



FACULTAD DE DERECHO Y CIENCIAS SOCIALES

I

#DERECHOALOLVIDODIGITAL – RECONOCIMIENTO DE LOS CRITERIOS DE
APLICABILIDAD DEL DERECHO AL OLVIDO DIGITAL EN EL ECUADOR

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para
optar por el título de Abogado de los Tribunales y Juzgados de la República

Profesor Guía

Ms. Lorena Naranjo Godoy

Autor

Christian Fabián Espinosa Velarde

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

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

Lorena Naranjo Godoy

Magister en Derecho de las Nuevas Tecnologías

C.I.: 170829378-0

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

Rafael Eduardo Serrano Barona
Especialista en Derecho de nuevas Tecnologías
C.I.: 171298093-5

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

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

Christian Fabián Espinosa Velarde

C.C.: 0918039710

AGRADECIMIENTO

“¡Gracias a Dios, porque nos ha hecho un regalo tan grande que no tenemos palabras para expresarlo!”
(Corintios II, 9,15).

A mi familia, maestros y amigos, que supo tenerme paciencia e impulsarme a alcanzar mis metas, siendo ejemplo y aliento. A Lucas, mi motor.

A las misiones, que fueron fuerza y fe para alcanzar esta meta, que estuvieron cuando caía y me levantaba.

A mi tutora, guía imprescindible.

A ti, por ser, por estar, por existir

DEDICATORIA

A ti nenita y a ti campeón, hoy comenzamos a brillar, y no habrá sol que brille más. ¡Victoria!

Christian

RESUMEN

La Constitución de la República del Ecuador, promulgada en 2008, reconoce, en su capítulo de "Derechos de Libertad" la protección de datos de carácter personal, pero el marco global ha desarrollado escenarios que el derecho no había contemplado inicialmente, en mayor parte gracias a los avances tecnológicos, que presuponen riesgos para las personas dada la manipulación de sus datos personales.

Este riesgo surge por los avances dados en la Internet, una red que permite el acceso a datos e información de diversas índoles en cualquier momento y en cualquier lugar, y que ha cambiado el paradigma de la memoria. Esto es lo que ha generado un riesgo latente para las personas pero dado su dinamismo, el Derecho ha logrado evolucionar y adaptarse hasta generar instrumentos que amparan a las personas para proteger sus datos personales.

El análisis de la legislación internacional, así como de diversa jurisprudencia, ha permitido establecer el surgimiento de una nueva figura como es el derecho al olvido digital, aplicable en el Ecuador, utilizando los elementos constantes en el marco constitucional vigente, así como la normativa existente, pero cambiando la visión de una acción reactiva hacia un derecho inherente a las personas.

Las personas, en el territorio ecuatoriano, ya gozan de la protección de sus datos personales, pero el derecho al olvido digital, marca un nuevo hito en este campo, permitiendo a las personas que ninguna persona, en ningún lugar a nivel mundial, pueda acceder a ellos.

Aún en la contraposición de derechos, como a las libertades de información y expresión, se encuentra una solución para proteger a aquellos que ven víctimas del tratamiento inadecuado, por decir lo menos, de sus datos personales, y así sienten vulnerados sus derechos.

Así el Derecho avanza y enfrenta a la tecnología, superándola, en pos de mejores condiciones para los seres humanos, para los ecuatorianos.

ABSTRACT

The Constitution of the Republic of Ecuador, enacted in 2008, recognizes the protection of personal data in its chapter on "Freedom Rights", but the global framework has developed scenarios that the law had not initially contemplated, mostly thanks to the technological advances, that presuppose risks for the people, given the manipulation of their personal data.

This risk arises from the advances made on the Internet, a network that allows access to data and information of various kinds at any time and at any place, and which has changed the paradigm of memory. This is what has generated a latent risk for people but, given its dynamism, the law has managed to evolve and adapt to generate instruments that protect people to protect their personal data.

The analysis of international legislation, as well as different jurisprudence, has allowed to establish the emergence of a new figure such as the right to digital oblivion (right to be forgotten), applicable in Ecuador, using the elements contained in the current constitutional framework, as well as the normative Existing, but changing the vision of a reactive action towards an inherent right to the people.

The people, in the Ecuadorian territory, already enjoy the protection of their personal data, but the right to be Forgotten, marks a new milestone in this field, allowing people that no person anywhere in the world can access to them.

Even in the opposition of rights, as well as freedom of information and expression, is a solution to protect those who are victims of inappropriate treatment, to say the least, of their personal data, and thus feel violated their rights.

Thus the right advances and confronts technology, surpassing it, in order to better conditions for human beings, for ecuadorians.

ÍNDICE

INTRODUCCIÓN	1
1. CAPÍTULO I: NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y DATOS PERSONALES	3
1.1 WEB 2.0 y las Nuevas Tecnologías de Información y Comunicación.....	3
1.1.1 WEB 2.0.....	3
1.1.2 Nuevas Tecnologías de Información y Comunicación	5
1.2 Memoria digital.....	11
1.3 Motores de búsqueda y el indexado de información	17
1.3.1 Motores de búsqueda	17
1.3.2 Indexado de la información	22
1.4 Datos personales, marco constitucional y legal en el Ecuador ...	26
1.4.1 Datos personales	26
1.4.2 Origen y evolución del derecho de la protección de datos. Legislación internacional	27
1.4.3 Marco constitucional y legal en el Ecuador.....	32
1.5 Sumario	39
2. CAPÍTULO II: DERECHO AL OLVIDO DIGITAL	41
2.1. ¿Qué es el derecho al olvido digital?	42
2.2. El movimiento europeo	45
2.3. Aspectos de análisis.....	50
2.4. La aplicación en razón al territorio	51
2.5. La Ratio Materiae de la Directiva 95/46/CE	56
2.6. Sobre el derecho al olvido digital.....	59
2.7. Ponderación de Derechos.....	62
2.8. Derechos ARCO y derecho al olvido.....	66
2.9. Derecho al olvido, una visión internacional.....	67

2.9.1. En Europa.....	67
2.9.2. En América	69
2.10. Sumario.....	73
3. CAPÍTULO III: DERECHO AL OLVIDO DIGITAL EN ECUADOR	75
3.1. Derecho a la Protección de Datos	76
3.2. Ecuador y Europa, una comparación en materia de derechos de protección de datos personales	79
3.2.1. Titularidad	80
3.2.2. Autodeterminación Informativa	81
3.2.3. En materia de datos personales.	83
3.2.4. Criterios no contemplados en el ordenamiento jurídico ecuatoriano.....	84
3.3. Habeas Data y Protección de Datos Personales.	86
3.4. La dignidad humana como base para el reconocimiento del derecho al olvido digital.	89
3.5. Progresividad de los derechos aplicada para el reconocimiento del derecho al olvido digital	94
3.6. Aplicación del derecho al olvido digital en el Ecuador.	97
4. CONCLUSIONES Y RECOMENDACIONES.....	100
4.1 CONCLUSIONES.....	100
4.2. RECOMENDACIONES	103
REFERENCIAS	104

INTRODUCCIÓN

Esta nueva era, en la cual la internet cumple un rol de gran importancia en la sociedad moderna, la información que circula a través de ella se perenniza, permaneciendo inalterable, y accesible en cualquier lugar y momento, sin ninguna consideración o importancia sobre la veracidad de dicha información, ni de quien la pública, causando una considerable afectación a los derechos de libertad de las personas.

Hoy las nuevas tecnologías de información y comunicación han afectado el concepto de memoria, no solo respecto a cómo la información es almacenada, sino también sobre cuánto tiempo permanece visible, sobre cómo se transmite y acerca de quiénes pueden acceder a ella.

Tanto públicos como particulares almacenan y manejan información de las personas, y el uso que se le da no está protegido adecuadamente, y es así que mucha de esa información termina siendo utilizada de manera inadecuada, incluso expuesta en internet, donde cualquier persona puede acceder a ella.

Con este uso inadecuado, se registran vulneraciones al derecho a la protección de datos de carácter personal con un alcance que llega hasta la dignidad de las personas y es el derecho al olvido digital el que surge como una reacción frente a las vulneraciones a la dignidad de las personas y a su derecho de protección de datos, causadas por la eternización de la información y a la facilidad con la que puede ser accedida gracias a la utilización de los motores de búsqueda (entiéndase Google, Bing, Yahoo!, entre otros).

En virtud de lo expuesto, esta investigación tiene como objetivo el establecer las condiciones del ordenamiento jurídico ecuatoriano que se deben considerar para el reconocimiento y aplicación del derecho al olvido digital.

De forma más específica, se buscará revelar, en primer término, la *WEB 2.0* y la Memoria Digital, el establecer que se entiende como datos personales y como el derecho ha cubierto su protección. Luego se procederá a definir el derecho al olvido digital, reconociendo sus bases y su alcance, y se llevará a cabo un análisis de la sentencia del Tribunal de Justicia de la Unión Europea

sobre el caso Costeja y AEPD vs Google INC y Google Spain SL., estudiando los criterios que sienta a la hora de reconocer el derecho al olvido digital.

En tercer lugar se abordará el ámbito ecuatoriano a fin de establecer cómo se lleva a cabo la protección de datos personales, el reconocimiento de la autodeterminación informativa, y cómo ambos criterios estructuran el marco para la aplicación del derecho al olvido digital. Asimismo, se analizará el cómo se reconoce la dignidad de las personas para sentar las bases constitucionales para la implementación de este derecho, haciendo uso del principio de progresividad.

Para el desarrollo del presente trabajo de titulación se utilizarán varios métodos de investigación, como el exegético, a través del cual se procederá a efectuar una análisis de diversas normas internacionales y ecuatorianas para reconocer las condiciones que se requieren y existentes, respectivamente, para el reconocimiento y aplicación del derecho al olvido digital

Luego con la utilización del método inductivo, se llevará a cabo el análisis de los casos conocidos, a nivel internacional, en materia de derecho al olvido digital, de tal manera que se pueda entender el desarrollo del mismo, las posiciones de quienes conocieron dichos casos, y como resolvieron, de tal manera que se pueda establecer un idea respecto la regla aplicable en el caso ecuatoriano.

Finalmente, el método analógico será de utilidad al momento de establecer los criterios de aplicación del derecho al olvido digital en el Ecuador

Luego del proceso de investigación y desarrollo del presente trabajo de titulación, se espera obtener como resultado los criterios necesarios para reconocer el derecho al olvido digital en el Ecuador, toda vez que en un mundo globalizado, las afectaciones se replican en cada país y la defensa de los derechos de las personas es una obligación.

1. CAPÍTULO I: NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y DATOS PERSONALES

“Me parece, Golan, que el avance de la civilización no es más que un ejercicio en la limitación de la intimidad” (Asimov, 1983)

La frase previa envuelve la visión que Asimov tenía del futuro, hoy, no tan lejos de la realidad, pareciera que su autor tuvo una premonición de como evolucionarían las tecnologías y de cómo los seres humanos generarían un vínculo tan fuerte con ellas, que generarían un alto nivel de dependencia.

A lo largo del presente capítulo se abordarán temáticas relacionadas con generalidades de las nuevas tecnologías de la información y a partir de las definiciones generales se llegará a discurrir sobre la WEB 2.0 y las nuevas tecnologías de la información y comunicación.

En ese mismo orden de ideas, se abordará la memoria digital desde diferentes aristas. Los motores de búsqueda y el indexado de la información, encuentran su espacio en este capítulo, al igual que los datos personales, con su correspondiente regulación en el marco constitucional y legal en el Ecuador con el objetivo de establecer las bases doctrinales y jurídicas de esta investigación, lo cual nos permitirá más adelante, diseñar una propuesta legislativa que regule la protección de datos y el derecho al olvido digital en Ecuador.

1.1 WEB 2.0 y las Nuevas Tecnologías de Información y Comunicación

En este acápite se discurrirá sobre la WEB 2.0 y las nuevas tecnologías de información y comunicación porque es el contexto en el cual se desarrolla la investigación, es decir, el ámbito de aplicabilidad del derecho al olvido digital. Es importante destacar que si bien este trabajo se desarrolla en el ámbito jurídico, estos criterios técnicos nos permitirán diagnosticar cuál sería la forma más idónea de legislar sobre esta materia en Ecuador.

1.1.1 WEB 2.0

La WEB 2.0 es una definición que vio la luz en el año 2004, por el estadounidense Dale Dougherty de la editorial O' Reilly Media, naciendo de la

necesidad de distinguir los sitios web más novedosos de los tradicionales, que ya se conocían como Web 1.0. En tal sentido, la WEB 2.0 se refiere al fenómeno social que, a partir del desarrollo de diversas aplicaciones en internet, ha surgido a nivel mundial

El concepto establece una distinción entre la primera época de la Web (donde el usuario era básicamente un sujeto pasivo que recibía la información o la publicaba, sin que existieran demasiadas posibilidades para que se generara la interacción) y la revolución que supuso el auge de los blogs, las redes sociales y otras herramientas relacionadas” (Definición. DE, recuperado el 20 de noviembre de 2016).

La WEB 2.0 es la evolución de tecnologías y la creación de otras que han posibilitado el desarrollo de páginas web más dinámicas, con una experiencia de usuario diferente a la tradicional, la cual implementa estándares de accesibilidad más rigurosos. Hoy la web, que todos apreciamos, es de manera general una WEB 2.0.

Según Rodríguez Palchevich:

“No podemos definir la WEB 2.0 como un producto o servicio acabado. Debemos considerarla más bien, como la web convertida en una plataforma de comunicación y trabajo colectivo, en constante cambio además. Es un conjunto de aplicaciones y servicios que promueven la participación y creación, publicación y diseminación de contenidos Si bien se apoyan en herramientas informáticas, la WEB 2.0 es una actitud más que una tecnología” (Rodríguez Palchevich, 2008, p. 7)

Es imperativo acotar que la principal diferencia entre la Web 1.0 y la WEB 2.0, es el grado de participación colaborativa que realizan los usuarios. Así, podemos decir, por ejemplo, que una página que se limita solo a presentar información, pertenece al modelo Web 1.0, mientras que por el contrario una página que permite que el usuario interactúe con ella y se actualiza con las colaboraciones de los usuarios, pertenece a la generación 2.0.

Para Rodríguez Palchevich (2008, p. 7) las principales diferencias radican en las que se muestran en la siguiente tabla:

Tabla 1.

Comparativa Web

WEB 1.0	WEB 2.0
Páginas estáticas	Páginas dinámicas
Sitios creados y modificados por Webmaster	Sitios creadas y modificados por Usuarios
Fuente de contenidos	Plataforma de comunicación, creación y
Flujo unidireccional de la información	Flujo de información en red s
Usuario consumidor de información	Usuario prosumidor de información

Tomado de (Rodríguez, 2008, p. 5)

Así, la Web 1.0 encuentra su fundamento en los medios de difusión masiva, medios tradicionales, como la televisión, la radio y el email; y la WEB 2.0, se centra en el entretenimiento y conocimiento activo.

El internet, o la red de redes, como también se le conoce mundialmente, es un sistema universal de comunicaciones, que garantiza el acceso a la información que se encuentra disponible en los distintos servidores del mundo. La red de redes y la WEB 2.0, de conjunto, nos brindan la posibilidad de interrelacionar personas que se encuentren distantes geográfica y temporalmente. Y es que, la WEB 2.0, en su esencia, busca ese intercambio viable de información entre los consumidores, los que con su participación y colaboración producen nuevas informaciones y contenidos. Se ha de resaltar la relevancia que tiene el estudio de estos aspectos para la investigación propuesta, porque precisamente es el marco contextual en el cual podremos corroborar la necesidad que tiene el Ecuador de legislar sobre el derecho al olvido digital.

1.1.2 Nuevas Tecnologías de Información y Comunicación

Antiguamente cuando hablamos de los medios de información y comunicación nos referíamos a la prensa plana, la radio y la televisión. Hoy día, con la

evolución constante de la tecnología han alcanzado un gran valor nuevos instrumentos electrónicos que permiten el entretenimiento, la información y la comunicación; es el caso de la televisión, el teléfono, el video y la computadora.

Es indudable, que el computador supera con creces el resto de los medios en la sociedad de hoy, permitiendo utilizar una gran variedad de aplicaciones, dígame, multimedia, programas ofimáticos, entre otros, pero un lugar preponderante ocupan la internet y, de manera aún más especial, las redes sociales.

Desde su aparición en los años 1970 y su desarrollo en los años 1990-95, internet (Internetting= interconectar redes) se ha convertido en una “red de comunicación” que permite la transferencia de datos, ideas, comentarios y soluciones, a una velocidad y con una extensión impensable hasta hace muy poco. Sin embargo, las redes sociales son un fenómeno reciente: es el caso de Facebook/Twitter/Tuenti, redes sociales que se estiman relevantes, que fueron creadas en 2006, salvo Twitter, que nació en 2007.

Actualmente internet forma parte de la vida de las personas, ya que ha pasado a integrarse en nuestras costumbres y hábitos en el plano personal y profesional. Internet tiene además un gran poder de penetración en el mundo, lo que le da una capacidad de acción muy importante.

Con la evolución constante de las tecnologías de información y comunicación, han emergido las redes sociales, así, se le ha dado la bienvenida a sitios donde las personas pueden incorporar sus criterios, opiniones, sus fotos, en fin, toda la información personal que gusten, estos son los casos de Facebook, Twitter, My Space, Tuenti. También se pueden compartir, mediante las redes sociales, videos, empleando YouTube, así como descargar, lo que otras personas hayan subido para la vista de todos.

“La WEB 2.0, por lo tanto, está formada por las plataformas para la publicación de contenidos, como Blogger, las redes sociales, como Facebook, los servicios conocidos como wikis (Wikipedia) y los portales de alojamiento de fotos, audio o vídeos (Flickr, YouTube) La esencia de

estas herramientas es la posibilidad de interactuar con el resto de los usuarios o aportar contenido que enriquezca la experiencia de navegación” (Muñoz, 2015).

Se tienen además los blogs, que son sitios web donde sus autores compilan sus artículos y textos, manteniendo siempre el criterio de cronología, manteniendo en primer orden los más novedosos. Los autores actualizan el sitio libremente. Los hay de distintos tipos, educativos, personales, de moda, empresariales, etc.

Un ejemplo de blog empresarial es el que puede ser creado por una empresa de mueblería, para interactuar con sus clientes o futuros clientes, en cuanto a la fabricación y venta de los muebles de su catálogo. En el caso de los libros, también es posible acceder a ellos, dado que existe un sitio, como Google books, que facilita la obtención e incorporación de material novedoso por parte de los usuarios. En tal sentido, se dispone de documentos colaborativos, como las wikis e incluso, los blogs, que ya se ha mencionado, donde pueden subir información sobre determinados temas y compartir su criterio al respecto.

Como es posible comprender, estos diferentes sitios, aprovechan la inteligencia colectiva y así crear páginas más interactivas, donde el propio usuario publica sus datos y los comparte con los demás. De ahí, la necesidad de estudiar la WEB 2.0, desde sus características, para poder determinar en qué sentido influye sobre los derechos de las personas que a ella acceden, ya sea para bien o para mal.

En la actualidad, la tecnología forma parte de la vida cotidiana, siendo utilizada en las cosas más simples, desde hacer un licuado en las mañanas o para calentar alimentos en el microondas, incluso para tostar un pan; hasta las más complicadas como desarrollar un software o un videojuego. La tecnología la encontramos en casi todos los ámbitos de la vida: en el trabajo, como la laptop; en la casa, por ejemplo la televisión; e incluso en la escuela.

Según Pere Simón Castellano (2012) las características fundamentales de la WEB 2.0, que se encuentran relacionadas entre sí, y que inciden directamente

en la manifestación de la web sobre el conjunto de derechos ciudadanos, son las siguientes:

- “La desaparición de la distancia espacio-temporal de la acción y la publicidad;
- La formulación de nuevos espacios de razonamiento público ciudadano a nivel global sin control estatal;
- Los ciudadanos como emisores y difusores de la información;
- La incorporación del aspecto afectivo, pasional, o emocional y la despreocupación en la transmisión de información;
- La perennidad y la conservación de la información en internet” (Castellano, 2012, p. 26)

Estas características, que enuncia Pere Simón, son un resumen ávido de la realidad social actual, donde como parte de la revolución tecnológica que se experimenta, donde a través de los teléfonos móviles se pueden hacer fotos y videos, y de manera casi instantánea difundirlos en la web.

Es así que, cuando no existía la publicidad inmediata, que acecha hoy, tenía en primer lugar la revisión y la censura, y luego después de haberse filtrado la información, ocurría su publicación. Hoy, tiene lugar la publicación y después que la misma ha sido generalizada, y frente a quejas u oposición por el contenido de la misma, es que tiene lugar la censura, es decir, primero ocurre el daño y luego es que se produce la rectificación o censura de la información que laceró el honor o el derecho a la privacidad de la persona.

En tal sentido se debe considerar uno de los ejemplos consignados por Pere Simón Castellano (2012), en su libro “El régimen constitucional del derecho al olvido digital”, cuando habla de lo intentos de censura de la información que es difundida en Internet:

“Otro caso fallido es el de Turquía, si bien muestra que, excepcionalmente, hay plataformas que son susceptibles de ser vetadas, como es el caso de *YouTube*, aun así, a pesar de que el Estado turco, además, también restringe el acceso a más de 5000 espacios web, no puede evitar la difusión de información y expresiones, a través de la WEB 2.0, y cuando lo hace, el control llega tarde. Observamos así, como el tiempo entre la decisión de publicar y la publicidad, se ha evaporado, de tal manera que las posibilidades de censura han quedado considerablemente restringidas” (Castellano, 2012, p. 28).

Ahora, se debe tomar conciencia además, que las nuevas tecnologías, también generan invasión de los derechos, por lo que debe se debe trabajar en base a la salvaguarda constante de los datos personales, a la protección integral de los mismos.

Así por ejemplo, la WEB 2.0 de conjunto con el internet, posibilita que las personas participen en el proceso de comunicación pública, donde los ciudadanos, sin importar en el lugar donde estén, pueden acceder al ciberespacio y emitir sus criterios, hacer juicios críticos, que a la larga fomentan el desarrollo cognitivo de los seres humanos. Así como las nuevas tecnologías abran las puertas al fortalecimiento de la democracia, se genera una responsabilidad para los usuarios de estas herramientas, que no siempre están dispuestos a asumir, aun y cuando sean ellos mismo los principales emisores y difusores de la información.

No obstante, y como resultado de esto se pueden tipificar, a juicio de Pere Simón Castellano (2012), dos tipos de conductas ciudadanas, cuando las personas suben o publican información que pertenece a tercera personas:

“Una primera conducta lesiva se produciría cuando el ciudadano publica con inmediatez en Internet una información que afecta al derecho a la protección de datos de terceros. La segunda se produce cuando el titular del medio, ya sea un foro, bitácora, cuenta de *Facebook* o *Twitter*, etc., no elimina la información los datos personales de terceros cuando es plenamente consciente de que ha realizado la publicación de los mismos sin el consentimiento del afectado” (p. 38).

La información se eterniza al ser compartida y difundida en la red de redes, lo que trae consigo la preservación del pasado, lo que es fuentes indubitable de problemas, tanto personales como sociales, si se tiene presente la cantidad y diferentes tipos de información que Internet socializa, como son: “fotos en línea, actualizaciones de estado, entradas de bitácoras, participaciones en foros, revelaciones personales o acciones vergonzosas publicadas en las redes sociales, etc.” (Castellano, 2012, p. 39)

De esto se colige una preocupación válida de muchas personas que en la línea del empleo las ventajas y utilidades de las tecnologías de la información, ven

en peligro la intimidad y la reputación de las personas, producto de la creciente acumulación de datos personales en la red.

Resulta oportuno, entonces, reflexionar con el análisis efectuado por José Luis Piñar Mañas (Piñar Maña, 2009, p. 23).

“Pensemos que hoy es posible conocer los contenidos de los correos electrónicos, de las llamadas efectuadas o recibidas mediante teléfonos móviles; que pueden tratarse para múltiples finalidades los datos genéticos; que el uso de datos biométricos está casi a la orden del día; que las nuevas tecnologías pueden afectar grave e intensamente a los derechos fundamentales e incluso pueden condicionar el contenido de las normas jurídicas”.

Se puede evidenciar, entonces, que la vida de las personas está constantemente monitoreada por la tecnología, y buena parte del tiempo ni siquiera se lo nota, pues sucede desapercibidamente, el más claro ejemplo de esto se da, hoy por hoy, en las redes sociales Facebook o Twitter, buscadores como Google e incluso sistemas operativos como Windows 10, donde se recopilan datos, en su mayoría de manera anónima pero otros, por su naturaleza la información generada se trata de manera anónima, pero por su naturaleza, revelan quien los genera.

