esta información, se guarden medidas de seguridad para mantener una calidad mínima y además que se cumpla con el objetivo por el cual se solicitó al titular.

El Habeas Data, es el mecanismo jurídico de protección de datos personales por excelencia, y además es el que intenta también proteger el derecho a la intimidad permitiendo que el titular ejercite el derecho a conocer de la existencia y a acceder, actualizar, rectificar, eliminar o anular 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 y la finalidad para la cual se están utilizando sus datos.

También establece que las personas responsables de los bancos de información en los que existan datos personales, no pueden difundirlos sin la

[55] Id. 54.

autorización del titular, por lo que se condiciona a los entes públicos a precautelar estos derechos y a que el titular conozca el destino de sus datos.

Por último, esta garantía jurisdiccional, abre la posibilidad de que la persona afectada pueda demandar por los perjuicios ocasionados, en el caso de mantener estas medidas de seguridad o cuando se divulguen estos datos y se ocasione una vulneración de derechos.

El Habeas data, tiene origen en la garantía del Habeas Corpus, y proviene de la palabra latina "*Habeas*" que significa "*téngase en posesión*" y la palabra inglesa "data" que significa datos, por lo que Habas Data significa "*traer los datos*", esto con el objetivo que el titular pueda conocerlos y disponer de ellos.

La finalidad del habeas data según el autor, es proteger los derechos del titular, por el llamado poder informático, es decir dentro de la recolección, almacenamiento, tratamiento y transferencia de la información personal que se puedan realizar en las instituciones públicas o privadas.

Se ha considerado, la presencia de esta garantía jurisdiccional, ya que el riesgo que tiene los administrados en que se manipule su información personal por medios electrónicos es grande, ya que el tratamiento de la misma, en todas sus etapas puede ser de manera superficial e irresponsable, y se puede dar lugar a una difusión inadecuada.

Esta garantía permite el control y disposición de la información a su titular, permitiendo su conocimiento, acceso, rectificación y hasta la supresión de datos que resulten ilegítimos.

El habeas data es una garantía de rango constitucional por lo que infiere que protege derechos fundamentales, como son el derecho a la intimidad y buen nombre, por medio de la protección de la información de los ciudadanos.

Su naturaleza jurídica es la de ser una acción, la cual general un proceso constitucional, que termina mediante una resolución del juez competente, al cual se acudió en busca de tutela. Además es una garantía, es decir, constituye un mecanismo procesal cuya finalidad es la de proteger derechos fundamentales, que se

plantea, se tramita y resuelve ante un juez competente con poder para hacer cumplir su resolución.

El Habeas Data, es de carácter autónomo, es decir que tiene su propia regulación y procedimiento específico y es de carácter abreviado, por lo que fluye con rapidez.

A pesar de esto, admite el ejercicio del derecho de contradicción y debido proceso del contradictor.

Es una garantía jurisdiccional que opera a petición de parte interesada, es decir el titular de los datos personales sensibles que están siendo tratados y se plantea ante la vulneración efectiva de un derecho constitucional o amenaza certera, antes de que se suscite el acto ilegitimo, por lo que es deber del juez prevenir el daño o rectificarlo o cesarlo.

El acto u omisión que vulnere el derecho constitucional deber ser ilegitimo.

El habeas data procura una protección personal que podría tener incluso un alcance familiar. Los derechos constitucionales que se procura proteger son el derecho a la intimidad, el honor, la buena reputación y la imagen, que aunque están relacionados, no siempre son conexos.

Gracias al desarrollo tecnológico, actualmente la doctrina hace referencia al derecho a la autodeterminación informática, el cual consiste en la potestad soberana que tiene toda persona a ser quien determine qué información puede ser de conocimiento de terceros, por lo mismo se entiende que el individuo también determinara que datos merecen ser rectificados, actualizados o anulados.

Puedo decir acerca de esta autodeterminación informativa, que en definitiva es la potestad de disponer acerca de la información y fiscalizar en que se la utiliza ajena de nuestro poder en las instituciones públicas y privadas.

Este derecho es más aplicable en la actualidad para disponer de la información, a tal punto que sobrepasa al derecho a la intimidad ya que es amplio y genérico, por lo que algunos autores defienden que el habeas data en la actualidad es la protección a la autodeterminación informática, en la medida que el individuo puede

resolver y decidir sobre sus datos; aunque considero, personalmente que en el trasfondo se sigue precautelando la intimidad de los ciudadanos con esta garantía.

Existen opiniones de que el habeas data también es útil para que la persona no se discriminada socialmente ante el conocimiento de sus datos por terceros, ya que se le pueden cerrar accesos a oportunidades laborales e incluso ejercicio de derechos, sin embargo defiendo que en el trasfondo del mismo está presente el derecho a la intimidad como el principal fin de esta garantía jurisdiccional.

Dentro de las formas de protección de datos personales, se encuentra el derecho de acceso a la misma por parte del titular y dentro de nuestra legislación, además del habeas data, para cumplir con este objetivo, está también la garantía jurisdiccional de acceso a la información pública, sin embargo no siempre persiguen la misma finalidad, ya que el habeas data procura acceso a información privada, donde se encuentran los datos personales sensibles. por lo que para el tema de la presente disertación, seria jurídicamente más útil el Habeas Data como mecanismo de protección de datos personales sensibles.

La finalidad del acceso a la información pública es la de fiscalización a la actuación pública mientras que el habeas data busca controlar los datos personales que reposen en instituciones públicas, por lo que es posible solicitar la rectificación o actualización de estos a diferencia de la acción de acceso a la información pública.

Los legitimados activos para plantear el habeas data, son los titulares de la información personal que consta en los registros o bases de datos, dicha persona puede ser natural o jurídica, aunque en cuestión de datos personales será natural, se requiere que la información que se solicite pertenezca a una persona determinada o al menos determinable.

Me parece importante aclarar que así la información no sea exacta o este incorrecta, cuando el titular de la misma solicite acceso a ella, no podrá ser negada por parte de la institución pública utilizando este argumento.

Los registros públicos, tales como el Registro civil, Registro Mercantil, y Registro de la Propiedad, forman parte del Sistema Nacional de Registro de Datos públicos, y su función es para el sustento de derechos como la libertad del trabajo, libertad de comercio, derecho a la propiedad intelectual, derecho a la información, pero

a pesar de que su actividad es protegida por la ley, no se justifica que almacenen información falsa o sensible, por ello la existencia en su contraparte de la garantía jurisdiccional del habeas data.

Estos registros también pueden estar presentes en el campo privado, como en un registro de empleados de una empresa por ejemplo, donde también está garantizado el derecho de protección de datos sensibles.
Los datos sensibles, son objeto de la protección jurídica, y corresponden a lo siguiente:

- Antecedentes penales o judiciales
- rasgos sicológicos o personales
- situación económica
- estado de salud
- convicciones políticas
- vida sexual
- ascendencia racial
- hábitos y gustos

Es evidente que estos datos conforman la vida íntima o privada del individuo y para las personas jurídicas, podrían ser los datos de "*su estado financiero, procesos de producción, comercialización, estrategias de venta, políticas internas, juicios y procesos administrativos planteados en su contra etc*."[56]

La pretensión principal que persigue el ciudadano plantea el habeas datas es acceder a la información personal, ejercitando su derecho de acceso, que como lo expuse anteriormente, es efectivo cuando se accede de forma clara, total y oportuna. Igualmente con esta garantía se busca la rectificación de información incorrecta o actualización de datos antiguos, o eliminar datos del registro o sistemas públicos o privados. Todas estas pretensiones se manejan dentro de la reserva o confidencialidad propia de la naturaleza de estos datos, ya que forma parte de las garantías del Estado en cuanto a la protección de los datos personales.

[56] SALMÓN ALVEAR, Carlos, *Régimen Procesal del Habeas Data en el Ecuador*, http://www.revistajuridicaonline.com/images/stories/revistas/2008/24/24-regimen-procesal-del-habeas.pdf, Acceso: 2 de enero de 2014 a las 13h00.

Se debe entender que los datos personales pueden también ser "*entregados a un Juez, Fiscal o Comisión Investigadora*"[57], en el caso de que sean requeridos, siempre bajo disposiciones legales, y respecto al caso o materia que se investigue. esto por cuanto se entiende que se precisa de los datos personales para impartir justicia, un derecho colectivo, que procura el bien común.

Además responde al principio de calidad de los datos personales, porque para su tratamiento, sea idóneo y con el consentimiento del titular.

2.3. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LAS LEYES PERTINENTES.

Es de interés conocer cuáles son los postulados legales de protección de los datos personales en nuestro país, y así implícitamente la protección del derecho a la intimidad, buen nombre, honra entre otros, que se ven afectados cuando no existe esa custodia adecuada de la información.

Es importante, justificar que la información de los ciudadanos, forma parte de su ser y de su relación con la sociedad, por lo que estos datos pueden producir derechos del titular y obligaciones conexas de terceros que manejen esta información.

2.3.1. EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL

En la actualidad, se han producido, algunos cambios en el ámbito de Derecho Penal, en nuestro país, por lo que considero oportuno verificar si existe alguna protección a los datos personales, dentro de esta rama del derecho.

Anteriormente, el objeto de investigación de la presente disertación, en materia penal, se desarrollaba dentro del concepto de "*Los delitos contra la inviolabilidad del secreto y la correspondencia*" que se encontraba en el capítulo 5 del Código Penal ecuatoriano, no obstante, desde el 10 de febrero del 2014, se encuentra en vigencia el Código Orgánico Integral Penal, Registro Oficial, Suplemente No 180. Por lo que realizare un breve análisis de los tipos penales anteriores y los que tenemos en la actualidad para la Protección de los Datos Personales.

[57] Id. 57.

La ley de Comercio Electrónico, instauraba reformas al artículo 202 del antiguo Código Penal, dentro de los siguientes términos:

> *Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados*:[58]
>
> *Art. ..- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.*
>
> *Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.*
>
> *La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.*
>
> *Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.*[59]

Este tipo penal se extendía a proteger información de seguridad nacional o secretos comerciales, aumentando la pena. Igualmente se aumentaba la pena en el caso de que la información protegida se divulgara por quien la obtuvo fraudulentamente. Igualmente, si la persona encargada la divulgaba, de su custodia su pena era más alta.

Estos tipos penales, eran los únicos establecidos para las conductas relacionadas con el acceso ilícito y fraudulento de información protegida, y dentro de esta de datos personales sensibles.

El siguiente artículo innumerado posterior al 202 del código penal establecía:

---

[58] REGISTRO OFICIAL Suplemento 557, última reforma 10 de abril de 2014, *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*

[59] Registro OFICIAL Suplemento 147, Fecha de publicación 22 de enero de 1971, *Código Penal*, primer artículo innumerado después del 202.

Art. ..- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.[60]

La conducta delictiva, en este caso era obtención o utilización de datos personales sin autorización del titular, puesto que la autorización del titular es fundamental para la transferencia de esta información, por lo cual lo que se sancionaba era el manejo sin autorización, ya que en esta circunstancia pudo darse un mal uso a la información, que provoque un daño moral o patrimonial al titular, o un uso diferente al deseado.

Todo esto era por una especial motivación. Eran distintos los bienes jurídicos los que el legislador pretendía resguardar, no solo el secreto como tal ya que depende de que información se revele para saber qué interés se dañaría y cuál es su gravedad o alcance, ya que en general los datos de carácter personal y su divulgación pueden traer consecuencias directas a la vulneración al derecho al honor y buen nombre

Hoy por hoy, el Código orgánico Integral Penal, también brinda una protección jurídica a los Datos Personales.

El primer tipo penal a ser analizado es el que corresponde a los Delitos contra el derecho a la intimidad personal y familiar, que textualmente cito a continuación:

Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley[61]

El tipo penal en mención, se compone de los siguientes elementos:

[60] Ibid. 59, segundo artículo innumerado después del at. 202.
[61] REGISTRO OFICIAL, Suplemento 180, Fecha de publicación 10 de febrero de 2014, última Reforma 11 de abril de 2014, *Código Orgánico Integral Penal*.

SUJETO ACTIVO: Quien no cuente con el consentimiento del titular de la información personal**.**

CONDUCTA PUNIBLE: acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio.

SUJETO PASIVO: El titular de la información protegida que no brindo su consentimiento o autorización sobre el uso de sus datos personales, ya que él es el único que puede disponer de esa información.

BIEN JURÍDICO PROTEGIDO: la vida privada e intimidad del titular de la información que fue divulgada.

PENA: Privación de la libertad de uno a tres años.

Este tipo penal, es el que sanciona la transferencia de los datos personales sin consentimiento de su titular, y permite efectivamente el ejercicio derechos fundamentales como la intimidad, ya que castiga la divulgación de la información, que puede suceder de diversas formas como interceptar, acceder o reproducir, etc., con el objetivo de brindar la mencionada protección jurídica a la información que por su naturaleza debe ser reservada.

Es oportuno notar, que no se sanciona el hecho de que el titular de la información intervenga en la grabación, o medio revelatorio de información, ya que en este caso el estaría disponiendo de su información y no atentaría contra ningún derecho. Igualmente no se sanciona la divulgación de información pública, ya que por su naturaleza se entiende que puede ser de dominio público.

Otro tipo penal, que sanciona conductas atinentes a la divulgación de información personal es el siguiente:

> *Artículo 180.- Difusión de información de circulación restringida.- La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años.*
>
> *Es información de circulación restringida:*

1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.

2. La información producida por la Fiscalía en el marco de una investigación previa.

3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.[62]

Este tipo penal tiene varios elementos que expondré a continuación:

	Primer Inciso	**Numeral Uno**	**Numeral Dos**	**Numeral Tres**
Sujeto Activo	Cualquier persona que difunda información restringida			
Conducta Punible	Difundir, por cualquier medio, información restringida			
Sujeto pasivo	Toda persona natural o jurídica, titular de la información restringida	Toda persona natural o jurídica, titular de la información restringida por medio de una reserva legal, entre ellos podría ser el titular de información personal sensible, jurídicamente protegida que ha sido divulgada sin su consentimiento	Todos los ciudadanos ya que se impide potestad punitiva del Estado, ya que podría interrumpirse un proceso penal, y no se llegaría a cumplir con los objetivos procesales del juicio penal o de una investigación; y tangencialmente seria el sujeto pasivo del delito o infracción que origino la investigación.	Las niñas, niños y adolescentes, ya que por su condición están provistos de una protección jurídica diferente en pro de la defensa de su interés superior.
Bien Jurídico Protegido	La intimidad o secreto, objeto de protección legal, del titular de la información restringida	La intimidad o secreto, objeto de protección legal, del titular de la información	El debido proceso y seguridad jurídica dentro de un proceso penal	El interés superior del menor

[62] Id. 61.

		restringida		
Pena	Privación de la libertad de uno a tres años			

Este delito, aunque no es específico para datos personales, está en posibilidad de brindar una protección penal al titular de estos datos, que puede ser divulgada su información personal sin que él lo autorice.

Los datos personales, se encuentran en la categoría de información restringida por reserva de ley, ya que en la Constitución y varios otros cuerpos legales como la Ley del Sistema Nacional de Registro de Datos Públicos y Ley de Comercio, está presente la premisa de que es información jurídicamente protegida y que necesita del consentimiento de su titular para ser difundida o transferida, y además este precepto solo modificar por el mandato de una ley o por un interés constitucional legítimo.

Otro de los delitos, que permite la protección jurídica de los Datos de Carácter Personal, es el que corresponde a los Delitos contra la seguridad de los activos de los sistemas de información y comunicación, que dice:

> *Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.*
>
> *Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.*[63]

Sus elementos son:

Sujeto Activo	Persona Natural que para beneficio propio o de terceros revele información	Servidor Público que para beneficio propio o de terceros revele información registrada.	Empleado Bancario que para beneficio propio o de terceros revele información registrada.	Empleado de una institución de la economía social popular y soldaría que realice intermediación

[63] Id. 62.

	registrada.			financia o contratistas que, para beneficio propio o de terceros revele información registrada.
Conducta Punible	Revelar información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas			
Sujeto Pasivo	El titular de la información o afectado en su intimidad y privacidad al relevar aquella información registrada.			
Bien Jurídico Protegido	El secreto, intimidad y la privacidad de las personas titulares de la información o afectadas por su revelación			
Pena	Privación de la libertad de uno a tres años	Privación de la libertad de tres a cinco años. . .		

En este tipo penal, se pretende sancionar conductas que revelen información restringida; que podría tratarse de datos personales, contenidos en bases de datos, que generalmente se encuentran en instituciones públicas o privadas que realizan actividades en las que manejan este tipo de datos, como registros públicos, bancos, cooperativas, etc.; y, estas bases de datos son obtenidas o destinadas a un sistema informático o de telecomunicaciones.

Se evidencia una vez más, el papel protagónico de los medios informáticos en la transferencia, almacenamiento y acceso de gran cantidad de datos, y que al facilitan el cometimiento de delitos de este tipo, que lesionan, directamente la privacidad de los titulares de la información.

También es importante, el análisis de la responsabilidad del encargado de la base de datos, a quien el tipo penal sanciona de manera especial, ya que por su condición tiene acceso a la información personal, sin embargo se procura que mantenga una responsabilidad sobre los ficheros a su cargo y que no se filtre información por medio de él.

Dentro del tema del uso de medios informáticos en el tratamiento de datos personales, el código Orgánico Integral Penal, también prevé sanción para aquellas conductas de violenten o intercepten este tipo de sistemas, con el objetivo de revelar información.

A continuación el tipo penal en su parte pertinente:

Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

[…] [64]

Los elementos de este Tipo Penal son:

SUJETO ACTIVO: Cualquier persona que no tenga orden judicial y que en su beneficio o el de un tercero intercepte de cualquier forma una transmisión de datos.

CONDUCTA PUNIBLE: Interceptar, escuchar, desviar, grabar u observar, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

SUJETO PASIVO: El titular del dato o dueño de la información que se intercepto

BIEN JURÍDICO PROTEGIDO: Al tratarse de información, con una finalidad determinada, el bien jurídico protegido depende de esta finalidad, sin embargo para el caso concreto de los datos personales, el bien jurídico protegido es la confidencialidad propia de esta información para precautelar la privacidad de su titular.

PENA: Privación de la libertad de tres a cinco años.

[64] Id. 63.

Este tipo penal, pretende sancionar conductas, que violenten los medios informáticos, medios en los cuales se almacena, actualmente, la mayor cantidad de datos personales en las instituciones públicas y privadas, además de ser el medio mediante el cual, en la mayoría de los casos se tratan estos datos: Por esto es necesaria la protección jurídica de estos medios también.

El tipo penal, no especifica que la información interceptada se trate de datos personales, pero existe esta posibilidad de que con este tipo, se sancione una conducta ateniente a revelar información personal.

El último de los tipos penales pertinentes, para la protección de datos personales, mediante el correcto uso de los sistemas informáticos es el siguiente:

> *Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.*
>
> *Con igual pena será sancionada la persona que:*
>
> 1. *Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.*
>
> 2. *Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.*
>
> *Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.*[65]

Este tipo penal, tiene varias conductas punibles, así como variadas, por lo que a continuación realizare el análisis correspondiente:

	Primer Inciso	**Numeral Uno**	**Numeral segundo**	**último Inciso**

[65] Id. 64.