La sociedad moderna ha puesto a las personas ante una avalancha de información con grandes y fáciles posibilidades de acceder a ella, sin considerar muchas veces el enorme peligro que representa el que existan tantas medidas para su protección en la flamante sociedad en que vivimos. Razón por la cual se termina aceptando que son justas y necesarias; e incluso, sin llegar reflexionar sobre cómo pueden llegar a afectar los derechos esencialísimos de los mismos usuarios.

No obstante lo antes planteado, surge como interrogante si los ciudadanos deben quedar condenados a que sus datos personales e información estén eternamente disponibles, gracias a la memoria digital, en estas redes sociales o motores de búsqueda sin que hayan brindado su consentimiento o a no contar con la opción de retirarlos una vez se haya cumplido el fin para el cual se concedió la aprobación.

Por ello estudiar en qué consiste y cuál es el alcance de las nuevas tecnologías y su relación con la comunicación resultó trascendental para esta investigación, pues de esa manera se pudo evaluar tanto los aspectos positivos como los contraproducentes que acarrearán tanta evolución y, ya centrados en el objeto de estudio de esta investigación, analizar cómo contrarrestar los efectos de la sobre exposición de la información en estos medios de comunicación tecnológicos, promoviendo así, la promulgación de una legislación que regule y garantice el derecho al olvido digital en Ecuador.

1.2 Memoria digital

Siguiendo la línea de investigación propuesta, esta sección versará sobre la memoria digital, buscando su análisis conceptual y el estudio de su alcance; de esta manera, se podrá definir, desde una perspectiva jurídica, la forma en la cual debería ser regulada y cómo debe ser limitada.

La memoria digital es un concepto novedoso, aunque no tan reciente, si tenemos en cuenta que hace ya más de una década vivimos inmersos en la era digital. Lo que antes conocíamos como memoria, recuerdos, evocaciones que muchas veces perecían en el tiempo, es un hecho del pasado, pues con la era de la digitalización nuestros recuerdos, vivencias y experiencias al ser digitalizadas se tornan en imperecederos.

Como ya lo dijo (Celorio, 2012) “la memoria es una mirada a la historia, llena de recuerdos y olvidos; *recuerdos* que toman la forma de documentos, archivos, mapas, planos, registros y acervos; de testimonios y narraciones orales individuales y colectivas (...)”.

Un estudio realizado a nivel internacional que fuera publicado en la revista *Science Express*, realizó un análisis sobre la capacidad tecnológica - analógica y digital - que se ha venido almacenando en las últimas décadas a escala global, y concluyó que “en 2007, la humanidad fue capaz de almacenar 295 billones de megabytes óptimamente comprimidos, comunicar casi dos cuatrillones de megabytes, y llevar a cabo 6,4 billones de MIPS (millón de instrucciones por segundo) en ordenadores de uso general” (Britton, 2011).

Poco a poco se ha ido creando una memoria histórico-digital, donde a través de las nuevas tecnologías de información y comunicación las personas han ido digitalizando y almacenando sus registros históricos personales. El hecho de que las personas a través de las redes sociales y demás recursos tecnológicos, compartan su información personal trae aparejado que esta se preserve en el tiempo para bien o para mal, y sin consideración a esto, cada día se socializa más la información.

Incluso, las nuevas tecnologías de la información, han posibilitado soñar a científicos con un implante de memoria digital en humanos. Conforme a lo que publicó Computerhoy (2015) se están realizando las primeras pruebas de dichos implantes. “Un neurocientífico estadounidense ha comenzado a probar en humanos unos implantes de memoria que podrían ayudar a combatir enfermedades como el Alzheimer y dignificar la última parte de la vida de cada ser humano” (Computerhoy, 2015).

Continúa el informativo digital diciendo en esa misma publicación:

“Theodore Berger, un ingeniero en biomedicina de la Universidad de California del Sur, lidera un proyecto financiado por DARPA que intenta desarrollar un implante de memoria capaz de imitar el proceso que se produce en el cerebro cuando las neuronas guardan recuerdos a largo plazo” (Computerhoy, 2015).

Se ha podido constatar el cambio de paradigma que ha venido teniendo lugar en la sociedad, donde lo común y normal era olvidar, como parte de la naturaleza humana; pero con la acelerada revolución tecnológica que se ha experimentado, incluso ha removido este hecho, dando como resultado un cambio de paradigma, que ha convertido en normal, lo que anteriormente era anormal o inimaginable. Es así, que hoy día lo normal es que se perpetúen los recuerdos en el tiempo, a través de la red de redes y de las distintas herramientas que se disponen actualmente.

Esto además de posibilitar determinados beneficios, porque permite el acceso a la información o contenidos por muy antiguos que sean, también generan profundos inconvenientes, si tenemos en cuenta que no en todos los casos vale la pena recordar.

La memoria digital es la llave que ha permitido almacenar información rompiendo las barreras del tiempo y del espacio, valiéndose de herramientas para poder acceder a ella. Uno de los medios que permite acceder a la información que se ha digitalizado con el decursar del tiempo y continúa digitalizándose, son los motores de búsqueda, y con ellos el proceso del indexado, que posibilita la búsqueda por términos o vocablos de más fácil acceso y que permite que la información, a menos que sea intencionalmente, no desaparezca, sino que permanezca asentada en los diferentes archivos disponibles al efecto.

En esta nueva era digital, donde la información se eterniza y perdura con el paso del tiempo, aparecen consecuencias adversas para las personas que son víctimas de este estancamiento informativo.

La memoria digital preserva los registros publicados en diarios o redes sociales desde su aparición y por todos los años venideros. Estas pudieron ser de mucho interés en algún momento, importantes o necesarias en el tiempo que fueron publicadas, pero que luego del paso del tiempo, su interés cayó o el tema sobre el que versaban cambió o se resolvió y sin embargo de esto, en todo momento que se efectúe una búsqueda relacionada con algún aspecto relacionado con esa noticia, sea la ciudad donde aconteció o el nombre de alguna persona relacionada, esta reporte noticioso aparecerá entre los resultados, creando una carga a manera de estigma sobre todo o todos los vinculados con el suceso reportado años antes.

Esta es la esencia de la memoria digital, permitiendo que se continúe cargando una culpa social por tiempo indefinido, y todo porque la red de redes no olvida, y la memoria digital tampoco. Y es que, el mantenimiento de ciertos datos, como pueden ser los antecedentes penales, si bien no son de interés público estatal, puede afectar el honor y el buen nombre de las personas.

Antes de la aparición y popularización de estas nuevas tecnologías de la información y comunicación, de forma contraria a lo que sucede hoy, una persona cuando extinguía su sanción, terminaba con ese hecho, tal vez

incluso, lamentable para esa misma persona, y a menos que él mismo lo contara o las personas que lo conocieran lo manifestaran, tenía la posibilidad de quedar en el olvido, luego del transcurso de un lapso de tiempo razonable.

Y es que, las nuevas tecnologías, como ya se ha analizado son fuente de fomento del cambio de paradigma que antes se enunció, y que ha vuelto el olvido como un recurso de pocos o de casi ninguno. Aun así, resulta oportuno cuestionar: ¿cuándo vale la pena recordar? A modo de complemento, se puede decir que obviamente no es saludable recordar en todos los casos, y sí es bien recomendable, no perder de vista la importancia que se tiene la capacidad de olvidar. En tal sentido, se debería aplicar este principio humano del olvido al mundo digital que el hombre ha creado en su beneficio, pero con un alto costo de perjuicio.

Sin embargo, frente a los argumentos antes expuestos, surge un debate relativo a la memoria digital, el derecho al olvido y hasta qué punto el derecho a la libertad de expresión es una limitante de este último.

Cabe resaltar la Declaración Conjunta sobre Libertad de Expresión e Internet, emitida en el año 2011 por Frank LaRue (Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión), Dunja Mijatović (Representante de la OSCE para la Libertad de los Medios de Comunicación), Catalina Botero Marino (Relatora Especial de la OEA para la Libertad de Expresión) y Faith Pansy Tlakula (Relatora Especial de la CADHP sobre Libertad de Expresión y Acceso a la Información), determinó que

“Ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios, siempre que no intervenga específicamente en dichos contenidos ni se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo ("principio de mera transmisión")” (Organización de Estados Americanos , 2011).

En el ámbito europeo, en cuanto a este tema, se debe mencionar la sentencia C- 131/12 del Tribunal de Justicia de la Unión Europea, que dictó el 13 de mayo de 2014, para resolver el caso entre un ciudadano español y Google con

respecto al derecho al olvido, la cual generó ardua polémica. De un lado, se encontraron quienes se alegraron por el fallo y solicitaron al buscador que retirará de sus resultados algunas de las acciones polémicas que aparecían en las búsquedas. Por otra parte, están quienes han encontrado en este caso un peligroso antecedente para el ejercicio de la libertad de opinión y expresión. Así pues, distintas voces reiteradamente han dicho que los intermediarios en Internet no deberían tener responsabilidad con respecto a los contenidos generados por terceros. Entran dentro de tal supuesto los proveedores de servicio de Internet (ISP), los motores de búsqueda o los servicios de almacenamiento de datos (Rosas, 2014).

No obstante, en este trabajo se acoge el criterio del Tribunal de Justicia de la Unión Europea, que en la sentencia anteriormente citada determinó

“En relación con una situación como la del litigio principal, que se refiere a la presentación, en la lista de resultados que el internauta obtiene al efectuar una búsqueda a partir del nombre del interesado con ayuda de Google Search, de vínculos a dos páginas de archivos en línea de un periódico que contienen anuncios que mencionan el nombre de esta persona y relativos a una subasta inmobiliaria vinculada a un embargo por deudas a la Seguridad Social, es preciso considerar que, teniendo en cuenta el carácter sensible de la información contenida en dichos anuncios para la vida privada de esta persona y de que su publicación inicial se remonta a 16 años atrás, el interesado justifica que tiene derecho a que esta información ya no se vincule a su nombre mediante esa lista. Por tanto, en la medida en que en el caso de autos no parece existir razones concretas que justifiquen un interés preponderante del público en tener acceso a esta información en el marco de tal búsqueda, lo que no obstante incumbe comprobar al órgano jurisdiccional remitente, el interesado puede, en virtud de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46, exigir que se eliminen estos vínculos de la lista de resultados” (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 21).

En este caso la balanza se inclina a favor de la prevalencia del derecho al olvido sobre el derecho a la libertad de expresión, pues se considera que ante la disyuntiva entre las dos prerrogativas, debería primar el derecho a la intimidad de una persona que no desea que información personalísima de su vida se vea expuesta de manera permanente como resultados de búsqueda en Google u otro buscador.

Otro aspecto que se debe analizar en relación con este tema, gira entorno a determinar hasta qué punto el derecho al olvido digital puede representar una limitante para la memoria histórica. Se parte de la idea que, la memoria histórica resulta una acepción historiográfica desarrollada recientemente, que tiene como precursor más común a Pierre Nora. El concepto hace referencia a un esfuerzo consciente de los grupos humanos por entroncar con su pasado, pudiendo ser este real o imaginado, valorándolo y tratándolo con un respeto especial. Dicho esfuerzo consiente de los grupos humanos engendra una memoria histórica colectiva, aunque igualmente cabe la existencia de otra memoria individual o particular que pertenece a cada individuo. (Díaz, 2010). Casos donde se hace evidente el concepto de memoria histórica se observan en los hechos acontecidos en Guerra Civil y la dictadura franquista en España, en la dictadura de Pinochet en Chile o en la dictadura cívico militar de Argentina; entre otros.

En relación a la tensión entre el derecho al olvido digital y la memoria histórica, se encuentran voces disidentes, por ejemplo, en Chile se debate una ley que incorpore el derecho a rectificación o derecho al olvido digital y al respecto algunos sectores expresan que: “Eso es una locura, porque atenta contra la libertad de expresión, el derecho a informarse y la memoria histórica. O sea, eso es terminar con Internet como repositorio de información como lo conocemos hoy en día”. (Becerra, 2016). No obstante, en contraposición se encuentran criterios como los de Ramón J. Moles, quien señala

“Curioso: **exigimos el derecho al olvido digital y a la vez reivindicamos la memoria histórica. La contradicción, en realidad, no es tal.** El derecho al olvido digital no es tanto un derecho al olvido como un derecho a la contextualización, como indica el Tribunal Supremo de Estados Unidos cuando lo denomina derecho a la oscuridad práctica, esto es, derecho a pasar desapercibido en las redes. En otras palabras: que la información contenida en las redes no pueda ser malinterpretada” (Resaltado propio) (Moles, 2015).

Se comparte aquí esta última idea, ciertamente las víctimas de los dictaduras tienen el derecho a la memoria histórica, a que se recuerden los nombres de los perpetradores de torturas y delitos de lesa humanidad; sin embargo, los presuntos verdugos también tienen derecho a que el uso de sus nombres en

redes sociales, motores de búsqueda etc., no atente contra su dignidad y a que el manejo de la información que los involucra sea el adecuado; e incluso, a que frente a una inadecuada exposición de su identidad, este error sea borrado.

1.3 Motores de búsqueda y el indexado de información

En consecuencia con el desarrollo del presente estudio, se abordará en los consiguientes sub acápites los motores de búsqueda y el correspondiente indexado de la información, ya que este punto, como ya se ha dejado ver anteriormente, es fundamental para el objeto de estudio de esta investigación y permitirá obtener conclusiones sobre cómo es el funcionamiento de estos sistemas y como se pueden regular jurídicamente su ámbito de acción.

1.3.1 Motores de búsqueda

Como todos conocen o suponen, la red de redes dispone de un enorme cúmulo de información, como publicara CCM Benchmark Group (2015) “miles de millones de documentos”. Debido a esto surge la necesidad de contar con una herramienta que permita a los usuarios localizar el documento o la información que necesita, dentro del gigante universo de contenido que reposa en internet. El resultado de esto es lo que todos conocemos hoy como motores de búsqueda, los cuales constituyen una herramienta fundamental en la gestión de datos.

En la actualidad se ha venido evidenciando una creciente preocupación por parte de los ciudadanos para evitar que sus datos personales aparezcan en los índices o resultados que presentan los motores de búsqueda de Internet, a partir de las búsquedas realizadas por los usuarios.

“Desde Wandex, el primer buscador desarrollado por Matthew Gray, Lycos, Excite, AltaVista, Naver, entre otros; hasta los más populares actualmente: Google y Yahoo!, los buscadores siempre han contribuido a la búsqueda de datos”. (Posicionamiento web, 2013).

Los motores de búsqueda son programas informáticos, software, que su función es encontrar los sitios web relacionados con el término de búsqueda

introducidos por el usuario. Un término de búsqueda es lo que generalmente las páginas solicitan que se introduzcan como *keywords*. Para accionar el motor de búsqueda la persona debe escribir en el buscador la información que desea le localice.

Así, el motor procesa las palabras introducidas por el usuario, gestionando en sus bases de datos cada término, procediendo a eliminar las páginas que no se correspondan con el criterio de búsqueda del usuario. “Estas respuestas se clasifican por relevancia según el criterio del motor de búsqueda, por ejemplo, el porcentaje de palabras que coinciden con la búsqueda, la densidad de las palabras claves (la cantidad de veces que éstas aparecen en la página), etc.” (CCM Benchmark Group, 2015)

Conforme se ha explicado en el párrafo anterior, se incluye el ejemplo introducido por Pere Simón (2012) cuando dice:

“Los términos que el buscador propone no responden necesariamente a los contenidos disponibles en la red, sino que depende de lo que otros ciberusuarios hayan tecleado con anterioridad. Así, por ejemplo, cuando alguien busca <leire pajín> el motor de búsqueda de *Google* propone <leire pajín es hija de Felipe González>, y cuando alguien busca <Felipe González>, el citado buscador propone <Felipe González falangista>. Evidentemente, estas sugerencias permiten asociar ideas de tal manera que pueden perjudicar la fama de una persona o una empresa, o suponer un auténtico ataque a su reputación” (Castellano, 2012, p. 46).

En tal sentido, alguna que otra vez, todos han accedido al gigante de Google, como buscador universal y prestigioso. Pero, ¿Existe solo Google como motor de búsqueda? ¿Es Google el más efectivo?

Posicionamiento web (2013) ha publicado que:

“Google posee en general 7.200 millones de visitas diarias, convirtiéndose actualmente en el más popular a nivel mundial; sin embargo, en algunos países asiáticos como Corea del Sur y China, el buscador Naver posee el primer lugar. En España, Bing, de Microsoft, ayuda a buscar de manera sencilla y fácil cualquier tipo de información en la red” (Posicionamiento Web, 2013).

Bueno, además de Google, existen otros buscadores alternativos que también son capaces de dar respuestas veraces y muy precisas. Yahoo!, es un ejemplo de esto.

Yahoo!, es más que un motor de búsqueda, a través de él puedes adentrarte al servicio de correo, agencias de viajes, noticias, tiendas, juegos, en fin, que ha llegado a entenderse como un portal web, dado que permite a quienes no poseen un amplio dominio en el área de búsqueda y navegación, acceder cómodamente a la información deseada.

Otro buscador que ostenta una posición preponderante en el mercado de los motores de búsquedas es el caso de Bing, que ya se había comentado anteriormente. Bing se ha convertido en el segundo motor de búsqueda a nivel mundial, y sistema de búsqueda nativo en los nuevos dispositivos de Microsoft equipados con Windows 8. Heredero directo del potente buscador MSN, recibió una profunda actualización en 2009. Como resultado se lanzó un producto totalmente nuevo, optimizado y capaz de plantarle cara al todopoderoso motor de Google (Computer hoy, 2013).

El conocido buscador profundo, que por esa característica de profundidad con que procesa la información, es que ha ido escalando posición es Yippy, convirtiéndose en uno de los buscadores más apreciados para determinada clase de usuarios. Y, aunque no muy utilizado por los usuarios, también como motor de búsqueda encontramos el Duck Duck Go. Este buscador, posee una gran similitud con Google, aunque se limita más a dar una respuesta concisa a la pregunta efectuada. A diferencia de Google, no posee una densa carga de anuncios y promociones.

Para finalizar este recorrido por lo más famosos, conocidos y utilizados motores de búsqueda del mundo, se debe mencionar al Internet Archive, que como su nombre bien lo indica, no es que sea un buscador diario, pero es de enorme viabilidad para realizar búsquedas en el desarrollo de investigaciones.

“Internet Archive más que un motor de búsqueda, es la hemeroteca de la Red. Destino obligado de los nostálgicos amantes de los inicios de la World Wide Web. Este motor de búsqueda ha estado guardando documentos de la Red prácticamente desde su nacimiento. En él puedes encontrar cómo eran las páginas en 1999, o que fue noticia tal día como hoy de hace 10 años” (Computer hoy, 2013).

De este modo, los motores de búsqueda han llegado a ser un mecanismo esencial para obtener información en Internet. Se puede decir que prácticamente el 100 por ciento de la información que se gestiona en internet se adquiere gracias a estas herramientas, que gestionan bases de datos de URLs con variedad de contenidos.

“Un motor de búsqueda (también llamado *Searchbot*) es una herramienta hardware y software que indexa páginas web para que se puedan buscar a través de palabras claves en un formulario de búsqueda” (CCM Benchmark Group, 2015).

También este sitio en la misma publicación agregó que:

“RTBot es un buscador que clasifica los resultados en categorías; estas categorías son Wikipedia, videos, Twitter, documentos, blogs y noticias; DuckDuckGo es un motor de búsqueda cuya finalidad es la de respetar la privacidad del usuario puesto que no recoge información de este que lo pueda delatar; Yacy, cuya funcionalidad es la de también poder funcionar para Intranet” (Posicionamiento web, 2013).

Ahora, si bien es cierto que los motores de búsqueda facilitan enormemente las búsquedas de la información requerida por el usuario y en múltiples ocasiones nada tienen que ver con los quebrantamientos de derechos, también es cierto que recae sobre estas herramientas, una enorme responsabilidad, al permitir el acceso a la información y además crear vínculos y relaciones entre las mismas, como el ejemplo ilustrativo de “Felipe González”, más arriba abordado o el ejemplo que a continuación se cita, también tomado del interesante libro de Pere Simón (2012):

“En Francia, en el año 2009, se condenó a *Google* por asociar la palabra <estafa> -arnaque- a la Empresa *Direct Energy*: en Italia, a principios del año 2011 una sentencia del Tribunal de Milán ha considerado que *Google*

es responsable de los daños derivados de la asociación de los datos de una empresa con la palabra <estafa> -*truffa*-(Castellano, 2012, p. 46).

Como se ha venido sosteniendo a lo largo de este Capítulo, con independencia de la responsabilidad de los motores y del resto de las herramientas que hacen posible la difusión, localización y vinculación de las información, es el propio ser humano, el usuario, quien la emite, lo que lo convierte por ende, en el primer gran responsable del camino que a lo largo del tiempo y de los múltiples adelantos tecnológicos, va recorriendo, positiva o negativamente, la información compartida.

Se pone a consideración un ejemplo, completamente pertinente, en cuanto a la responsabilidad ciudadana se refiere, en el entendido de la divulgación de información personal a través de los diferentes espacios destinado a este fin.

“(...) el caso del <padre Bru>, conocido director de los contenidos sociales y religiosos de la Cadena COPE, que solicitó a los tribunales la adopción de medidas cautelares contra los responsables del <Grupo Risa>, que se dedican a la programación satírica. En concreto, pedía el cierre de un grupo de *Facebook* llamado <Salvemos al padre Bru>, en el que se exponía una imagen del <padre Bru> acompañado de dos jóvenes, todos ellos en bañador. Según el demandante, esta imagen suponía un ataque a su derecho a la propia imagen, a la intimidad y también al honor, este último supuestamente afectado por los usuarios de la red social *Facebook*, que al visualizar la fotografía, dejaban comentarios imaginativos al respecto” (Castellano, 2012, p. 47).

Ante el caso antes citado, se debe señalar que en noviembre de 2010, un Juzgado de Madrid, denegó la adopción de medidas cautelares cuyo fundamento en primer lugar fue la inocuidad (no se deducen tendencias pedófilas) de la citada fotografía; para luego determinar que, en el hecho que la fotografía fuese alojada por el propio demandante en su página personal de la red social *Facebook*. Así pues, que haya sido el propio <padre Bru> quien publicó su propia fotografía tuvo un especial interés en la resolución del caso concreto. En otras palabras, el tribunal entendió que el <padre Bru> era responsable de haber situado su propia imagen ante la tribuna de un público

que tiene derecho, sin violar el orden jurídico-constitucional, a dar su opinión sobre las imágenes" (Castellano, 2012, p. 47).

El ejemplo anterior ilustra sobre la responsabilidad ciudadana ante la información personal que comparte y divulga, pero igualmente, en otros casos la responsabilidad sí alcanza a los motores de búsqueda; y, sin lugar a dudas, esta responsabilidad de los motores, es compartida con el fenómeno del indexado, toda vez, que sin este procedimiento, los mencionados motores no pudieran llevar a cabalidad su función. Véase entonces, como un hecho indisoluble, donde coexisten necesaria e imprescindiblemente, dos herramientas, el motor de búsqueda y el indexador.

Es oportuno en este punto citar nuevamente la sentencia C-131/12 del Tribunal de Justicia de la Unión Europea que determinó

"...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" (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 22).

Ciertamente el estudio de los motores de búsqueda requiere de un análisis técnico que hasta este punto hemos realizado, pero todo ello dentro del contexto jurídico que enmarca esta investigación, es decir, el ámbito de aplicabilidad del derecho al olvido digital, ese derecho que deberían tener los ecuatorianos a que su información y datos personales desaparezcan de los resultados de búsqueda de motores como Google, si así lo desean tal como ya sucede en el ámbito europeo, y que será analizado más adelante en el presente documento.

1.3.2 Indexado de la información

Como es lógico, para que los buscadores puedan realizar la función para la cual fueron diseñados y permitan a los usuarios acceder a la información que

buscan, se requiere que las páginas se encuentren indexadas. Cuando se habla de indexar una página nos referimos a incluirla en un índice, que nos da su ubicación para poder hallarla posteriormente. Estudiar este aspecto resulta relevante para esta investigación, siendo un eje fundamental para sustentar la dinámica del ejercicio al derecho del olvido digital y como podría ser legislado en Ecuador.

Para indexar la información, en primer lugar se efectúa un proceso de análisis de la documentación, la recogida y el análisis de la información se puede procesar lo mismo manual que automáticamente. Así, se tiene que la mayoría de los formularios de ingreso que tienen los distintos buscadores solicitan algunos datos precisos como son: el título de la página, URL, descripción y clasificación del recurso.

En otros casos, también piden datos como descriptores o palabras clave, persona o entidad responsable de la página, tipo de información (académica, comercial, personal, informativa, etc.), localización geográfica, idioma, etc. En tal sentido, la clasificación va encaminada a que se incluya en alguna categoría jerarquizada de las que luego se presentarán en el índice temático. Por su parte, los responsables del buscador se encargan de fiscalizar si la información provista se ajusta a la realidad.

Por eso cuando se plantea que un artículo, documento o trabajo se encuentra indexado, es porque ya ha sufrido un proceso de análisis y selección, hecho que es desarrollado por las empresas que se ocupan de este tipo de trabajo.

Por ello, Córdoba González (2005) alega que: “un índice facilita la búsqueda de información y ayuda a seleccionar con mayor exhaustividad, la más pertinente de acuerdo con las características de los usuarios”.

Ahora bien, en cuanto al proceso de indexado se refiere existen diversas maneras de indexar un documento, página *Web* o información. Todo depende de la forma en que funcione el motor de búsqueda, así como la tecnología que posea, pero lo que resulta innegable es que los motores de búsqueda de Internet, tienen una gran impacto en la obtención de todo tipo de información,

incluidos los datos de cualquier persona, y estos pueden ser obtenidos por un tercero, desde cualquier lugar del mundo, en cualquier momento y sin ningún procedimiento administrativo, por lo que quien busca no está obligado a revelar su identidad.

El indexado como proceso, no ha sido tratado por muchas legislaciones en cuanto a las consecuencias legales que el mismo puede acarrear. Este fenómeno, más bien ha sido tratado por la doctrina y la jurisprudencia, no obstante, existen algunos ordenamientos jurídicos de avanzada y bastante progresistas que valientemente han hecho sus intentos regulatorios.

Tal es el caso de España, la cual implementó la Directiva 2000/31/CE, de Comercio Electrónico, mediante la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio. Portugal, por su parte, introduce una exención para motores de búsqueda e *hiperlinks* sujeta a las mismas condiciones previstas para la exención de hosting (Xalabarder Plantada, 2006, pág. 7).

El caso de Hungría, es diferente, pues esta legislación optó por introducir una exención para motores de búsqueda, pero no para los hiperlinks. Por otro lado, pero en igual sentido, Austria y Liechtenstein han introducido exenciones específicas para los motores de búsqueda y los hiperlinks, pero sujetándolas a condiciones diferentes (Smith, 2007, p. 342).

Francia, en otra línea, no ha abordado la responsabilidad por la provisión de motores de búsqueda y enlaces a páginas con contenido infractor, por el legislador, sino por el llamado «Forum des Droits sur Internet» (una organización compuesta por industria y usuarios), la cual ha concluido que

“...quien introduce un enlace a contenido infractor sólo puede ser declarado responsable penal si se demuestra que tenía la intención de cometer una infracción o de participar en la misma y sólo podrá ser declarado civilmente responsable (indemnización por daños y perjuicios) cuando su actuación carezca de la mínima prudencia debida (y establece criterios para determinar cuándo se produce una actuación imprudente)” (Xalabarder Plantada, 2006, p. 7)”.

Holanda, ha registrado un caso en el que el “operador de una página web que contenía enlaces a escritos de grupos radicales (que eran constitutivos de delito) fue obligado a deshabilitar tales enlaces, aplicándole las mismas reglas y condiciones previstas para la exención por hosting (Deutsche Band vs. Indymedia, Tribunal de Distrito, Ámsterdam, 20 Junio 2002)”. Otra experiencia que vale la pena traer a colación es la sentencia de “los Estados Unidos, por la cual se declaró la responsabilidad por la introducción de un enlace a una página web ajena con contenido ilícito, ya que el operador del enlace conocía (o tenía motivos para conocer) la naturaleza ilícita del contenido enlazado (Intellectual Reserve Inc. vs. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999)” (Xalabarder Plantada, 2006).

A grosso modo, con este breve recorrido por las legislaciones foráneas, que de algún modo se han pronunciado y ha abordado el tema de la indexación y los motores de búsqueda, desde una óptica jurídica, en búsqueda de la delimitación de responsabilidad, se ha podido comprender el valor y el peso de estos procesos y herramientas, que tanto inciden sobre el universo de derechos de las personas.

Un caso muy tratado mediáticamente, y que guarda relación con este tópico, es el caso que tuvo lugar en Argentina, donde la modelo María Belén Rodríguez, demandó a Google y a Yahoo! por asociar su nombre a sitios pornográficos. Esta demanda devino con un fallo que condenó a Google por “considerar que había utilizado y reproducido imágenes de la modelo sin su consentimiento y que por ello debía responder en los términos del artículo 31 de la Ley 11.723. La demanda no prosperó contra Yahoo! porque no se acreditó que en su “buscador por imágenes” hayan existido imágenes reducidas (thumbnails) de la modelo” (Tomeo, 2014).

El caso antes expuesto es un referente obligado en relación al tema estudio de esta investigación, pues es un ejemplo de cómo debe entenderse legalmente el derecho al olvido digital y su efectividad, representa entonces, un ejemplo dentro del ámbito latinoamericano que un país como Ecuador debe considerar y podría acoger.

1.4 Datos personales, marco constitucional y legal en el Ecuador

1.4.1 Datos personales

El significado de los datos personales y cuál es su valor jurídico es un tema que necesariamente debe abordarse en esta investigación porque de allí se desprende el análisis de hasta qué punto los ciudadanos pueden disponer de los mismos y qué aspecto debería abordar una ley que pretenda regularla su protección.

En este aparte es idóneo comenzar a desarrollar las ideas mediante la definición de información pública, expuesta por la Dirección Nacional de Registro de Datos Públicos, como

“Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a un ciudadano identificable y determinado, cuya publicación y utilización no requiere del consentimiento del titular, para su uso o tratamiento, por parte de cada entidad registral, de conformidad con su competencia” (Dirección Nacional de Registro de Datos Públicos, 2013).

Frente al contexto de la definición antes citada, se debe recalcar como el titular de la información no tiene ninguna limitación para acceder a toda la información que descansa en los registros públicos, esta limitación será para el resto de las personas naturales y jurídicas que pretendieran acceder a ella; las cuales deberán aportar la autorización expresa del titular, debe estar clasificada la información como asequible o bien por mandato judicial, pudiendo darse algún que otro supuesto en dependencia del ordenamiento jurídico de que se trate.

Estamos entonces ante el derecho fundamental de protección de datos, el cual fue definido por Idrovo Mosquera cuando manifiesta que

“A la protección de datos debemos entenderla como: “El amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad. Se trata por tanto, de una protección a la persona ante el manejo o manipulación, no autorizada o no permitida por

la Ley, de sus datos de carácter personal. Es, consecuentemente, una protección jurídica ante la potencial agresividad de la informática” (Idrovo Mosquera 2011, p. 31).

De allí, se pueda conceptualizar a los datos personales como el conjunto de información que le es intrínseca a una persona. Los mismos pueden ser catalogados como sensibles o inocuos. Para definir los datos personales sensibles cabe citar el concepto presentado por Novoa, Eugenia (2015).

“...los datos sensibles pueden definirse desde un punto de vista formal y desde un punto de vista material. Formalmente son aquellas categorías de datos que requieren unas especiales y reforzadas garantías de tratamiento. Desde el punto de vista material hacen referencia a las cualidades de la persona que definen su dignidad, que configuran su personalidad, que dibujan su forma de ser y de comportarse” (Serrano, 2003, p. 380).

Por su parte, los datos inocuos son los que de acuerdo al principio de seguridad exigen medidas de seguridad baja. Aunque se debe aclarar que si los datos inocuos son asociados con su titular, estos se convierten en datos personales y deben exigírseles un régimen normal de tratamiento de datos personales (Novoa, 2015).

Luego de definir los datos personales para contextualizar el tema del derecho al olvido digital, se determinará cual ha sido la evolución de la protección de estos en el tiempo y su desarrollo en la legislación internacional.

1.4.2 Origen y evolución del derecho de la protección de datos.

Legislación internacional

Corresponde a este sub acápite el estudio del origen y evolución de la protección de datos, así como su regulación en el ámbito internacional. Este ejercicio de derecho comparado permitirá tomar las ideas fundamentales de los sistemas jurídicos que han evolucionado en la reglamentación del derecho al olvido digital y analizar cuáles de esos criterios podrían adoptarse en una propuesta de ley en Ecuador.

El origen del derecho de la protección de datos, se conoce que encuentra su punto de partida en la década de los sesenta del siglo XIX, siendo meritorio

resaltar el aporte doctrinal realizado anterior a esta fecha por Thomas Cooley, quien ya en la fecha tan temprana de 1888, se había referido a “the right to be let alone”, así mismo tenemos el caso del artículo publicado por Warren y Brandies titulado “The Right to Privacy”, el que fuera publicado en Harvard Law Review.

El derecho a la privacidad, por su parte, fue recogido por la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derecho Civiles y Políticos, en 1966.

No obstante, estos referentes, se puede decir que hasta el año 1967, no es que se configura el derecho a la protección de datos de la forma en que lo conocemos hoy, cuando se crea en el Consejo de Europa una Comisión Consultiva con la finalidad de estudiar las tecnologías y su efecto perjudicial en los derechos de las personas.

El trabajo de la Comisión trajo como resultado, la Resolución 509 de la Asamblea del Consejo de Europa, con relación a los derechos humanos y los nuevos logros científicos y técnicos. Esta norma jurídica está considerada como los inicios del movimiento legislativo en el continente europeo en lo que a protección de datos se refiere.

También Estados Unidos dio pasos de avance en este sentido, cuando en 1973 el Departamento de Salud, Educación y Bienestar de ese país, emitió un informe relativo a las bases de datos telemáticas del Estado, proponiendo un Código que regulaba los principios que regirían el empleo de la información por parte del Gobierno.

Alemania, es reconocida por ser pionera en esta materia, con su popular Ley del Land de Hesse, y la Ley Federal Alemana de 1977. Siguiendo en Europa, tenemos a Francia, quien ya para el siguiente año, 1978, aprobaba la Ley francesa de Informática, Ficheros y Libertades, que luego fuera modificada para atemperarla a la Directiva 95/46/CEE, Ley No. 2004-801, de fecha 6 de agosto de 2004, sobre la protección de las personas físicas en cuanto al tratamiento de datos de carácter personal.

En el mismo año 1978, Dinamarca sacó a la luz dos legislaciones, una sobre registros privados y otra sobre registros públicos. También Austria, se hizo eco de este acontecimiento, cuando este mismo año aprueba su Ley de Protección de Datos. Para el próximo año, 1979, Luxemburgo pondría en vigor la ley sobre utilización de datos en tratamientos informáticos. Posteriormente el Parlamento Europeo, promulgó una resolución sobre “La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática”.

Ya para la década de los años ochenta, el Consejo de Europa, se pronuncia con la Convención No.108 sobre la Protección de las Personas en lo que se refiere al manejo automatizado de los datos personales. Esta Convención como norma rectora a observar por los países europeos, recoge los principios y derechos que toda legislación nacional debe incorporar para proteger los datos de carácter personal.

España en su Constitución de 1978, específicamente artículo 18.4, se plantea la problemática de la informática y el riesgo que implica para la vida privada. Es así, que en el 2000, se comienza a entender la protección de datos de carácter personal como derecho fundamental ya independiente del derecho a la intimidad. Esto queda plasmado en la Carta de los Derechos Fundamentales de la Unión Europea, que tuvo lugar en la Cumbre de Niza en fecha 7 de diciembre de 2000, cuando planeta que todo ser humano goza del derecho a que se le protejan sus datos personales, mientras que en otro artículo, es que dispone el derecho a la vida privada y familiar.

De esto se colige, que el derecho a la protección de datos ostenta, desde ese momento, un lugar aparte y se reconoce como derecho autónomo. En otro orden, tenemos las sentencias dictadas por el Tribunal Europeo de Derechos Humanos, la de Amann contra Suiza, de 16 de febrero de 2000 y Rotaru versus Rumanía, en fecha 4 de mayo del propio año, donde el tribunal desarrolla una interpretación amplia sobre el derecho a la vida, y se remonta al concepto de datos personales.

Actualmente, con los adelantos tecnológicos cada día más avanzados, resulta necesario proteger los datos personales de los disímiles fenómenos que pueden lacerarlo, toda vez, que de ser vulnerado este derecho fundamental, acarrearía el quebrantamiento de otros derechos y libertades, o que dicha información pueda ser usada en contra de esos derechos.

Se conoce que un mal empleo de ciertos datos personales, ha ocasionado restricciones en cuanto a la libertad religiosa, el derecho al trabajo, o a ocupar funciones públicas. Muchas veces, los titulares, no son conscientes de que son víctimas de la violación de este derecho y solo alcanzan a notar los efectos nocivos que impone a su vida, sin siquiera alcanzar a notar el evento desencadenante de la misma.

En tal sentido, se ha producido que personas resultan no contratadas, para una plaza a pesar de ser idóneas y cumplir con los requisitos que exige, como resultado de que el empleador obtuvo información sobre sus datos personales y conoció sus creencias religiosas, afiliación sindical o información genética; por solo mencionar un ejemplo. El adelanto tecnológico, ha convertido todo lo imaginable, en prácticamente posible, así también somos objeto de una mirada y escucha casi constante, a través de las cámaras de videovigilancia o de aparatos de radiofrecuencia.

Un ejemplo de esto lo constituye España, donde las reclamaciones de los ciudadanos son cada más crecientes, tanto es así, que para el año 2009, la Agencia Española de Protección de Datos dio inicio a 156 investigaciones sobre los servicios que brinda Internet. La mayor parte de los casos guardaba relación con la difusión no autorizada de datos personales. “La agencia tramitó 2.000 solicitudes (el 58% más que el año anterior) sobre acceso, cancelación o rectificación de datos”. (Gómez, 2011).

Según fuentes informativas, las peticiones cada día son más crecientes, fenómeno que se ha venido desarrollando desde el año 2008, cuando las cifras y valores comenzaron a dispararse, como muestra de ello se presentan las siguientes cifras:

“Las solicitudes de tutela de derechos para cancelar datos de páginas *Web* o impedir que sean difundidos por buscadores de Internet aumentaron el 200%. El número casos pasó de 18, en 2008, a 57, en 2009. La mayoría afecta a recuperación por buscadores de datos en boletines oficiales o medios de comunicación digitales sobre sanciones administrativas ya cumplidas, edictos de deudas vencidas o datos de víctimas de violencia doméstica” (Gómez, 2011).

Ahora, se debe tener en cuenta que es necesario equilibrar la protección de los datos personales, la intimidad y la seguridad. Debiendo respetarse siempre en todo caso los derechos fundamentales. Cada país tiene la responsabilidad de tomar las medidas pertinentes para proteger a sus ciudadanos ante la inseguridad, pero siempre sin menoscabar los derechos fundamentales de las personas, así como sus datos personales.

Otro elemento que debe observarse en este sentido, es la transferencia internacional de datos, que hoy día, ocupa un lugar importante y que resulta indetenible, por la estrepitante intensidad que ha alcanzado. Para ello han surgido las conocidas Reglas Corporativas Vinculantes, que facilitan el intercambio de datos entre grupos multinacionales.

De manera general, en el orden internacional los datos personales y el derecho fundamental de la protección de los datos de carácter personal, se encuentran legislados en los términos explicados. Por otra parte, en el plano doméstico también los datos personales han sido contemplados y amparados en el marco legal ecuatoriano.

Todo esto ha sido un preámbulo para las figuras actuales de protección de datos personales, en sus legislaciones más detalladas a nivel local o a nivel comunitario, lo que nos lleva a que se introduzca esta nueva figura de derecho al olvido digital, que busca, en última instancia la protección de la dignidad de las personas a través de la protección de los datos que de ellas existen en la internet, y que pueden estarle causando algún perjuicio. Este, como fundamento de este trabajo de titulación, será abordado en detalle en los capítulos posteriores.

1.4.3 Marco constitucional y legal en el Ecuador

Con este sub acápite se busca conocer cómo se ampara la protección de los datos personales en el ordenamiento jurídico ecuatoriano para analizar cuáles son las debilidades de este orden jurídico sobre la materia y cómo se podría aportar con una ley que incluso vaya más allá, contemplando el derecho al olvido digital.

Así, Ecuador, por su parte, reconoce y protege los datos personales, y lo hace desde la Constitución de la República del Ecuador hasta su marco legal más concreto. La Constitución ecuatoriana parte en su artículo 66 numeral 19 y 20, salvaguardando los siguientes derechos:

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

20. El derecho a la intimidad personal y familiar.” (Constitución de la República del Ecuador, 2008), Art. 66, Numerales 19 y 20)

De esta forma quedan instrumentados constitucionalmente el derecho a la protección de datos de carácter personal, que dispone como requisito *sine qua non*, la autorización del titular, o en su defecto el mandato legal, que determina el imperio de la ley, en el caso en cuestión, y el derecho a la intimidad personal y familiar.

También la misma Constitución, en su artículo 92 legisla la Acción de Hábeas Data. Regulándola conforme se explica a continuación:

“Toda persona, por sus propios derechos o como representante legitimado para el efecto tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o

anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados” (Constitución de la República del Ecuador, 2008).

El *Habeas Data*, es una garantía constitucional que permite el ejercicio loable del derecho a la protección de los datos personales y de la intimidad, dado que no solo establece como presupuesto indispensable, la autorización del titular de los datos para el tratamiento de los mismos, sino que además dispone que en el caso de los datos sensibles, la parte que se considere afectada por el tratamiento que han recibido dicho datos, y no hayan procesado su solicitud, tendrá expedita la vía para el ejercicio de este derecho en el ámbito judicial, ante el juez competente.

En el caso del *Habeas Data*, sería bueno hacer un aparte, dado al valor que tiene esta institución, máxime en la presente investigación que se viene desarrollando.

Como *Habeas Data* se puede entender, *a priori*, como un remedio urgente, mediante el cual la persona que incoe esta acción puede obtener:

- “El conocimiento de los datos a ellos referidos y de su finalidad que consten en registros o bancos de datos públicos o privados;
- O en su defecto, para exigir su actualización, rectificación, eliminación o anulación; y su confidencialidad, esto es el derecho a conocer el dato de carácter personal y el derecho de rectificación en caso de que la información sea errónea” (Palacios González, 2013).

El *Habeas Data* en su esencia comprende como aristas o ámbitos: el derecho a la intimidad, las fuentes de información y la prensa, los registros propiamente dichos, archivos y banco de datos; los Derechos Humanos; así como la informática y la telemática.

El *Habeas Data* está encaminado a proteger a las personas de los abusos que la misma pueda sufrir respecto del conocido poder informático y de las consecuencias que le traería a su honra y buen nombre en caso de que la

información difundida no se veraz o sea errónea. Se entiende por tal, la producción, almacenamiento y transferencia de información personal que pueden realizar instituciones públicas y privadas, empresas y personas en general, en base a los avances tecnológicos que hoy existen y a la información que estos poseen o almacenan.

Tal información personal, a más de poder ser incorrecta o desactualizada, puede abarcar situaciones pasadas ya superadas, así como también ser de carácter sensible, esto es, referirse a las convicciones políticas o religiosas de la persona, a su comportamiento sexual, a su estado de salud, etc., información ésta que al ser realmente íntima no debería ser de conocimiento y manejo público, salvo que su mismo titular así lo acepte expresamente, cuestión que en nuestro país no se le da el tratamiento que merece pues lo que más ocurre a diario es precisamente agravios sufridos a consecuencia de información errónea y de situaciones ocurridas en el pasado que deberían quedar en donde ocurrieron.

El riesgo que tiene la persona ante el poder informático de las instituciones es grande, no sólo por la facilidad que tienen para almacenar u obtener información, sino por la rapidez con que ella puede ser transferida y difundida no solo dentro del país sino del mundo. Junto con lo anterior, y sin perjuicio del peligro que significa el registro de información falsa o errónea acerca de la persona, la simple manipulación de la información personal es en sí ya un grave riesgo para todos.

El poder informático es grande, y la tecnología avanza a pasos agigantados tanto en el proceso de acopio como de difusión de la información que posea; ese acopio y recolección de datos puede ser realizado de manera superficial e irresponsable, sin la debida investigación, revisión y el cuidado suficiente que aquella merece; así mismo, esa difusión puede ser realizada de manera inadecuada, desmedida o fuera de lugar.

Por lo tanto, mediante esta garantía se tiene a más de un acceso efectivo a la información personal existente en poder de terceros, un control efectivo a la

calidad de información que reposa en tales registros, permitiendo no solo un proceso de corrección y actualización sino hasta de anulación y supresión de los datos ilegítimos, erróneos o desactualizados que puedan llegar a causar graves perjuicios a sus titulares.

Es oportuno afirmar entonces, que en lo relativo al derecho a la protección de datos personales, no existe en el orden legal de Ecuador un cuerpo normativo que lo prevea y garantice en su amplitud. Así pues, en este sistema se encuentran leyes especiales ligadas a este derecho, como lo son: Ley Orgánica de Transparencia y Acceso a la información Pública, Ley del Sistema Nacional de Registro de Datos Públicos y, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Novoa, 2015).

Luego encontramos la Ley No. 67-2002, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que fuera publicada en Registro Oficial No. 557 de fecha 17 de abril del 2002, aún bajo el contexto de la Constitución ecuatoriana de 1998, que en realidad preveía solo el derecho a la intimidad que para su ejercicio requiere de un transgresión externa; es decir, se necesita un daño producido a la intimidad para que proceda un reclamo, a diferencia de la protección de datos personales, en donde los datos son de autodeterminación informativo, en otras palabras, son de propiedad personal y cada persona decide a quien lo entrega, lo cual garantiza el derecho al libre desarrollo de la personalidad, siendo una acción positiva.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, siguiendo una perspectiva negativa, regulando el derecho a la intimidad y dejando a un lado el enfoque de la protección de los datos personales, presenta el siguiente glosario de términos:

“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” (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, Disposición General Novena).

Esta norma rectora en materia de tecnología, fija los supuestos en que debe desarrollarse la utilización y transferencia de datos, prescribiendo en su artículo 9, la exigencia del consentimiento expreso, en los siguientes términos

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

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

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

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo” (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, Art. 9).

La disposición antes citada se aleja de la tendencia actual de la regulación de protección de datos que exige el consentimiento libre e informado. Tal omisión precisamente justifica y fundamenta la propuesta de una ley de protección de datos, la cual se presentará en el siguiente capítulo. Además, profundizando en el análisis, es oportuno preguntarse ¿Qué sucede cuando las personas violan lo dispuesto no solo en la Ley de Comercio Electrónico (...)? Para estos casos,

también los legisladores, previeron soluciones legales, y esto lo encontramos primeramente en el Código Orgánico Integral Penal en su precepto 178, cuando penaliza la obtención y utilización no autorizada de información.

“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.” (Código Orgánico Integral Penal, 2014, Art. 178).

Constituye este, un intento por evitar la constante difusión de información sin la correspondiente autorización de su titular, y que es susceptible de ser manipulada, difundida y socializada de múltiples maneras.

Ya el propio Código Penal anterior, en su numeral 606 sancionaba a los que violaren el derecho a la intimidad.

Con la promulgación y entrada en vigor del Código Orgánico Integral Penal se tipificaron los delitos contra la seguridad de los activos de los sistemas de información y comunicación, quedando contenida como ilícita la revelación ilegal de base de datos, en el artículo 229 del citado Código Orgánico. Así, la persona que para su propio provecho o de una tercera persona, revele información que se encuentre registrada, contenida en ficheros, archivos, bases de datos y otros medios semejantes, a través o dirigidas a un sistema informático, telemático o de telecomunicaciones; materialice consciente e intencionalmente la violación del secreto, la intimidad así como la privacidad de las personas, será objeto la aplicación de una sanción de entre uno a tres años de privación de libertad. (Código Orgánico Integral Penal, 2014, Art. 229).

Ahora bien, en apartados anteriores se expuso la tensión existente entre el derecho al olvido digital y la libertad de expresión, así pues cabe señalar como el artículo 4 de la Ley Orgánica de Comunicación del Ecuador determina:

“Contenidos personales en internet.- Esta ley no regula la información u opinión que de modo personal se emita a través de internet. Esta disposición no excluye las acciones penales o civiles a las que haya lugar por las infracciones a otras leyes que se cometan a través del internet” (Ley Orgánica de Comunicación, 2013 Art. 4).

Queda claro entonces como la Ley Orgánica de Comunicación del Ecuador no excluye expresamente la regulación de la protección de datos personales difundidos por internet; por lo tanto, una propuesta legislativa que profundice en su regulación resulta necesaria.

Luego cabe citar los artículos 17 y 18 de la ley antes mencionada que exponen:

“Art. 17.- Derecho a la libertad de expresión y opinión.- Todas las personas tienen derecho a expresarse y opinar libremente de cualquier forma y por cualquier medio, y serán responsables por sus expresiones de acuerdo a la ley.