Sujeto Activo	Cualquier persona que ataque los sistemas informáticos			
Conducta Punible	Destruir, dañar, borrar, deteriorar, alterar, suspender, trabar, causar mal funcionamiento o comportamiento no deseado o suprimir datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen	Diseñar, desarrollar, programar, adquirir, enviar, introducir, ejecutar, vender o distribuir de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso.	Destruir o alterar sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.	Cualquiera de las conductas punibles, establecidas en el primer inciso y los dos numerales anteriores, si se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana.
Sujeto Pasivo	Titulares de la información	Titulares de la Información	Titulares de la información y dueños de la infraestructura tecnológica destruida o alterada	Encargado de brindar el servicio
Bien Jurídico Protegido	Privacidad de los titulares de la información	Privacidad de los titulares de la información	Privacidad de los titulares de la información	Seguridad Ciudadana
Pena	Privación de la Libertad de tres a cinco años.	Privación de la Libertad de tres a cinco años.	Privación de la Libertad de tres a cinco años.	Privación de libertad de cinco a siete años

Este tipo penal, es relevante en la protección de datos personales ya que su tratamiento, en mayor cantidad, se realiza por medio de sistemas informáticos, y si existiera un ataque a la integridad de estos sistemas se podría acceder a estos datos,

y seria revelados o divulgados y afectar la intimidad de su titular, además que el afectado, no tendría conocimiento del uso que se le esté dando a esta información.
El último de los delitos pertinentes, en cuanto a la protección jurídica de los datos de carácter personal es el que cito a continuación:

> *Artículo 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.*
>
> *La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.*
>
> *Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.*[66]

	Primer Inciso	**Segundo Inciso**	**Tercer Inciso**
Sujeto Activo	Cualquier persona que destruya información pública reservada legalmente	Servidor público, que por su condición, obtenga información reservada por la ley	Servidor Público que revele información reservada
Conducta Punible	destruir o inutilizar información clasificada por la ley	Usar cualquier medio electrónico o informático para obtener este tipo de información	El servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la

[66] Id. 65.

			seguridad del Estado, siempre que no se configure otra infracción de mayor gravedad
Sujeto Pasivo	Titular de la información, o el Estado si es información atinente a su seguridad	Titular de la información, o el Estado si es información atinente a su seguridad	El Estado o administración Publica
Bien Jurídico Protegido	Privacidad del titular de la información o Seguridad Ciudadana	Privacidad del titular de la información o Seguridad Ciudadana	Seguridad Ciudadana
Pena	Privación de la Libertad de cinco siete años	Privación de la libertad de tres a cinco años.	Privación de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses

Este delito, sanciona conductas que atenten contra la información pública reservada legalmente, es decir, datos que estén almacenados en fuentes públicas, que la ley haya determinado como reservada, y dentro de ella pueden existir datos personales. Esta información no puede ser destruida ni mal utilizada porque se entiende que es necesaria dentro de las actividades y políticas públicas.
Igualmente, es relevante la responsabilidad de la custodia de esta información que tiene el servidor o funcionario público que la tenga a su cargo, por lo que su pena es mayor, en caso de que violente esa reserva legal.

Considero que el actual Código Orgánico Integral Penal, se ha regulado de mejor manera la protección de datos personales, ya que anteriormente esta regulación era una reforma establecido por el Código de Comercio Electrónico, por lo que se ha permitido sancionar conductas atentatorias relativas al mal uso de la información, como al mal uso de los sistemas informáticos sirven de medio para su tratamiento y almacenaje.

Otra consideración seria, que las penas han aumentado en cada uno de los tipos. Asimismo han aumentado las conductas punibles, con relación a vulneración del

derecho a la intimidad y autodeterminación informática, aumento que pienso es positivo por cuanto la realidad informativa varía cada día y se necesita de una regulación que prevea todos los casos.

A pesar de que en el ámbito penal, existe regulación para la protección personal, en el caso específico de datos personales, persiste la idea de una dispersión normativa, es decir que se regula en varios cuerpos legales sin que se le preste una atención jurídica específica y propia para esta información personal.

2.3.2. LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS:

Como ya lo hemos establecido anteriormente, en el Art 6 de la ley del Sistema Nacional de Registro Datos Públicos, establece cual es los datos de carácter personal que son sujetos a una protección especial, por parte del derecho, estos son:

> *Artículo 6: Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.*
>
> *El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial. […]*[67]

Se enuncia entonces, cuales son los datos de carácter personal, y se los vincula con la intimidad personal de su titular, ya que su nexo es evidente, por lo que puedo inferir que la revelación de estos datos provocaría mayormente perjuicios morales a su titular y además vulneraria directamente su derecho a la intimidad.

Igualmente este artículo instituye, en su tercer inciso, como confidenciales los datos que han sido declarados como tales, por la autoridad competente, que bien podría ser un juez; y estos son los amparados en el sigilo bancario o bursátil u los que puedan afectar la seguridad del estado. Aunque estos datos no siempre pueden ser personales, podrían eventualmente resultar sensibles para el titular o para el Estado, por lo que se les brinda también un trato especial.

[67] REGISTRO OFICIAL, Suplemento 162, Fecha de publicación 31 de marzo de 2010, Ultima Reforma 3 de diciembre de 2012, *Ley del Sistema Nacional de Registro de Datos Públicos*.

En el cuarto inciso, se habla de la responsabilidad que los funcionarios tienen por tener a su cargo estos datos de carácter personal, ya que debe tomar medidas de seguridad para la protección y reserva de esta información. Estas medidas de seguridad deben ser técnicas, aplicadas al medio en el cual se esté tratando o almacenando la información; y jurídicas, en la regulación que debe existir para el manejo y uso de la misma.

En el caso que un tercero, desee acceder a la información sobre sobre el patrimonio de las personas, el quinto inciso establece:

> *El solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer*[68]*.*

En principio considero que solo el titular podría acceder a su información personal, así sea esta patrimonial, ya que solo él puede disponer de sus datos, además la difusión o mal uno de la información patrimonial, podría eventualmente también vulnerar derechos constitucionales. El solicitante podría ser un tercero autorizado, situación en la cual también se le debe pedir sus datos de identificación para verificar si participación en la solicitud.

Sin embargo, si se trata de un tercero diferente del titular, quien desea acceder a esta información, ya que la ley lo permite, considero que los requisitos que debe presentar el solicitante, es lo mínimo para que la institución se los otorgue, ya que podría tratarse de algún proceso judicial o de intereses válidos.

Siendo este el caso, debe notificársele al titular del acceso que se le ha otorgado al solicitante, con el objetivo de que tenga el conocimiento de lo que está sucediendo con su información y destino que la misma tiene, para que también pueda ejercer sus derechos de protección de datos si se ve afectado o lo encuentra pertinente.

[68] Id. 67.

En el caso de que se contrapongan dos derechos, se debe dar lugar a la protección del que sea más cercano al bien común y orden público, por lo que eventualmente, un tercero podría acceder a información patrimonial de terceros.

El sistema Nacional de Registro de Datos Públicos, maneja la información que reposa en las instituciones registrales públicas, por lo que el ámbito de aplicación del artículo 6 son el Registro Civil, Registro Mercantil y Registro de la Propiedad.

Al manejarse datos de los ciudadanos, muchos de ellos son de carácter personal y además sensibles, por ello la importancia su reserva y de establecer el impedimento de transferirlos sin el consentimiento del titular de los mismos, y que a su vez el titular pueda disponer de ellos.

No obstante, la información que maneja este sistema, es clasificada como publica por lo que en general los ciudadanos tienen derecho a su acceso y más bien es un servicio para mantener correctamente almacenados y procesados los datos públicos. La finalidad del registro es positiva ya que permite mantener el orden público y la seguridad jurídica en los negocios y actos que realicen los administrados. Sin embargo los ciudadanos también tienen derecho a que sus datos no sean divulgados y sean correctamente utilizados y con su autorización, por lo que es necesaria una regulación especial para los datos personales sensibles que se encuentran en estos bancos de datos públicos.

2.3.2.1. NORMA SOBRE PROTECCION Y SEGURIDAD DE INDORMACION, RESOLUCIÓN No. 7 de la DIRECCION NACIONAL DE REGISTRO DE DATOS PUBLICOS DE 14 DE JULIO DE 2013

En general esta ley prevé mecanismos de acceso y consulta de datos, como también medidas de seguridad para preservar la información de los ciudadanos, sin embargo al no existir esta regulación referente a datos personales sensibles se ha emitido Resolución 7, publicada en el Registro Oficial Suplemento 43 de 24-jul-2013 emitida por el Director Nacional de Registro de Datos Públicos, denominada Norma sobre Protección y Seguridad de Información; resolución que tiene lineamientos más específicos referentes al objeto de la presente disertación.

Esta norma tiene como objetivo general, asegurar y garantizar una apropiada protección y reserva de todos los activos de información se manejan en la Dirección

Nacional de Registro de Datos Públicos, y reducir y controlar los riesgos legales y tecnológicos a los que se enfrenta la información.

Igualmente, en base al acuerdo de confidencialidad, que debe ser suscrito por todos los servidores públicos esta norma pretende, garantizar que toda la información esté protegida del uso no autorizado, violación de la privacidad, y es aquí donde encaja la información personales sensible, por lo que en general ya se habla de medidas de seguridad y probidad en las actuaciones de los encargados de estos datos para que existan abusos ni negligencias.

2.3.2.2. NORMA DE ASEQUIBILIDAD A DATOS PERSONALES DE LOS REGISTROS PUBLICOS, RESOLUCIÓN No. 21 de la DIRECCION NACIONAL DE REGISTRO DE DATOS PUBLICOS DE 5 DE ENERO DE 2013

La Resolución No 21 emitida por el Director Nacional de Registro de Datos Públicos, en consideración con la Constitución, a la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, en donde dispone que las personas responsables de los bancos de datos personales únicamente podrán difundir la información con autorización del titular o de la ley; y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, donde dice que es posible la recopilación de datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, pretende regular la asequibilidad a los datos personales de los registros públicos.

Su ámbito de aplicación son los datos personales que integren:

- La Base Única de Datos que establezca la Dirección Nacional de Registro de Datos Públicos (DINARDAP)
- El Sistema Nacional de Registro de Datos Públicos (SINARDAP).

Y tiene como objeto determinar los datos personales que son libremente asequibles y aquellos que son restringidos, y establecer las condiciones para su asequibilidad.

Esta resolución clasifica a la información personal en:

- Información restringida, que es la información que no es de acceso público, y como norma general, toda información personal es información restringida.
- Información asequible: Es la información que a ley permite a tener acceso. La información personal es asequible por excepción.

La resolución 21, establece que el titular de la información podrá acceder, sin limitación alguna, a su información personal que repose en los distintos registros públicos y que terceros podrán acceder a esta información en los siguientes casos:

- **Cuando cuenten con la autorización expresa del titular de la** información;
- Cuando estén expresamente autorizados por la ley;
- Por mandato judicial u otra orden de autoridad con competencia para ello; y,
- Las instituciones públicas, cuando lo requieran para el ejercicio de sus respectivas competencias.

Estas condiciones, son vitales para el ejercicio de derechos del titular de la información, y para cumplir con la garantía constitucional de que solo el titular puede disponer de sus datos. La Resolución hace una precisión, que en el caso del consentimiento y mandato judicial, estas pueden constar en un soporte material o en uno informático.

Igualmente, esta resolución aclara que toda persona que utilice datos personales restringidos, estará obligada a dar el uso exclusivo para el que le fue concedido, debiendo custodiarlos con prudencia, poniendo en práctica los principios que aseguran la protección de los datos y esta obligación se extiende a sus empleados y funcionarios, y será responsabilidad de la máxima autoridad institucional implementar las medidas, políticas y procedimientos necesarios para estos efectos.
En el anexo de esta norma consta el formato solicitar la entrega de información asequible, además, se establece que la persona requerida llevará un registro de todas las solicitudes recibidas y de las atendidas.

En el caso de los datos sobre el patrimonio, el solicitante debe cumplir con los siguientes requisitos:

- *Justificar y motivar con las razones pertinentes la necesidad de requerir la información;*
- *Declarar el uso que hará de la información. Se aclara que un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer;*

- *Cuando se trate de personas naturales consignarán: sus nombres y apellidos completos, número del documento de identidad o ciudadanía y dirección domiciliaria; y,*
- *Cuando se trate de personas jurídicas indicarán: su razón social o denominación objetiva, número del Registro Único de Contribuyentes (RUC) y dirección domiciliaria.*[69]

Y no se podrá acceder a:

- *La información amparada por el sigilo bancario como es aquella referente a depósitos y captaciones de cualquier índole efectuados en las instituciones del sistema financiero o en las organizaciones del sector financiero popular y solidario;*
- *La información amparada por la reserva bancaria como es la correspondiente a los bienes y derechos de propiedad de las instituciones del sistema financiero y de las organizaciones del sector financiero popular y solidario, entre los cuales se incluyen los créditos concedidos por ellas, en cualquiera de sus formas, sean estos sobre firmas, con garantía prendaria o hipotecaria; y,*
- *La información amparada por el sigilo bursátil como es la referente a los nombres de los comitentes que reposa en poder de los intermediarios del mercado de valores y en los depósitos centralizados de compensación y liquidación de valores.*[70]

Concluyo que esta norma impone correctas medidas para la protección de datos como el consentimiento del titular y la regulación en acceso a datos personales en general, sin embargo considero que tiene un rango inferior al necesario, por lo que estos puntos deberían estar mejor regulados en un reglamento en general, con las resoluciones de la DINARDAP, con relación al tema.

2.3.3. LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN.

El acceso a la información pública, también está regulada por la Ley Orgánica de transparencia y acceso a la información pública, publicada en el Registro Oficial Suplemento 337 del 18 de Mayo del 2004. Es relevante el análisis de esta norma, en primer lugar porque la Ley del Sistema Nacional de Registro de Datos Públicos, la toma en cuenta en sus considerandos, justificando la necesidad de una regulación específica del SINARDAP, y en segundo lugar porque como ya conocemos, dentro de la información pública podrían hallarse datos de carácter personal de los ciudadanos.

El artículo 1 establece el Principio de Publicidad de la Información Pública en los siguientes términos:

---

[69] REGISTRO OFICIAL, Suplemento 863, Fecha de publicación 5 de enero de 2013, Ultima Reforma 3 de junio de 2013, *Resolución 21 de la Dirección Nacional de Registro de Datos Públicos, Norma de Asequibilidad A Los Datos Personales de os Registros Públicos*, Articulo 7 Artículo sustituido por Resolución de la DINARDAP No. 18, publicada en Registro Oficial 6 de 3 de Junio del 2013.

[70] Id. 69.

El acceso a la información pública es un derecho de las personas que garantiza el Estado. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONG's), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley.[71]

La información pública entonces, es la que emana o está en poder del Estado o sus concesionarios, todo documento que se encuentre en poder de las instituciones públicas que hayan sido, contenidos, creados u obtenidos por ellas y que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado. Y es un derecho de los ciudadanos acceder a ella. La naturaleza de publica, es justificada la potestad que los administrados tenemos para conocer las actividades y funciones estatales que se están llevando a cabo en nuestro beneficio, es claro la razón de su interés público.

Sin embargo en algunas de estas actividades estatales se pueden estar procesando o almacenando datos personales por ello la necesidad de regular su acceso a un ámbito más reservado y que sea propio del titular de la información de carácter personal.

Por ello, dentro de los objetivos de la presente ley se encuentra la protección de información personal, tal como cito a continuación:

Art. 2.- Objeto de la Ley.- La presente Ley garantiza y norma el ejercicio del derecho fundamental de las personas a la información conforme a las garantías consagradas en la Constitución Política de la República, Pacto Internacional de Derechos Civiles y Políticos, Convención Interamericana sobre Derechos Humanos y demás instrumentos internacionales vigentes, de los cuales nuestro país es signatario.

Persigue los siguientes objetivos:

[…]

[71] REGISTRO OFICIAL, Suplemento 337, 18 de mayo de 2004, *Ley orgánica de Transparencia y Acceso a la Información Publica.*

c) *Garantizar la protección de la información personal en poder del sector público y/o privado,*

[…] [72]

El espíritu de esta norma es garantizar el derecho a la información de los ciudadanos, conforme a las normas internaciones y a la constitución de 1998, que al igual que a la de 2008, consagraba este derecho, y persigue el objetivo de garantizar la protección de la información personal, objeto de investigación de la presente disertación, que se encuentre reposando en algún poder el sector público o privado.

El Ámbito de Aplicación de esta ley, son los organismos y entidades que conforman el sector público,[73] las personas jurídicas cuyas acciones o participaciones pertenezcan en todo o en parte al Estado, ONG's[74] que mantengan convenios o contratos con instituciones públicas o cuando la finalidad de su función sea pública; Las personas jurídicas privadas, que tengan cualquier forma contractual con el Estado, en los términos del respectivo contrato; Las personas jurídicas privadas, que se financien con recursos públicos y las personas jurídicas de derecho privadas que posean información pública.

Estos organismos o entidades, donde es aplicable esta ley, se puede manejar información de carácter personal, por motivos de su actividad, sea pública, privada o mixta, por cuanto, infiero que esta norma puede ser apropiada para proteger jurídicamente dicha información.

Para la presente norma, se considera Información Confidencial:

Art. 6. Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.

[72] Id. 71.
[73] N.B. Artículo 225 de la Constitución del Ecuador
[74] N.B. Las corporaciones, fundaciones y organismos no gubernamentales

No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las 5 declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas[75]

Se entiende por información confidencial, la que no está dentro del principio de publicidad, por lo que entendemos que, los datos personales sensibles, que son propios del derecho fundamental de la autodeterminación informática, protección de datos y derecho a la intimidad, no son parte del principio de publicidad, a pesar de que muchas veces se encuentres en estas instituciones públicas o privadas, donde se maneja información pública.

En el texto citado, inciso primero del artículo 6 de la ley,[76] se refiere a que son confidenciales que aquellos datos que sean derivados de los derechos fundamentales consagrados en los artículos 23 y 24 de la constitución de 1998, que son referentes a los derechos civiles, donde se encuentran los siguientes:

- Desarrollo de la personalidad
- Honra
- Guardar reserva de convicciones políticas y religiosas
- Identidad
- Elección libre acerca de la vida sexual

Estos derechos, son fundamentales, ciertamente, y podrían ser vulnerado si la información sensible de los ciudadanos, que muchas veces contiene datos acerca de las convicciones y elecciones del individuo, es revelada o filtrada, ya que resultado de esta difusión, se podría poner en duda la honra, identidad y en general la intimidad del titular. Esta es la justificación para que estos datos sensibles sean confidenciales.

En el caso de que se requiera esta información personal para investigaciones que realicen las autoridades, públicas competentes, se permitirá su acceso sin la reserva establecida; esta disposición es en pro del orden público y de impartir justicia por lo que es correcto.

[75] Op. Cit. 71. Art 6.
[76] Id. 75.

La custodia de la Información es responsabilidad de las instituciones públicas, deben crear y mantener registros públicos correctamente, para que los derechos de los ciudadanos se puedan ejercer a plenitud.

El título tercero, de la presente ley se refiere a la Información Reservada y Confidencial que es aquella que en la que no procede el derecho a acceder a la información pública. Esta información es:

a) Los documentos calificados de manera motivada como reservados por el Consejo de Seguridad Nacional, y

b) Las informaciones expresamente establecidas como reservadas en leyes vigentes.