Art. 18.- Prohibición de censura previa.- Queda prohibida la censura previa por parte de una autoridad, funcionario público, accionista, socio, anunciante o cualquier otra persona que en ejercicio de sus funciones o en su calidad revise, apruebe o desaprobe los contenidos previos a su difusión a través de cualquier medio de comunicación, a fin de obtener de forma ilegítima un beneficio propio, favorecer a una tercera persona y/o perjudicar a un tercero. Los medios de comunicación tienen el deber de cubrir y difundir los hechos de interés público. La omisión deliberada y recurrente de la difusión de temas de interés público constituye un acto de censura previa” (Ley Orgánica de Comunicación, 2013, Arts. 17-18).

Los dos artículos antes citados dejan evidencia que en el sistema jurídico ecuatoriano existe una legislación consistente que regula el derecho a la libertad de expresión y la prohibición a la censura previa, en concordancia con los artículos 18, 165 y 384 de la Constitución de Ecuador. Sin embargo, se considera que una propuesta legislativa bien contextualizada que prevea el derecho al olvido digital, no se contrapondría con el derecho a la libertad de expresión y prohibición a la censura previa, siempre y cuando se aclaren los límites y alcances de todos los derechos involucrados.

Por último, cabe mencionar la Ley Orgánica de Transparencia y Acceso a la Información Pública, publicada en el Registro Oficial de la República del Ecuador, No.337 Suplemento, del 18 de mayo del año dos mil cuatro, y su

correspondiente Reglamento que se publicó por intermedio del Decreto Ejecutivo No. 2471, en Registro Oficial 507 de 19 de Enero del 2005.

Estas normas regularon para beneplácito de todos lo referente al derecho de acceso que tienen los ciudadanos a la información pública que maneja el Estado, hecho este que va encaminado al fortalecimiento de la democracia, basada en la transparencia de los actos del gobierno, encaminado a evitar hechos escandalosos de corrupción y abuso de poder, por parte de los funcionarios del gobierno.

Y es por esta, entre otras razones que la Ley Orgánica de Transparencia y Acceso a la Información Pública es de vital importancia para la sociedad civil, dado que permite monitorear los actos del Gobierno y controlar el accionar de la gestión pública, mediante la exigencia de una permanente rendición de cuentas por las decisiones que se toman.

1.5 Sumario

Luego de la exposición técnica sobre como la evolución de la internet en la *WEB 2.0*, donde los procesos son más interactivos y la velocidad de reacción se vuelve casi instantánea luego de contar con usuarios en todas partes del mundo con capacidad de acceso a información en cualquier momento, podemos visualizar el riesgo que corren los datos personales de todos sus usuarios.

La internet ha cambiado el paradigma de la memoria radicalmente, cuando antes era común olvidar, hoy es la regla el recordar, gracias a la casi infinita memoria de la red de redes, en una memoria digital.

Los buscadores son hoy la herramienta para acceder a la información almacenada en esa memoria digital, y para esto, realizan un proceso de indexación de la información, haciendo que la misma sea ubicable de manera más rápida y por cualquier usuario.

Esta indexación de información resulta ser una forma de tratamiento de datos efectuado por parte de estos buscadores, datos que, en ciertas ocasiones, no son publicados u otorgados por sus titulares, sino por terceros.

Frente a esto, en el caso ecuatoriano, el marco constitucional otorga un régimen de protección de los datos personales y establece la garantía constitucional para exigir ese derecho, sin embargo, el marco constitucional, y con un desarrollo más amplio, la Ley Orgánica de Comunicación, promueven la libertad de expresión que, bajo ciertas condiciones, se puede contraponer contra el derecho a la protección de datos personales.

El capítulo precedente ha abierto el análisis, en los posteriores se presentarán a profundidad la problemática y los criterios mínimos.

2. CAPÍTULO II: DERECHO AL OLVIDO DIGITAL

“Para conmemorar la más gloriosa de las noches, el Gobierno de Su Majestad se complace en devolverles a ustedes, sus leales súbditos, el derecho a la privacidad. Durante tres días, sus movimientos no serán vigilados sus conversaciones no serán escuchadas y el “haz lo que quieras” será la única ley. Buenas noches y que Dios les bendiga” (Moore & Lloyd, 1989, p. 8).

La cita precedente se toma de una revista de caricaturas, para ser exactos V de Vendetta, donde se plantea una era distópica, donde por la seguridad de las personas se han perdido derechos, entre estos, el de privacidad, la intimidad, la autodeterminación informativa, entre otros y por citar solamente aquellos que atañen al presente documento.

Distópico como se podría haber apreciado en su momento, hoy hemos caído en prácticas, por cuenta propia o de terceros, donde prácticamente se han cedido los mismos derechos. Atados a tecnologías cada vez más avanzadas y sin saber que uso se le da nuestros datos, a nuestra información, y sin saber quien la tiene en su poder.

Para eso el derecho ofrece instrumentos, y este trabajo pretende presentar uno de los más útiles.

En este capítulo se presentará el derecho al olvido digital en su acepción más completa y se efectuará una contraposición frente a las alternativas introducidas por los detractores del mismo, y esta aproximación se la efectuará desde la base de los elementos que componen el derecho al olvido digital y su comportamiento típico frente a las otras alternativas.

Uno por uno iremos desvirtuando los argumentos de los opositores del derecho al olvido digital y para el efecto tomaremos el movimiento más significativo al respecto que corresponde a la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en el asunto C-131/12, Costeja y AEPD vs Google INC y Google Spain SL.

2.1. ¿Qué es el derecho al olvido digital?

Se ha visto como las nuevas tecnologías han generado cambios en la forma en que la información se mueve en la *WEB 2.0*, sin mayores miramientos a la hora de publicar algo en alguna de las tantas redes sociales que se encuentran al alcance de la mano de los usuarios a nivel mundial y cómo esta información publicada supera la barrera de la temporalidad o el espacio, y se vuelve accesible en todo el mundo en cualquier momento luego de que la misma haya sido “lanzada al ruedo”.

Adicionalmente, se pudo establecer, en el capítulo anterior, el cómo estas nuevas tecnologías de la información y comunicación han llevado a que el paradigma de la memoria de un giro de ciento ochenta grados, al punto que lo que antes era la regla, olvidar, ahora es la excepción, mientras recordar se impone en el nuevo modelo global. Esta es la nueva memoria, almacenada en un gran archivo que de apariencia se determina infinito.

Pero, es necesario comprender que este nuevo paradigma y los avances tecnológicos han abierto la puerta para que nuevas formas de afectación a los derechos de las personas se presenten, más allá de los enormes beneficios que estos han traído para la humanidad.

Lo primero que debemos conocer es que muchos años atrás, cuando la información era divulgada en lo que ahora se conoce como medios tradicionales, esta pasaba por un proceso de verificación, dada la responsabilidad de quien la publicaba frente a la veracidad de la misma, sin embargo, en años más recientes, el dinamismo de la *WEB 2.0*, ha hecho que se cambie ese esquema por uno más participativo, donde el usuario ya no es un mero espectador o consumidor de información, sino que se ha vuelto un proveedor de la misma, el primer problema se plantea en que esta nueva forma no presenta más control que aquel que la misma conciencia del usuario pueda generar.

El segundo problema deviene de que en épocas anteriores, la credibilidad era ganada a pulso por los diarios, televisoras, emisoras de radios, hoy, los afectos

personales hacen que muchos usuarios creen más en individuos a ellos vinculados, por ellos conocidos o simplemente de sus medios, sin obviar a lo que hoy se conoce como *influencers*, que no son sino “estrellas” de las redes sociales, con una gran cantidad de seguidores, fanáticos, que en algunos casos, creen a ojos cerrados lo que estos publiquen.

Otro problema, dentro del cúmulo de ellos, es que la verificación y contrastación de la información ya no pasa por los controles antes utilizados, sino que circula libremente e incluso puede ser presa de las pasiones, estados emocionales e incluso una mera y simple actitud dolosa, que no busca sino el daño.

Cabe mencionar que la información, puede incluso ser real y verdadera, comprobada, verificada y cumpliendo todos los estándares que otrora se siguieran, pero en ambos casos se debe señalar que la publicación de la mismas en la internet, que no desaparece ya que esta no olvida, puede afectar a una o varias personas en varios aspectos de su vida, y el acceso a esta información se ve potenciado por los buscadores, que como se pudo apreciar en el capítulo anterior, tienen su cuota de responsabilidad.

La sala de lo Contencioso - Administrativo de la Audiencia Nacional española señaló:

“(...) internet traspasa fronteras y límites temporales y los buscadores potencian ese efecto, permitiendo una difusión global de esa información y facilitando su localización, de tal modo que una información que antes de la aparición de estas nuevas tecnologías tenía una difusión limitada territorial y temporalmente, y que al cabo del tiempo caía en el olvido, en estos momentos puede ser localizada fácilmente, con una difusión global y, sobre todo, no se olvida, permanece en la red indefinidamente” (Audiencia Nacional, 2012).

Todo empeora cuando se habla de esquemas participativos como las *Web* colaborativas, donde toda la información ni siquiera proviene del mismo autor, y la lluvia de ideas o de comentarios generados sobre una idea original pierden sentido y se vuelven meras expresiones “viscerales”.

Pero entonces, ¿con qué elementos cuenta el ciudadano promedio para defenderse de las lesiones sobre sus derechos?

La Constitución ecuatoriana, contiene en su cuerpo valores, principios y derechos, y en su artículo 66 numerales 5, 18 y 20, ha salvaguardado varios derechos de las personas, como el derecho al libre desarrollo de la personalidad, sin más limitaciones que los derechos de los demás; el derecho al honor y al buen nombre, donde la ley protegerá la imagen y la voz de la persona; y, el derecho a la intimidad personal y familiar (Constitución de la República del Ecuador, 2008, Art. 66, Numerales 5, 18 y 20).

El mismo cuerpo, dentro del mismo artículo antes citado, en su numeral 19 señala:

“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” (Constitución de la República del Ecuador, 2008, Art. 19).

Confundirse es una posibilidad, por lo que se debe entender que si bien estos derechos pueden ser vulnerados día a día, y por toda la vida de una persona, gracias a internet y al cambio en el paradigma de la memoria, el enfoque que se debe dar es respecto de los datos personales.

David Ordoñez Solís ya lo dijo muy acertadamente:

“Internet está planteando nuevos desafíos para los derechos fundamentales hasta el punto de que precisamente la informática ha propiciado el desarrollo extraordinario de un derecho fundamental consagrado recientemente por la Carta de Derechos Fundamentales de la Unión Europea: el derecho a la protección de los datos personales” (Ordoñez Solís, 2014, p. 3).

Y es que Europa ha dado la respuesta, ya que desde hace algunos años se vino discutiendo en la Unión Europa la posibilidad de instaurar un nuevo derecho para la protección de datos personales, el conocido derecho al olvido (se suma la palabra digital en el presente trabajo para contextualizarlo), que

superaría por bastante al tradicional conjunto de derechos ARCO (acceso, rectificación, cancelación y oposición), incluso al bien conocido Habeas Data.

La pregunta es ¿qué es el derecho al olvido digital?, pues Pere Simón Castellano ofrece una definición amplia al respecto:

“Puede concluirse que el derecho al olvido es la capacidad que atribuye el ordenamiento jurídico a las personas físicas para que puedan obligar, dentro de la sociedad de la información, a que los responsables del tratamiento de datos, borren o dificulten la localización de los datos relativos a su persona que, por encontrarse a disposición de la sociedad digital interfiere de manera gravosa en la vida social, familiar y laboral del individuo” (Castellano, 2012).

Sin embargo, Alejandro Touriño da una definición un tanto más acotada:

“Derecho del individuo a eliminar o hacer inaccesibles ciertos datos o información publicados en el entorno digital y que se encuentran indexados por buscadores de internet” (Touriño, 2014, p. 140).

Touriño señala en su concepto la responsabilidad de los buscadores, al mencionar que la información se encuentra indexada por ellos, y al resultar ser el medio de navegación de casi todos los usuarios de internet, por no decir todos.

En contraste Castellano no limita el alcance de su concepto a los buscadores, sino que se refiere a aquellos que efectúen tratamiento sobre datos personales en alguna manera.

2.2. El movimiento europeo

Se debe destacar el intento italiano de definir el derecho al olvido digital ya en 1998, cuando la Corte Suprema italiana lo establece como: “justo interés de toda persona a no quedar indefinidamente expuesta a los daños ulteriores que producen a su honor y a su reputación la publicación reiterada de una noticia que en el pasado fue legítimamente divulgada” (Mate, 2016, p. 214)

Luego, en Francia, la entonces Secretaria de Estado Nathalie Kosciusko-Morizet, en el año 2010, lideró una consulta pública a ciudadanos y empresas sobre el derecho al olvido digital, cuyo resultado fueron dos cartas, cuya traducción informal podría ser “Carta de derecho al olvido digital de la

publicidad dirigida”, y la “Carta del Derecho al Olvido en los sitios colaborativos y en los motores de búsqueda”.

La segunda de estas perseguía “(...) el compromiso de sitios *Web* y motores de búsqueda para el respeto de los principios básicos de protección de datos, entre los que se encuentra el derecho al olvido de los usuarios de la Red.” (Mate, 2016, p. 216)

Estas cartas carecían de valor legal, por lo que era potestativo de los firmantes su cumplimiento. Google y Facebook, no la firmaron.

Pero, para llegar a una definición muchos eventos sucedieron en el viejo continente, finalmente impulsados en gran parte desde España.

Un elemento sustancial en el análisis de la definición antes expuesta es la que hace referencia a los buscadores de internet, esto no quiere decir que esta definición no será sometida a un extremo escrutinio, sino que el mayor movimiento en esta materia se da desde la posición de los buscadores, Google, significativamente.

Los vacíos del marco legal, en su momento impedían que se pudieran solucionar los casos que frecuentemente eran presentados por ciudadanos de origen europeo en los que solicitaban la supresión de sus datos personales que eran mostrados por los motores de búsqueda, y que como causa tenía su técnica de indexación.

Las páginas *Web* solían acatar las decisiones de la Agencia Española de Protección de Datos en virtud de las demandas de cancelación y oposición al tratamiento de los datos (conforme se encuentra establecido y permitido por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y su Reglamento de Desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre).

Sin embargo, Google, que encabeza la lista de buscadores, siempre se opuso a acatar dichas decisiones, alegando que las páginas que incluyeron la información eran las que debían satisfacer las demandas de cancelación y

oposición de los titulares de los derechos, protegiendo los derechos como la libertad de expresión o de información.

Todo esto nos lleva al caso de Mario Costeja González recogido en el asunto C-131/12, Costeja y Agencia Española de Protección de Datos vs Google INC y Google Spain SL, ante el Tribunal de Justicia de la Unión Europea.

Me permito relatar los supuestos de hecho, para contextualizar el análisis de los elementos del derecho al olvido digital frente a la mentada sentencia.

Los días 19 de enero y 9 de marzo del año 1998, el diario español “La Vanguardia” publicó, en su edición impresa, dos anuncios referentes a una subasta de inmuebles, la cual estaba relacionada con un embargo derivado de deudas. En dichos anuncios se mencionó al señor Mario Costeja González, de nacionalidad española y domiciliado en España, como propietario de los citados bienes inmuebles a los que hacían referencia los citados anuncios. Luego, el diario emitió la versión electrónica del periódico on-line, en cuyo contenido se encontraban dichos anuncios.

Con estos antecedentes, en noviembre del año 2009, Mario Costeja tomó contacto con el diario, señalando que cuando efectuaba una búsqueda de su nombre y apellidos en el motor de búsqueda de Google, en sus resultados este mostraba vínculos a las dos páginas del diario que contenían los anuncios referentes a las subastas.

Mario Costeja alegó que el embargo de estos bienes inmuebles había sido resuelto años atrás y que no eran relevantes, a lo cual la editorial propietaria del diario contestó que no era procedente la cancelación de sus datos, toda vez que la publicación de los anuncios que los contenían se había realizado en virtud de una orden dada por el Ministerio de Trabajo y Asuntos Sociales.

Ya en el mes de febrero del año 2010, el afectado envió una carta a Google Spain, en la cual solicitaba a esta que tome las medidas que correspondan para que al introducir su nombre y apellidos en el motor de búsqueda, en sus

resultados de la búsqueda, no aparecieran los enlaces al periódico La Vanguardia.

Google Spain remitió a Google Inc. la solicitud del señor Costeja, (Google Inc. tiene su domicilio en California, Estados Unidos), por ser ésta la que presta efectivamente el servicio de búsqueda en Internet, mientras Google Spain centra y limita su actividad en la venta de espacios publicitarios en Internet, es decir que alegaba ser, únicamente, representante comercial de Google Inc. para sus actividades publicitarias (se encargaba de la gestión de AdWords, que es un sistema de publicidad a partir de palabras clave).

Google Spain creía que su responsabilidad estaba limitada al tratamiento de datos personales relativos frente a sus clientes españoles de servicios publicitarios.

Antes de continuar, se señala que esos mismos argumentos de Google Spain, suelen ser utilizados por Bing y Yahoo!, teniendo el primero su sede operativa en Luxemburgo y el segundo un convenio firmado con Microsoft Corp., cuya sede se encuentra en Redmond, Estados Unidos de América.

Retomando el caso de Mario Costeja, el 5 de marzo del año 2010, este presentó una reclamación ante la Agencia Española de Protección de Datos, en contra de La Vanguardia Ediciones, S. L., Google Spain y Google Inc. Solicitaba:

“(…) por un lado, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no aparecieran sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitaba que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia.” (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 7)

Estas herramientas para la protección de datos personales son protocolos conocidos como códigos de exclusión (robots.txt), que impiden que el buscador, a través de su código de indexación, proceda a generar resultados utilizando nombres y apellidos de una persona. Este mecanismo no es infalible,

ya que el motor de búsqueda puede decidir pasarlo por alto, ignorándolos por completo.

Mediante resolución del día 30 de julio del año 2010, el Director de la Agencia Española de Protección de Datos desestimó la reclamación contra La Vanguardia Ediciones, S. L., tras considerar que la publicación de los anuncios que ésta había llevado a cabo estaba legalmente justificada, pero estimó la reclamación formulada contra Google Spain y Google Inc., instando a ambas compañías a tomar las medidas que fueren necesarias a fin de retirar los datos del solicitante de sus listas de resultados, y de esta manera imposibilitar el acceso futuro a los mismos.

La Agencia Española de Protección de Datos consideró que:

(“...”) quienes gestionan motores de búsqueda están sometidos a la 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“. (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 7)

La Agencia Española de Protección de Datos consideró contar con facultades para: 1) ordenar la retirada; y, 2) imposibilitar que los gestores de motores de búsqueda tengan acceso a determinados datos, cuando esta considere que el hecho de su localización y de su difusión puede causar lesiones al derecho fundamental a la protección de datos y, también a la dignidad de la persona, en sentido amplio, lo que, según esta afirma, incluye la voluntad del afectado cuando este no quiera que tales datos sean conocidos por terceros.

La Agencia Española de Protección de Datos identificó que el requerimiento pueda ser dirigido de forma directa a los explotadores de motores de búsqueda, “sin suprimir los datos o la información de la página donde inicialmente esté alojada, incluso cuando el mantenimiento de esa información en dicha página esté justificado por una norma legal.” (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 7)

Google Spain y Google Inc. interpusieron, ante la Audiencia Nacional, sendos recursos, en los cuales solicitaban la nulidad de la resolución de la Agencia Española de Protección de Datos.

La Audiencia Nacional acumuló dichos recursos y planteó, ante el Tribunal de Justicia de la Unión Europea, una cuestión prejudicial, siendo la primera vez que un Tribunal de un Estado, que fuera miembro de la Unión Europea, solicitase al Tribunal de Justicia de la Unión Europea, sea este el que fije las obligaciones de un motor de búsqueda que maneja información de personas y que esta afecta sus datos personales, a pesar de que esta haya sido publicada en sitios *Web* pertenecientes a terceros.

2.3. Aspectos de análisis

Hay tres aspectos que deben ser considerados al momento de efectuar un análisis al derecho al olvido digital, mismos que fueron abordados por el Tribunal de justicia europeo.:

1. **La aplicación en razón del territorio:** Es necesario analizar el ámbito de aplicación territorial de la legislación comunitaria sobre protección de datos personales, señalada en la Directiva 95/46/CE que trata acerca de la protección de datos personales. Dentro del caso Costeja, esto resulta aplicable toda vez que Google mantiene su sede en California.
2. **La *Ratio Materiae* de la Directiva 95/46/CE:** Se concretiza en la singularización de los proveedores de servicios de búsquedas en Internet (gestores de motores de búsqueda) como responsables del tratamiento de los datos que sus motores indexan (Costeja y AEPD vs Google INC y Google Spain SL., 2014). Es decir del ámbito de aplicación *Ratio Materiae* de la Directiva 95/46/CE, específicamente de su artículo 2. Que se refiere a los siguientes aspectos:
 - 2.1. Si las acciones de un motor de búsqueda, consistentes en encontrar información publicada en Internet, que indexan de forma automática y permite se almacene temporalmente y luego que sea

puesta a disposición de los usuarios, según un orden determinado, puede calificarse como tratamiento de datos personales.

2.2. La obligación del motor de eliminar los resultados los datos personales o información sobre un solicitante o interesado, aunque estos o esta no sean eliminados del sitio *Web* que las publicó.

3. Sobre el derecho al olvido digital:

3.1. El alcance del “derecho al olvido” en lo referente a la Directiva 95/46/CE, antes mencionada, es decir, se refiere a si un interesado puede dirigirse a los motores de búsqueda para que sus datos personales o la información sobre su persona no sean indexados.

3.2. Si se puede proceder con la solicitud de no indexación en atención a los derechos de supresión y bloqueo de datos, incluso si la misma es verídica y fue lícitamente publicada, pero que aun así puede causarle daño.

3.3. Se incluye también una consulta sobre las competencias que tienen las agencias nacionales de protección de datos, y;

3.4. Finalmente, “¿Equivalen los derechos de rectificación, supresión, bloqueo y oposición establecidos en la Directiva a un «derecho al olvido» del interesado?”.

Sobre esto, hay dos análisis claves que deben ser abordados, siendo el primero el pronunciamiento del Abogado General de la Unión Europea, Niilo Jääskinen, del 25 de junio de 2013; y luego la sentencia del Tribunal de Justicia de la Unión Europea.

A partir de este punto se abordarán cada una de las preguntas expuestas

2.4. La aplicación en razón al territorio

Sobre el primer grupo de ideas, que se refieren al aspecto geográfico, es necesario tomar como referencia de análisis los resultados del Grupo de Trabajo 29.

Este Grupo de Trabajo 29 es un órgano consultivo independiente, que se encuentra integrado por las Autoridades Nacionales de Protección de Datos de los Estados miembros, por el Supervisor Europeo de Protección de Datos y por la Comisión Europea, cuyas funciones reconocidas por la Directiva 95/46/CE son:

1. El estudio de todo asunto relativo a la aplicación de las disposiciones nacionales para la aplicación de la Directiva 95/46/CE.
2. La emisión de dictámenes (que es uno de sus medios de pronunciamiento junto con documentos de trabajo, recomendaciones e informes) sobre el nivel de protección de datos que existe en la Comunidad y en terceros países.
3. El asesorar a la Comisión sobre cualquier propuesta de modificación de la Directiva 95/46/CE.
4. El formular recomendaciones sobre cualquier cuestión relacionada con protección de datos dentro de la Unión Europea.

El Dictamen 8/2010 del citado Grupo de Trabajo 29 señala:

“The main criteria in determining the applicable law are the location of the establishment of the controller, and the location of the means or equipment being used when the controller is established outside the EEA. This means that neither the nationality or place of habitual residence of data subjects, nor the physical location of the personal data, are decisive for this purpose” (Grupo de Trabajo 29 sobre Protección de Datos, 2010, p. 8)

Una traducción informal sería: “Los principales criterios para la determinación de la ley aplicable son la ubicación del establecimiento del controlador, y la ubicación de los medios o equipo utilizados cuando el controlador está establecido fuera de la EEA. Esto significa que ni la nacionalidad o lugar de residencia habitual de los interesados, ni la ubicación física de los datos personales, son decisivos para este propósito”

El art. 4, apartado 1, letra a) de la Directiva 95/46/CE señala el derecho aplicable, en razón particular al “establecimiento” del responsable del tratamiento de los datos:

“Artículo 4.- Derecho nacional aplicable: 1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;...” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995, p. 39)

Bajo esta premisa, se debe tomar en cuenta el modelo de negocio en uso por los buscadores, donde su principal fuente de ingresos es otra la publicidad a partir de palabras clave, para lo cual un motor de búsqueda necesita posicionarse en los mercados nacionales en lo referente a publicidad, y esto lo hace a través de filiales o divisiones en los territorios de los estados miembros.