Los datos personales sensibles de los administrados, están establecidos como reservados en constitución en la ley, por lo que entran en esta categoría. Aunque esta categorización no es muy clara, considero que los datos personales sensibles pueden ser sujetos a la aplicación de esta ley. No obstante la necesidad de crear procedimientos claros para el manejo y tratamiento de los mismos.

A continuación la ley establece los procedimientos y requisitos necesarios para acceder a la información pública, que son básicamente la solicitud con identificación del solicitante, a quien está dirigida, detalle de la información que se requiere y la finalidad que se le dará a la misma. El plazo que tiene la institución para su respuesta o como debe negarse y, bajo qué condiciones y requisitos que ya fueron analizados en el primer capítulo de la presente disertación.

La presente ley también establece el procedimiento de recurso de acceso a la información pública, catalogado como de justicia constitucional, existente en la constitución ecuatoriana de 1998. Sin embargo como ya se analizó actualmente existe la acción de acceso a la información pública, regulada por la Ley de Garantías Jurisdiccionales y Control Constitucional, también analizados.

Hay que puntualizar también que el mejor mecanismo para acceder a la información personal, en el Ecuador es el Habeas Data, ya que cumple con el objetivo de precautelar los datos, para que no sean mal utilizados y dar a conocer a su titular su tratamiento. Mientras que el acceso a la información pública, tiene un objetivo

diferente, el de fiscalizar o transparentar las actividades públicas y acceder a este tipo de información.

2.3.4. LA LEY ESPECIAL DE TELECOMUNICACIONES

En su artículo 14 declara que es prohibido a terceras personas divulgar la información sin el consentimiento de las partes como cito a continuación:

> *Art. 14.- DERECHO AL SECRETO DE LAS TELECOMUNICACIONES.- El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones*[77]*.*

Las telecomunicaciones son una de las innovaciones tecnológicas que contribuyen a la transferencia y difusión de grandes cantidades de información, a sus receptores y entre ellos, que en general son gran porcentaje de la población, por lo que la ley no permite que se interfiera estas redes de servicios.

Es posible que en la información que se transfiere por este medio estén presentes, se encuentre información personal sensible, y puede revelarse y dejar en evidencia la intimidad de sus titulares.

En el Artículo 39 de esta ley[78] están consagrada la protección de los derechos de los usuarios de las telecomunicaciones, y la protección al derecho a la privacidad en el contenido de las telecomunicaciones, como cito a continuación:

> *El Estado garantiza el derecho al secreto y a la privacidad del contenido de las telecomunicaciones. Queda prohibido interceptar, interferir, publicar o divulgar sin consentimiento previo de las partes la información cursada mediante los servicios de telecomunicaciones, bajo las sanciones previstas en la ley para la violación de correspondencia. Los operadores de redes y proveedores de servicios deberán adoptar las medidas necesarias, técnica y económicamente aceptables, para garantizar la inviolabilidad de las telecomunicaciones.*"[79]

Se establece entonces el derecho al secreto y privacidad en el contenido de lo que se transmita, y además que se debe solicitar el consentimiento previo de las

[77] REGISTRO OFICIAL 996, Fecha de publicación: 10 de agosto de1992, Ultima Reforma 13 octubre de 2011, *Ley Especial de Telecomunicaciones*
[78] Id. 77.
[79] Ibid. 78. N.B.: Artículo sustituido por Ley No. 94, publicada en Registro Oficial 770 de 30 de Agosto de 1995. Nota: Artículo sustituido por Art. 58 de Ley No. 4, publicada en Registro Oficial Suplemento 34 de 13 de Marzo del 2000.

partes, es decir el titular de la información y el emisor y responsable del servicio de las telecomunicaciones, y se tomaran las medidas para la inviolabilidad, precisamente para que esta información no se divulgue de una manera inadecuada.

Claramente, esta ley no tiene normas explicitas a cerca de la protección jurídica de los datos personales; por lo que hay que especificar que lo que se precautela en esta norma es la privacidad de las personas que brindan su información para diferentes propósitos dentro de los contenidos de los servicios de telecomunicaciones.

2.3.5. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS

Otra de las normativas que alberga la protección de los datos personales es La Ley de Comercio Electrónico, como cito a continuación:

Artículo 1 del Título Preliminar dentro del objeto de la ley se establece:

> *Regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas*[80].

Dentro de las circunstancias que regula esta ley, pueden estar inversas transferencias de datos personales sensibles.

Además esta norma, establece confidencialidad y reserva para los mensajes de datos, ya que la información que se transfiere en estos mensajes es de dominio del emisor y el receptor solamente, no puede interferirse o divulgarse. Toda violación a la confidencialidad como intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada.

Con esta norma, se protege el derecho a la intimidad en las comunicaciones y garantiza que no se filtre información sensible de los mensajes.

Acerca de la protección de los datos el artículo 9 establece que:

[80] Op. Cit. 58. Art 1

Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros[81]*.*

El consentimiento expreso del titular, es la forma que se determinado como ideal para hacerle conocer al interesado que su información va a ser utilizada o transferida, sin embargo la complejidad radica en cómo se recepta este consentimiento en la práctica, ya que debe ser expresa y se debe brindar los elementos necesarios para que el titular lo consienta.

Dentro de los procesos de La recopilación y uso de datos personales se guardara las medidas para la resguardar los *"derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente."*[82]

La ley también establece que:

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

Las fuentes accesibles al público, son las relacionadas con las funciones del Estado, por lo que el consentimiento es innecesario, y se entiende que son para usos de orden público, no obstante cuando pueda existir contacto con datos de particulares que puedan lesionar derecho, considero que debe valorarse los mismos, para que se garantice objetivamente los derechos de os titulares.

"El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo."[83]

Puede ocurrir que el titular después consentir en compartir sus datos, encuentre problemas con que se divulguen o procesen, por lo que se puede revocar el mismo, aunque no se establece la forma en que se debe revocar, concluyo que se lo debe hacer por escrito y debe ser expreso, es decir de la misma forma como se consintió.

[81] Ibid. 80. art. 9.
[82] Id. 81.
[83] Id. 82.

El artículo 32 de la ley de comercio electrónico, protege a los datos, por parte de las entidades de certificación de información acreditadas, afirmando que *"Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley"*[84]

Las entidades de certificación como son los registros públicos o en general cualquier entidad pública, que emita alguna certificación debe guardar las medidas jurídicas y técnicas para la protección de los datos sensibles, en virtud del artículo 9 y sin duda las garantías establecidas en la constitución, es decir siempre con la autorización o conocimiento del titular de la información.

Esta ley, instauraba reformas al Código Penal, incluyéndose al artículo 202 con el objetivo de no violar la intimidad de los titulares de datos personales, que ya se analizaron anteriormente.

Por último la ley de comercio electrónico, coloca en el glosario de términos los siguientes:

> ***Intimidad:*** *El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.*
>
> ***Datos personales:*** *Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.*
>
> ***Datos personales autorizados:*** *Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.*[85]

Esta ley, es relevante en el tema investigado, por cuanto intenta proteger los datos dentro de las comunicaciones y comercio que se mantenga por un medio electrónico.

La ley de comercio electrónico, tiene su reglamento, Decreto Ejecutivo 3496, publicado en el Registro Oficial 735 el 31 de diciembre de 2002, que en relación a la protección de datos personales, en el artículo 21 establece que para la prestación de

[84] ibid. 83. art. 32.
[85] ibid. 84. disposición general novena.

servicios electrónicos, que impliquen el envío por parte del usuario de información personal, se requerirá el empleo de sistemas seguros, que no permitan su difusión.

La información que debe brindarse al usuario acerca del servicio que se le está brindando, es obligación de los presta.

Esta información debe contener en detalle las medidas de seguridad que se le brinda a los datos, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema que se ofrece cumple con la ley.

Este conocimiento del servicio por parte del usuario, delega en cierto sentido la responsabilidad de sus datos al usuario, quien decidirá si admite el servicio y por ende el grado de protección de tendrán sus datos. Es claro que la participación del titular es importante, porque él es quien dispone de su información y debe escoger la mejor opción a la hora de precautelar su información sensible.

Los datos objetos de esta protección son aquellos datos sensibles del consumidor sus datos personales, información financiera, través de los cuales puedan cometerse fraudes o ilícitos que afecten sus derechos**.**

Por el incumplimiento de las disposiciones contenidas en este reglamente en cuanto a la falta de veracidad o exactitud en la información, o sobre seguridades, garantizar la confiabilidad del intercambio de datos ofrecida al consumidor, el organismo de control, en este caso la Superintendencia de telecomunicaciones, podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria o podrá incluso ordenar la suspensión del acceso al servicio, como puede ser un sitio web o proveedor de servicios electrónicos, hasta que se cumplan las condiciones legales para que continúe con sus actividades.

2.4. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LEYES EXTRANJERAS

En diferentes países ya se ha tratado el tema de Protección jurídica a los datos personales de sus ciudadanos, con la promulgación de leyes que permiten llevar a cabo estas normas de seguridad, con el objetivo de que el titular, conozca el destino que se le está dando a la misma, en el caso de que sea sometida a tratamiento por parte de alguna institución pública o privada.

Como ha lo hemos puntualizado, existe avance en el tema en la Unión europea y particularmente en España, que tiene la Ley Orgánica de Protección de datos, ley en la que he basado bastante de la presente investigación y que establece los principios básicos en el tema, regula los procedimientos para el ejercicio de los derechos que tiene el titular sobre su información y propone medidas de seguridad tanto técnicas como jurídicas con el objetivo de que no se dé un mal uso a los datos o que no se filtren en ninguno de los procesos y finalmente evitar que se violente el derecho a la intimidad.

Para mi presente investigación tome países latinoamericanos para el análisis correspondiente a la protección de datos, ya que son países con realidades similares a la nuestra, a pesar de no tener un nivel de protección jurídica igual a la nuestra.

El objetivo es crear regulación importante en cuanto al tratamiento de los datos sensibles y por ende la protección jurídica que debe existir en todos estos procesos.

2.4.1. COLOMBIA

En el vecino país colombiano, se ha trabajado en una ley expedida el 17 de octubre de 2012, la Ley 1581 de 2012, Ley Estatutaria de Protección de Datos Personales (LEPD), que se hizo obligatoria también, para las empresas a partir del 18 de abril de 2013.

Igualmente, existe una ley especial, la ley 1266 de 2008, para los datos personales financieros, que se recolectan y usan para cálculo de riesgo crediticio, que también son sujetos de protección jurídica por ser sensibles para su titular.

La sentencia c-748 de 201127, de Agosto de 2012, trata de una decisión constitucional sobre ley de protección de datos personales, en la que se revisa el texto de la ley, por lo que se convertirá en un referente para su interpretación y alcance.
De igual forma, al ser un referente para la interpretación de la futura ley, lo será también para su reglamentación.

2.4.2. CHILE

Chile es uno de los países latinoamericanos que más ha despuntado realizando gran cantidad de análisis en el tema de protección y tratamiento de datos; por ello la importancia de citar algunas de sus conclusiones para el desarrollo de la presente disertación.

Primero, los datos personales, especialmente protegidos jurídicamente son los catalogados como sensibles y la ley Chilena 19.628, sobre Protección de Datos Personales, en su artículo 2 letra g los define como:

> *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*.[86]

Considero esta definición es vital, primero porque permite la existencia de seguridad jurídica ya que al tener claro que datos son protegidos, la administración sabrá en qué medida debe poner en acción su aparataje administrativo para este fin, además que crea un límite para el individuo, ya que solo puede reclamar la reparación del derecho en el caso de exista una lesión notoria por la divulgación de estos datos sensibles.

El Habeas Data, constituye, la garantía esencial de protección de datos y sus facultades en Chile, están reguladas por la ley de protección de dato personales, dentro del Título II sobre "Derechos de los titulares de datos", ya que se entiende como un ejercicio que deviene del derecho del titular de la información a disponer de ella, y se ejerce ante quien aparezca como responsable del registro.

2.4.3. México

En México también existe la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), que evidencia el desarrollo legal que este país mantiene en cuanto a la protección de la información personal

Esta ley, define como dato personal a: Cualquier información concerniente a una persona identificada o identificable, y estos son los datos que son sujeto de especial atención en el ordenamiento jurídico.

---

[86] HUICHALAF, Pedro. *De la Protección de Datos Personales en Chile*. http://oiprodat.com/tag/proteccion-de-datos/, Acceso: 13 de febrero de 2014.

Asimismo, México tiene un órgano ocupado solo de la regulación y control de la información pública, llamado Instituto Federal de Acceso a la Información Pública, el cual en Pleno. Este órgano, emitió los Lineamientos Generales para la Clasificación y Desclasificación de la Información de las Dependencias y Entidades de la Administración Pública Federal; que clasifica a los datos personales como información confidencial, es decir que no son accesibles a todos los ciudadanos. Estos datos son:

- Origen étnico o racial;
- Características físicas;
- Características morales;
- Características emocionales;
- Vida afectiva;
- Vida familiar;
- Domicilio particular;
- Número telefónico particular;
- Patrimonio;
- Ideología;
- Opinión política;
- Creencia o convicción religiosa;
- Creencia o convicción filosófica;
- Estado de salud física;
- Estado de salud mental;
- Preferencia sexual, y
- Otras análogas que afecten su intimidad, como la información genética.

Algo novedoso es que estos datos personales, serán confidenciales en todos los casos incluso cuando no hayan sido obtenidos de su titular.

También se consideran confidenciales y jurídicamente protegidos, los datos de una persona fallecida, y los únicos que podrán tener acceso y disposición sobre ellos son el cónyuge y los familiares en línea recta ascendente o descendente sin limitación de grado, y en línea transversal hasta el segundo grado. Y en caso de que no existan

familiares con este parentesco, los parientes en línea transversal hasta cuarto grado tendrán derecho a solicitar la corrección de datos.[87]

2.4.4. Uruguay

En Uruguay existe la Ley N° 18.331, aprobada el 11 de agosto de 2008, sobre Protección de Datos Personales y Acción de Habeas Data.

Este cuerpo legal, es bastante avanzado con relación a los preceptos establecidos en Latinoamérica, y establece que *"el derecho a la protección de datos personales es inherente a la persona humana"*[88].

También en Uruguay existe un órgano regulador en este sentido, llamado, La Unidad Reguladora y de Control de Datos Personales (URCDP) fue creada por el artículo 31 de la Ley N° 18.331, se trata de un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento de Uruguay AGESIC.

Uruguay ha sido reconocido como país adecuado en materia de datos personales por la Unión Europea, y también ha sido el primer país en América Latina en ser invitado a adherir al Convenio 108 del Consejo de Europa; y fue designado como anfitrión de la 34ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad, la que se realizó en Punta del Este, en 2012.[89]

2.4.5. Argentina

En Argentina, existe la Dirección Nacional de Protección de Datos Personales (DNPDP), como órgano de control para la efectiva protección de los datos personales. La Ley 25.3264, de Protección de Datos Personales tiene como objeto:

> *La protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como*

---

87 *Ley Federal de Federal de Protección de Datos Personales en Posesión de Particulares* (LFPDPPP), http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf, Acceso: el 20 de marzo de 2014 a las 18h13

88 *Ley de Protección de datos personales y Acción de Habeas Data*. http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Anchor, ingresado el 2 de marzo de 2014 a las 16h00

89 *La Ley 25.3264, de Protección de Datos Personales*, http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/texact.htm, Acceso el 20 de marzo de 2014 a las 18h29.

también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

Argentina, es el país pionero en cuanto a la regulación de la protección de datos personales, por cuanto fue primer país que emitió una ley en este sentido y el primero que creo un órgano fiscalizador y regulador relativo al tratamiento y manejo de los datos de carácter personal.

2.4.6. Perú

Perú, también tiene una ley para este propósito, la Ley 29733, Ley de Protección de Datos Personales, que tiene por objeto garantizar el derecho fundamental a la protección de datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

La Ley fue reglamentada por el Decreto Supremo 003-2013-JUS.

Esta ley, define a los datos personales como: "*Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados*".

Asimismo, define como datos sensibles:

Datos personales constituidos por datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud y a la vida sexual.

El reglamento tiene por objeto desarrollar la Ley 29733, a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto para las entidades públicas como para las instituciones pertenecientes al sector privado.

Sus disposiciones constituyen normas de orden público y de cumplimiento obligatorio.

Los principios rectores que la ley establece, son:

- legalidad
- consentimiento
- finalidad
- proporcionalidad
- calidad
- seguridad
- disposición de recurso
- nivel de protección adecuado.

Los derechos del titular de datos personales, son:

- información
- acceso
- actualización
- inclusión
- rectificación
- supresión
- impedir el suministro
- oposición
- tratamiento objetivo
- tutela.

2.4.7. Nicaragua:

En Nicaragua existe la ley 787 de Protección de los Datos personales, que sigue los lineamientos del modelo europeo de protección de datos.

2.5. ANÁLISIS DE JURISPRUDENCIA DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES

Para el mejor análisis práctico de la manipulación de datos personales son consentimiento de su titular, citare y analizare algunas jurisprudencias y casos relevantes:

En España, se ha desarrollado jurisprudencia al respecto del derecho fundamental de la protección de datos personales, como son las sentencias 254/1993, 11/1998 y 292/2000, entre otras, que han impuesto el objeto y alcance de esta protección y que generan postulados importantes en cuanto a la implementación de este derecho en el sistema jurídico, por lo que realizare un análisis breve de cada una de ellas:

2.5.1. SENTENCIA ESPAÑOLA 254/1993, DE 20 DE JULIO DE 1993 DEL TRIBUNAL CONSTITUCIONAL. RECURSO DE AMPARO

La presente sentencia se trata de un recurso de amparo presentado ante la Sala Primera del Tribunal Constitucional, por el Procurador en contra la denegación presunta de un Gobernador Civil y del Ministro del Interior, de una solicitud relativa a los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado, confirmada en la vía contencioso-administrativa.[90]

En los antecedentes se establece que el recurrente en el año 1986, fundamentado en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[91]; solicita:

- Que se le comunique si en los ficheros estatales constan sus datos de carácter personal

- De ser así, que se le comunique con que finalidad de los ficheros, y por ende de los datos personales que ahí son almacenados, la autoridad que nos controla y su residencia habitual

- Que se le comunique que datos son los que se almacenan

Cabe anotar que precisamente se trata de un ejercicio de su derecho de acceder a sus datos personales, propio del derecho objeto de la presente disertación.

---

[90] *Sentencia Española 254/1993*, de 20 de julio de 1993 http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/x13._Sentencia_254-1993_de_20_julio_1993._def.pdf, ingresado el 21 de febrero de 2014 a las 12 h 53

[91] N. B. Hecho en Estrasburgo el 28 de enero de 1981, y ratificado por España mediante Instrumento de 27 de enero de 1984 (publicado en el «B.O.E.» de 15 de noviembre de 1985, y que había entrado en vigor de forma general, y para España, el anterior día 1 de octubre)

Esta solicitud que nunca fue contestada por la administración bajo ninguna figura. Una vez denunciada la mora, se interpone un recurso judicial[92], que fue desestimado en las dos instancias**.**

En Audiencia se desestimó el recurso contencioso-administrativo ya que aunque la petición del actor goza de apoyo mediato en el Convenio, sus preceptos no pueden ser aplicados directamente ya que la ejecución de los tratados o convenios puede exigir medidas legislativas y reglamentaria interna para la aplicación de práctica de sus disposiciones es España.

La cuestión dentro del recurso de amparo es determinar si la negativa a la solicitud de suministrar los datos personales del actor, que la Administración del Estado posee, vulnera o no los derechos fundamentales a la intimidad y a la propia imagen que reconoce la Constitución.

Se establece que los derechos consagrados en la constitución son exigibles y procedentes a pesar de que el recurrente se haya fundamentado en convenios internaciones o a pesar del argumento del Gobernador de no tener la posibilidad física y material de responder a esta solicitud

Igualmente se establece la competencia del gobernador de responder a la solicitud.

Otra cuestión de este recurso es determinar si las dos primeras letras del art. 8 del Convenio del Consejo de Europa sobre protección de datos personales surten efecto directo, o en su caso interpretativo, en relación con los derechos fundamentales de la Constitución.

El creciente uso de la informática en los procesos de administración y gestión han descuidado la protección de los datos, por sobre los demás Derechos naciones por cuanto gran parte de las decisiones que afectan a los individuos descansan en datos registrados bases públicas, sin embargo muchos errores son causados por el uso no controlado de estos datos personales de los ciudadanos y no pueden ser

[92] N. B. Recurso judicial fundamentado en el interesado fundó su solicitud en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, y ratificado por Instrumento de 27 de enero de 1984 (publicado en el «B.O.E.» de 15 de noviembre de 1985). En el «Boletín Oficial del Estado» se hace constar que el Convenio entró en vigor de forma general y para España el 1 de octubre de 1985, tras haber sido ratificado por cinco de los Estados contratantes, de conformidad con lo establecido en su art. 22.2.

afrontados por los particulares afectados, ya que no se encuentran en posibilidad de reclamar, rectificar o prevenir su mal uso.

Gran parte de la discusión jurídica dentro de la presente sentencia es el efecto vinculante que este constitucional reconoce a los Tratados permite hacer valer los derechos recogidos en el art. 8 del Convenio de protección de datos, sin embargo esto suscita una cuestión ajena al recurso de amparo, por lo que se concluye que:

> La adecuación de una norma legal, o de una disposición o actuación de los poderes públicos, a lo preceptuado por un tratado internacional, y por consiguiente si las autoridades españolas han cumplido o no los compromisos derivados de un acuerdo internacional, son cuestiones que, en sí mismas consideradas, resultan indiferentes para asegurar la protección de los derechos fundamentales comprendidos en la Constitución española, que es el fin al que sirve la jurisdicción de este Tribunal en el ámbito del recurso de amparo.[93]

En la constitución española, como la mayoría de cartas fundamentales garantiza el ejercicio de derechos, sin embargo se establece que *"la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*"[94].

Se infiere de esta forma que se ha incorporado una nueva garantía constitucional en este caso, para contrarrestar la amenaza de a la dignidad de los ciudadanos; por lo que nos encontramos ante una garantía que precautela del honor y la intimidad y que se trata de un derecho y libertad, para defenderse de posibles agresiones a la dignidad y al uso ilegítimo del tratamiento de datos que pueden ocurrir ante el inevitable uso de la informática.

No obstante, este razonamiento también posee problemas, como la ausencia de un desarrollo legislativo al respecto, pero a pesar de este antecedente, para el momento histórico de este fallo, no se puede, negar los derechos constitucionales fundamentales, que vinculan a los poderes públicos y son "*origen inmediato de derechos y obligaciones, y no meros principios programáticos*."[95]

Se concluye entonces que este principio general de aplicabilidad inmediata tiene más excepciones que las que imponga la propia Constitución.

---

[93] Op. Cit. 90.
[94] Id. 93.
[95] Id. 94.

Por lo que el Tribunal decide otorgar el amparo y, en consecuencia anular la denegación administrativa de la información; Declarar el derecho del actor a que las autoridades administrativas demandadas le comuniquen sin demora la información solicitada por él, en los términos expuestos en el último fundamento jurídico.

Comentario:

Este caso es un ejemplo del ejercicio del derecho fundamental de protección de datos personales, y las facultades, relativas a este derecho, como por ejemplo el acceso y disposición de la información, por parte de su titular, que posee datos que se encuentras reposando en bases de datos o ficheros públicos.

Como se explicó en la sentencia citada con anterioridad, el derecho debe ser garantizado no solo en forma de principios, sino también, de manera que se pueda materializar esta tutela consagrada en la Constitución y las leyes la mayoría de países.

2.5.2. SENTENCIA ESPAÑOLA 11/1998 DE 13 DE ENERO DE 1998 ANTE EL TRIBUNAL CONSTITUCIONAL. RECURSO DE AMPARO.

En la presente sentencia la Sala Primera del Tribunal Constitucional, conoce acerca del recurso de amparo núm. 2.264/96, en contra de la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid, de 30 de junio de 1995, dictada en procedimiento de tutela de derechos fundamentales.

Antecedentes:

El ahora recurrente, afiliado aun sindicato de trabajadores, presta servicios para una empresa y el Comité General de Empresa convocó huelga, apoyada por ciertos sindicatos relacionados. Pese a que el recurrente no participó en la huelga y así lo comunicó a la se le descontaron retribuciones a las que tenía derecho.
Este descuento, que nunca fue reconocido, afecto a los empleados que afiliados al sindicato y también aunque en menor medida a los trabajadores afiliados a otros sindicatos y a los que no tenían ninguna afiliación.

Se debe tener en cuenta que la empresa conoce el dato de la afiliación.

El trabajador, entonces, formula una demanda por la tutela de sus derechos fundamentales, dentro de la Litis se condenó a la Empresa a indemnizar al demandante, por la lesión de su derecho a la libertad sindical ya que este tipo de información o datos están especialmente protegidos ha sido utilizado para una finalidad distinta a la que debe tener.

Por estos hechos el Director de la Agencia de Protección de Datos, en Resolución de 18 de diciembre de 1995, impuso a la Empresa una multa por la infracción ya que de la prueba se desprende que existió una afectación a trabajadores afiliados a los Sindicatos convocantes de la huelga.

La demanda de amparo,[96]

En la parte pertinente para la presente disertación, en la sentencia se dice que:

> *Un dato que pertenece a la privacidad del trabajador, que posee la Empresa con una exclusiva finalidad -descontar la cuota de afiliación sindical- sirve para impartir instrucciones al sistema informático y que se descuenten todos los días de paro a los que tienen la clave 893, correspondiente a los afiliados a CC.OO, atenta contra la privacidad del trabajador*[97]

Por esta razón la Agencia de Protección de Datos en Resolución de 18 de diciembre de 1995, impuso una multa por una infracción tipificada[98]

La acción de Amparo fue admitida a trámite, y el Fiscal ante el Tribunal Constitucional se refirió al otorgamiento del amparo por lesión del derecho de libertad sindical.

En general el amparo gira en torno a la lesión del derecho fundamental a la libertad sindical; A criterio de la Sala, los elementos de la Sentencia legitiman la actuación de la Empresa en el descuento generalizado de cantidades a personas afiliadas al Sindicato; Sin embargo, para la solución de la litis no interesa tanto si se descontaron sumas a personas afiliadas o no afiliadas a los Sindicatos no convocantes, como el hecho del método usado para llevar a cabo el descuento que es

---

[96] *Sentencia Española 11/1998 de 13 de Enero de 1998*. http://hj.tribunalconstitucional.es/HJ/es-ES/Resolucion/Show/SENTENCIA/1998/11, ingresado el 22 de febrero de 2014 a las 15h00

[97] Id. 88

[98] N. B. Esta conducta se encuentra tipificada en como muy grave en el art. 43.4 c) de la Ley Orgánica 5/1992.

la utilización del dato informático o clave de su nómina sin una averiguación alternativa.[99]

Lo importante es señalar que la sentencia forma parte de la protección de datos personales ya que el dato de la afiliación sindical es atinente a la ideología del individuo y por tanto parte de su información sensible. La utilización fuera de propósito de un dato entregado voluntariamente, puede repercutir en la intimidad del individuo o incluso causarle un daño material como lo vemos en este caso.

En este caso se ven claramente afectados los derechos de la libertad sindical, "*cuales son la afiliación o no a un sindicato, la actividad sindical y la consecución de un cierto grado de indemnidad por la pertenencia a una organización sindical*[100]", que responden a una inclinación ideológica del individuo y que debe ser respetada por sus pares.

No existe prueba alguna en el proceso, que acredite error en por parte de la empresa en los descuentos a sus trabajadores.

Respecto al derecho de protección de datos personales, se relaciona, en este caso con la garantía de la intimidad, se dice que:

> *Adopta hoy, un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención*.[101]

Además, se debe tomar en cuenta que el dato de afiliación sindical del trabajador, fue otorgado por su titular, con el único objetivo licito de que descontara de la retribución la cuota sindical y la transfiriera al Sindicato, de acuerdo con la ley; pero el dato, fue objeto de un tratamiento automatizado y se hizo uso de la correspondiente clave informática para una finalidad totalmente distinto que fue retener la parte proporcional del salario relativa al período de huelga**.**

El hecho que el responsable de la dependencia donde el recurrente presta servicios había participado que éste no se adhirió a la huelga, la Empresa procedió al

[99] Cfr. Op. Cit. 96.
[100] Id. 99.
[101] Id. 100.

descuento in realizar una comprobación simplemente lo presumió, por lo que esto agrava la situación, y pone en evidencia el manejo incorrecto de los datos personales, en este caso la filiación sindical de los trabajadores; se corrobora por lo tanto que tan sólo el 1 por cien de los errores afectara a trabajadores afiliados a otros sindicatos o sin militancia sindical conocida.

Por tanto, estamos ante una decisión unilateral del Empresario da mal trato al trabajador, por razón de su adhesión a un Sindicato que le pudiera perjudicar.
En relación a la protección de datos personales, la constitución española en el art.18.4, en su último inciso establece las limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, lo que significa que, en ciertos casos como el presente, este derecho corresponde a un orden instrumental con el objetivo de la protección de otros derechos fundamentales, entre los que se encuentra, la libertad sindical, que en este caso es el derecho que ha sido vulnerado.

Posterior al debate se concluyó que si hubo una lesión tangencial a la protección de datos personales, y que éste, no sólo es un instrumento de protección de los derechos del individuo frente al uso de la tecnología informática, sino que además, consagra un derecho fundamental autónomo que controlar el flujo de información que relativas a cada persona, pertenezcan o no al ámbito de la intimidad, para así preservar el pleno ejercicio de sus derechos. Este derecho evita que la automatización de los datos personales propicie comportamientos discriminatorios. En este caso se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra distinta y así se perjudico ejercicio del derecho de libertad sindical.

Otro análisis interesante de la corte, en este caso es que: “la vulneración de derechos fundamentales no queda supeditada a la concurrencia de dolo o culpa en la conducta del sujeto activo, a la indagación de factores psicológicos y subjetivos de arduo control.” Es decir que solo hace falta un nexo de causalidad entre el hecho y el perjuicio para determinar la vulneración.

La Corte falla, entonces, y decide reconocer al recurrente su derecho a la libertad sindical, y declarar la nulidad de la Sentencia recurrida.

Comentario:

Esta sentencia, me pareció importante, ya que revela otra realidad, en donde los datos personales objeto de protección, en este caso un dato sensible, al tratarse de la filiación sindical del recurrente, se encuentran en un medio diferente a los ficheros públicos, y más bien revelan más información que las registrales, y su mal uso, sin consentimiento del titular, ocasionan un perjuicio material en su derecho al trabajo y a su intimidad.

Por ende la resolución del caso es reconocer la libertad sindical y con ello permitir que no se utilice la información personal de este ciudadano, con el fin de que se elabore un perfil de su persona errado y además utilizado para fines no legítimos.

2.5.3. SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA DE 13 MAYO DE 2014:

La presente sentencia es entre la Empresa Google[102], y la Agencia Española de Protección de Datos por la reclamación de un ciudadano español, por cuanto se discute el alcance la Protección Jurídica de los Datos Personales y protección de las personas físicas en lo que respecta al tratamiento de dichos datos cuando están contendidos en internet y la participación de los motores de búsqueda en Internet.

La situación jurídica principal en la presente sentencia es una petición de decisión prejudicial que versa sobre la interpretación de la Directiva 95/46/CE[103]

Esta Directiva 95/46 es parte del Derecho Español por la ley Orgánica 15/1999, de 13 de diciembre, relativa a la protección de datos de carácter personal.[104]

Litigio Principal y cuestiones prejudiciales

Se presentó ante la AEPD[105], una reclamación contra *La Vanguardia Ediciones, S.L.,* que realiza publicaciones de un periódico de mucha difusión, y contra Google; ya que el momento de introducir el nombre del reclamante en *el motor de búsqueda de*

[102] N.B. Google Spain, S.L., Google Inc.
[103] N.B. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
[104]N.B. Publicada en el Boletín Oficial del Estado Español nº 298, de 14 de diciembre de 1999, p. 43088).
[105] N.B. Agencia Española de Protección de Datos

Google[106] se obtenían vínculos del periódico *La Vanguardia*, donde aparecía un anuncia de subasta de inmuebles por un embargo por deudas a la Seguridad Social.

En la reclamación, se solicitaba:

- Que *La Vanguardia*, elimine o modifique la publicación para que no aparezcan datos personales del reclamante, o utilizar herramientas en los motores de búsqueda para proteger estos datos.

- Que Google elimine u oculte los datos personales del reclamante para que no se incluyan en los resultados de búsqueda y dejen de ser ligados a los enlaces de *La Vanguardia*

Esto en virtud de que el reclamante ya solucionó el embargo publicado en La Vanguardia.

La AEPD desestimó la reclamación ya que la publicación en La Vanguardia, estaba legalmente justificada, por orden del Ministerio de Trabajo y Asuntos Sociales; sin embargo consideró que "*quienes gestionan los motores de búsqueda están sometidos a normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información*"[107]

Por esto la AEPD, consideró estar facultada para ordenar retirar e imposibilitar el acceso a ciertos datos, en los motores de búsqueda en los casos en los que su difusión "*puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en su sentido amplio*"[108]. Y por ende la voluntad del afectado de que sus datos no sean conocidos por terceros.

Google, por su parte interpuso recursos contra la resolución de la AEPD, ante la Audiencia Nacional.

---

[106] *Sentencia del Tribunal de Justicia de la Unión Europea*, de 13 de mayo de 2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=245907, acceso el 21 de mayo de 2014

[107] Id.106.

[108] Id.107.

El tribunal manifiesta que la cuestión es determinar cuáles son las obligaciones de los gestores de motores de búsqueda en la protección de datos personales de los interesados en que no desean que sus datos publicados en páginas web, sean relacionados con las mismas.

La respuesta de esta cuestión, depende de la interpretación que se le dé a la Directiva 95/46, en relación con las tecnologías desarrolladas después de su publicación.

En este orden de ideas, es necesario entender que la actividad que realiza un motor de búsqueda como Google, es encontrar información publicada en Internet e indexarla automáticamente, almacenarla temporalmente y proveer de ese contenido al internauta

Este proceso se consideraría tratamiento de datos personales, ya que pone a disposición de los usuarios de internet información personal; Sin embargo, en este punto, no se precisa si de ser este el caso de tratamiento de datos personales, el gestor de un motor de búsqueda como Google, debe considerarse responsable de dicho tratamiento.

Según Google la actividad de los motores de búsqueda, no puede considerarse como tratamiento de datos ya que se solo se muestra páginas web de terceros, además solo tratan la información accesible en internet sin haya una diferencia entre datos personales y el resto de información. Y aun así el gestor no puede ser considerado responsable de ese tratamiento ya que desconoce dichos datos y no tiene control sobre ellos.

Por otro lado, el reclamante junto con los Gobiernos español, italiano, austriaco y polaco y la Comisión Europea, sostienen que dicha actividad implica un tratamiento de datos según la Directiva 95/46, distinto al tratamiento de datos realizado por los editores de sitios en Internet, y por ello el gestor es responsable del tratamiento de datos "*efectuado por él desde el momento en que es él quien determina la finalidad y los medios de dicho tratamiento*"[109].

[109] Id. 108.

Según Grecia, la dificultad radica en que las empresas que gestionan los motores de búsqueda, no pueden considerarse responsables del tratamiento de los datos sino solo cuando almacenan los datos en una "*memoria oculta o memoria intermedia por un periodo de tiempo que supere lo técnicamente necesario*"[110]

Por todo esto, se considera que los gestores de un motor de búsqueda en internet recoge, extrae, registra y organiza los datos y en sus programas de indexación comunica y facilita el acceso a sus usuarios; y estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46, por lo que deben calificarse de tratamiento en el sentido de dicha disposición.

Igualmente, se debe entender que el artículo 2, letra d), de la Directiva 95/46 define al responsable como "*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales*"[111]. El gestor del motor de búsquedas es quien determina los fines y los medios de esta actividad y, así, del tratamiento de datos personales que efectúa él mismo, por consiguiente, debe considerarse responsable de dicho tratamiento,

Cabe recalcar que la actividad que realizan los motores de búsqueda es fundamental en la difusión global de dichos datos ya que facilita el acceso a los mismo, y por esta razón puede afectar a la de los editores de sitios de Internet, a los derechos fundamentales de privacidad y de protección de datos personales;

> El motor de búsqueda *como persona que determina los fines y los medios de esta actividad, debe garantizar, que dicha actividad satisface las exigencias de la Directiva 95/46 para que las garantías establecidas en ella puedan tener pleno efecto y pueda llevarse a cabo una protección eficaz y completa de los interesados, en particular, de su derecho al respeto de la vida privada.*[112]

> El hecho de que los editores de sitios de internet indiquen a los gestores de motores de búsqueda que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores, no significa que la falta de tal indicación por parte de estos editores libere al gestor de un motor de búsqueda de su responsabilidad por el tratamiento de datos personales que lleva a cabo en el marco de la actividad de dicho motor.

[110] Id. 109.
[111] Id.110.
[112] Id. 111.

Esto no cambia que el gestos determina los fines y medos de este tratamiento y no elimina la responsabilidad del gestor, "*ya que el artículo 2, letra d), de la Directiva 95/46 prevé expresamente que esta determinación puede realizarse «sólo o conjuntamente con otros*".

Por todo lo expuesto, debe interpretarse la Directiva 95/46 de la siguiente forma:

- La actividad de un motor de búsqueda, debe calificarse de tratamiento de datos personales, cuando esa información contiene datos personales.

- El gestor de un motor de búsqueda debe considerarse responsable de dicho tratamiento

De Igual forma, se concluye que la Directiva 95/49 se de interpretar en el sentido de que:

> *Para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.*

Relativo los derechos del titular de los datos personales, garantizados por la Directiva 95/46, se tendrá que examinar, si el interesado tiene derecho a que sus datos ya no estén vinculados a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de su nombre, sin que esto presuponga que la inclusión de la información personal en la lista de resultados en sí, cause un perjuicio, ya que se puede acceder a datos de la vida pública del titular de manera justificada.