Al remitirse al dictamen del Abogado General de la Unión Europea, haciendo uso de los argumentos antes planteados, este sostuvo que existe tratamiento de datos personales “en el marco de las actividades de un establecimiento del responsable del tratamiento” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995, p. 39) en el momento que la empresa proveedora, controladora o gestora del motor de búsqueda establece dentro del territorio de un Estado miembro una oficina, división o filial, buscando la promoción y venta de espacios de publicidad en su motor de búsqueda, estando su actividad dirigida hacia los habitantes u operadores del país donde se encuentra dicha filial. (Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2013)

Con esto, el Abogado General da por solventado el primer conjunto de cuestiones presentadas por la Audiencia Nacional española como materia de consulta prejudicial.

Duro golpe para el buscador más utilizado del mundo, que durante mucho tiempo había logrado y seguía buscando evitar el tener que aplicar la normativa de protección de datos europea, durísima en comparación a la norteamericana.

Sobre este primer grupo de preguntas, el Tribunal de Justicia de la Unión Europea, en su sentencia reafirma lo señalado por el Abogado General, con lo cual Google vuelve a ser golpeada.

El Tribunal expone que el concepto de “establecimiento” no puede ser interpretado de forma restrictiva, toda vez que es necesario para que se garantice una protección de las libertades y de los derechos fundamentales de las personas naturales, de forma completa y eficaz, y en particular, del derecho a la intimidad, respecto al tratamiento de los datos personales (es necesario que se tomen en cuenta lo señalado en los considerandos 2 y 10 y en el art. 1 de la Directiva 95/46/CE, donde se le confiere una importancia especial a este tratamiento),

Para esta interpretación el tribunal nuevamente hace uso del art. 4, numeral 1, literal a) de la Directiva 95/46/CE ya citado previamente, que no exige que el tratamiento que se le dé a los datos personales sea efectuado “por” el propio establecimiento, sino que es suficiente con que este tratamiento se realice “en el marco de las actividades” de éste.

Pues bien, se debe entender que la actividad llevada a cabo por Google Spain constituye una parte esencial de la actividad comercial del grupo Google y que está estrechamente vinculada con Google Search y, por ello, el tratamiento de datos personales realizado por este buscador se lleva a cabo en el marco de las actividades del establecimiento de Google Spain, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda sea económicamente rentable y pueda continuar con sus actividades, entre otras el tratamiento de datos personales. El Tribunal europeo enfoca su análisis en esta idea

Esta relación se vuelve notable cuando al mostrar resultados de una búsqueda, la página de resultados los acompaña de publicidad vinculada.

“La actividad de Google se lleva a cabo en Europa porque existe un vínculo indisociable entre la actividad del motor de búsqueda y la actividad comercial de Google Spain.” (Silva, 2014, p. 21)

Es necesario conocer que luego de emitida la sentencia del Tribunal de Justicia de la Unión Europea, correspondió a la Audiencia Nacional resolver sobre el caso presentado en España y que fue objeto primigenio para la consulta efectuada, sin embargo su resolución, apegada a la sentencia, fue sometida a casación ante el Tribunal Supremo español, el cual, en sentencia RJ/2016/1525, del 14 de marzo de 2016, modifica lo sentado ya como doctrina jurisprudencial por la Audiencia Nacional.

Cabe mencionar que el recurso de casación presentado por Google Spain se encontraba fundamentado en siete puntos, pero este análisis se remite exclusivamente al papel de Google Spain, en virtud de ser ésta la que se aborda en la sentencia original.

Dentro del proceso se expone el organigrama de Google donde "Google Search es el prestador a nivel mundial de los servicios, su función es indexar páginas *Web* de todo el mundo, pero no sólo facilita contenidos alojados en las web, sino que además incluye publicidad asociada a sus patrones de búsqueda. Por su parte Google Inc. es la empresa matriz de Google tiene sede en EEUU y gestiona Google Search. Finalmente, Google Spain –poseedora de personalidad jurídica propia y con domicilio en Madrid– es utilizada por Google Search como agente promotor de las ventas de espacios publicitarios; es decir, su función es de agente comercial del Grupo en España". (Mate, 2016, p. 212)

Sobre el objeto de análisis de este acápite, el Tribunal Supremo señaló:

(...)entiende el Alto Tribunal que «Google Spain (...) no participa en forma alguna en la determinación de los fines y medios del tratamiento, frente a lo cual el Tribunal señala que no es preciso a los efectos que examina, aplicación de la normativa comunitaria, que se produzca tal participación, asumiendo así que Google Spain no interviene como responsable del tratamiento.» (Costeja y AEPD vs Google INC y Google Spain SL., 2016)

Este criterio expuesto en la citada sentencia haría que los interesados, de forma obligatoria, expongan sus pretensiones de hacer valer sus derechos contra la sede central del buscador contra el cual decidan ejecutarlo.

Si bien el criterio del Tribunal Supremo español falla y complica la aplicabilidad del derecho al olvido digital, la jurisprudencia norteamericana ha fallado sobre el lugar donde se puede demandar al causante del perjuicio, y para esto un análisis de la interactividad fue la herramienta a utilizar, definiendo que “es de estructura interactiva, se ha asumido que el responsable de la página *Web* sea demandado en el lugar de la apertura de la página” (Patriot Sys Inc. v. C-Cubed Corp., 1998)

En consecuencia, la aplicabilidad de todos estos criterios solo suma bases para sustentar la no necesidad de demandar en el domicilio de Google Inc., al ser esta es una página *Web* de estructura interactiva.

2.5. La Ratio Materiae de la Directiva 95/46/CE

Luego, se encuentra el segundo conjunto de temas, que versa sobre el ámbito de aplicación *Ratio Materiae* de la Directiva 95/46/CE, en lo que respecta al término “tratamiento”, utilizado ya en la explicación de aplicabilidad territorial de la normativa. La particularidad, en este caso específico es que la información no fue publicada por Google Spain o Google Inc., sino por un tercero (diario la Vanguardia, en su versión online).

El artículo 2 de la Directiva 95/46/CE, en su literal b) habla de que actividades corresponden ser identificadas y establecidas como tratamiento de datos:

“b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995, p. 38).

Con esto se puede entender que un motor de búsqueda, con sus operaciones de recopilación, almacenamiento, grabación y organización de los contenidos de una página *Web* fuente, y de los datos personales en cuestión dentro del caso en estudio, siendo estas acciones automáticas o no, implican tratamiento de datos personales.

Sin embargo, remitiéndonos al caso Costeja, el Abogado General, Jääskinen, sostuvo que señala que no se puede establecer responsabilidad del buscador, Google en este caso, en función de lo señalado en el literal d) del mismo artículo 2 de la Directiva 95/46/CE:

“d) «responsable del tratamiento»: 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; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995, p. 38)

Con esto se podría sostener que esta responsabilidad no es aplicable al motor de búsqueda porque el proveedor de este servicio simplemente proporciona una herramienta para la localización de información para sus usuarios, y que éste no ejerce ningún tipo de control sobre los datos personales que se encuentren incluidos en los sitios *Web* de terceros.

Incluso el buscador no muestra la información tal como se encuentra en el sitio original o fuente.

En consecuencia, las Autoridades Nacionales de Protección de Datos no podrían exigir al buscador que elimine de su índice la información, con la excepción de que este haga caso omiso de las instrucciones dadas por el editor de la página fuente, y proceda con la indexación de información o el almacenamiento de datos personales.

El Abogado General de la Unión Europea fija su posición en que los buscadores no son responsables del tratamiento de datos.

La situación antes expresada se da cuando se ignora el protocolo de exclusión o robot.txt que se mencionan con anterioridad en el presente documento.

En lo referente al alcance de la responsabilidad, Google presentó sendos argumentos sobre la afectación a los derechos de los editores de los sitios *Web* e incluso sobre los derechos del gestor del motor de búsqueda, y finalmente

señaló que la responsabilidad última debe recaer sobre el editor de la página *Web* fuente.

Sin embargo, se deben considerar los derechos, a la vida privada, y a la protección de datos personales, en contraposición con el tratamiento de datos personales.

“Por ello, el análisis del concepto de responsable del tratamiento de datos personales ha de ser funcional, de manera que la asignación de responsabilidad se haga en función de la capacidad de influencia real en el tratamiento de datos.” (Minero, 2014, p. 143)

Bajo esta premisa, la operación o actividad del buscador se añade a las acciones efectuadas por el editor del sitio *Web* fuente y por ende se presenta una afectación de carácter adicional a los derechos del interesado

El Tribunal de Justicia Europeo señaló en su sentencia que la autoridad nacional (autoridad de control u órgano jurisdiccional) podrá ordenar al gestor del motor de búsqueda que sean eliminados los vínculos a sitios *Web* publicados por terceros de la lista de resultados, siempre que estos contengan información sobre el interesado, incluso a pesar de que no se haya ordenado, de forma previa o simultánea, que esta información sea eliminada de la página *Web* fuente aunque su publicación haya sido hecha de forma lícita.

Tanto la responsabilidad de la página fuente y la del motor de búsqueda deben entenderse como independientes una de la otra, siendo irrelevante que se cumpla la primera para que el segundo ejecute las acciones de eliminar o volver inaccesibles los datos del interesado, en caso particular y a manera general. Incluso señala que la afectación mayor se da desde el buscador, al jugar un rol decisivo a la hora de difundir la información publicada en el sitio fuente. Sobre esto el Tribunal se pronuncia de la siguiente manera:

“En efecto, en la medida en que la inclusión, en la lista de resultados obtenida tras una búsqueda llevada a cabo a partir del nombre de una persona, de una página *Web* y de información contenida en ella relativa a esta persona facilita sensiblemente la accesibilidad de dicha información a cualquier internauta que lleve a cabo una búsqueda sobre el interesado y puede desempeñar un papel decisivo para la difusión de esta información, puede constituir una injerencia mayor en el derecho

fundamental al respeto de la vida privada del interesado que la publicación por el editor de esta página *Web*.” (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 19)

La base fundamental de este argumento enarbolado por el Tribunal de Justicia de la Unión Europea, se sustenta en lo señalado en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que versan sobre el respeto a la vida privada y familiar, y sobre la protección de datos personales, respectivamente.

De igual forma el tribunal, en su análisis, recoge lo expresado en el literal b) del artículo 2 del a Directiva 95/46/CE, ya expuesto por el Abogado General, y establece que el motor de búsqueda efectúa tratamiento de datos cuando, con los datos de las personas, realiza un proceso concatenado de recolección, extracción, registro, organización, conservación (durante su indexación), para concluir con la comunicación y facilitación de acceso a los internautas de estos datos.

Adicionalmente, el Tribunal señala que, como ya se lo había establecido en la sentencia del caso Lindqvist, C-101/01, EU:C:2003:596, cuando en una página web se hace referencia a datos personales, esto debe ser considerado como tratamiento de los mismos, lo cual refuerza su criterio de que el buscador se vuelve responsable de dicho tratamiento.

2.6. Sobre el derecho al olvido digital

Finalmente, sobre el tercer aspecto a considerar versa sobre la existencia de un derecho al olvido (digital), se encuentra lo siguiente.

Luego del análisis de la *Ratio Materiae* y superado este tema, se establece que el interesado puede solicitar de forma directa al gestor del motor de búsqueda las mismas acciones que la autoridad nacional puede disponer, señaladas en el artículo 28, apartados 3 y 4 de la Directiva 95/46 es decir, que sean eliminados los vínculos a sitios *web* publicados por terceros de la lista de resultados, cuando estos sitios tengan en su contenido información sobre él, datos que pudieran ser verídicos, publicados legalmente en estos sitios *web* (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995)

No es relevante si estos datos perjudican al interesado o no, toda vez que este puede solicitar dichas acciones simplemente porque desea que esos datos caigan en el olvido.

En la sentencia del Tribunal de Justicia de la Unión Europea existe una salvedad, y se refiere al interés público,

“Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.” (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 21)

Este tema será revisado más adelante en el presente capítulo.

Dentro del análisis, sobre el derecho al olvido digital es necesario contrastar lo expresado por el Abogado General y lo establecido por el Tribunal de Justicia dentro del caso Costeja, sobre sí: “¿Equivalen los derechos de rectificación, supresión, bloqueo y oposición establecidos en la Directiva a un «derecho al olvido» del interesado?” (Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2013, p. 17).

El Abogado General es categórico al decir que no, ya que es de su entendimiento que la Directiva 95/46/CE no faculta a quien sea el interesado a restringir o finalizar la difusión de sus datos personales que pueda llegar a considerar lesivos o en oposición a sus intereses.

En su pronunciamiento lo señala de esta manera:

“Los derechos de cancelación y bloqueo de datos, establecidos en el artículo 12, letra b), y el derecho de oposición, establecido en el artículo 14, letra a), de la Directiva 95/46, no confieren al interesado el derecho a dirigirse a un proveedor de servicios de motor de búsqueda para impedir que se indexe información que le afecta personalmente, publicada legalmente en páginas *Web* de terceros, invocando su deseo de que los usuarios de Internet no conozcan tal información si considera que le es perjudicial o desea que se condene al olvido.” (Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2013, p. 22)

El artículo 12 y literal b) citados por el Abogado General de la Unión Europea señala que se obtendrá la rectificación, la supresión o el bloqueo de datos cuando el tratamiento no se ajuste a lo establecido en la directiva 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 (Directiva 95/46/CE), de forma especial cuando los datos sean incompletos o inexactos

Tratando de entender el criterio de Jääskinen, también debemos remitirnos al artículo 14 de la Directiva 95/46/CE, literal a):

“Artículo 14.- Derecho de oposición del interesado: Los Estados miembros reconocerán al interesado el derecho a: a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995, pp. 42-43).

Estas abundantes citas, se vuelven necesarias para entender que el Abogado General de la Unión Europea buscaba demostrar que ese deseo de suprimir su información, no es sino una preferencia de carácter subjetivo, y que esta no podía de ninguna manera constituir una razón legítima.

Sin embargo, el Tribunal, considera improcedente lo antes mencionado por el Abogado General, toda vez que considera que en virtud de lo señalado en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, superando los intereses económicos de terceros y el interés de los internautas de acceder a la información de una persona, incluso si la información fuera lícitamente publicada y verídica. Se exceptúa la salvedad antes expuesta.

“Derecho al olvido, cuando el particular considere que una información pueda perjudicarlo, o bien simplemente cuando una información ha perdido su relevancia por el paso del tiempo, interés que prevalecerá sobre el económico del gestor y el de los internautas a obtener información, circunstancias que deben apreciarse por las autoridades nacionales” (García, 2014).

Los puntos 3.3 y 3.4 del tercer grupo de preguntas se resuelven, tras considerar que los temas de aplicación territorial y de tratamiento de datos ya se encuentran superados, toda vez que la Directiva 95/46 reconoce que las autoridades de control conocerán las solicitudes relativas a la protección de los derechos y libertades vulnerados cuando tengan relación con el tratamiento de datos personales. Asimismo, estas autoridades disponen de capacidades plenas para investigar e intervenir, permitiéndoles estos últimos “ordenar el bloqueo, la supresión o la destrucción de datos, o prohibir provisional o definitivamente un tratamiento” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995)

“Los particulares pueden dirigirse directamente ante los buscadores en Internet, a fin de que una información referente a su persona no sea suministrada, el derecho al olvido, aunque esa información no haya sido borrada en las páginas *Web*” (García, 2014), confiriendo capacidad para dirigirse directamente a los buscadores.

Y cuando el buscador, en calidad de responsable del tratamiento de datos no acceda a las pretensiones del interesado, este último puede acudir a las autoridades nacionales para que actúen en consecuencia.

2.7. Ponderación de Derechos

Es necesaria la ponderación, para el correcto ejercicio de este derecho, y esta debe efectuarse entre el derecho a la vida privada y a la protección de datos personales del “perjudicado”, que habrá de acreditar razones legítimas que justifiquen el que este derecho sea ejercido, en las particularidades de su caso y, en contraparte, el interés legítimo de tendrían los usuarios (internautas) que estén interesados (potencialmente) en acceder a los datos o información.

“Esto supone un proceso cuyo contenido material es complejo y que requiere ser estructurado secuencialmente. En esta secuencia resulta prácticamente seguro que pueda aparecer lo que Dworking denominó casos difíciles, en particular cuando los intereses en conflicto puedan afectar a derechos fundamentales”. (Martínez, 2014)

Esta consideración se presenta frente a la necesidad de efectuar ponderaciones a la hora de ejecutar el derecho al olvido, y es que en ciertas circunstancias, derechos como la libertad de expresión, de información, o consideraciones como el interés público o la memoria histórica, la oportunidad, hacen que sea necesario un análisis mayor por parte de la autoridad nacional o el órgano jurisdiccional antes de ordenar su aplicación a los gestores de motores de búsqueda.

“Dado que existe consenso universal en que la privacidad y otros derechos pueden ser afectados, en distintos niveles o grados, por el interés superior existente en la libre publicación de informaciones y opiniones relativos a determinados hechos con relevancia social, cualquier modificación del factor legitimador –el interés público informativo– alterará necesariamente los juicios de ponderación asociados, permitiendo, por ejemplo, una mayor protección de la honra y la privacidad por sobre el ejercicio informativo”. (Leturia, 2016, p. 98)

En términos generales los derechos a la vida privada y a la protección de datos deberían prevalecer sobre el interés de los internautas, pero esta situación puede cambiar en atención de la naturaleza de la información, el interés público, entre otras consideraciones que pueden hacer que la balanza cambie de lado.

Si bien, los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea (Carta de Derechos Fundamentales de la Unión Europea, 2000) establecen la capacidad de los ciudadanos de la zona comunitaria de presentar su solicitud sin mayor justificación, la sentencia del Tribunal de Justicia de la Unión Europea señala: “no obstante este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública.” (Costeja y AEPD vs Google INC y Google Spain SL., 2014, p. 18)

Este es el primer punto de contraposición encontrado, pero se supera con el análisis de la autoridad competente, en cada caso, de si la información que se pretende condenar al olvido, no está superada por el interés público.

Más allá de lo antes mencionado, Ricard Martínez presenta criterios para determinar si algo es o no de interés público, superando el criterio que señala algo como de interés público si es necesario que sea conocido por una sociedad democrática para formar una opinión pública libre.

Para definirse como interés público debe pasar por las siguientes consideraciones:

- 1) “Si la información es relevante para una comunidad dada, con independencia de su extensión y volumen.
- 2) Si esa información resulta “útil” a esa comunidad en orden a conocer aspectos relevantes de su entorno, o formarse una determinada opinión.
- 3) Si, en caso de que afecte a una persona física se dan dos circunstancias adicionales:
 - a) Que el impacto en su vida privada se limite a lo estrictamente necesario;
 - b) si su relación activa o pasiva en relación con la información le obliga a soportar la imitación en sus derechos que la publicación comporta.” (Martínez, 2014)

Estos criterios deberían aplicarse al momento de establecer si el interés público prima respecto de los datos o la información.

“(…) los sistemas jurídicos europeos han visto una evolución centrada en la valorización de los derechos de la personalidad como los elementos estructurales del ordenamiento jurídico (...). Lo anterior ha obligado a comprender las disposiciones legales de un modo más amplio, así como a considerar y balancear intereses contrapuestos, que en el caso que nos ocupa incluyen, por un lado, el derecho del individuo a vivir sin interferencias injustificadas que limiten sus derechos, su autonomía y sus posibilidades de desarrollo; y por otro, la resistencia que debe existir ante la demanda de limitar la libertad de expresión e información, atendido su

rol fundamental en una sociedad democrática, especialmente notorio cuando se refiere a materias de interés público”. (Leturia, 2016, p. 96).

Frente a la libertad de expresión, podemos establecer que el principal límite son los contenidos que contengan carácter injurioso o calumnioso podrían ser reputados como ilícitos.

Frente al derecho a la información, el límite se encuentra en la veracidad de la información, donde cualquier mensaje de carácter objetivo encuentra su protección a nivel constitucional en su veracidad, lo que implica acciones de verificación y contrastación de forma previa a su publicación, caso contrario, este no gozará de dicha protección.

Pero en todos los casos, debemos sumar las características antes señaladas para que los derechos de libertad de expresión y de información prevalezcan sobre aquellos que se resguardan tras la protección de datos, siendo ésta misma protegido y protector, y luego el derecho a la intimidad:

Primero deberá cumplirse la condición de interés público, implicando reconocer su vigencia y su pertinencia, y luego el no incurrir en el insulto o en la falta de veracidad, según corresponda. Esto contempla los principios rectores para el tratamiento de datos, a saber la veracidad, la temporalidad, la pertinencia y, destacándose, el consentimiento.

Y es que el derecho a la protección de datos personales se encuentra revestido de un elemento que debe ser resaltado, que es la autodeterminación o autonomía informativa “consistente en la capacidad de la persona de decidir en cada momento qué información personal será revelada, a quién y con qué objetivo”. (De Terwangne, 2012, p. 55). Frente a esto, el contar con el consentimiento del afectado se vuelve una obligación del que efectúe el tratamiento de los datos personales, pudiendo salvar algunas excepciones.

Se ha señalado que, a la hora de legitimar restricciones a los derechos de libertad de expresión y de libertad de información, el derecho al olvido resultaría una fórmula mucho más ágil a fin de beneficiar otros derechos, como la honra, la privacidad, la intimidad, entre otras; y que resulta ser una respuesta

natural frente al conflicto resultante de la incompatibilidad entre dos pretensiones.

2.8. Derechos ARCO y derecho al olvido

Se abren muchas interrogantes, que parecieran resueltas en la sentencia del Tribunal de Justicia de la Unión Europea, sin embargo, es preciso que se proceda con cierto tipo de análisis frente a alguna de ellas, siendo la primera si el derecho al olvido (digital) no es sino una aplicación concreta y tangible de los derechos ARCO.

Antes de continuar con ese análisis, ¿qué son los derechos ARCO?

El acrónimo procede de las primeras letras de cuatro acciones que proceden sobre datos personales: Acceso, Rectificación, Cancelación y Oposición; como se aprecia, ARCO

Estos se pueden definir:

1. Derecho de acceso: Aquel que permite a los ciudadanos, gratuitamente, conocer y obtener información sobre sus datos personales que se ven sometidos a tratamiento.
2. Derecho de rectificación: Está caracterizado por permitir la corrección errores, y la modificación de datos que se estiman inexactos o incompletos y, de esta forma, se garantiza que la información sometida a tratamiento sea cierta.
3. Derecho de cancelación: Permite que aquellos datos inadecuados o excesivos sean suprimidos.
4. Derecho de oposición: Es el derecho con el que cuenta un afectado para que sus datos personales no se vean sometidos a tratamiento o se detenga cualquier tratamiento en curso. (Silva, 2014, p. 30)

El ciudadano solamente puede ejercer este conjunto de derechos frente a quienes sean los titulares, ya bien públicos o bien privados, de bases de datos personales, y de igual manera solamente puede ejercerse a partir del

conocimiento de la existencia de tales bases y de lo que estas contienen, el uso y el destino de las mismas.

Es sumamente necesario que los titulares de datos o afectados por el sometimiento de los mismos a tratamiento hayan sido informados del mismo y que, en base a esa información, hayan procedido a dar su consentimiento.

A pesar de la existencia de los citados derechos, se considera que no contemplan el derecho al olvido digital, lo cual se explica porque los derechos ARCO, de manera singular, los derechos de oposición y cancelación de datos personales, se oponen, frente a terceros que efectúan acciones y deciden sobre el tratamiento de datos del interesado, los cuales son difundidos a través de la Internet, dejando fuera así a los gestores de buscadores que no son los que publican y divulgan la información contenida en las páginas *Web*, en sentido estricto.

Pero habiendo sentenciado que efectivamente las acciones de los buscadores constituyen un efectivo tratamiento de datos personales, estas acciones son las que se encuentran recogidas en el derecho al olvido digital.

2.9. Derecho al olvido, una visión internacional.

2.9.1. En Europa

Cerrada la sentencia del Tribunal de Justicia de la Unión Europea, cabe mencionar que esto no resolvió el caso en cuestión, sino que recayó en manos de la Audiencia Nacional española, sin embargo, lo expuesto por el Tribunal, es vinculante a todos los estados miembros, y sus tribunales nacionales.

La Audiencia Nacional recogió los criterios del Tribunal y su Sentencia de la Audiencia Nacional, de 29 de diciembre de 2014, se convirtió en el primer reconocimiento expreso sobre el derecho al olvido respecto de los motores de búsqueda y ha establecido una serie de criterios interpretativos:

- Criterio del transcurso del tiempo;
- justo equilibrio entre el interés legítimo del internauta; y,
- los derechos de la persona.