Tribunal de Justicia declara:

- El artículo 2, letras b) y d), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, debe interpretarse de la siguiente forma:

    - La actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de tratamiento de datos personales, cuando esa información contiene datos personales.

    - El gestor de un motor de búsqueda debe considerarse responsable de dicho tratamiento.

- Para el artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse dentro del tratamiento de datos personales, como responsable que el gestor de un motor de búsqueda, cuando crea en el Estado miembro una sucursal destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro.

- Para los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46, se debe interpretar que:

  Para respetar los derechos que establecen estas disposiciones, siempre que se requisitos establecidos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.[113]

- Por último para la aplicación los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46, se debe que examinar, en particular, si el titular

[113] Id. 112.

de los datos personales tiene derecho a que dicha información ya no sea, "*vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre*"[114], sin que esto presuponga que la inclusión de esta información en la lista de resultados cause un perjuicio al interesado; ya que esto pude afectar otros derechos como el interés económico del gestor del motor de búsqueda, o el derecho del público en acceder a la por razones concretas, como el papel desempeñado por el interesado en la vida pública.

Comentario:

La sentencia citada anteriormente, se constituye en una decisión importante en cuanto a la protección jurídica de los datos personales subidos a la nube de la información, tomando en cuenta que no se ha hablado del tema mayormente en nuestro medio y el desarrollo tecnológico potenciado anualmente en el mundo.

Es necesario entender que el Tribunal de Justicia de la Unión Europea, en esta sentencia pretende solucionar el problema de interpretación de la Directiva 95/46, ya que esta norma es claramente anterior a la aparición de esta problemática propia del acceso y transferencia de información personal por internet; sin embargo con este fin trata temas importantes que deben ser discutidos también, como por ejemplo si reamente se considera un tratamiento de datos personales lo que hace la empresa Google, y el alcance de su responsabilidad, así como el alcance de los derechos del titular de los datos personales y su "*derecho al olvido*" en internet, es decir requerir a los motores de búsqueda como Google eliminen o bloqueen los enlaces a contenidos que perjudican sus intereses o ya no son oportunos.

Por ello es necesario también hacer las siguientes precisiones como que el Tribunal dictaminó que Google, icono principal de búsquedas en internet, retire resultados de búsquedas si los enlaces obtenidos contienen datos personales, cuando un ciudadano interesado lo solicite así, y siempre que se cumpla con los preceptos establecidos en la ley. Esto, incluso cuando las páginas web que contengan la información personal no la eliminen o cuando su publicación en la web sea licita.

Es importante entonces entender la importancia de las herramientas informáticas en estos casos, ya que solo estas nos permiten hacer bloqueos o

[114] Id. 113.

rectificación de información en la web, por lo que se debe mantener una relación estrecha entre los avances tecnológicos y nuestra realidad tanto jurídica como social.

En cuanto al derecho al olvido, podríamos decir que es la facultad del ciudadano a que se eliminen sus datos personales en la red, cuando ellos le causen un perjuicio o cuando ya no sean precisos o actuales. Y Según la Agencia Española Protección de Datos, "*su ámbito de aplicación coincide con el que corresponde a los derechos de cancelación y oposición*"[115].

Este derecho al olvido tiene relación con la facultad que tenemos todos a disponer de nuestros datos personales, con el fin de que su divulgación no nos cause un perjuicio nuestra vida privada o buen nombre, por ello es una decisión de cada uno sobre la imagen que los demás tienen de nuestra persona, y se constituye en una facultad perfectamente legítima.

En el desarrollo de la sentencia analizada, se hace una importante referencia a la Directiva 95/46 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación los mismos, ya que se discute acerca de la interpretación que se le debe dar a sus disposiciones en España, en cuanto a las actividades de los motores de búsqueda en internet; por lo que debe establecer que Google deberá someterse a las legislaciones europeas de protección de datos ya que tiene una filial en el territorio de los países miembros aunque éstas sean "*una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios*".

Otra de las conclusiones importantes de la sentencia es que puede imperar la protección de datos, no necesariamente personales o sensibles sobre el interés económico de los gestores de motores de búsquedas, a menos que el afectado tenga una relevancia pública o que el acceso a esta información sea justificado por el interés público; ya que como hemos establecido antes el derecho fundamental a la protección de datos personales tiene límites en el ejercicio del derecho de los demás y el orden público.

Este fallo es relevante para la presente investigación ya que además de ser un precedente en toda la Unión Europea, porque es necesario determinar que sucede con los datos personales presente en la web, como si puede el titular disponer de ellos y

[115] Id. 114.

ejercer su derecho de rectificación, a pesar de que se puede acceder a ellos por un medio universal, entre otras cuestiones bastante presentes en nuestros días gracias al uso creciente de estos medios informáticos. Y ya que es importante entender que la problemática jurídica de la vulneración al derecho fundamental a la protección de datos personales, se extiende no solo a los ficheros de instituciones registrales, entes públicos o empresas privadas, sino que también está latente en la web y sistemas informáticos, por lo que le corresponde al derecho regular todos estos supuestos con el fin de precautelar la intimidad e información de sus ciudadanos

A lo largo del litigio Google argumenta que la responsabilidad en este sentido es propia de los editores de las páginas webs, ya que su actuación era solo de un intermediario neutral, sin embargo se dictamina que Google es en parte responsable de dichos datos y debe respetar la Directiva de protección de datos personales, con esto se crea la posibilidad de que el afectado pueda dirigir su exigencia directamente a Google con el objetivo de que sus datos sean modificados o eliminados.

Como conclusión se ha determinado entonces que las personas están facultados para solicitar los gestores de los motores de búsqueda, dentro de los preceptos legales pertinentes, la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexación; caso contrario, interesados pueden solicitar tutela administrativa o judicial y en caso de no atenderse su solicitud, las personas tienen derecho.

2.5.4. Caso Ecuatoriano:

En nuestro país, no existe jurisprudencia en cuando a la protección de datos personales, sin embargo, existe la garantía del habeas data que es el mecanismo mediante el cual se ejercitan las facultades del titular para disponer de su información como el derecho de acceso y rectificación, por lo que para el desarrollo de la presente disertación, he analizado una sentencia de habeas data.

Habeas Data por Juicio De Paternidad.

Resolución de la Corte Constitucional 74, Registro Oficial Suplemento 8 de 4 de Septiembre del 2009. No. 0074-2008-HD

Antecedentes:

Una ciudadana, comparece ante el Juez Vigésimo Tercero de lo Civil de Pichincha, e interpone recurso de habeas data en contra del Representante Legal de la Cruz Roja Ecuatoriana, y manifiesta:

El 17 de Noviembre del 2005, su ex pareja, su hija y ella, se sometieron a un examen de ADN (Ácido Desoxirribonucleico) en el Departamento de Genética de la Cruz Roja Ecuatoriana, sin embargo no estuvo conforme con el resultado, por lo que se solicitó al Departamento de Genética que le entregue todos los documentos que tenían archivados dentro de su caso. No obstante, la respuesta de la fue que las copias certificadas de todos los documentos de su caso sólo podía ser entregadas con orden de juez.

La accionante, se mantuvo la duda acerca de si el examen de ADN, había sido realizado correctamente, ya que nunca estuvo de acuerdo con los resultados, por no ajustarse a la verdad de los hechos.

Por lo expuesto, la accionante solicita mediante la acción de Habeas Data que se le entregue lo siguiente:

- Todos los documentos certificados donde consten el examen realizado a las muestras de sangre, el procedimiento que se siguió antes de entregar el informe final;

- Fotos y toda la documentación certificada que reposa sobre el caso en el Departamento y Laboratorio de Genética de la Cruz Roja Ecuatoriana.

En la audiencia pública, el representante de la Cruz Roja Ecuatoriana, ente accionado, manifestó que en el examen al que hace referencia la compareciente, intervienen tres personas, la accionante, su ex pareja y su hija, todos mayores de edad.

Que, el examen de ADN se lo realizó por disposición del Juez Octava de lo Civil de Pichincha, dentro del Juicio de Paternidad que llevan la accionante y su ex pareja y que dicho examen de ADN, fue remitido a la mencionada judicatura.

Igualmente solicita que se deseche el presente recurso por cuanto violenta en forma expresa normas Constitucionales, por constar la información requerida en el Habeas Data, dentro del Juicio de Paternidad tramitado en el Juzgado Octavo de lo Civil de Pichincha, el mismo que es un proceso público al que tiene acceso sin restricciones; por cuanto la información solicitada no se trata solo de la peticionaria, sino que afecta directamente derechos constitucionales de personas que no intervienen en esta solicitud, como son la hija de la accionante y su ex pareja.

También arguye que la acción está en contra del sigilo profesional que la Ley Orgánica de la Salud exige expresamente.

El Juez Vigésimo Tercero de lo Civil de Pichincha niega el presente recurso de habeas data, decisión que ha sido apelada.

Consideraciones de la Corte:

La Sala es competente para conocer y resolver el presente caso.

No se advierte omisión de solemnidad sustancial alguna.

La corte considera que:

> *El hábeas data es una garantía constitucional que tiene por objeto proteger el acceso a la información personal, así como el derecho a la honra, a la buena reputación y a la intimidad personal y familiar, en consecuencia es derecho de toda persona para acceder a los documentos, banco de datos o informes que sobre sí misma, o sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellas y su propósito; de ello, se advierte que toda persona natural o jurídica está facultada para requerir del poseedor de la información, que haga relación a ella y que le sea entregada en los términos que establece la norma constitucional*.

Del libelo inicial se desprende que la peticionaria pretende que se le entregue "*todos los documentos certificados donde conste el examen realizado a las muestras de sangre, así como el procedimiento que se siguió antes de entregar el informe fina*l". Al respecto, la misma accionante se refiere al examen sanguíneo realizado en base a su muestra así como a las muestras de sangre pertenecientes su hija y su ex pareja, mayores de edad, y que están relacionados con un juicio de paternidad que no viene al caso analizarlo.

Esta situación hace que la Sala considere que la pretensión de la accionante no está encaminada a obtener información de documentos, bancos de datos e informes únicamente sobre sí misma o sus bienes conforme lo dispone la Constitución Política, sino adicionalmente de dos personas distintas que tampoco le han autorizado plantear la presente acción, por lo que se estaría desnaturalizando el recurso de Habeas Data que, según lo la Constitución, claramente señala quien puede proponerlo y en qué consiste el ejercicio del derecho para acceder a los documentos, bancos de datos e informes sobre sí mismas.

Considerando que una de las personas que proporcionó la muestra sanguínea, así como la foto individual que le tomaron, corresponde a la accionante, la información a la que puede acceder es únicamente en lo relacionado al análisis de su tipo de sangre y a su fotografía individual más no a los documentos o análisis de sangre de las otras personas mientras éstas no lo soliciten o autoricen solicitarlo; precisamente en eso consiste la garantía constitucional establecida en la Constitución relativa al Habeas Data. Es más, la misma accionante señala que los interesados son la peticionaria así como su hija y su ex pareja; siendo así, no puede exigir documentos, banco de datos o información que no le corresponden de manera exclusiva.

En otras palabras, los documentos, bancos de datos o información que corresponde a las tres personas, en la parte indivisible que sería el resultado del análisis conjunto, no puede ser exigida por una sola de ellas, sino en la parte que le corresponde, esto es, lo relacionado a la muestra que la recurrente proporcionó y a la fotografía individual que dice le han tomado.

En el caso que se realizara un nuevo examen que se haya practicado en un laboratorio distinto, y diere como resultado final, uno diferente al emitido por la Cruz Roja; cualquiera de las tres partes involucradas podría solicitar toda la información con el fin de proceder a la rectificación conforme lo determinaba la misma Constitución.

La Corte Resuelve:

Revocar la resolución adoptada por el Juez Vigésimo Tercero de lo Civil de Pichincha y, en consecuencia, conceder parcialmente el hábeas data solicitado por la recurrente, en la medida de que solo puede acceder su información personal.

Comentario:

En el presente caso de Habeas Data, la peticionaria pretendía de acceder a la información personal que se encontraba en posesión de la Cruz Roja Ecuatoriana. el Habeas Data, es la acción que permite el ejercicio de este derecho, de la manera más clara en nuestra legislación, por lo que considero correcto la interposición de la acción Los datos personales a los que se pretendía acceder, son datos sensibles, ya que revelan la datos genéticos, vinculación filial de los implicados y la ascendencia biología de la hija de la accionante, por ello considero que es un ejemplo claro de que se maneja muchos de estos datos en instituciones con un propósito claro, sin embargo deben ser manejados con regulación para evitar la violación de derechos.

Me llamo la atención que a lo largo de la sentencia se trata a la Acción de Habeas Data como un recurso y no como una Garantía Jurisdiccional como lo es hoy en día, supongo porque en el 2005 no existía la regulación del Habeas Data, mediante la Ley de Garantías Jurisdiccionales y Control Constitucional.

Considero que la actuación del Juez Constitucional, es la correcta, por cuanto, como regla general, tenemos derecho de acceso a nuestros datos, mas no de los demás, pese a que sean nuestros familiares, caso contrario deben consentir expresamente, para que se le de esta información a uno de los implicados, a pesar de tratarse de un examen de ADN.

Conclusión Segundo Capitulo.

Posterior a los contenidos revisados a lo largo del capítulo en primer lugar que el derecho a la intimidad es conexo al derecho a al protección de datos personales, ya que en términos generales, se pretende cuidad la integridad de la persona y de su vida privada. Además es notorio el hecho de que si no existe una adecuada protección de los datos personales sensibles de los ciudadanos, en derecho a la intimidad tampoco estaría adecuadamente garantizado, por lo que es deber del Estado precautelar los dos derechos que por su naturaleza de conexos.

También fue notorio que en nuestro país, existen varias leyes que pretenden precautelar a los datos personales de los administrados, sin embargo las estas normas no son especificas ni regulan todos los preceptos necesarios para un adecuado ejercicio del derecho.

Estas normas se encuentran repartidas en varios cuerpos legales, y por ello no son completamente concordantes y más bien conforman una dispersión normativa que impide la correcta regulación del derecho a la protección jurídica de información personal.

Por ello la necesidad de una norma que regule uniformemente este derecho, de manera específica y que incluya principios y además de mecanismos prácticos de protección como el consentimiento del titular de los datos, en el sentido de que autorice el tratamiento de sus datos con ciertas condiciones; esta carencia de regulación del consentimiento no permite que el ciudadano tenga mayor disposición de su información, impidiéndole ejercitar sus facultades relativas al derecho de protección de dato personales.

Podemos reconocer que el único mecanismo existente en nuestro ordenamiento, e la actualidad, es el Habeas Data, sin embargo deberían existir mas formas de hacer efectivo los derechos y facultades relativos a precautelar la información personal.

En cuanto al desarrollo sobre este tema en otros países de Latinoamérica, considero que si se puede tomar como ejemplo estos avances, en el sentido de que se elabore leyes que regulen la protección de este derecho y que se creen mecanismos viables en la práctica para su ejercicio.

Po último, en cuanto a las jurisprudencias analizadas, nos ofrecen una visión más práctica de los casos que se pueden presentar y que requieren de tutela administrativa para que sea exigida la reparación un daño material causado por la vulneración de un derecho.

CAPITULO III

3. ANÁLISIS FÁCTICO DE LA PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR

Una vez expuesta, en los anteriores capítulos, la protección jurídica que se debe brindar a los datos personales, es oportuno analizar cuál es la realidad de nuestro país en relación al tema.

El derecho fundamental de Protección de los Datos Personales y el derecho a la intimidad personal, como consecuencia, son vulnerables en la medida en que, no existe una regulación unificada, especializada y actualizada, que garantice su tutela y correcto ejercicio. Debido a la realidad cambiante en los avances tecnológicos, exige un marco jurídico especializado en nuestro país, en cuanto a regulación de tratamiento de datos y de los sistemas informáticos que realizan estos procesos.

En consecuencia de estos avances tecnológicos inminentes, se han presentado algunos problemas prácticos para el derecho, que citare a continuación:

- Los productos o servicios disponibles en internet, no siempre mantienen la privacidad de sus usuarios.

- Algunos proveedores de servicios, usan los datos de sus usuarios para vender sus productos, con datos actualizados y analizados con los cuales se generan perfiles de usuarios, lo cual solo es licito cuando el usuario brinde información veraz y suficiente, acerca del servicio ofertado.

- Los Servicios gratuitos también están obligados a dar información veraz a sus usuarios ya que también pueden usar los datos para generar perfiles, que pueden ser usados para fines ilegítimos, caso en el que se vulnera la privacidad del titular de los datos.

- El desarrollo de aplicaciones que generan plataformas de intercambio de datos y contenidos, donde los consumidores de estas aplicaciones generan los contenidos, colocando sus datos personales, poniendo en riesgo su privacidad.

- Descargar información en portales web, acceder o consultar datos, utilizada por instituciones públicas y privadas, contribuyen a la transferencia de grandes cantidades de información que muchas veces puede contener datos personales sensibles, que posteriormente puede ser utilizada con el objetivo de causar perjuicio a su titular.

Este tipo de conductas, bastante normales para los usuarios de internet, pueden ser lesivas de derechos, por lo que se debe entender que para estos diferentes usos y finalidades del internet y de las herramientas tecnológicas, el usuario y titular de los datos personales, debe contar con información veraz, relevante, oportuna, fácilmente accesible y de fácil comprensión; al momento de entregar su información.

Es decir, que en todos los casos en que se entreguen datos personales, a través del internet, se debe contar con la autorización o consentimiento del titular, con el objetivo de que él tenga conocimiento de las condiciones y el motivo por el cual se le solicitaron sus datos sensibles, de manera que los pueda transferir, con la total seguridad de que van a ser utilizados con el fin y de la forma en que se le fue informado y bajo las condiciones de reserva necesarias.

Puntualmente, el internet, al ser universal, genera la dificultad de que las diferentes legislaciones no pueden brindar una correcta regulación que prevea todos los casos en los que se pueden vulnerar la intimidad personal de los usuarios por lo que muchos autores ven la necesidad de que las legislaciones se unifiquen en este sentido y se garanticen así, la privacidad de estos usuarios.

De acuerdo a lo establecido en los ordenamientos jurídicos internaciones, la regla general es que debe existir un consentimiento previo, inequívoco e informado para el tratamiento de datos personales, no obstante, en internet, interesa que las formas de dar el consentimiento estén acordes a los usos y costumbres de sus usuarios de Internet y a la vez provean a éstos la información suficiente para que tomen una opción.

Otra de las sugerencias para los proveedores de servicios en internet es que no se cumpla con el mero hecho brindar información de manera textual, si no que se represente a través de una animación la relación de consumo o que se envíe un correo electrónico al usuario con información relevante para hacer valer sus derechos.

En definitiva, se debe garantizar y brindar las herramientas necesarias para que los usuarios tengan un control del tratamiento de sus datos y de los contenidos publicados en la red.

Pedro Huichalaf Roa, en su artículo, *"Hacia una unificación de criterios sobre seguridad y protección de datos en Internet",* elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, explica que "*los organismos encargados de control tratamiento de los datos personales, deben promover políticas públicas para educar o instruir a las personas con el fin de que tomen control de su seguridad y privacidad*."[116]

Como conocemos, la principal preocupación de los usuarios de internet es que sus datos personales se filtren y sean utilizados para fines ilegales o ilegítimos sin su consentimiento, realidad que no es ajena a la que se vive en el mundo del comercio electrónico o de los servicios que ofrece el internet, por lo que es necesaria educar a los usuarios, para que no entreguen información personal si no tienen certeza de la autenticidad de la página web y del servicio que contratan, se debe propender entonces a correctas prácticas de seguridad digital.

El internet junto con las herramientas de telecomunicaciones y aparatos electrónicos, han dado lugar a una verdadera revolución tecnológica, que a su vez facilita el movimiento de gran cantidad de información de manera rápida y eficaz, hecho que hace algunos años era imposible imaginar.

La red, maneja gran cantidad de información que, al ser accesible fácilmente a sus usuarios, se revelan datos personales incluso fuera de las fronteras de los países de sus titulares, y se han visto afectadas en muchos casos, la intimidad, vida privada y dignidad de los dueños de esa información.

Los datos personales que corresponden a la vida privada de los individuos se ven revelados ante las redes telemáticas como el internet y afectan directamente a la privacidad del dueño de esa información, ya que la recolección de y comunicación de los datos puede realizarse con sencillez y las viejas estructuras burocráticas son obsoletas para hacer algo en contra de estas conductas ilegitimas y más bien un impedimento para los individuos afectados a la hora de hacer justicia; por lo que la

[116] HUICHALAF Roa, Pedro, *Hacia una unificación de criterios sobre seguridad y protección de datos en Internet*, http://oiprodat.com/declaracion-de-santiago/, Acceso: cinco de noviembre de 2013.

sociedad exige un replanteamiento de políticas con miras a solucionar estos problemas sociales.

Concluyo con que la protección de datos personales en el internet, debe convertirse en un tema de importancia en las actividades legislativas de nuestro país, y más a un a futuro por el creciente entorno digital, haciendo énfasis en la necesidad de crear procedimientos adecuados para brindar el consentimiento o autorización legal, con miras a proteger la privacidad, intimidad y honor de las personas.

En el caso de los Datos Personales Sensibles constantes en los Registros Públicos, la posible vulneración del derecho a la Intimidad es latente, por cuanto no se han tomado medidas, en el campo jurídico ecuatoriano, como la existencia de una norma especializada, como en el caso de otros países como España o Argentina; como en el campo técnico, con la implementación de sistemas informáticos como prácticos, en los que sea factible solicitar la autorización expresa al titular de los datos personales sensibles para una transferencia de los mismos entre instituciones públicas por ejemplo, todo con el objetivo de cumplir con los principios doctrinales de protección de datos como materializar la protección del derecho a la intimidad.

Las instituciones privadas, también carecen de estos sistemas conducentes a la protección de datos personales sensibles, muchas veces solicitan información personal a sus consumidores o usuarios a cambio de servicios o bienes

Por lo que la implementación de estos sistemas y regulaciones, es inevitable, como política dirigida a que la intimidad de individuo no sea vulnerada y se mantenga un correcto manejo y tratamiento de los datos personales sensibles.

3.1. DATOS OBTENIDOS EN ÓRGANOS PÚBLICOS DE CONTROL.

Dentro de las Instituciones públicas de control, no hay un conocimiento profundo del tema de la Protección Jurídica que se le debe brindar a los Datos Personales Sensibles.

La Superintendencia de la información y Comunicación, inaugurada en diciembre de 2013, por mandato de la Ley de Comunicación, es un organismo técnico de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, prestadas por diferentes entidades, con el propósito de que estas

actividades se sujeten al ordenamiento jurídico y a la normativa de regulación de la Información y Comunicación.

Sus atribuciones son:

- Fiscalizar, supervisar y ordenar el cumplimiento de las disposiciones legales y reglamentarias sobre los derechos de la comunicación;

- Atender, investigar y resolver las denuncias o reclamos formulados por las personas naturales o jurídicas, a través de sus representantes, en materia de derechos de la comunicación;

- Requerir a los ciudadanos, instituciones y actores relacionados a la comunicación, información sobre sí mismos que fuere necesaria para el cumplimiento de sus atribuciones;

- Aplicar las sanciones establecidas en el marco de esta Ley y de la regulación que emita la autoridad reguladora;

Si bien es cierto que dentro de sus atribuciones no hay una específica para la Protección Jurídica de los Datos Personales, éste órgano de control interviene en los procesos de acceso y ejercicio de los derechos de las personas a recibir información de calidad es decir, veraz, objetiva, oportuna, plural, contextualizada; y además según lo que establece la ley de Comunicación, debe liderar la vigilancia y control permanente del cumplimiento de los derechos de la información y comunicación.

En estos procesos donde se accede a información o se la transfiere, como parte del ejercicio de los derechos a la comunicación e información, pueden estar inmersos datos personales sensibles que son entregados sin consentimiento de su titular. por lo que considero que a pesar de que la Superintendencia de la Información y Comunicación, es un órgano oportuno y cumple con un objetivo esencial en cuanto a regulación del contenido de la información; no tiene una norma o proceso claro establecido para los datos personales sensibles.

En la práctica, este órgano de control no posee denuncias o solicitudes en este sentido, ya que no se encuentra dentro del rango de su control.

En la **Dirección Nacional de Registro de Datos Públicos**, se mantiene este nivel de poco conocimiento sobre el tema, ya que actualmente se ocupan de cumplir con procesos organizar y almacenar correctamente los registros públicos de las instituciones relacionadas, como son el Registro Civil, Registro de la Propiedad y Registro mercantil, de cada uno de los cantones del país.

Esta institución permite al usuario acceder a sus datos, no siempre sensibles, por medio de sus portales que son dato.seguro, que mediante una contraseña generada por internet, facilita el acceso datos que están almacenados en las instituciones públicas registrales. Con la garantía de que esa información es actualizada y de calidad.

Muchas veces no es información actualizada, ya que simplemente es un reflejo de lo que está registrado en dichas instituciones.

Este acceso, al ser de forma electrónica, puede ser usado por quien tenga la contraseña y haya pasado por un proceso previo de generación de la misma contraseña, y por ende se supone seguro.
Sin embargo no es un sistema infalible y pueden existir casos de filtración de la información.

La ley del Sistema Nacional de Registro de Datos Públicos establece que quien puede solicitar algún cambio en la información constante en los registros públicos que la Dinardap maneja, es el titular de los datos cuando estos cambios no estén en contra le ninguna disposición legal judicial o administrativa y el derecho de terceros, caso en el que se requerida de la resolución administrativa o sentencia judicial.

Esta información personal, se clasifica como publica, y por ello se entiende que pertenece a los ciudadanos, el Estado únicamente es un depositario de estos archivos y dentro de su potestad, facilitan el derecho a la información y su acceso y las instituciones privadas depositarias de archivos públicos son sus administradores y están obligados a garantizar el acceso a la información…" Por lo

tanto dicha información por regla general será gratuita a excepción de los casos de reproducción.

Entonces, se infiere que, en el caso de existir información personal sensible en estos archivos públicos, están clasificados como información pública y podrían accederse a pesar de contar con una investidura de confidenciales.

La responsabilidad de la integridad y protección de los registros de las bases de datos públicos, es de las instituciones públicas o privadas y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos.

Es importante puntualizar que la responsabilidad sobre la veracidad y autenticidad de los datos registrados, es del declarante, es decir del titular cuando éste la entrega para registro en la institución pública

El acceso a estos datos, corresponde únicamente al titular de los mismos, a través del portal Dato Seguro, y se creó con la finalidad de que el individuo pueda consultar si información rápidamente, sin acudir a la institución registral y desde todas partes.

Los Datos Públicos que el ciudadano puede consultar son los siguientes:

- Datos de identificación personal del ciudadano
- Antecedentes personales
- Movimientos migratorios
- Listado de bienes inmuebles y sus gravámenes
- Listado de actos mercantiles sobre bienes muebles
- Información de RUC y estado tributario
- Información de licencias de conducir
- Títulos registrados
- Datos del Ministerio de Relaciones Laborales
- Datos de Registro Electoral

- Datos de Instituto Ecuatoriano de Seguridad Social IESS
- Datos del Instituto Nacional de Contratación Pública INCOP

De la información anunciada, están presentes datos personales sensibles como son, movimientos migratorios o antecedentes personales, que entiendo yo, se deben topar con más tino, ya que si son transferidos sin consentimiento de su titular pueden afectar su derecho a la intimidad.

Igualmente, en esta línea de cosas, La ley del sistema Nacional de Registro de Datos Públicos, tiene como finalidad prever procesos en los que se ejercitan los derechos propios a la protección de datos personales, como el derecho de acceso y consulta de información personal

En cuanto al derecho de consulta, el artículo 28 de la Ley del Sistema Nacional de Datos Públicos, con la finalidad de garantizar el derecho al acceso de información, regula a la Ficha de Registro Único, que contendrá la información requerida, y de esta forma el titular puede acceder e esta información como cito en la parte pertinente:

> *Art. 28.- […] Con la finalidad de garantizar el ejercicio del derecho constitucional del acceso a la información, se crea la Ficha de Registro Único del Ciudadano, documento público electrónico y/o físico certificado, que contendrá todos los datos de registro público del ciudadano constantes en el Sistema Nacional de Registro de Datos Públicos*.[117]

Esta ficha es un mero documento de verificación y consulta por lo que se puede acceder a la información requerida, es un mecanismo por el cual el ciudadano puede acceder a su información eficientemente.

Continuando con el análisis de la resolución 7, dentro de sus objetivos, se encuentra el derecho al acceso a la información, según la norma este acceso debe darse por medio de Dato Seguro, o cualquiera de los servicios brindados por esta institución pública. Es deber de la administración pública garantizar los procesos de acceso, consulta en general todas las transacciones que se realicen respecto a la información personal que repose en los archivos públicos.

En cuanto a la regulación para el acceso a los datos personales sensibles, la presente resolución dice:

[117] Op. Cit. 67. Art 28.

Art. 8.- La información que se encuentra en las bases de los Registros de Datos Públicos que Interoperan con el Sistema Nacional de Registro de Datos Públicos, es información pública de carácter sensible a la cual solo se puede acceder, por mandato legal, con autorización del titular o por orden judicial, por lo tanto la DINARDAP ha establecido procesos y protocolos que garantizan el acceso seguro a esta información a través de Dato Seguro e Info Digital (Relaciones de Confianza) y mediante servicios en línea que están a disposición de los ciudadanos, instituciones y el Estado.[118]

En este artículo de la resolución se hace referencia a que los datos sensibles interoperan con el Sistema Nacional de Registro de Datos Públicos, y que a pesar de ser información pública, por su naturaleza solo se puede acceder por mandato legal o autorización del titular u orden judicial, precisamente por la naturaleza de confidencial y potencialmente lesivo de los datos personales sensibles.

Esta es la importancia de esta norma en cuanto al derecho del titular de los datos personales, a acceder a ello cuando la administración los tenga en sus archivos, o cuando estén siendo objeto de tratamiento en alguna de las instituciones públicas de registro.

Los protocolos y procesos que nombra este articulo aún no están definidos y aquí radica el problema del acceso a este tipo de datos, ya que sin una regulación clara en cuanto al acceso a ellos por parte del titular, con el objetivo de prevenir abusos, se pueden violentar derechos fundamentales; por lo que pongo énfasis en que deben existir en la legislación ecuatoriana estas reglas claras en cuanto a la protección, acceso y tratamiento de los datos personales.

Si bien el consentimiento es un elemento que permite la seguridad del titular, el procedimiento para obtenerlo no es claro y puede escaparse en la práctica a los ojos de los funcionarios o servidores públicos.

El artículo 10 de la resolución 7 son dice:

Art. 10.- La presente Norma, amparada en lo que determina la Constitución del Ecuador y las Leyes vigentes, establece que son activos de información de la Dirección Nacional de Registro de Datos Públicos, toda la información que se genera, recibe, trata, transmite y almacena en la Institución, sus Direcciones Regionales o el Registro de Datos Crediticios, la misma que se clasifica en:

[118] Op. cit. 67.

1. Información Pública.- Es todo documento en cualquier formato, que se encuentre en poder de la DINARDAP, sin embargo para su publicidad o acceso se debe cumplir con los procedimientos establecidos en la Ley, estos son:

Proceso para Publicitar la Información Pública.- La información administrada por la DINARDAP solo puede ser publicitada por la Institución, mediante la publicación de la información en el portal de la misma o cuando exista una petición expresa de autoridad competente o de cualquier ciudadano.

En lo referente a los Procesos Precontractuales y Contractuales, éstos se publicitan en el Portal de Compras Públicas y en el Portal de la Institución.

Proceso de Acceso a Información Pública.- La Ley dispone que toda la información que emana o se encuentra en las instituciones públicas es pública, sin embargo su acceso está sujeto a:

1. Un mandato legal;
2. Petición del titular de la información;
3. Autorización del titular de la información en favor de un tercero; y,
4. Por orden judicial.

2. Información Protegida y no Sujeta a Divulgación.- Es toda la información pública respecto a la cual no se ha cumplido con los procedimientos establecidos en la Ley para su publicidad y acceso.
Proceso de Acceso a Información Protegida y no Sujeta a Divulgación.- Para publicitar y acceder a este tipo de información se deberá cumplir con lo dispuesto en el numeral uno.

3. Información Protegida Sensible.- Es la información que se encuentra en las Bases de Datos de los Registros de Datos Públicos y Registro Crediticio que interoperan con el SINARDAP, así como toda información que pueda presentar riesgos de seguridad para la DINARDAP, sus Regionales y para los sistemas que interoperan en Dato Seguro e Info Digital (Relaciones de Confianza).
Proceso de Acceso a Información Protegida Sensible.- Para publicitar y acceder a este tipo de información se deberá cumplir con lo dispuesto en el numeral uno.

4. Información Confidencial.- Es aquella información pública personal, que no está sujeta al principio de publicidad y comprende derechos personalísimos y fundamentales como son: la condición médica, filiación política, preferencia sexual, creencias religiosas y condición migratoria.
Proceso de Acceso a Información Confidencial.- Para publicitar y acceder a este tipo de información se deberá cumplir con lo dispuesto en el numeral uno[119]

En este artículo se define cuáles son los activos de la información que maneja la Dirección Nacional de Registro de Datos Públicos, que en general son los datos que se clasifican como públicos y que permanecen en los bancos de información de las Instituciones Estatales, lo relevante de esto, para mi investigación es que en estos bancos, puede existir datos personales sensibles, por ello la importancia de que exista

[119] Id. 118.

una regulación específica para ellos, ya que se les puede dar un trato inadecuado por ser públicos.

Sin embargo, haciendo un análisis solo de información pública, en el supuesto que exista entre ella datos personales sensibles, esta resolución ampliando la regulación de la ley del Sistema Nacional de Registro de Datos Públicos, dice que la publicación de estos datos se realizara en el portal de acceso público, como la mayoría de información que maneje este ente público. Se realizara la publicación, de igual manera cuando exista una petición de un autoridad competente, como el caso de un juez o de cualquier ciudadano interesado, estas últimas dos premisas son realidades más cercanas a los datos personales sensibles, ya que se pueden ocasionar cuando se han vulnerado derechos y el titular de la información, está ejercitando su derecho de acceso a esta información potencialmente dañosa.

Respecto al proceso de acceso a la información pública, se establece que a pesar de su naturaleza pública, su acceso esta también condicionado a mandato legal, petición del titular, por petición de un titular autorizado u orden judicial. Considero que estas premisas permiten que solo los interesados a la información puedan acceder a ella, es correcto, ya que no es saludable que cualquier tercera persona, que no tenga algún interés legítimo pueda acceder a datos, que aunque sean registrales o públicos, por el hecho pertenecen a un ciudadano y solo él o el Estado con fines de orden pueden acceder y disponer de ellos.

Noto que estas condiciones son características del consentimiento y permiten que el titular de los datos este informado de lo que sucede con sus datos y disponer de ellos.

En el numeral 2 del presente artículo se establece que existe información Protegida y no sujeta a Divulgación, que también forma parte del banco de datos públicos que maneja la DINARDAP y de igual forma establece un procedimiento de cómo se debe acceder a ella. Esta información es aquella que no cumple con los requisitos que establece la ley para su acceso, esto quiere decir es confidencial y puede ser información de secreto nacional y de las cuatro formas establecidas en el numeral uno se puede autorizar su divulgación o acceso.

En el numeral 3, se encuentra la clasificación de la información sensible, que en ciertos casos podría tratarse de datos personales sensibles, y también solo se

podrá acceder a ella por mandato legal, autorización de juez o autorización del titular, lo que limita el ámbito de acceso

Por ultimo en el numeral 4, se encuentra clasificada la información que compete a la presente investigación, como son los datos personales sensibles, denominada como confidencial por el presente instrumento. Es clasificada de esta manera porque forma parte de la gama de derechos fundamentales de los ciudadanos y su acceso es también limitado con las condiciones del numeral primero.

El artículo 31 establece quien debe dar la autorización al acceso de la información será autorizada por el Director de cada área, dándola mayor especificidad al proceso y además se debe comunicar cuales son las razones para permitir este acceso, como cito a continuación:

> *Art. 31.- La autorización al acceso de la información clasificada como pública, será autorizada por el Director de cada Área.*
>
> *Para permitir el acceso a esta información se lo deberá hacer mediante un memorando, en el cual se justifique y motive las razones para permitir el acceso a dicha información.*[120]

El artículo 32 establece:

> *Art. 32.- La autorización al acceso de la información clasificada como protegida no sujeta a divulgación, será autorizada por el Coordinador de cada Área. Para permitir el acceso a esta información se lo deberá hacer mediante un memorando, en el cual se justifique y motive las razones para permitir el acceso a dicha información*[121]

Los datos personales sensibles pueden ser parte de la información protegida por lo que toda solicitud de acceso a ella, cuando se encuentre el bancos de datos de instituciones públicas que formen parte de la SINARDAP , debe ser autorizada por el Director del Área específica, y se deben especificar las razones por las cuales se permite este acceso. Se entendería que esta medida permite la no divulgación de la información y que su acceso sea preciso para los solicitantes.

El artículo 33 y 34 establecen:

[120] Id. 119.
[121] Id. 120.

Art. 33.- La autorización al acceso de la información clasificada como protegida, será autorizada por el Coordinador de cada Área, previa autorización del Presidente o Presidenta del Comité de Seguridad. Para permitir el acceso a esta información se lo deberá hacer mediante un memorando, en el cual se justifique y motive las razones para permitir el acceso a dicha información

Art. 34.- El acceso a la información clasificada como sensible o confidencial, será autorizada por el Coordinador de cada Área, previa aprobación del Presidente o Presidenta del Comité de Seguridad.
Para permitir el acceso a esta información se lo deberá hacer mediante un memorando, en el cual se justifique y motive las razones para permitir el acceso a dicha información.

Dentro de la información clasificada como protegida no sujeta a divulgación, sensible o confidencial, pueden existir también datos personales sensibles; por lo que solo se pueden acceder a ellas, con autorización del coordinador del Área y en el último caso con autorización previa del Presidente del Comité de Seguridad, esto por motivos de seguridad y para precautelar su naturaleza de confidencial. al igual que en el caso del artículo 31, en estas clasificaciones pueden existir datos personales sensibles, por lo que estas condiciones permiten la protección de ellos y que no se filtren en los procesos de acceso además que solo lleguen a manos del solicitante y que sean concedidos si su derecho es legítimo.