También ha ajustado la sentencia del Tribunal a la interpretación que sobre ponderación de derechos viene realizando en materia de doctrina jurisprudencial.

2.9.1.1. Francia

Podemos ver los efectos que esta sentencia ha tenido en la Unión Europea, cuando el Tribunal de Grande Instance francés, basado en sentencia del Tribunal de Justicia de la Unión Europea, que se acaba de analizar, ha sentenciado a Google France a pagar 1.000 euros al día a los demandantes que vieron violados sus derechos fundamentales por la publicación de información que se llegó a considerar difamatoria.

La sentencia del citado tribunal exhorta a Google France a efectuar los arreglos para la eliminación de los enlaces y dispone una multa coercitiva de 1.000 euros por día de retraso (Tribunal de grande instance de Paris, 2014).

Francia da un paso adelante en la aplicación del derecho al olvido, entendiendo que por cada día que pasa, sin que los enlaces sean removidos, permanecen las afectaciones a las personas involucradas.

2.9.1.2. Italia

Los efectos más crudos de la no aplicación oportuna del derecho al olvido se vivieron en septiembre del 2016, cuando Tiziana Cantone, una ciudadana italiana, cometió suicidio luego una batalla de meses para que se retirara un video de carácter sexual donde ella aparecía y que fue publicado en internet, sin su consentimiento y que fue el causante de un incesante acoso y burla por parte de la comunidad. (Rubio, 2016)

Días antes de su suicidio, Cantone finalmente obtuvo sentencia favorable sobre el derecho al olvido, donde se dispuso la supresión de los videos y el pago de costas a varios sitios que los difundieron, sin embargo, también fue condenada a pagar una suma de veinte mil euros, al considerarse que ella consintió las grabaciones (BBC Mundo, 2016)

Esto nos plantea algunas preguntas como ¿Esta afectación a su intimidad debe ser perennizada en internet? ¿Esto tiene algún interés público? ¿Podría volverse el derecho al olvido digital una herramienta para evitar el ciberacoso? Hoy la Fiscalía de Nápoles ha abierto una investigación por incitación al suicidio (Mazzola, 2016).

Las mentadas preguntas se responden por sí solas.

Esto es lo que se ha podido recopilar y mostrar respecto del caso de Tiziana Cantone, en virtud de las limitaciones lingüísticas encontrándose la mayoría de la información en italiano.

2.9.2. En América

2.9.2.1. México – Caso Carlos Sánchez vs Google México

México ha tenido un gran movimiento respecto a derecho al olvido en el último par de años.

Se encuentra el caso de Carlos Sánchez Peña, empresario mexicano, que había solicitado a Google México que se retiraran varios resultados de búsqueda que se relacionaban a su nombre. Entre estos uno que titulaba “Fraude en Estrella Blanca alcanza a Vamos México”.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), antes llamado Instituto Federal de Acceso a la Información, siendo la autoridad de protección de datos personales mexicana inició, en enero del 2015, un proceso sancionatorio contra Google México porque un ciudadano no había podido ejercer sus derechos constitucionales de oposición y cancelación al tratamiento dado a sus datos personales.

Cabe mencionar que en fechas anteriores, y desde el 22 de julio del 2014, el interesado ya había intentado ejercer los citados derechos ante Google México, S de R.L. de C.V. y es ante la negativa de la empresa que el 9 de septiembre de 2014 presenta una solicitud al citado instituto a fin de que sea este quien proceda a disponer al buscador se proceda con sus pretensiones, a la que se

le otorga el número de expediente PPD.0094/14. (Google México, S. de R.L. de C.V, 2015)

En su resolución dispone, como en efecto lo hace, a Google México aplicar los derechos de oposición y cancelación a favor del interesado, y sustenta conforme a los siguientes criterios:

- Google México, S de R.L. de C.V. es quien efectúa el tratamiento de datos personales, toda vez que el buscador es parte de su objeto social, según su acta constitutiva y esto cumple con lo estipulado en el numeral XIV del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que señala como responsable del tratamiento de datos a la “Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.” (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010, Art. 3)
- Siendo Google México, S de R.L. de C.V. responsable del tratamiento de datos, debió acoger la solicitud de oposición y cancelación interpuesta por el interesado.
- El Instituto Federal de Acceso a la información recoge el criterio de la sentencia C-131/12 del Tribunal de Justicia de la Unión Europea en términos de responsabilidad del motor de búsqueda.
- El Instituto “ordena a Google México, S. de R.L. de .C.V., llevar a cabo las acciones necesarias a efecto de hacer efectivos de manera indubitable los derechos de oposición y cancelación objeto de protección (...)” (Google México, S. de R.L. de C.V, 2015).
- Finalmente, resuelve iniciar un procedimiento sancionatorio contra Google México, S de R.L. de C.V.

Con fecha 27 de enero de 2015, el Instituto Federal de Acceso a la Información comunica que:

“En un hecho sin precedente, el Pleno del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) inició un procedimiento de imposición de sanciones en contra de Google México, S. de R.L. de

C.V., filial del gigante de las redes sociales, por posibles infracciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).” (Instituto Federal de Acceso a la Información, 2015, p. 1)

La Red de Defensa de los Derechos Digitales, definida en su sitio web como una organización dedicada a la defensa de los derechos humanos en el entorno digital, presentó un amparo contra la resolución del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, representando a la revista Fortuna.

El recurso de amparo fue negado en primera instancia por el Juzgado Décimo Quinta de Distrito en Materia Administrativa en el Distrito Federal, sin embargo, ante el recurso de revisión presentado por la mentada Red, el Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región concedió el amparo solicitado por la revista Fortuna, lo cual anula la orden emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de remover un enlace de una nota periodística sobre actos de corrupción.

Los argumentos aducidos por la parte quejosa son varios, pero el único recogido por el Tribunal es el referente a la violación al derecho de audiencia dentro del procedimiento PPD.0094/14, en el cual aduce que “cuando el acto reclamado tiene como efecto el obstaculizar la disponibilidad de enlace en un motor de búsqueda, que disminuye y menoscaba de manera directa el derecho de las quejas a difundir información en internet, lo que representa así una interferencia con su derecho de libertad de expresión, previsto en el artículo 6° constitucional.” (Revista Fortuna vs INAI, 2016)

En su análisis el Tribunal señala que no es “dable en esta vía de amparo el análisis del derecho de libertad de expresión, que como tercero interesado defiende la parte quejosa, porque en este momento los alcances del amparo se limitan a su derecho de audiencia para que en la instancia ordinaria el órgano especializado decida lo que en derecho proceda respecto de las pretensiones de las partes”.

Este caso no termina de resolver el tema de fondo que versa sobre el conflicto que se presenta, tratando de favorecer el derecho a la libertad de expresión contra el derecho al olvido digital.

Los temas de fondo ya han sido tratados con anterioridad en el presente documento, donde se debe considerar si la información es de carácter lícito en la publicación y luego el interés público que puede tener esta, para proceder con la ponderación de la misma.

2.9.2.2. México – Situación #LadyCoralina

Con el afán de fortalecer los argumentos de la cotidianeidad con que se presentan situaciones en las cuales el derecho al olvido digital es aplicable, a fin de salvaguardar la intimidad de las personas, se presenta el caso de #LadyCoralina, como se reconoce a Emma Alicia Paz Ayala, quien fue grabada en video durante su despedida de soltera en Playa del Carmen, México, siendo infiel a su novio en las instalaciones de Coralina Daylight Club (El Universal, 2016)

En redes sociales el evento fue explotado tremendamente, siendo motivo de críticas y burlas, y hasta la presente fecha, al efectuar una búsqueda en Google del nombre del sujeto en cuestión, son las noticias y comentarios sobre este hecho los que se muestran en los primeros lugares de los resultados.

Este caso se percibe con todos los elementos para aplicar el derecho al olvido digital, al no contar con el elemento de interés público, dado que el sujeto no ejerce ningún cargo en el gobierno o en alguna de las otras funciones del gobierno federal o del estado de Quintana Roo, ni el acto per se hace referencia a algún hecho de corrupción o similar.

Se deduce que los derechos a la cancelación y oposición no son procedentes en este caso, puesto que la información ya no se encuentra limitada a un solo sitio *Web*, contra quienes se podría interponer, sino que la misma se ha viralizado y se encuentra reproducido en varios sitios, de tal forma que el

control se podría llevar a cabo a través del buscador, como medio masificador para acceder a la información.

A la fecha, todo muestra que se vuelve a repetir el caso de Tiziana Cantone, el cual debe ser evitado.

2.10. Sumario

Luego de lo expresado en este capítulo se deduce que la aplicabilidad del derecho al olvido digital, conforme al estándar más alto a nivel mundial, establecido en Europa, protege a las personas, frente a la tecnología y la digitalización de la memoria, salvaguardando el círculo más interno de su existencia, su intimidad y los datos personales, como un derecho fundamental y por ende inherente a él.

A lo largo de este capítulo se han abordado los aspectos relevantes y necesarios dentro del derecho al olvido digital, donde el tratamiento de datos y su responsable, la aplicación en razón del territorio y la existencia del derecho al olvido digital, son caracterizados y resueltos.

Relevados estos aspectos, también se abordó contra quien se puede ejercer la tutela del derecho al olvido digital, siendo los buscadores el objetivo de cualquier acción, dado su rol como herramienta para la masificación de la información.

Es importante destacar que en la corriente europea, donde el estándar es mucho más alto y estricto, se han analizado varios factores que deben ser considerados, entre ellos la capacidad del sujeto a decidir sobre sus datos personales, conocido como autodeterminación informativa.

Se establece que las afectaciones a los sujetos se dan contra su intimidad y contra sus datos personales.

El análisis del caso más relevante hasta el momento en Europa nos ha permitido llegar a varias conclusiones, el hecho de que en efecto las actividades de los buscadores consisten en tratamiento de datos, como que la

aplicación en relación al territorio es posible toda vez que las actividades entre sucursales y matriz están vinculadas y sin una no existiría la otra y finalmente, se desvirtúa que el derecho al olvido digital sea innecesario, toda vez que existen los derechos de cancelación y de oposición, puesto que este es aplicable contra los buscadores, más allá de quienes publican la información, evitando la masificación de esta y que así las afectaciones sean mayores para el interesado.

Luego, frente a una posible colisión de derechos, la ponderación de los mismos será el medio de resolver el conflicto generado, y los conflictos más comunes se encuentran con el derecho a la libertad de expresión y de información, pero bajo condiciones generales, siempre será la protección de datos y la intimidad quienes prevalezcan. Si en el escenario se suma el interés público, es entonces cuando la balanza cambia de lado.

3. CAPÍTULO III: DERECHO AL OLVIDO DIGITAL EN ECUADOR

Scott McNeally, quien fuera Presidente y fundador de Sun Microsystems, dijo en 1999, “You already have zero privacy. Get over it” (Solove, 2004), que es casi un llamado a la resignación a no tener privacidad o intimidad, aunque a veces ha intentado suavizar lo antes mencionado ha dicho que si se tiene privacidad es porque alguien tolera que la tengamos (McNeally, 2007), que sigue siendo igual de impactante.

Sin embargo, el camino en la defensa de la intimidad y de los derechos personales, vuelve impensable que tal afirmación, en el marco legal vigente, sea acertada.

En este último capítulo se presentará la propuesta de aplicación del derecho al olvido digital en Ecuador, mostrando que se reúnen todos los elementos jurídicos necesarios para su aplicabilidad.

Se mostrarán los citados elementos tanto dentro del contexto constitucional y de igual manera en las normas de menor jerarquía, con su respectivo análisis, que permitirá entender porque se considera que su aplicación no solo es posible, sino necesaria.

Este análisis pretende abarcar los aspectos elementales del derecho al olvido digital, como la protección de datos personales, que incluye un análisis de la situación ecuatoriana en relación al *Habeas Data*, el tratamiento de dichos datos en el marco de la *Internet*, la aplicabilidad de esta novísima figura en relación al territorio y finalmente el criterio de ponderación frente a la posible colisión de derechos.

El Ecuador pasa por un momento muy importante en el marco de protección de datos personales, al tener un proyecto de ley en proceso de aprobación, por lo que este aporte no se encuentra fuera de tiempo, sino que resulta oportuno y procedente.

3.1. Derecho a la Protección de Datos

Es necesario, previo a todo, definir lo que es un dato desde el punto de vista jurídico, y para esto Miguel Davara (2008) nos ofrece una definición al respecto:

“(...) el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad y aceptamos que ese dato se encuentra en un documento o un soporte –físico o lógico- con la calidad de testimonio, debemos diferenciarlo de información, entendiendo por tal la acción de informar o dar noticia de algo (...)” (Davara, Manual de Derecho Informático (10ma Ed.), 2008, p. 46)

Entendemos entonces que el dato busca absolver una consulta específica y permite a un posible investigador, iniciar su proceso. Esta definición es la base que nos servirá para introducirnos en el campo de datos personales.

Luego debemos entender que, en virtud de un concepto generalmente aceptado, un dato personal es aquel que se encuentra atado o vinculado a una persona natural, identificada o identificable, relacionado o concerniente a esta, Esta idea es tomada y reforzada por Lina Ornelas cuando señala que “En ese sentido, el ámbito de protección es hacia la persona en relación con el tratamiento que se dé a su información, la cual se puede encontrar en posesión de los gobiernos o de los particulares.” (Gregorio & Ornelas, 2011)

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, antes Instituto Federal de Acceso a la Información y Protección de Datos, recoge ese concepto general y profundiza la idea diciendo que siendo cualquier información que identifique, permita identificar o haga identificable al titular del dato personal, este puede estar expresado “(...) en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otra modalidad.” (Secretaría de Protección de Datos Personales, 2014)

La Directiva 95/46/CE (1995) recoge todas las ideas antes mencionadas y señala en su artículo 2, que un dato personal es: “toda información sobre una persona física identificada o identificable (...); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos

específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995, p. 38)

Este último, caracteriza los datos personales, tratando de no dejar un ápice de duda sobre lo que estos llegan a ser y su procedencia.

Los señalamientos antes mencionados permiten abrir el análisis de un aspecto que llega a presentar confusiones a los más neófitos en materia de datos personales, y es sobre si existen o no datos personales públicos, y es que si bien varios autores tratan de diferenciar o clasificar los datos personales, se debe entender que no es tal, toda vez que el dato no pierde su característica de personal, y por ende no pierde sus características frente la protección debida para ellos, sino que hay ciertos datos que se encuentran alojados en registros públicos.

Ahora, con ideas claras respecto a datos personales, es necesario establecer que idea maneja la legislación ecuatoriana al respecto, sobre lo que es un dato personal.

Para esto la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos señala, en su Novena Disposición General que datos personales: “Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.” (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, Novena Disposición General)

La citada ley tomó como base la teoría de las esferas para establecer el concepto antes señalado. Esta teoría señala que lo íntimo y lo privado se encuentran ubicados en esferas concéntricas, donde lo íntimo se ubica en el círculo más interno, mientras lo privado en el círculo más amplio. Esto explicaría porque esta ley solo le concede protección basada en los principios de confidencialidad y reserva.

Sin embargo de lo antes mencionado, la teoría más moderna considera a la de las esferas insuficiente para enfrentar ataque de una índole más sofisticada.

Esta nueva teoría es conocida como del mosaico, desarrollada y propuesta por Fulgencio Madrid Conesa.

La teoría del mosaico “estima lo privado y lo público como conceptos relativos” (Ruiz Miguel, 1994, p. 243)

Esta teoría concluye que, por un lado, lo privado y lo público son relativos en atención a quién sea el otro participante o sujeto en la relación informativa; y por otro lado, reconoce la existencia de datos *A Priori* considerados con carácter de irrelevante, pero que en conexión con otros datos, tal vez con el mismo carácter de irrelevantes, puedan servir para que la personalidad de un ciudadano, se transparente en su totalidad, “al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, puede que unidas puedan formar conjuntos plenos de significado” (Madrid Conesa, 1984, p. 45)

Bajo esta teoría, los datos personales están sometidos a la protección del conjunto más amplio de acciones, elementos y herramientas que se han expuesto en el presente documento.

Se debe diferenciar, entonces, que el derecho a la intimidad busca proteger a los individuos frente a cualquier invasión que pueda afectar el ámbito de su vida personal o familiar y que este desea que permanezca excluido del conocimiento ajeno y de las posibles intromisiones de terceros en contra de su voluntad.

En cambio, el derecho fundamental a la protección de datos personales pretende garantizar al individuo el poder de controlar sus datos personales, su uso y su finalidad, a fin de impedir su tráfico lesivo e ilícito.

“El derecho al olvido se integra dentro del derecho a la protección de datos personales al entender que nos encontramos ante elementos que identifican a personas físicas y cuyo tratamiento automatizado permite diversas acciones por parte de terceros con ellos” (López Portas, 2015, p. 158)

Es así que el derecho a la protección de datos personales le otorga a su titular una gama de facultades consistente en una serie de poderes jurídicos cuyo ejercicio impone a terceros varios deberes jurídicos, mismos que no se encuentran contenidos en el derecho a la intimidad. Este derecho fundamental garantiza al individuo el control sobre sus datos personales, siendo esto posible y eficaz en la imposición de deberes de hacer a terceros. Ésto implica el derecho a que se requiera el consentimiento previo al momento de recopilar y usar datos personales, el derecho a ser informado sobre la finalidad y sobre el uso de dichos datos y, finalmente los derechos a su acceso, rectificación y cancelación.

3.2. Ecuador y Europa, una comparación en materia de derechos de protección de datos personales

Abordado el concepto de dato personal, procede efectuar una comparación entre los cuerpos legales de jerarquía superior en materia de declaración de derechos a nivel ecuatoriano y a nivel europeo, a fin de establecer las similitudes entre ambos y de esta manera aproximar la realidad ecuatoriana a la aplicación del derecho al olvido digital

A efectos de esta equiparación es necesario remitirse a lo establecido en nuestra Constitución, y es que en el numeral 19 del artículo 66 reconoce la protección de los datos de carácter personal, entre otras cosas.

“(...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.”
(Constitución de la República del Ecuador, 2008, Art. 66 Numeral 19)

Comparable, en sus sentido más amplio con lo señalado en la Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 8, donde señala, en sus dos primeros párrafos, lo siguiente:

“1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación” (Carta de los Derechos Fundamentales de la Unión Europea, 2000).

Para el análisis comparativo se efectuara una descomposición de los dos artículos y se compararán con sus correlativos a fin de establecer las similitudes o diferencias entre los mismos, en el contexto del derecho al olvido digital.

El mentado análisis se llevará a cabo contrastando elementos de la Carta de derechos fundamentales europea y la Constitución ecuatoriana, partiendo desde la titularidad activa, para pasar al reconocimiento de la autodeterminación informativa y finalmente a las acciones reconocidas en su contenido y que se pueden aplicar en el ámbito de los datos personales, y cuales no

3.2.1. Titularidad

Ambos cuerpos consagran la protección de datos de carácter personal, diferenciando que en el caso de la Carta de los Derechos Fundamentales de la Unión Europea se establece la limitación hacia los datos concernientes a la persona sujeto de protección, natural o jurídica.

Ya el Tribunal de Justicia Europeo en el caso de Costeja y AEPD vs Google INC y Google Spain SL, señalo que el interesado, que es quien considera vulnerado sus derechos puede acudir directamente por vía judicial o administrativa en cuanto a la presentación de su petición de aplicación del derecho al olvido digital.

La legislación ecuatoriana, complementa lo expresado en su Constitución en el numeral 19 del artículo 66 con lo estipulado en el artículo 9 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, el cual establece que para el ejercicio de garantías cualquier persona, comunidad, pueblo, nacionalidad o colectivo, cuyo o cuyos derechos constitucionales se encuentren

vulnerado o amenazado, podrá actuar por sí misma o a través de representante o apoderado; y, a través de la Defensoría del Pueblo.

3.2.2. Autodeterminación Informativa

“(...) definición y naturaleza del derecho a la autodeterminación informativa, enunciando en su fundamento jurídico segundo lo siguiente: “El derecho general de la personalidad(...) abarca(...) la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y en qué límites procede revelar situaciones referentes a la propia vida (...) la eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos de protección del individuo contra la recogida, el almacenamiento y la transmisión de sus datos personales” (Higareda, 2014, pp. 105-106)

Con base en lo antes mencionado, es posible entender que la protección de datos personales tiene su cimiento primigéneo en la autodeterminación informativa, como la facultad de decidir sobre sus datos.

Es necesario destacar que la autodeterminación o autonomía informativa se recoge en ambos tanto en la Constitución ecuatoriana y la Carta de los Derechos Fundamentales de la Unión Europea.

La Constitución ecuatoriana estipula la necesidad de autorización para la recolección, archivo, procesamiento, distribución o difusión de los datos o información. Acciones que corresponden a tratamiento de datos.

El texto recogido de la antes citada carta europea, habla sobre el consentimiento del tratamiento que se le dará a los datos, considerando los aspectos de lealtad y que el fin para el cual se los va a tratar, sea concreto, es decir, que sea específico, sin delimitar el tipo de acciones para las que requeriría la autorización.

Existen condiciones bajo las cuales la ley establece cuando puede darse algún tipo de tratamiento a datos personales, sin consideración de la autorización o consentimiento de su titular, y esta posibilidad se encuentra contemplada tanto el caso europeo como el ecuatoriano.

Para entender lo expresado en ambos marcos jurídicos, se requiere adentrarse en esta autonomía o autodeterminación informativa, y lo primero que se debe

reconocer es el bien jurídico subyacente, que no es otro sino la intimidad y en algunos otros ordenamientos la privacidad.

Frente al tratamiento de datos personales, aún encontramos en nuestros días quienes siguen viendo en la protección a la intimidad el *Nomen iuris* desde el cual responder a las agresiones que sufren nuestros datos de carácter personal. Hoy se entiende que, frente al tratamiento de datos personales, los instrumentos que permitían tutelar el derecho a la intimidad resultan ineficaces, en la mayoría de los casos, porque los datos personales no reflejan necesariamente los espacios íntimos.

Desde antes de que las tecnologías se involucren en el proceso es “excluir del conocimiento ajeno cuanto guarda relación con sus relaciones sexuales, conyugales, paterno-filiales y familiares, con su cuerpo, con su salud, con su muerte, con sus pensamientos, creencias, aficiones y afectos” (Lucas, 2008), era parte de la autodeterminación informativa.

Se debe recordar que la teoría del mosaico rompió el esquema bajo el cual se podía decir que la autodeterminación informativa abordaba exclusivamente la esfera de lo íntimo, sino que se refiere incluso a los datos personales, que podrían parecer inocuos, pero que en conjunto, permiten identificar o vuelven identificable a la persona.

Entonces, se establece “una nueva dimensión, en virtud de la cual ya no se entiende tan solo en un sentido puramente negativo, de rechazo de intromisión de extraños a la vida privada (...) sino que ha pasado a tener un carácter positivo, por medio del cual se reconoce a cada persona el ejercicio de un control sobre el uso que pueda hacerse de los propios datos personales recogidos en un archivo electrónico” (Fernández Segado, 1994, p. 227)

Podemos colegir entonces, que el derecho a la autodeterminación informativa, que la apreciación de Ma. Borgoña López es acertada al decir que “atribuye a su titular un conjunto de poderes jurídicos cuyo ejercicio se impone como deberes ante terceros con un carácter

instrumental ya que pretende garantizar a los ciudadanos el pleno ejercicio de sus derechos, todos ellos” (López Portas, 2015, p. 155).

Permitiendo exigir consentimiento de su recolección, el informar sobre su uso y destino, así como concederle las acciones incorporadas en la garantía de *Habeas Data*.

3.2.3. En materia de datos personales.

El acceso a los datos se recoge tanto en la Constitución ecuatoriana y la Carta de los Derechos Fundamentales de la Unión Europea.

En la Carta europea, se reconoce adicionalmente la rectificación del dato de carácter personal, mientras en la Constitución ecuatoriana no se hace mención específica, sino que se habla de “decisión”, que tiene un concepto bastante menos limitado: “Formar el propósito de hacer algo tras una reflexión.” (Real Academia de la Lengua Española, 2016).

Este concepto sobre “decisión”, definido por la Real Academia de la Lengua Española, se entendería con amplitud suficiente para abarcar a todos los aspectos posibles y reconocidos sobre un dato de carácter personal, a saber, a manera ejemplificativa y sin ser taxativo, la rectificación, la oposición, la cancelación, el compartirlo, el reservarlo, considerando los marcos legales ya existentes y establecidos en varios otros cuerpos legales nacionales.

Sin embargo de lo antes mencionado, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009), establece que las únicas acciones que se podrían interponer son las de acceso, rectificación, eliminación o anulación de los datos personales, señaladas en el *Habeas Data*, pero sin limitarse a esta única garantía constitucional, contando con la posibilidad de exigir de forma directa el cumplimiento de lo establecido en el numeral 19 del artículo 66 de la Constitución ecuatoriana, o recurrir a la vía civil.