Lo importante es clasificar correctamente la información dentro de estos cuatro grupos y utilizar el mecanismo jurídicamente correcto para acceder a ella.

En conclusión el Derecho a Acceder a Datos Personales, por parte de su titular es una de las facultades de las que se ve provisto el ciudadanos para ejercer eficazmente su derecho fundamental, solo de esta forma llega al conocimiento de que datos están siendo tratados y bajo de modalidad por lo que se trata de uno de los ejercicios más claros de disposición de su información.

Además de esto, en la Dirección Nacional de Registro de Datos Públicos, no tiene solicitudes de acceso a información personal sensible por parte de sus titulares a físicas de casos particulares a las que se pueda acceder; primero porque los ciudadanos desconocen de la posibilidad de ejercitar estos derechos, segundo, porque en realidad no se han presentado casos en este sentido, y tercero porque, aun si existieran estos expedientes son confidenciales y solo el titular de la información o interesado puede acceder a ellos

Por estas razones, me fue imposible conocer de casos en los que se haya solicitado esta autorización expresa para transferir datos sensibles por lo que concluyo que no está correctamente precautelado el derecho a la intimidad en estas bases registrales, a pesar de que la norma establece que datos personales son sensibles y confidenciales.

Fiscalía General del Estado.

La fiscalía General del Estado, capta las denuncias conducentes a la sanción de estos delitos; y, los delitos en contra de la vulneración del derecho a la intimidad o revelación de información personal son objeto de estas denuncias, ya que se encuentran, sin embargo, al realizar mi investigación no encontré denuncias sobre este tema y además no existen estadísticas ni información en las publicaciones y archivos que reposan en la oficia de delitos copio[122] de la Fiscalía

Esto, releva que la vía penal tampoco brinda una protección jurídica a los datos personales sensibles en la práctica. Considero esto se debe a que si bien Código Orgánico Integral Penal, si prevé muchas de las conductas que podrían vulnerar el derecho a la protección de datos, la ciudadanía desconoce el alcance de su derecho a denunciar y a procurar la reparación de un daño eventual a su derecho a la intimidad.

Además, este hecho hace presumir que el problema es inexistente, situación que no concuerda con la realidad del mundo de la información y conocimiento en el que vivimos actualmente.

Defensoría del Pueblo

En la defensoría del Pueblo, tendrá como funciones la protección y tutela de los derechos de los habitantes del Ecuador y la defensa de los derechos de las ecuatorianas y ecuatorianos que estén fuera del país. Serán sus atribuciones, además de las establecidas en la ley, las siguientes:

1. El patrocinio, de oficio o a petición de parte, de las acciones de protección, hábeas corpus, acceso a la información pública, hábeas data, incumplimiento, acción

[122] N.B. Dependencia de la Fiscalía General del Estado que realiza estadísticas y estudios de los delitos denunciados para publicaciones y políticas criminales en el Ecuador.

ciudadana y los reclamos por mala calidad o indebida prestación de los servicios públicos o privados.

2. Emitir medidas de cumplimiento obligatorio e inmediato en materia de protección de los derechos, y solicitar juzgamiento y sanción ante la autoridad competente, por sus incumplimientos.

3. Investigar y resolver, en el marco de sus atribuciones, sobre acciones u omisiones de personas naturales o jurídicas que presten servicios públicos.

4. Ejercer y promover la vigilancia del debido proceso, y prevenir, e impedir de inmediato la tortura, el trato cruel, inhumano y degradante en todas sus formas".

El Defensor del Pueblo puede, además, emitir censura pública en contra de los responsables materiales o intelectuales de actos o comportamientos contrarios a los derechos humanos; así como pronunciamientos públicos en los casos sometidos a su consideración, con criterios que pasan a constituir doctrina para la defensa de los derechos humanos.

Con esto se infiere que es una institución donde se puede acudir para exigir los derechos de protección de datos personales, sin embargo, tampoco pude encontrar denuncias con resolución que evidencien la exigencia de la protección jurídica de los datos personales sensibles.

Concluyo entonces, que el problema sería la falta de conocimiento tanto de los ciudadanos acerca de sus derechos y de los órganos de control estatales que no dan la importancia requerida para este tipo de derechos.

3.2. Diagnostico general de la protección de datos personales en el Ecuador

El diagnóstico de la Protección de datos personales sensibles en el Ecuador, es evidente en el sentido de que no existe una norma específica que regule los procesos de tratamiento de datos sensibles y además porque tampoco existe un órganos de control en este sentido que fiscalice la obtención, tratamiento y almacenaje de datos personales, con miras a que no se vulneren derechos como la intimidad, Buen nombre y Honra.

Partiendo de la consecuencia fáctica enunciada anteriormente, y haciendo un análisis más profundo, podemos determinar las normas existentes no son suficientes y no apuntan a una solución jurídica y fáctica del problema como en otros países.

Lo que nos permite concluir que no existe un procedimiento operativo que permita el buen manejo y custodia de la información personal obtenida por las instituciones, para distintos procesos y finalidades, por lo que es necesario unificar lo que ya está establecido las distintas normas como en las resoluciones de las DINARDAP por ejemplo, y emitir un cuerpo legal con mayor rango legal, que cuente con procesos viables, que permitan el ejercicio de las facultades del titular de la información y su respectiva tutela.

El hecho de que dentro de los entes del Estado, no exista un conocimiento o procedimientos claros a la hora de responder a las solicitudes de los ciudadanos en cuanto a la disposición de sus datos personales, como son el acceso, rectificación, o reserva de dicha información, refleja claramente que en nuestro medio, no se maneja una protección de estos derechos fundamentales efectiva y que más bien se pretende dar una solución judicial en el caso de controversias en este sentido, es decir, que se pretende dar una solución en últimas instancias en los casos específicos, mas no brindar una protección legal vigente para todos los casos, con independencia de sus antecedentes y gravedad.

Otra de las razones para que no exista una preocupación por parte de las instituciones públicas acerca de la protección jurídica de los datos personales sensibles, puede ser que reconocen otros problemas jurídicos como emergentes y de mayor atención social, sin embargo considero que a pesar de no tener una repercusión social mayor debe prestársele la misma atención que las demás vulneraciones de derechos, ya que todos tenemos derechos a que nuestra información, inherente a nosotros y que forma parte de nuestro patrimonio, sea protegida adecuadamente.

Por lo que considero, después de realizar esta investigación, que el procedimiento para la protección de los datos personales, establecida en una ley, es fundamental para que se precautelen los derechos fundamentales de los ciudadanos, titulares de datos personales sensibles, que se encuentran en bancos de datos públicos o privados, independientemente de la finalidad de su tratamiento.

3.3. Mecanismos actuales de protección del derecho de Protección de Datos personales.

Por lo expuesto con anterioridad, enunciare mecanismos que permitirían que las instituciones públicas o privadas protejan jurídicamente los datos personales sensibles, cumpliendo con el principio de la transferencia de Datos personales sin autorización de sus titulares.
Estos mecanismos son:

3.3.1. Legales:

La ley, es el mejor mecanismo en cuanto a la regulación de comportamientos sociales, por lo que en defensa de la hipótesis planteada en la presente disertación, es necesaria una norma especializada que regule la transferencia, acceso y tratamiento de datos personales sensibles en las instituciones públicas y privadas.

Las leyes analizadas a lo largo de la disertación pretenden esta regulación y protección del derecho a la intimidad, sin embargo son bastante vagas en cuanto al tema y no prevén procedimientos claros, como procesos para acceder a los datos, debidamente regulados o formatos de que debe contener un consentimiento expreso en este sentido.

Por lo que a continuación enunciare los mecanismos legales, idóneos en nuestro país para la protección de los datos personales:

Habeas Data: Existe como mecanismo primordial para el ejercicio de acceso, rectificación y cancelación de información personal en el Ecuador.

Esta garantía constitucional, en nuestro país esta provista de un procedimiento establecido en la ley de garantías jurisdiccionales y control constitucional, que pretende ser ágil y garantizar el cumplimiento efectivo de los derechos fundamentales, entre ellos el derecho a la protección de datos personales y al derecho a la intimidad.

Ejercicio de Derechos: Como ya lo hemos señalado anteriormente, la efectiva protección del derecho de protección de datos sensibles, comprende el ejercicio de varios derechos, como el derecho a la rectificación y cancelación, que también están

establecidos en la ley, como en la ley del Sistema Nacional de Registro de Datos Públicos

En el caso puntual del derecho de rectificación de información personal en bases de datos públicos en nuestra legislación se encuentran establecidos mecanismos en este sentido, en el caso de que la información personal sensible, carezca de calidad o que no sea precisa.

El Habeas Data como mecanismo primordial en el caso de rectificación, actualización, anulación y eliminación de ellos, además de que deben existir medidas adecuadas en el caso de datos sensibles y la autorización del titular de la información. Cabe anotar que en el texto constitucional donde se consagra la garantía del habeas data, se deja abierta la posibilidad de acudir ante el órgano jurisdiccional para reclamar su derecho, que bien podría hacerse mediante un habeas data.

También existe la posibilidad de que se demande por los daños ocasionados, en el caso de que esta información incorrecta cause algún daño a su titular o se vulnere algún otro derecho fundamental, que se llevara por cuerda separada y se entiende que también se exigirá mediante órganos jurisdiccional.

La ley del sistema Nacional de Registro de Datos Públicos, en su artículo 21 dice:

> *Art. 21.- Cambio de información en registros o bases de datos.- La o el titular de los datos podrá exigir las modificaciones en registros o bases de datos cuando dichas modificaciones no violen una disposición legal, una orden judicial o administrativa. La rectificación o supresión no procederá cuando pudiese causar perjuicios a derechos de terceras o terceros, en cuyo caso será necesaria la correspondiente resolución administrativa o sentencia judicial.*[123]

Se puede modificar o rectificar alguna información constante en las bases de datos públicos, siempre que el solicitante sea su titular, y cuando no se viole disposición legal u orden judicial o administrativa y además nunca podrá violentar derechos de terceros; sin embargo existe esa prerrogativa del titular de la información para que se rectifique cualquier dato que este errado, inexacto o desactualizado.

[123] Op. Cit. 67. Art 21

Esta posibilidad de rectificar información no veraz, logra mayor seguridad para los dueños de los datos, como para los que los manejan en instituciones públicas, y más aún en los entes registrales donde pueden existir más casos de presencia de datos personales sensibles en sus archivos, además de mejorar el sistema de protección de datos siendo que se garantiza la calidad de los mismos y calidad en su tratamiento.

En cuanto al derecho de cancelación de la información personal requiere que se dé cumplimiento en un plazo de tiempo. En el caso de que la información personal esté cedida a otra administración o entidad se debe dar noticia de esta cesión al interesado para que pueda accionar su derecho en la entidad adecuada, este derecho garantiza el derecho a la intimidad, entre otros fundamentales.

Cuando se realiza una cancelación de datos, estos no pueden ser sometidos a tratamiento y tampoco pueden ser difundidos, simplemente se eliminan de la base de datos y los respaldos que existan de estos datos; supone el fin de la relación jurídica entre el titular de la información y la entidad responsable del tratamiento de la misma.
Si se desea volver a procesar los datos, la entidad deberá volver a solicitarlos de la manera establecida en los principios y en la ley siempre respetando los derechos fundamentales.

Y por último el derecho de Indemnización, donde los titulares de los datos personales, pueden reclamar indemnización en el caso de que se haya ocasionado algún daño o lesión a derechos fundamentales, en la materia o falta de protección en general, siempre que se justifique el daño, que haya una relación jurídica y que el perjuicio sea significativo.

Todos estos derechos son propios de la Protección de Datos, y los he tomado como ejemplo de la legislación española, estos derechos son derechos personalísimos, es decir que solo pueden ejercerse por su titular y pueden presentar excepciones en el caso de derechos de terceros y son en general derechos gratuitos y fundamentales.

En nuestra legislación, se encuentra presente en derecho de indemnización, cuando existe vulneración a la protección de datos personales, como cito a continuación:

Ley del Sistema Nacional de Registro de Datos Públicos:

> Art. 4.- Responsabilidad de la información.- Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo.
>
> Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información.
>
> Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal.
>
> La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución.[124]

Se establece entonces la responsabilidad de quien maneja o tiene a cargo información personal, con el objetivo de que no se divulgue y además que se mantenga la calidad de esta información, por lo que en el tercer inciso de este artículo encontramos el derecho de solicitar una indemnización en que caso de que la información que reposa en las instituciones públicas no sea veraz o sea imprecisa o sea divulgada; ya que bajo estos supuestos pueden ocasionarse perjuicios desde patrimoniales como morales.

Es importante hacer la precisión de que a pesar de que el habeas data, se reconoce como el mecanismo jurídico que garantiza el derecho de los ciudadanos a disponer de sus datos, no es el único. Es verdad que ninguno de los ejercicios de los derechos por sede administrativa, se iguala a la garantía constitucional, en cuanto a tutela de derechos, sin embargo estos procedimientos administrativos como el de acceso o rectificación en los registros públicos, pueden eventualmente ejercitar efectivamente los derechos y evitar un daño posterior.

Después de realizar este análisis, se entiende que existen en normas que en teoría cumplirían el objetivo de precautelar el derecho a la intimidad, mediante la protección de los datos personales sin embargo poseen los siguientes problemas:

[124] Op. cit. 67. Art 4.

- Estas normas no son especializadas para la protección de los datos personales sensibles, es decir son destinadas a la información confidencial en general.

- Estas normas no regulan el otorgamiento del consentimiento del titular de los datos personales al momento de la recolección de los mismos y la posterior disposición de la información por parte de las instituciones públicas o privadas.

- El tema del consentimiento del titular de los datos personales sobre la disposición de su información, es complejo, ya que debe darse una solución práctica a los problemas como:

    - Si el consentimiento debe ser expreso o tácito y en qué caso cada uno de ellos.
    - ¿Qué clase de documento debe contener el consentimiento?
    - ¿Qué formato debe tener el consentimiento?
    - ¿Qué información básica acerca del uso de los datos personales debe contener el consentimiento?
    - ¿El formato del documento debe ser el mismo para instituciones públicas o privadas?

      Por lo que en la ley debe existir la respuesta a estas interrogantes, dándole una regulación clara y práctica.

- Estas normas no regulan adecuadamente la responsabilidad de los empleados o funcionarios que tengan a su cargo la recolección, tratamiento y almacenamiento de los datos personales sea cual sea su finalidad.

- No existe una regulación acerca de la protección jurídica a los datos personales que también deben tener las instituciones privadas, por lo que es necesario que una ley también tenga disposiciones en este sentido.

- En las normas vigentes no existe ningún órgano regulador a cargo de a protección de datos personales, que maneje el control jurídico y técnico del tratamiento de datos.

- Tampoco se prevén en estas normas el acceso a la información personal sensible en medios como Internet o nuevas tecnologías que proveen de variada información, por lo que se debe disponer a las instituciones tanto

publicas y privadas en qué casos subir información personal sensible a la nube de la información.

3.3.2. Administrativos:

Dentro de los mecanismos administrativos se encuentran todas las medidas técnicas que permitan el correcto manejo de la información personal sensible, Por ejemplo en la Ley Orgánica de Protección de Datos Española se prevén tres tipos de medidas de seguridad para el tratamiento de los Datos personales estas son:

Medidas de Organización: Estas medidas son organizativas y suponen que los responsables ordenen la información de tal forma que sea identificable y que no se pueda extraviar ni confundir, esto permitirá que el trabajo del responsable de la custodia de la información sea más eficiente y que se cumpla con los principios de Protección de Datos.

Medidas Jurídicas: estas son garantías que el derecho proporciona a los afectados o titulares de la información personal, y que deben ser observadas por el responsable del tratamiento de la información. Estas regulaciones deben abarcar desde la recolección, inclusión en ficheros o documentos, uso de los mismos y custodia de la información personal sensible.

En los países en los que existen entes de control sobre el tema, estos órganos son los que regulan las actividades atenientes con el tratamiento de los datos, en nuestro país no existe un órgano que se dedique solo a la protección de datos, por lo que evidente que no exista un control en cuanto al flujo de información personal, su acceso y correcta custodia, especialmente, cuando existen datos personales sensibles en los bancos, que están siendo sometidos a tratamiento.

Medidas Técnicas: son medidas que aseguran la integridad de los datos, que se deben incluir en la ley, por ejemplo si va a ser automatizado, manual, si es que existe un sistema informático para acceder a la información entre otras.

Al igual que en las medidas anteriores no existe un órgano que emita estos lineamientos en materia de Datos personales sensibles, pero considero que el órgano que realiza el tema es la Dirección Nacional de Registro de Datos Públicos

Considero adecuado acotar en este punto que la LOPD española, prevé que exista una cesión de Datos entre Administraciones Publicas, en este caso basta con que las competencias de los entes versen sobre las mismas materias, para que se pueda ceder la información. Sin embargo en el caso de que sea con fines históricos de estadísticos o científicos, se necesita autorización del interesado porque el fin de la utilización de los datos varia, y en el caso de que el interesado solicite alguno de estos datos personales o información respecto de ellos deben ser informados de modo expreso, preciso e inequívoco de sus derechos.

Daniel Santos García, en su obra, "Nociones Generales de la Ley Orgánica de Protección de Datos", admite la posibilidad que el Estado pueda subcontratar a terceros o a empresas particulares para que den tratamiento a la información personal sensible, pero se aclara que tendrán igual responsabilidad porque actual actuarían a nombre y representación de la entidad pública, y que de todas formas deben ceñirse a las medidas de seguridad que procuran la integridad de los datos.

Acerca de las medidas tanto técnicas, como jurídicas y de organización que se deben tomar en nuestro ordenamiento jurídico, considero que el sistema español es un buen ejemplo, ya que estas medidas están muy bien constituidas y permiten mantener políticas claras de manejo de información y además permiten la resolución de problemas ocasionados en el tratamiento de los datos, que pueden ser de organización o de procedimiento.

Las resoluciones 21 y 7 de la emitidas por la Dinardap, mencionadas en la presente disertación pretenden vagamente establecer medidas de protección, sin embargo no son especificas ni claras y no permiten una generalidad en los casos de vulneración de derecho y la consecuencia es que no se precautela debidamente los datos personales sensibles en cuanto a su reserva.

Conclusión del Capítulo Tercero

Es necesario precisar que en el Ecuador no existe una correcta protección del derecho de disponer sobre datos personales, por parte de su titular, y más aún, tampoco se puede garantizar que un ejercicio de derechos relacionados con el tema, como acceso o rectificación de información y por todo esto todos podemos ser sujetos de vulneración de derechos y por ende sufrir una lesión a nuestra privacidad y buen nombre.

CAPITULO IV

4. PROPUESTA PARA LA PROTECCION DE DATOS SENSIBLES EN EL MANEJO INCORRECTO DE INFORMACION PERSONAL DE PARTICULARES

Después de realizar la presente investigación, tomando en cuenta los principios existentes en la doctrina, que son los enunciados normativos que aunque no se han incluido en el ordenamiento jurídico, sirven como fundamentos para lo prescrito en la ley, ya que a pesar de ser abstractos tiene una naturaleza axiológica y permiten la estructura normativa; además de analizar que en nuestro país el tema de la protección de datos sensibles, no ha sido sustentada jurídicamente, ya que existe una dispersión normativa insuficiente en cuanto al tratamiento de datos personales, es necesario hacer el siguiente cuestionamiento:

¿Qué norma, permitiría que las instituciones públicas o privadas den una correcta custodia de los datos personales sensibles, que reciben de sus usuarios o consumidores, sin que exista transferencia de Datos personales sin autorización de sus titulares, o la acumulación de datos innecesarios o desproporcionados, con el bien o el servicio que se recibe, y garantizaría que esa información no sea mal utilizada por terceros en el Ecuador?