Los derechos de acceso y rectificación de los datos personales, a los cuales hace mención el articulado europeo, forman parte de los derechos ARCO, que

hemos visto en el capítulo anterior, y más allá de eso, la Directiva 95/46/CE nos habla de la capacidad de los interesados de solicitar al responsable del tratamiento de sus datos personales el acceso libre, irrestricto, sin retrasos ni gastos excesivos, dentro de una periodicidad razonable, a información sobre ellos. Asimismo, puede obtener del mismo responsable la rectificación del dato, cuando este sea inexacto, incompleto o no se ajuste a las disposiciones de la citada directiva (Dir. 95/46/CE del Parlamento Europeo y del Consejo, 1995).

Comparados los dos cuerpos legales, la Constitución ecuatoriana y la Carta de los Derechos Fundamentales de la Unión Europea, vemos un apareamiento entre los dos y se reconoce existen grandes y marcadas similitudes entre ambos.

Siendo así que ambas cuerpos legales llevan consigo tanto el reconocimiento del derecho a la protección de datos como la autodeterminación informativa, elementos claves para la aplicación del derecho al olvido digital

3.2.4. Criterios no contemplados en el ordenamiento jurídico ecuatoriano.

Las sentencia del caso Costeja y AEPD vs Google INC y Google Spain SL establece dos criterios que la legislación ecuatoriana no recoge dentro de su ordenamiento jurídico y que son fundamentales para el reconocimiento del derecho al olvido digital en el país.

Lo primero que se debe señalar es, ante todo, que Ecuador no cuenta con una ley especial que regule la protección de datos personales, por lo que cualquier análisis debe restringirse a nivel constitucional.

El primero de estos criterios contempla la posibilidad que tiene el usuario, titular de la información de interponer, ante los buscadores en internet, un recurso que permita la eliminación de su información de sus registros e índices, es decir, se lo elimine de su indexado o que no se proceda con la indexación.

En cuanto al segundo criterio, se establece que no se recoge, en el marco de la Constitución, la posibilidad de decisión de cancelación de la información que

puede constar en la *Web*, que siendo datos personales y verdaderos, causan un perjuicio a la dignidad de un particular.

El Artículo 92 de la Constitución de la República del Ecuador y el artículo 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, recogen la garantía de *Habeas Data*, misma que contempla varias acciones posibles para garantizar la protección de datos personales.

“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” (Constitución de la República del Ecuador, 2008, Art. 92).

Como se analizará más adelante, esto constituiría la presencia de los derechos ARCO en el marco constitucional ecuatoriano, pero de ninguna forma se reconoce una acción específica contra el buscador para que la eliminación de datos de su indexado.

El derecho de cancelación se interpone cuando los datos son inexactos, inadecuados o excesivos, sin embargo, en el caso del derecho al olvido digital, este surge ante el perjuicio que la publicación de los datos causa al titular de los mismos, a pesar de que estos sean verdaderos, constituyéndose en memoria histórica, pero que de alguna forma le causan un perjuicio o que por el devenir del tiempo han perdido relevancia.

Es apreciable como ambos criterios se articulan de tal forma que permiten la defensa del honor, de la intimidad y, en mayor grado, de la dignidad de la persona.

Estos elementos juegan un rol determinante dentro del derecho al olvido digital, el primero por establecer la acción necesaria para interponerlo y segundo por reconocer bajo qué situación es posible aplicable.

Se puede concluir entonces que, tras el análisis de la norma constitucional ecuatoriana, estos dos elementos no han sido establecidos o reconocidos de manera formal.

3.3. Habeas Data y Protección de Datos Personales.

En esta sección procederemos a hacer un análisis de la garantía constitucional conocida como *Habeas Data* y su postura frente a la protección de datos personales., como única garantía existente en el marco constitucional ecuatoriano direccionada a la protección de datos personales.

La Constitución de la República de Ecuador estipula:

“Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.” (Constitución de la República del Ecuador, 2008, art. 92).

Esta acción fue creada, según sentencia de la primera Sala del Tribunal Constitucional del Ecuador, dictada el 15 de octubre del 2015 para: “salvaguardar el derecho a la autodeterminación informativa, esto es, mantener el control de los datos que existan sobre una persona o sobre sus bienes, y para proteger el derecho a la honra, a la buena reputación y a la intimidad personal y familiar” (Caso 0049-2008-HD, 2008)

Lo antes señalado se ratifica en la sentencia de la Sala Tercera de la Corte Constitucional del Ecuador, en la cual se señala que la garantía de *Habeas Data* fue “creada para salvaguardar el derecho a la autodeterminación informativa, procura mantener el control de los datos que existan sobre una persona o sobre sus bienes, y para proteger el derecho a la honra, a la buena reputación y a la intimidad personal y familiar” (Caso 0065-2008-HD, 2009)

Ambas sentencias recogen en su texto los derechos protegidos y es destacable el hablar de autodeterminación informativa, que es el meollo del asunto materia del presente documento, esa facultad de la persona de decidir quién, qué y cómo se efectúa el tratamiento de sus datos personales.

Pero al parecer la Corte olvidó que la teoría de las esferas ya fue superada por la teoría del mosaico, y entonces la autodeterminación informativa resguarda los datos como tal, incluso si estos resultaren, de forma aparente, inocuos, en virtud del derecho a la protección de datos personales.

Ahora bien, se debe recordar que el *Habeas Data* nace como una garantía, según consta en el artículo 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional:

“La acción de hábeas data tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos” (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009, Art. 49).

Desde esta acción se deduce la existencia los derechos ARCO en el Ecuador: conocimiento, acceso, actualización, rectificación, eliminación y anulación de datos personales. No se reconoce, de entre los derechos ARCO, el de oposición.

Es así que esta garantía pretende evitar que se utilice de forma inadecuada la información, que la misma no sea apegada a la realidad en atención a una posible desactualización, permitiendo su adecuación. De igual manera busca que los datos recopilados en bases, públicas o privadas, sean utilizados para fines diferentes a aquellos para los cuales se los recopiló o que estos se mantengan por más tiempo que el para el cual se los debía almacenar.

Mediante su utilización se evita lesiones a los derechos fundamentales de las personas, permitiendo que la información que se tiene de ellas sea exacta,

pertinente, actualizada, fidedigna y no sea utilizada con otra finalidad que aquella para la que se recogió, almacenó y se efectuó su tratamiento, pero sobre todo, porque es la que directamente se vincula a la protección de datos personales.

Las acciones recogidas en esta garantía son aquellas que permitirían que el derecho al olvido digital sea aplicable, evidenciando de alguna manera la existencia de derechos ARCO en el marco constitucional ecuatoriano.

En un primer momento, se entiende a la protección de datos personales como ese resguardo que se efectúa sobre los datos, pero la importancia debe recaer sobre el tratamiento de los estos y la protección jurídica de su titular, siendo que es su manejo el que puede causarle perjuicios.

De esta manera, el derecho a la protección de datos personales, se entiende como “(la tutela de la) persona, con relación a las afectaciones de sus derechos fundamentales que pudieran sufrir a partir del tratamiento de datos por parte de terceros, que pueden ser las autoridades estatales, las empresas privadas e incluso los particulares” (Puente de la Mora, 2007) respecto de las nuevas tecnologías de la información, destacando a los motores de búsqueda, en los cuales se indexan datos personales de los individuos y se muestran en los resultados que ofrecen frente a las búsquedas efectuadas a través de ellos.

Para esta tutela, en nuestro marco constitucional, es el *Habeas Data* la garantía que otorga a la persona el poder de control sobre el destino de sus datos y sobre su uso.

El derecho al olvido digital, como se verá más adelante, se convierte en un derecho de libertad, en una forma de derecho instrumental de la autodeterminación informativa, que ya existe como un derecho fundamental en su forma consagrada en el numeral 19 del artículo 66 de la Constitución de la República del Ecuador.

Sin embargo, a diferencia de los Derechos ARCO, que recoge acciones específicas sobre los datos personales que pueden ser interpuestos contra

quien tiene en su poder dichos datos, el derecho al olvido digital busca constituirse como un derecho global para la eliminación del interesado de los índices de los buscadores.

Adicionalmente, el *Habeas Data* se constituye como una garantía, con un espíritu reactivo frente a una afectación frente al tratamiento inadecuado de los datos personales, no así el derecho al olvido digital que busca su reconocimiento como un derecho, exigible desde su declaración como tal.

Sin contar con su reconocimiento como un derecho, el control de las acciones que se efectúan sobre los datos personales recae en el *Habeas Data*, siendo esta la acción utilizable a fin de decidir quien efectúa tratamiento sobre ellos y quien puede accederlos, con demasiada facilidad, gracias al uso de los buscadores.

3.4. La dignidad humana como base para el reconocimiento del derecho al olvido digital.

El derecho fundamental a la protección de datos personales conlleva, como se ha mencionado en diferentes ocasiones, los poderes de disposición y control sobre los datos personales de una persona y facultados a esta.

Se debe considerar que se incluye, de forma adicional, la facultad de decidir que datos se proporcionarían a terceros, pudiendo ser el Estado o un particular, o que datos pueden ser recopilados por un tercero y, de igual manera, mantener informado al titular de los datos personales sobre quién los posee y su finalidad, permitiéndole oponerse a dicha posesión o uso, de así requerirlo. Todo esto inmerso en la autodeterminación informativa ya antes mencionada.

Entendiendo que se cuenta con el derecho a la protección de datos personales, el cual se encuentra estrechamente vinculado a la autodeterminación informativa, no es menos cierto que el derecho al olvido digital también mantiene ese vínculo, y así lo destaca Pere Simón Castellano:

“La conexión del derecho al olvido con la autodeterminación informativa, consciente y responsable de la propia vida es, a mi juicio, inevitable, siendo una manifestación directa de la dignidad humana y de la integridad

moral del ser humano. Luego el derecho al olvido protegería un bien jurídico más amplio que la vida privada(...)" (Castellano, 2012, p. 220)

Y es que Pere Simón Castellano va más allá, al hablar del libre desarrollo de la personalidad, que se recoge en el artículo 10.1 de la Constitución Española, al igual que en el numeral 7 del artículo 11 de la Constitución de la República del Ecuador.

Esto deriva del respeto a la dignidad personal, generadora de derechos, tal como lo reconoce la Constitución, y que acepta los derechos derivados de esta, colocándolos al mismo nivel de los derechos y garantías constitucionales, así como de los derechos humanos reconocidos en instrumentos internacionales.

"El ejercicio de los derechos se regirá por los siguientes principios:(...) 7. El reconocimiento de los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, no excluirá los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento". (Constitución de la República del Ecuador, 2008, Art. 11, Numeral 7)

Al hablar del principio de dignidad humana se debe reconocer que el mismo es soporte del orden constitucional y se encuentra presente en la mayoría de las constituciones latinoamericanas.

Esta posición es extendida en América Latina, pudiendo establecerse como ejemplo la Constitución de Brasil de 1988, artículo 1º señala que la República Federal de Brasil tiene como fundamentos...III la dignidad de la persona humana"; la Constitución de Colombia de 1991, artículo 1º, prescribe "Colombia es un estado social de derecho [...] fundado en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que lo integran y en la prevalencia del interés general"; la Constitución Chilena, en su artículo 1º determina: "Las personas nacen libres e iguales en dignidad y derechos"; la Constitución Peruana de 1993, en su artículo 1º, señala "la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y el Estado"; la Constitución de Honduras de 1982, artículo 5º, precisa: "la persona humana es el fin supremo de la sociedad y del Estado. Todos tienen la obligación de respetarla y protegerla"; la Constitución de Guatemala de 1985 establece en su artículo 1º "Protección de la persona. El Estado de Guatemala se organiza para proteger a la persona y a su familia; su fin supremo es la realización del bien común" (Nogueira Alcalá, p. 1).

La dignidad de la persona se constituye en el principio jurídico que conforma la espina dorsal del ordenamiento constitucional, siendo fuente de los derechos fundamentales.

Si es necesario definir la dignidad de la persona parecería preciso entender que es el “valor y pretensión de respeto intrínseco y simultáneamente social, al cual pertenece cada ser humano por su condición humana” (Häberle, 2005, p. 107).

Instrumentos internacionales parten de la dignidad de la persona para comenzar a desarrollar los derechos más instrumentales, tal es el caso de la Declaración Universal de Derechos Humanos, que en su artículo 1 señala: “Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros”. (Declaración Universal de Derechos Humanos, 1948, Art. 1).

Partiendo de esa premisa, y siendo suscriptor de la citada declaración, la *Norma Normarum* ecuatoriana recoge en su preámbulo la decisión de construir: “Una sociedad que respeta, en todas sus dimensiones, la dignidad de las personas y las colectividades” (Constitución de la República del Ecuador, 2008, Preámbulo), y luego el precitado artículo 7.

Es en ese sentido, enmarcado en la Declaración Universal de Derechos Humanos y en la Constitución de la República, que debe aplicarse la normativa, que se convierte en una especie de guía de interpretación a seguirse por los administradores de justicia y demás operadores jurídicos.

Se podría acotar entonces que “el derecho a la protección de datos persigue el garantizar al individuo un poder de control sobre sus datos personales, no sólo desde el punto de vista de su uso sino también de su destino, con el fin de impedir una lesión de nuestra dignidad y derechos”. (López Portas, 2015, p. 154)

Esta dignidad personal, bajo su forma de valor jurídico, garantiza a toda persona el derecho de diseñar, establecer y ejecutar su proyecto de vida, sin que sus derechos fundamentales se vean lesionados.

La autodeterminación informativa emerge como derecho personal para poder controlar los datos personales que, por su mal uso, pueden afectar el desarrollo vital de un ciudadano, y para esto se configura el denominado el derecho al olvido digital (López Portas, 2015)

Es entonces que se debe entender que el propuesto derecho al olvido digital busca la protección de la dignidad de las personas físicas (sobre las personas jurídicas existe un amblio debate en curso al respecto, pero eso no es materia de este trabajo de titulación). La dignidad humana fundamenta el hecho de que exista la autodeterminación informativa, y es esta conexión existente entre ambos lo que define la titularidad del derecho a la protección de datos.

“El olvido digital se entiende como un derecho a controlar los datos personales propios que permitan el desarrollo del proyecto vital, amparándose en la dignidad humana, y que encuentra su fundamento en el derecho a la autodeterminación informativa, cuyo bien jurídico protegido sería más amplio que el bien jurídico protegido por el derecho a la protección de datos” (Castellano, 2012)

Dentro del ámbito de la internet, el derecho al olvido digital recoge el amparo a una persona para requerir a los buscadores o motores de búsqueda el que no los indexen o eliminen su rastro. La finalidad de este amparo ofrecido por el derecho al olvido digital es proteger la dignidad de las personas y evitar que sean objeto de ofensas o agresiones, de forma permanente.

La concordancia entre los expresado por López Portas y Castellano nos demuestra que la visión del desarrollo de proyecto de vida de las personas, sustentado en su dignidad, es el eje que hace surgir derechos de carácter instrumental como el derecho a la protección de datos y, para su aplicación, el derecho al olvido digital.

Finalmente, la Corte Constitucional ecuatoriana, recoge en la sentencia 048-13-SEP-CC del 31 de julio de 2013, correspondiente al caso 0169-12-EP, sus criterios sobre el derecho a la dignidad:

“La Constitución de la República, desde su preámbulo, así como en los artículos 11 numeral 7; 22, 30, 393 etc., reconoce al ser humano como sujeto y fin, lo cual es esencial de la dignidad. Por tanto, la dignidad es, en primer lugar, un valor absoluto que ha de ser tenido siempre como fin. Una ofensa contra la dignidad personal ofende a toda persona y a todo ser humano. En palabras de Larrea Holguín, "después de la vida, la integridad y la dignidad de la persona son los derechos que más directamente derivan de la naturaleza misma y deben ser garantizados en forma amplia y plena" (Oswaldo Yépez contra Elías Barberán, Caso 0169-12-EP, 2013, p. 9)

En ese sentido, reconoce a la dignidad como un valor absoluto, sumado a lo establecido en la Constitución donde se lo consagra como principio, y señala su necesidad de garantía.

Más adelante, la ponencia continúa señalando que: "La dignidad de la persona, limita el derecho a la libertad de expresión reconociendo los denominados derechos de la personalidad: el derecho al honor, a la intimidad y a la propia imagen. (Oswaldo Yépez contra Elías Barberán, Caso 0169-12-EP, 2013, p. 10). Todos esos citados derechos instrumentalizan su protección a través del derecho a la protección de datos personales, que los cobija.

El derecho a la protección de datos personales busca impedir el mal uso o tratamiento de estos, conducta que actuaría de forma contraria a la dignidad de las personas.

La Constitución contiene valores, principios y derechos y como ya se ha mencionado, consagra la protección de la dignidad de las personas, a la cual le ha otorgado categoría de valor absoluto con capacidad de ser fundamento para otros derechos.

Esta misma dignidad mantiene una relación estrecha o intrínseca con los derechos de la personalidad (honor, intimidad y protección de datos personales) recogidos en el artículo 66 de la Constitución de la República del Ecuador, y el poder recordar hechos pasados podría suponer un riesgo de

afectaciones a estos derechos. Estos derechos han sido incorporados dentro del grupo de derechos de libertad, al pretender proteger a los individuos de las acciones de terceros.

Es así que, el numeral 7 del artículo 11 de la Constitución de la República del Ecuador reconoce la figura doctrinaria de “cláusula abierta”, la cual supera el sentido formal de la Constitución, y permite que aquellos derechos no reconocidos en ella ni en instrumento internacional alguno puedan ser justiciables, abriendo el campo para mejorar la situación de la protección de la dignidad humana.

Ramiro Ávila Santamaría reconoce la necesidad de la cláusula abierta: “¿Pueden existir necesidades de reconocimiento de derechos, que el ser humano de ahora no puede visualizar con las amenazas de la técnica? De ahí la necesidad de una cláusula abierta en beneficio de los seres humanos y como herramienta de protección contra los males o amenazas no identificadas.” (Ávila Santamaría, 2012, p. 87)

Podemos concluir, en este punto, que el derecho al olvido digital se podría convertir en un derecho de libertad, que busca proteger los datos personales de los individuos, controlando la situación y estableciendo los límites a fin de que los buscadores eliminen los datos de las personas para que estos que no sean de fácil acceso y difusión, pero su razón de existir se encuentra en la necesidad de mejorar las condiciones de protección de la dignidad humana.

- Progresividad de los derechos aplicada para el reconocimiento del derecho al olvido digital

Desde la promulgación de la Declaración Universal de Derechos Humanos, los derechos han estado en una constante evolución. Sus preceptos que se refieren a cada uno de los diferentes derechos han ido evolucionando ya sea a través de tratados o convenciones, que han ampliado el ámbito del derecho, y de las garantías de los mismos.

Existe, de forma apreciable, una tendencia manifiesta a acrecentar los niveles de protección de los derechos humanos.

“El principio de progresividad lleva a aplicar siempre la disposición más favorable a los derechos de las personas, por lo que siempre debe aplicarse aquel instrumento que en mejor forma garantice el derecho, no importando si la mayor garantía se encuentra en la norma interna del Estado o en la norma de derecho internacional de los derechos humanos incorporada al derecho interno, lo que lleva a una interpretación *Pro-Cives* o *Favor Libertatis*, o sea, a la interpretación que mejor favorezca y garantice los derechos humanos” (Nogueira Alcalá, 2003, p. 71).

El Ecuador, como Estado constitucional de derechos y justicia, tal como se establece en la Constitución de la República en el artículo 1, está destinado a garantizar la protección y vigencia de los derechos humanos, conforme a principios de orden constitucional como el de progresividad.

“El reconocimiento de los Derechos Humanos es progresivo, lo que significa una restricción para la función legislativa de los distintos Estados (así como también de cualquier otra instancia competente para la expedición de normas imperativas que no necesariamente tienen forma de ley), en cuanto a disminuir o eliminar el reconocimiento de derechos, pues el contenido de las normas” (Mancilla, 2015, p. 83).

Este principio, tiene su base normativa en el derecho internacional de derechos humanos que contempla la obligación de todos los Estados de lograr el desarrollo progresivo de los derechos constitucionales de cada uno de ellos. (Mark Evan Hester contra Angélica López Valero, 2015, p. 17).

“La Asamblea General: Proclama la presente Declaración Universal de Derechos Humanos como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos, tanto entre los pueblos de los Estados Miembros como entre los de los territorios colocados bajo su jurisdicción” (Declaración Universal de Derechos Humanos, 1948, Preámbulo)

Esta obligación, vigente desde 1948, se recoge en la Constitución ecuatoriana en el numeral 8 de su artículo 11.

“El ejercicio de los derechos se regirá por los siguientes principios: 8. El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio. Será inconstitucional cualquier acción u

omisión de carácter regresivo que disminuya, menoscabe o anule injustificadamente el ejercicio de los derechos” (Constitución de la República del Ecuador, 2008, Art. 11 Numeral 8)

Esta progresividad de los derechos busca mejorar la situación de los derechos reconocidos en la Constitución, llevándolos a la mejor aplicación posible para las personas, pero así mismo, restringe cualquier posibilidad de reducir su alcance o su aplicación, y la Corte Constitucional lo reconoce de tal forma en la sentencia 008-13-SIN-CC del 13 de junio de 2015, correspondiente al caso 0029-11-IN:

“(…) se debe considerar que la progresividad de los derechos supone, en concreto, que el Estado no puede implementar medidas que tengan como finalidad o como efecto, la disminución del nivel de reconocimiento y cumplimiento de los derechos contenidos en la Constitución y en los Instrumentos de Derechos Humanos. Este principio constitucional conlleva la responsabilidad del Estado de velar por el respeto y la garantía de los derechos constitucionales, los cuales deben ser garantizados a favor de todas las personas. Así, según el principio de progresividad, los derechos constitucionales tienen tal importancia que una vez que han sido establecidos o consagrados en la Constitución o los Instrumentos Internacionales, no podrán ser disminuidos, desmejorados ni eliminados” (Jaime Velasco (Acción Pública de inconstitucionalidad), Caso 0029-11-IN, 2013, p. 12).

Ya antes se había mencionado como el derecho a la dignidad es la columna vertebral del catálogo de derechos, es entendible entonces que el principio de progresividad de los derechos busque la protección de la dignidad humana a través de dos formas, la primera aceptando las posibles mejoras y la incorporación de nuevos derechos; finalmente, al impedir que los derechos existentes y reconocidos sean desmejorados, eliminados o disminuidos, a esto se lo conoce como principio de no regresividad.

El complemento más importante del principio de progresividad es la prohibición “de regresividad que proscribe desandar lo avanzado en las condiciones establecidas para el goce efectivo de los derechos.” (Ávila Santamaría, 2012, p. 90)

Ferrajoli señala que “la validez de una norma no solo dependerá de los procedimientos para su creación, sino de la observancia y correspondencia de

sus contenidos y la armonía que guarde con los valores, principios y reglas manifestados en la Constitución” (Ferrajoli, 2001, pp. 261-262).

Esto quiere decir que se rompe el sentido formal por el cual eran dimensionadas, sino que se empieza a considerar su sentido material, pero amén de lo antes expresado, se debe entender que una Constitución se compone de la coexistencia de valores y principios que rigen y definen el marco general para los derechos y demás normas.

“Si bien la Constitución es suprema como resultado primigenio de la voluntad ciudadana, dicha supremacía no puede violentar o transgredir el contenido esencial de los derechos fundamentales de su propio titular, reconociendo su dignidad como un elemento superior y anterior al Estado” (Kant, 2009, p. 10).

Entonces, la definición podría ser, parafraseando a Bidart Campos, disposiciones, principios y valores que son materialmente constitucionales, pero que se encuentran fuera del texto documental de la Constitución, pero cuya finalidad es servir de parámetro para el control de constitucionalidad de normas inferiores. (Bidart Campos, 2001)

Todos estos elementos permiten incorporar mejoras en el catálogo de derechos, dado el caso de implementar nuevas figuras jurídicas como es el caso del derecho al olvido digital, que buscan, esencialmente, proteger la dignidad humana.

Debido a la constante evolución y desarrollo de la tecnología, sería plausible el efecto de progresividad del derecho, y más cuando la sociedad se encuentra plagada de elementos y situaciones que pueden causar un perjuicio a la dignidad de las personas.

3.6. Aplicación del derecho al olvido digital en el Ecuador.

A lo largo de este tercer capítulo se ha procedido a analizar, dentro del ordenamiento jurídico ecuatoriano, los elementos existentes y no existentes para la aplicación del derecho al olvido digital, y sobre estos últimos, la forma

de superar los vacíos y permitir solventar la necesidad de protección de la dignidad de las personas frente a una situación no contemplada.