La respuesta a este cuestionamiento, se encuentra afincada en una norma especializada, que guarde los principios analizados con anterioridad y que además establezca procedimientos claros en cuanto al ejercicio de derechos de los titulares de los datos personales sensibles, que están siendo tratados por instituciones públicas o privadas.

De acuerdo al ordenamiento jurídico vigente, considero que esta norma debería ser una ley orgánica, por cuanto según el artículo 133 de la Constitución de la Republica, las leyes orgánicas serán las que regulen el ejercicio de los derechos y garantías constitucionales.

En esta ley orgánica de Datos Personales, deberán estar presentes los enunciados analizados en la presente disertación, como el consentimiento como mecanismo de protección de los datos personales sensibles, procedimientos para el

tratamiento de datos, entre otros, tomado como el ejemplo algunos países como España, México o Argentina, que incluyen ya en su ordenamiento estos temas.

Igualmente, en esta norma debe constar la creación de un órgano de control especializado en los procedimientos de acceso, rectificación, cancelación e indemnización, de los que los titulares de los datos personales se encuentran investidos, y que además imponga y controle las medidas técnicas, jurídicas y de organización que deben estar presentes en los diversos tratamientos de datos personales.

El tema del consentimiento o autorización expresa, en la transferencia de datos personales, es fundamental para la efectiva protección de datos personales, sin embargo actualmente no está correctamente regulado, por lo que la ley orgánica de Protección de Datos Sensibles en nuestro país, debe regular el hecho de que el consentimiento debe ser solicitado por la persona o entidad responsable del proceso de tratamiento que se le vaya a dar a la información, y por lo mismo debe brindar los medios necesarios para hacer conocer al dueño de los datos personales, el motivo por el cual se recaban, el trato que se les va a dar y el resultado final.

El consentimiento debe ser expreso o por escrito, sin embargo no es siempre es práctico, por lo que en la ley propuesta, debe preverse la utilización de medios electrónicos o grabaciones de voz, de esta manera el responsable de la recolección de datos podrá probar el consentimiento, en caso de existir un desacuerdo o Litis en ese sentido.

Igualmente es esta norma deberían preverse, situaciones variadas como la Excepción al Consentimiento ya que se debe entender que existen casos en los que no será necesario en consentimiento para recolectar datos personales como cuando los datos se recojan para el ejercicio de las funciones propias de la administración en el ámbito de sus competencias, esto se debe a que la administración pública realiza actividades propias a las de su naturaleza, ya que responde a una necesidad social. Claro que estas instituciones públicas deben tener una finalidad establecida, por lo que no podrán recolectar datos sin consentimiento, si esa información tiene otro objetivo del supuesto, por ejemplo.

Debe tratarse de una norma que en la práctica brinde una adecuada custodia a la información, que facilite el tema del el otorgamiento del consentimiento del titular y

de que en el mismo se encuentre información sustancial en cuanto al propósito de la recolección de datos, por lo que se debe regular de igual forma el procedimiento de recolección de los datos, ya que debe ser de forma transparente y para un fin específico.

En este orden de ideas, es necesario precisar que las normas ya existentes que pretenden precautelar el derecho de protección de datos personales en el Ecuador, como las resoluciones de la Dirección Nacional de Registro de Datos Públicos, deben ser derogadas y más bien unificarse esos enunciados en la ley orgánica propuesta.

En cuanto al recurso de Habeas Data, considero que debe mantenerse ya que es una garantía jurisdiccional, que precautela, además del derecho analizado en la presente disertación, otros derechos fundamentales, por lo que debe mantenerse como el mecanismo fundamental para la protección de datos y para la disposición de la información personal por parte de su titular.

Igualmente los tipos penales analizados, deben mantenerse ya que deben sancionarse las conductas que vulneran la privacidad de los ciudadanos, por lo que la ley propuesta tiene independencia de la norma penal, no obstante debe mantener congruencia con esta y con los preceptos fundamentales establecidos en la Constitución de la Republica.

Es necesario recomendar de igual forma que se deben mantener políticas públicas para que se materialicen las medidas técnicas, de organización y jurídicas en cuanto al manejo de información personal, si bien es cierto que estas políticas se materializan a largo plazo, sin embargo se debe mantener una conciencia de la realidad de la autodeterminación informática en nuestro país y el Estado debe intervenir en este sentido, realizando estudios y posteriores reformas en los sistemas tanto informáticos como jurídicos para que se mantenga una reserva adecuada de la información personal en bases públicas y privadas.

Estas políticas públicas, merecen tener varias aristas, tanto jurídicas como sociales, con el afán de brindar una conciencia social, en este sentido, e igualmente permitir que el ciudadano conozca los derechos de los que se ve provisto y que los ejercite adecuadamente, con el fin de que se proteja su derecho, en la medida que no se vulneren otros como el orden público o derechos de terceros.

CONCLUSIONES

- En el Ecuador, actualmente existe una dispersión jurídica, es decir que algunas normas constitucionales, penales, de carácter administrativo e incluso de rango de resolución, citadas y analizadas a lo largo del desarrollo de la presente disertación, que pretenden proteger a los datos personales que se encuentran en bases de datos de instituciones, en su mayoría públicas, sin embargo estas normas no brindan una protección material y adecuada de los datos personales y de forma conexa al derecho a la intimidad de los titulares de la información.

- Pude inferir en mi investigación que no existe mayor conocimiento de los ciudadanos acerca de su facultad de exigir el cumplimiento de los derechos de acceso y rectificación de la información personal que reposa en los bancos de datos de instituciones públicas y privadas; derechos que brindan una protección jurídica adecuada de la información, por lo que se torna lejana la idea de la reparación material de la vulneración del derecho a la intimidad o protección de datos.

- El consentimiento sobre la disposición de terceros, de su información personal, otorgada por el titular de los datos, cuando estos son recolectados, es el mecanismo práctico más adecuado para brindar protección jurídica al mal uso divulgación de la información, ya que el titular está respaldado es este documento para exigir reparación cuando se vulnere alguno de sus derechos; Sin embargo en nuestro país no está previsto, en muchos casos y carece de regulación adecuada, ya que debe existir disposiciones que establezcan en qué casos en consentimiento debe ser expreso o tácito, en que documento debe estar contenido, el formato que debe guardar, entre otros detalles que hagan viable la implantación de este mecanismo en todos los casos de manejo de información personal sensible.

- La falta de regulación es notoria, por lo que concluyo que debe existir una norma de rango ordinario que contenga los principios del derecho constitucional a la protección de datos personales, y además que regule todos los momentos del proceso de tratamiento de datos personales, como son su recolección, organización, uso, almacenamiento, archivo, anulación o eliminación. Igualmente esta norma debe contener disposiciones en cuanto al consentimiento del titular de la información personal, disposiciones que

normalicen el tratamiento de datos personales de particulares en instituciones públicas y privadas acorde a sus funciones y actividades propias, y la existencia de un órgano regulador que controle en cumplimiento de la norma y de las actividades conducentes a esta protección.

- La mayoría de normas existentes que pretenden brindar una protección jurídica de los datos personales, tiene un alcance público, es decir que la normativa para regular el tratamiento de datos personales en instituciones privadas es casi inexistente, y esto permite que la mitad del campo de uso de la información este desprotegida, por lo que es imperante una regulación a respeto, principalmente en el tratamiento de los datos personales sensibles

RECOMENDACIONES:

- Se recomienda que en la ley propuesta en la presente investigación, se procure también la implantación de normas técnicas y de organización, al momento de manejar información personal, ya que debemos entender que en la práctica pueden presentarse problemas que deben ser resueltos técnicamente, como los procedimientos de debe seguir el encargado de la información, manejo de software, formas de almacenas la información, registros diarios de manejo entre otros.

- La realidad muchas veces supera los preceptos establecidos en la norma por lo que se debe prever todas las posibilidades de acceso a la información personal sensible por medio de herramientas informáticas, en donde los usuarios pueden mal utilizar datos personales, por lo que la ley propuesta debe también cumplir con estos objetivos.

- En la mayoría de países donde existe una regulación especializada atinente a la protección de datos personales existe un órgano regulador de naturaleza pública que controla todas las actividades de tratamiento de datos, facilita el ejercicio de derechos de acceso, anulación o rectificación de la información y dedica su función a la protección de este derecho, por lo que es recomendable que existe este ente en nuestro país para tome esta competencia.

- Es necesario educar a los que participan en el manejo de información con el objetivo de que en el proceso no se vulneren derechos y de mantenga un

proceso transparente y se cumpla con la finalidad para la cual se utilizaron los datos personales.

BIBLIOGRAFÍA:

Libros:

- BRERON Philippe. *Historia y Critica de la Informática*, Madrid, Editorial, Cátedra, 1989.
- FERREIRA RUBIO, Delia M, *El derecho a la Intimidad*, Buenos Aires Argentina, Editorial Universidad SRL, Año 1982.
- GARCÍA FALCONÍ, José C. *Manual de Práctica Procesal Constitucional*, editorial Librería Jurídica Cevallos, año 2000.
- REAL ACADEMIA DE LA LENGUA. *El Diccionario de la lengua española (DRAE)*, La edición actual 22.ª, publicada en 2001
- SANTOS GARCÍA, Daniel. *Nociones generales de la Ley Orgánica de Protección de Datos*. Madrid, España, editorial Tecnos, Año 2005.
- UICICH, Rodolfo Daniel. *Los Bancos de Datos y el Derecho a la Intimidad*. Buenos Aires, Argentina, editorial AD-HOC, julio 1999.
- VILLALBA, Carlos Alberto. *La Protección Intelectual de los Bancos de Datos sobre sus propios Datos*, Quito, Ecuador, editorial Librería Jurídica Cevallos, año 2000.

Páginas Web

- CHIAVENATO, Idalberto, *Concepto de Información*, http://definicion.de/informacion/#ixzz2bEdZfpWy, acceso: seis de agosto de 2013 a las 18h37.
- GARCÍA FALCONÍ, José, *Derecho a la Intimidad Personal y Familiar*, http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechocivil/2011/02/02/derecho-a-la-intimidad-personal-y-familiar, acceso: primero de septiembre de 2013 a las 17h00
- HONORABLE CÁMARA DE DIPUTADOS DE MÉXICO. *Compendio de Protección de Datos. Ciudad de México*, Tiro Corto editores, año 2013, http://inicio.ifai.org.mx/Publicaciones/CompendioProteccionde Datos8.pdf, acceso: veinte de agosto de 2013 a las 16h10

- HUICHALAF ROA, Pedro, *De la Proteccion de Datos Personales en Chile*, datos_personales Por Pedro Huichalaf Roa http://oiprodat.com/tag/proteccion-de-datos/, acceso: trece de febrero de 2014, a las 13h00.

- HUICHALAF ROA, Pedro, *Hacia una unificación de criterios sobre seguridad y protección de datos en Internet*, http://oiprodat.com/declaracion-de-santiago/, acceso: cinco de noviembre de 2013, a las 14h00.

- *Ley de Protección de datos personales y Acción de Habeas Data*, Uruguay http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Ancho, acceso: dos de marzo de 2014 a las 16h00.

- *Ley Federal de Protección de Datos Personales en Posesión de Particulares*, México, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf, acceso: veinte de marzo de 2014 a las 18h13.

- *Ley 25.3264, de Protección de Datos Personales*, Argentina, http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/texact.htm, acceso: veinte de de marzo de 2014 a las 18h29.

- SALMÓN ALVEAR, Carlos, *Régimen Procesal del Habeas Data en el Ecuador*, http://www.revistajuridicaonline.com/images/stories/revistas/2008/24/24-regimen-procesal-del-habeas.pdf, acceso: dos de enero de 2014 a las 13h00.

- *Sentencia del Tribunal de Justicia de la Unión Europea*, de 13 de mayo de 2014,http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=245907, acceso el 21 de mayo de 2014 a las 8h00

- *Sentencia Española 11/1998 de 13 de Enero de 1998*. http://hj.tribunalconstitucional.es/HJ/es-ES/Resolucion/Show/SENTENCIA/1998/11, acceso; veintidós de febrero de 2014, a las 14h00.

- *Sentencia 254/1993*, de 20 de julio de 1993, http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/x13._Sentencia_254-

1993_de_20_julio_1993._def.pdf, acceso: veintiuno de febrero de 2014, a las 12 h 53.

- SILEC, http://www.lexis.com.ec/website/content/servicio/esilec.aspx, ultimo acceso 21 de mayo de 2014 a las 9h00.

Leyes Internacionales:

- Declaración Universal de los Derechos Humanos, ONU, Resolución 217 A (III), el 10 de diciembre de 1948, Paris, Francia

- Decreto 164/94, relativa a la Protección de Datos Personales, de 3 de febrero de 1994, Argentina.

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

- Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), México.

- Ley Orgánica de Protección de Datos Personales, España**.**

- Ley No. 78/17, relativa a la Protección de Datos Personales, de 6 de enero de 1978, Francia.

- Ley No. 787 de Protección de los Datos personales, Nicaragua

- Ley No.1581, Ley Estatutaria de Protección de Datos Personales (LEPD), de 17 de octubre de 2012, España

- Ley No. 18.331, sobre Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008, Uruguay.

- Ley No.19.628, sobre Protección de Datos Personales, Chile

- Ley No.29733, Ley de Protección de Datos Personales, Perú

- Resolución del Consejo de Ministros de la Organización de Cooperación y Desarrollo Económico (OCDE),1961, Unión Europea

Leyes Nacionales:

- REGISTRO OFICIAL 320, de 19 de mayo de 1998, *Ley de Propiedad Intelectual*

- REGISTRO OFICIAL 449, de 20 de octubre de 2008*, Constitución de la República del Ecuador*

- REGISTRO OFICIAL, Suplemento 22, de 25 de junio de 2013, *Ley Orgánica de Comunicación.*

- REGISTRO OFICIAL, Suplemento 43, 24 de junio de 2013, Resolución 7 de la Dirección Nacional de Registro de Datos Públicos, *Norma Sobre Protección y Seguridad de Información.*

- REGISTRO OFICIAL, Suplemento 116, Fecha de publicación 10 de julio del 2000, Ultima reforma 13 de octubre 2011, *Ley Orgánica de Defensa al Consumidor.*

- REGISTRO OFICIAL, Suplemento 147, Fecha de publicación 22 de enero de 1971, *Código Penal*

- REGISTRO OFICIAL, Suplemento 180, Fecha de publicación 10 de febrero de 2014, última Reforma 11 de abril de 2014, *Código Orgánico Integral Penal..*

- REGISTRO OFICIAL, Suplemento 337, 18 de mayo de 2004, Ley orgánica de Transparencia y Acceso a la Información Pública..

- REGISTRO OFICIAL, Suplemento 557, 10 de febrero de 2014, *Ley de comercio electrónico, firmas y mensajes de datos.*

- REGISTRO OFICIAL, Suplemento 863, 5 de enero de 2013, Ultima Reforma 3 de junio de 2013, *Resolución 21 de la Dirección Nacional de Registro de Datos*

Públicos, Norma de Asequibilidad A Los Datos Personales de Los Registros Públicos.

- REGISTRO OFICIAL Suplemento 863, Fecha de Publicación 5 de enero de 2013, Ultima modificación: 3 de junio de 2013, Resolución de la Dirección Nacional de Registro de Datos Públicos, Asequibilidad a Los Datos Personales se los Registros Públicos

- REGISTRO OFICIAL, Suplemento 996, 10 de agosto de 1992, *Ley especial de telecomunicaciones.*

- REGISTRO OFICIAL, Suplemento 52, 22 de Octubre de 2009. *Ley de Garantías Jurisdiccionales y Control Constitucional*

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Yo, Andrea Paola Merizalde Reinoso, C.I. 171616636-6, autora del trabajo de graduación titulado "Protección Legal de Datos Personales y la Reserva de Información Personal y su Transferencia sin consentimiento del titular", previa a la obtención del grado de **ABOGADO** en la Facultad de **JURISPRUDENCIA:**

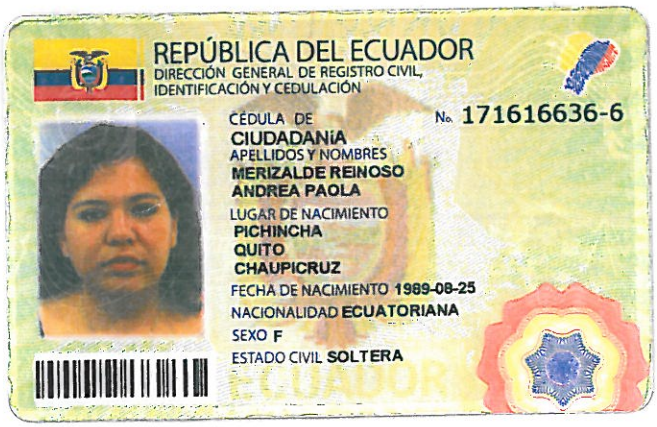
Declaro tener pleno conocimiento de la obligación que tiene la Pontifica Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

Autorizo a la Pontifica Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE el referido trabajo de graduación respetando las políticas de propiedad intelectual de Universidad.

Quito 30 de junio de 2014

171616636.

FIRMA Y CEDULA



REPÚBLICA DEL ECUADOR
DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN

CÉDULA DE CIUDADANÍA No. 171616636-6

APELLIDOS Y NOMBRES
MERIZALDE REINOSO ANDREA PAOLA

LUGAR DE NACIMIENTO
PICHINCHA
QUITO
CHAUPICRUZ

FECHA DE NACIMIENTO 1989-08-25
NACIONALIDAD ECUATORIANA
SEXO F
ESTADO CIVIL SOLTERA

INSTRUCCIÓN
SUPERIOR

PROFESIÓN / OCUPACIÓN
ESTUDIANTE

E3343I2242

APELLIDOS Y NOMBRES DEL PADRE
MERIZALDE FREDDY BAYARDO

APELLIDOS Y NOMBRES DE LA MADRE
REINOSO TERESA MARGARITA

LUGAR Y FECHA DE EXPEDICIÓN
QUITO
2013-01-07

FECHA DE EXPIRACIÓN
2023-01-07

DIRECTOR GENERAL

FIRMA DEL CEDULADO

REPÚBLICA DEL ECUADOR
CONSEJO NACIONAL ELECTORAL

CERTIFICADO DE VOTACIÓN
ELECCIONES SECCIONALES 23-FEB-2014

011

011 - 0197
NÚMERO DE CERTIFICADO

1716166366
CÉDULA

MERIZALDE REINOSO ANDREA PAOLA

PICHINCHA
PROVINCIA

QUITO
CANTÓN

CIRCUNSCRIPCIÓN 1
RUMIPAMBA
PARROQUIA

3
ZONA

f.) PRESIDENTA/E DE LA JUNTA