Es así que este último acápite se dedicará a presentar la forma de articulación de todos los elementos y soluciones jurídicas identificadas para la inclusión del derecho al olvido digital dentro del catálogo material de derechos fundamentales ecuatoriano.

En el Ecuador se cuenta con el reconocimiento del derecho a la protección de datos personales, consagrado en el numeral 19 del Artículo 66, que incorpora en su texto la facultad de autodeterminación informativa para el titular de los datos y los principio de aplicación de la protección de datos personales.

Se cuenta con un titular activo, que es una persona natural, y con un titular pasivo que es el gestor del motor de búsqueda.

La Constitución de la República del Ecuador consagra los derechos a las libertades de expresión e información, tal como consta en sus artículos 18, 66, numeral 6 y artículo 384. La primera se encuentra reforzada por lo establecido en el artículo 17 de la Ley Orgánica de Comunicación, mientras que el segundo se fortalece por lo establecido en el artículo 22 del mismo cuerpo normativo.

El marco constitucional recoge en el artículo 92, referente al *Habeas Data*, los llamados Derechos ARCO, donde se establecen las acciones de acceso, actualización, rectificación, eliminación y anulación de datos personales.

Por lo antes expuesto, se puede señalar que el ordenamiento jurídico ecuatoriano ya reconoce varios de los elementos esenciales para la aplicación del derecho al olvido digital, sin embargo existen dos elementos que no son considerados, que se refieren a contar con una acción de derecho al olvido digital, que supera a los derechos ARCO, con la cual se puede requerir a un gestor de búsqueda la eliminación de los registros de páginas *Web* que contengan datos personales de una persona, a pesar de que estos se han considerados información verdadera y lícita, en virtud de que causen un perjuicio o se hayan vuelto irrelevantes por el paso del tiempo.

Todo este conjunto de elementos se encuentran en la sentencia del Tribunal de Justicia de la Unión Europea sobre el caso Costeja y AEPD vs Google INC y Google Spain SL, que reconoce la existencia del derecho al olvido digital y establece las condiciones para su aplicación.

El marco constitucional ecuatoriano establece los elementos para la aplicación de los criterios contenidos en dicha sentencia.

En primer lugar, el artículo 11, numeral 7 de la Constitución ecuatoriana estipula que, en lo referente a la dignidad humana, se reconoce la cláusula abierta, misma que permite que aquellos derechos no reconocidos en ella, ni en instrumento internacional alguno, puedan ser justiciables.

Esto supera el sentido formal de la constitución y abre campo a la aplicación de nuevos derechos con la finalidad de mejorar las condiciones de protección de la dignidad humana.

Luego, el principio de progresividad de los derechos, establecido en el numeral 8 del artículo 11 de la Constitución, reconoce el desarrollo progresivo de los derechos a través de instrumentos como la normativa y la jurisprudencia. Este desarrollo progresivo implica la posibilidad de incorporar mejoras en el catálogo de derechos.

Al tener la caracterización del derecho al olvido digital, propuesta y establecida por el Tribunal de Justicia de la Unión Europea, y haciendo uso de los elementos existentes en el marco constitucional ecuatoriano, se abre la puerta a un nuevo camino para la protección de las personas, cuando su dignidad está en juego.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Actualmente, las nuevas tecnologías han propiciado un cambio en el paradigma de la memoria, dado que ahora la información permanece en la red, por un tiempo indefinido, facilitando su acceso de manera mucho más ágil, sin restricciones ni control de clase alguna, a través de herramientas como buscadores. De igual forma se ha cambiado la relación de interacción de los usuarios en la *Web*, al haber pasado del rol de consulta a uno más participativo y dinámico, donde se han vuelto consumidores y proveedores de información. Los buscadores son las herramientas de uso generalizado por los internautas para navegar a través de la *Web*, realizando un proceso de indexado de las páginas *Web* y de la información que estas contienen, lo cual facilita enormemente su acceso y difusión.

Se generan nuevos riesgos para las personas por el hecho de que esta información se eternice en la *Web* y su acceso sea indiscriminado, teniendo como consecuencia la posibilidad de causar perjuicios a las personas sobre quien verse dicha información, incluso si esta es verdadera, constituyéndose en memoria histórica, pero que a pesar de eso, por el devenir del tiempo, ya ha perdido relevancia.

Estos riesgos amenazan a la dignidad de las personas, afectando sus derechos de libertad y de personalidad, su protección de datos personales, su honor, su intimidad, su proyecto de vida, solo por el mero hecho de que esta información se encuentre disponible en cualquier momento y por cualquier persona.

El derecho a la protección de datos personales se encuentra reconocido, derivándose este de la necesidad de proteger la dignidad humana y si bien el derecho a la protección de datos personales tiene su origen primigenio en el derecho a la intimidad, ha superado a este en alcance evolucionando hasta ser independiente autónomo, cobijando tras de sí a todo el conjunto de datos de las personas, incluso si este se percibe inocuo, ya que en conjunto, estos permiten identificar o vuelven identificable a la persona.

La autodeterminación informativa surge como herramienta elemental y natural para la protección de los datos personales, y por ende de la dignidad humana, al permitir a las personas definir los límites para el almacenamiento, publicación y tratamiento de sus datos personales. Para este fin, la autodeterminación informativa encuentra en el derecho al olvido digital la instrumentalización necesaria para llevar a cabo el control pleno de sus datos personales, siendo así que a pesar de existir los llamados derechos ARCO (acceso, rectificación, cancelación y oposición), el derecho al olvido digital permite al titular de los datos detener la facilidad con la que estos son accedidos y difundidos a través de los buscadores.

El derecho al olvido digital busca satisfacer la necesidad de proteger la dignidad de las personas, al permitirles requerir a los buscadores de internet la eliminación de sus datos de sus índices. Su existencia surge como resultado de una pretensión, por demás urgente, de la sociedad a la necesidad de establecer límites para privados y públicos. Esta pretensión del titular de los datos supera los intereses económicos que pudiera tener el gestor de búsqueda, siendo obligación de este último el cumplir con la eliminación de los datos del interesado.

Se determina que los titulares de datos pueden interponer requerimientos de eliminación del indexado de su información en los buscadores, pretendiendo que se detener el acceso que los usuarios de la internet puedan tener a su información, sin considerar que esta información es verdadera o falsa, pero que causa un perjuicio a la persona. Si la información es verdadera, convirtiéndose en memoria histórica, pero por el paso del tiempo, ha perdido relevancia, de igual forma es aplicable el requerimiento de eliminación de la información de los índices de los buscadores

En relación a la aplicación en relación del territorio, se ha determinado posible la interposición del requerimiento de eliminación del indexado de los buscadores en el país de domicilio del titular de los datos, cuando se cuente con una dependencia encargada de la actividad comercial del mismo en el territorio donde resida el requirente toda vez que su actividad y la del gestor de

búsqueda se encuentran estrechamente relacionada al considerar que las actividades comerciales de la primera sostienen la operación del gestor de búsqueda

Se pueden presentar situaciones en los cuales se pueda apreciar un conflicto entre la pretensión del titular de los datos y el interés de los internautas, apreciable en un conflicto de derechos a nivel fundamental, pero para este tipo de situaciones se encuentra solución en la ponderación de derechos. Los conflictos más usuales que se presentan son entre el interés público, la libertad de expresión y la libertad de información, donde en la mayoría de los casos debe prevalecer el derecho al olvido digital, sin embargo, existen situaciones donde pueden prevalecer los otros derechos señalados, por ejemplo en el caso de la memoria histórica de interés público, y he ahí la razón para determinar que la aplicación del derecho al olvido digital debe ser analizada individualmente en cada caso.

Con la caracterización del derecho al olvido digital, utilizando la sentencia del Tribunal de Justicia de la Unión Europea en el asunto asunto C-131/12, Costeja y AEPD vs Google INC y Google Spain SL, se ha podido identificar que la Constitución de la República del Ecuador cuenta con las bases necesarias para aplicar el derecho al olvido digital, siendo así que ya reconoce varios elementos necesario, como el derecho fundamental a la protección de datos personales que conlleva la autodeterminación informativa.

De igual forma, se determina que a misma Constitución establece los mecanismos para la aplicación de aquellos elementos no considerados en el ordenamiento jurídico nacional, al incorporar la “cláusula abierta” dentro del ámbito de la dignidad humana, permitiendo que sean justiciables aquellos derechos que no se hayan recogido dentro del texto formal constitucional o en instrumentos internacionales, esto se suma al principio de progresividad del derecho establecido en la misma Constitución para la mejora de los derechos.

4.2. RECOMENDACIONES

En primer lugar es recomendable el desarrollo y promulgación de una norma de protección de datos personales que incorpore los principios rectores de la materia y establezca el derecho al olvido digital, con las consideraciones pertinentes respecto de la titularidad, la aplicación en razón del territorio, la autoridad competente para su presentación y el procedimiento a seguir.

En concordancia con la recomendación anterior, sería materia de análisis la creación de una entidad administrativa que vele por el cumplimiento de la norma antes señalada y establezca las directrices a seguir, para entidades públicas y privadas, sobre cómo deben proceder en materia de protección de datos personales, así como promover acciones para dicha protección

Luego, como materia de análisis para futuros trabajos de titulación, se recomienda estudiar a profundidad la posibilidad de que las personas jurídicas también puedan tener acceso a la aplicación del derecho al olvido digital, en razón de contar con acceso a ciertos derechos que se pueden ver vulnerados al igual que con las personas naturales.

Asimismo, las escuelas de derecho y el Consejo de la Judicatura, debería establecer capacitaciones específicas en materia de protección de datos personales y las nuevas situaciones que se presentan frente a las nuevas tecnologías de la información y comunicación. Incorporando, las primeras, en su pensum, la materia de derecho de nuevas tecnologías, y el segundo, con un plan de capacitación para los operadores de justicia.

REFERENCIAS

- Abogado General de la Unión Europea, (2013). Conclusiones Generales del Asunto C-131/12 del caso Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González del 25 de junio de 2013. Recuperado el 19 de mayo de 2015 de <http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES>
- Arzt Colunga, S. (2013). México, el derecho al olvido en internet: ejercicio de los derechos de cancelación y oposición, derecho al olvido versus derecho a la libertad de información, su incidencia en los medios de comunicación. *XI Encuentro Iberoamericano de Protección de Datos* (p. 18). Cartagena: IFAI.
- Asimov, I. (1983). *Los Límites de la Fundación*. Recuperado el 20 de Octubre de 2016, de La Prensa de la Zona Oeste: <http://laprensadelazonaoeste.com/LIBROS/Letra.A/A/Asimov,%20Isaac%20-%20Saga%20de%20la%20Fundacion%204%20-%20Los%20Limites%20de%20la%20Fundacion.pdf>
- Audiencia Nacional, (2012). *Auto de la sala Contencioso Administrativa de la Audiencia Nacional 19/2012 del 27 Febrero 2012*. Recuperado el 13 de abril de 2015 de <http://www.informatica-juridica.com/anexos/auto-de-la-audiencia-nacional-19-2012-27-febrero-2012/>
- Ávila Santamaría, R. (2012). *Los derechos y sus garantías. Ensayos Críticos*. Quito: Centro de Estudios y Difusión del Derecho Constitucional.
- BBC Mundo. (2016). *Tiziana Cantone: el caso de la joven que se suicidó tras la difusión de un video sexual suyo que conmociona a Italia Mundo*. Recuperado el 15 de septiembre de 2016 de http://www.bbc.com/mundo/noticias-internacional-37380350?ocid=socialflow_twitter
- Becerra, A. (2016). *Diario UChile Advierten que proyecto de rextificación de datos en internet afecta acceso a la información*. Recuperado el 22 de febrero de 2016 de <http://radio.uchile.cl/2016/02/22/advierten-que-proyecto-de-rectificacion-de-datos-en-internet-afecta-acceso-a-la-informacion>
- Bergel, S. (1988). Informática y responsabilidad civil. *Revista de Informática y Derecho Aportes de Doctrina Internacional*, 164.

- Bidart Campos, G. (1994). La Interpretación de los derechos humanos. *Lecturas Constitucionales Andinas*(3), 34. Lima: Comisión Andina de Juristas.
- Bidart Campos, G. (2001). El derecho de la Constitución y su fuerza normativa. En A. Gil Domínguez, *El Bloque de la Constitucionalidad Federal y los informes de la Comisión Interamericana de Derechos Humanos* (pág. 58). Buenos Aires: Ediar.
- Cabanellas, G. (1993). *Diccionario Jurídico Elemental*. Buenos Aires: Heliasta .
- Britton, I. (2011). *Divulgación y Cultura Científica Iberoamericana*. Recuperado el 7 de enero de 2016, de http://www.oei.es/divulgacioncientifica/noticias_657.htm
- Caicedo, D. (2009). El bloque de constitucionalidad en el Ecuador. Derechos Humanos más allá de la Constitución. *FORO*(12).
- Castellano, P. (2012). *El régimen constitucional del derecho al olvido digital*. Valencia: Tiranto Lo Blanch.
- CCM Benchmark Group. (2015). *CCM*. Recuperado el 30 de noviembre de 2015 de <http://es.ccm.net/contents/830-web-motor-de-busqueda>
- Celorio, M. (11 de enero de 2012). *Revista mexicana de comunicación*. Recuperado el 7 de enero de 2016, de <http://mexicanadecomunicacion.com.mx/rmc/2012/01/11/internet-plataforma-ambivalente-para-la-memoria-de-la-humanidad/>
- Código Orgánico Integral Penal. (2014). Quito: Registro Oficial Suplemento 180.
- Computerhoy. (2013). Computer hoy.com Primeras pruebas en humanos de implantes de memoria digitales. Recuperado el 12 de Enero de 2016, de <http://computerhoy.com/noticias/life/primeras-pruebas-humanos-implantes-memoria-digitales-36949>
- Computerhoy. (2015). Recuperado el 12 de enero de 2016, de <http://computerhoy.com/noticias/life/primeras-pruebas-humanos-implantes-memoria-digitales-36949>
- Constitución de la República del Ecuador. (2008). Montecristi: Registro Oficial 449.

- Córdoba González, S. (2005). *Boletín Girasol*. Recuperado el 8 de julio de 2016 de <http://www.vinv.ucr.ac.cr/girasol-ediciones/archivo/girasol26/indexada.htm>
- Corte Constitucional del Ecuador, (2013). *Sentencia 048-13-SEP-CC del caso Oswaldo Yépez contra Elías Barberán*. Recuperado del 17 de octubre de 2015 de <https://www.corteconstitucional.gob.ec/sentencias/relatoria/relatoria/fichas/048-13-SEP-CC.pdf>
- Corte Constitucional del Ecuador, (2015). *Sentencia 064-15-SEP-CC del caso Mark Evan Hester contra Angélica López Valero*. Recuperado el 17 de octubre de 2015 de <https://www.corteconstitucional.gob.ec/sentencias/relatoria/relatoria/fichas/064-15-SEP-CC.pdf>
- Corte Constitucional del Ecuador, (2013). *Sentencia 008-13-SIN-CC de la Acción Pública de Inconstitucionalidad propuesta por Jaime Velasco*. Recuperado el 18 de octubre de 2015 de <https://vlex.ec/vid/inconstitucionalidad-abg-ramiro-freire-451965138>
- Davara, M. (2008). La protección de datos y las comunicaciones electrónicas. En E. Ferrer Mac-Gregor, & A. Zaldívar Lelo de Larrea, *La ciencia del derecho procesal constitucional. Estudios en homenaje a Héctor Fix-Zamudio en sus cincuenta años como investigador del derecho* (Vol. 7). Mexico: UNAM.
- Davara, M. (2008). *Manual de Derecho Informático (10ma Ed.)*. Navarra, España: Arazandi.
- De Terwangne, C. (2012). Privacidad en Internet y derecho a ser olvidado/Derecho al Olvido. *Revista de Internet, Derecho y Política*, pp. 53 - 66.
- Asamblea General de las Naciones Unidas (1948). Resolución 217 (III) sobre la Declaración Universal de Derechos Humanos del 10 de diciembre de 1948. de la Asamblea General de las Naciones Unidas. Recuperado el 21 de enero de 2015 de http://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf
- Definicion. DE. (2016). *Definicion. DE*. Recuperado el 7 de enero de 2016, de <http://definicion.de/web-2-0/>
- Díaz, P. (2010). *Revista Digital Sociedad de la Información*. Obtenido de <http://www.sociedadelainformacion.com/19/memoriahistorica.pdf>

- Digitales, R. e. (2016). *Ganamos! Tribunal anula resolución del INAI sobre el falso «derecho al olvido»*, *Red en Defensa de los Derechos Digitales*. Recuperado el 24 de Agosto de 2016 de <http://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/>
- Dirección Nacional de Registro de Datos Públicos. (2013). *Dato Seguro*. Recuperado el 6 de enero de 2016, de <https://www.datoseguro.gob.ec/web/guest/datos-del-ciudadano>
- El Universal. (2016). *#LadyCoralina: se besa con otro y le cancelan boda, Estados*. Recuperado el 22 de septiembre de 2016 de <http://www.eluniversal.com.mx/articulo/estados/2016/09/22/ladycoralina-se-besa-con-otro-y-le-cancelan-boda>
- Fernández Segado, F. (1994). *La dogmática de los derechos humanos*,. Lima: Ediciones Jurídicas.
- Ferrajoli, L. (2001). La democracia constitucional. En C. Courtis, *Desde otra mirada* (pp. 261-262). Buenos Aires: Eudeba.
- García, J. (2014). El derecho al olvido en la red. *Revista Aranzadi de Derecho y Nuevas Tecnologías*(36).
- Gómez, R. (2011). *Quiero que Internet se olvide de mí*. Recuperado el 15 de julio de 2016 de El País: http://elpais.com/diario/2011/01/07/sociedad/1294354801_850215.html
- Gregorio, C., & Ornelas, L. (2011). *Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes. Memorandum de Montevideo*. Ciudad de México: Instituto Federal de Acceso a la Información y Protección de Datos - Instituto de Investigación para la Justicia.
- Grupo de Trabajo 29 sobre Protección de Datos. (2010). *Dictamen 8/2010 sobre aplicabilidad de la ley*. Bruselas. Recuperado el 17 de agosto de 2015 de ec.europa.eu/justice/data-protection/article-29/documentation/.../wp216_es.pdf
- Häberle, P. (2005). A dignidade humana como fundamento da comunidade estatal. En W. Sarlet, *Dimensoes da Dignidade* (p. 104). Porto Alegre: Livraria Do Advogado.
- Hernández, M. (2013). *El Derecho al olvido digital en la WEB 2.0*. Salamanca: Universidad de Salamanca.

- Hernández, M. (2013). El derecho al olvido en internet como nuevo derecho fundamental en la sociedad de la información. Perspectiva constitucional española y europea. En *Quid Iuris* (Vol. 21).
- Higareda, L. (2014). El derecho a la protección de datos personales y la configuración del derecho al olvido. En Y. Amoroso, *Género, Código y Juventud: construir sociedades más justas e inclusivas* (pp. 102-113). La Habana: Unión Nacional de Juristas de Cuba.
- Idrovo Mosquera, S. V. (2011). *La protección de datos de carácter personal en el Ecuador*. Cuenca: Universidad del Pacífico. Recuperado el 6 de mayo de 2015 de <http://repositorio.upacifico.edu.ec/bitstream/40000/65/1/TDC-UPAC-19041.pdf>
- Instituto Federal de Acceso a la información, (2015). *Resolución PPD.0094/14 del caso Google México, S. de R.L. de C.V, del 26 de Enero de 2015*. Recuperado el 12 de febrero de 2015 de https://sontusdatos.org/wp.../ina_resolución-ppd0094-14_google-méxico_parte1.pdf
- Instituto Federal de Acceso a la Información. (2015). *En un hecho sin precedente, el ifai inició un procedimiento de imposición de sanciones en contra de google México. IFAI-OA/009/15*, págs. 1-2. Recuperado el 23 de octubre de 2015 de <http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-009-15.pdf>
- Juzgado Distrital de Utah, (1998). Decision Case 2:97-CV-0536-S.Patriot Sys Inc. v. C-Cubed Corp del 25 Septiembre de 19981. Recuperado el 18 de diciembre de 2015 de http://www.leagle.com/decision/1998133921FSupp2d1318_11186/PATRIOT%20SYSTEMS,%20INC.%20v.%20C-CUBED%20CORP.
- Kant, I. (2009). The doctrine of virtue. En D. Caicedo, *El bloque de constitucionalidad en el Ecuador. Derechos Humanos más allá de la Constitución*. Quito: UASB.
- Leturia, F. (2016). Fundamentos jurídicos del derecho al olvido. ¿Un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos derechos fundamentales? *Revista Chilena de Derecho*, 43(1).
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos. (2002). Quito: Registro Oficial Suplemento 557.

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (2010). *Diario Oficial de la Federación*. Ciudad de México, México: Diario Oficial de la Federación.
- Ley Orgánica de Comunicación. (2013). Quito: Registro Oficial Suplemento 22.
- Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. (2009). Quito: Registro Oficial Suplemento 52.
- López Portas, M. (2015). La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE. En UNED, *Revista de Derecho Político*. UNED.
- Lucas, P. (2008). El derecho a la autodeterminación informativa y la protección de datos personales. En E. Ikaskuntza, *Cuadernos de Derecho Nro. 20*. Donostia: Eusko Ikaskuntza.
- Madrid Conesa, F. (1984). *Derecho a la Intimidad Informática y Estado de Derecho*. Valencia: Universidad de Valencia.
- Mancilla, R. (2015). El principio de progresividad en el ordenamiento constitucional mexicano. *Cuestiones Cosntitucionales*(33).
- Martínez, R. (2014). Aplicar el derecho al olvido. *Revista Aranzadi de Derecho y Nuevas Tecnologías*(36).
- Mate, L. (2016). ¿Qué es realmente el derecho al olvido? *Revista de Derecho Civil*, pp. 187-222.
- Mazzola, M. (2016). *IlFattoQuotidiano.it*. Tiziana Cantone, perché è stata condannata a pagare le spese legali. Recuperado el 16 de septiembre de 2016 de <http://www.ilfattoquotidiano.it/2016/09/16/tiziana-cantone-perche-e-stata-condannata-a-pagare-le-spesse-legali/3036999/>
- McNeally, S. (2007). Frase pronunciada durante la IAPP Privacy Summit. Washington.
- Minero, G. (2014). A vueltas con el “derecho al olvido”. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital. *RJUAM*.
- Moles, R. (2015). *Olvido Digital y Memoria Histórica La Vanguardia* . Recuperado el 11 de diciembre de 2015 de <http://www.lavanguardia.com/opinion/20151211/30724904343/olvido-digital-y-memoria-historica.html>

- Moore, A., & Lloyd, D. (1989). *Vox Populi. V de Vendetta, 8 de 10(8)*. España: Zinco.
- Muñoz, F. (2015). *Web 2.0*. Recuperado el 7 de enero de 2016, de <http://salseoblog.blogspot.com/>
- Nogueira Alcalá, H. (2003). *Teoría y Dogmática de los Derechos Fundamentales. Serie Doctrina Jurídica(156), Primera*. (R. Márquez Romero, Ed.) México: UNAM.
- Nogueira Alcalá, H. (s.f.). *Dignidad de la persona, derechos fundamentales, bloque constitucional de derechos y control de convencionalidad Centro di Ricerca sui Sistemi Costituzionali Comparati*. Recuperado el 16 de Octubre de 2016, de <http://www.crdc.unige.it/docs/articles/Dignidad.pdf>
- Novoa, E. (2015). *El Derecho a la protección de datos de caracter personal ecuatoriano analizado a partir de las relaciones B2C*. Recuperado el 13 de diciembre de 2015 de <file:///F:/CLIENTES%20CAAP%20SORILY%20FIGUERA%20VARGAS/Cliente%20Christian%20Espinosa/UDLA-EC-TAB-2015-62.pdf>
- Ordóñez Solís, D. (2014). *El derecho al olvido en internet y la sentencia Google Spain*. Aranzadi Unión Europea(6).
- Organización de Estados Americanos. (2011). *Relatoría Especial para la Libertad de Expresión*. Recuperado el 12 de diciembre de 2015 de <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849>
- Palacios González, M. (2013). *Observatorio Iberoamericano de protección de Datos*. Recuperado el 13 de Febrero de 2016, de <http://oiprodat.com/2013/04/24/la-accion-del-habeas-data-en-el-derecho-ecuatoriano/>
- Parlamento, Consejo y Comisión Europea, (2000). *Carta de Derechos Fundamentales de la Unión Europea, 2000/C 364/01*. Recuperada el 15 de mayo de 2015 de <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3AI33501>
- Parlamento Europeo, (1995). *Directiva 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, 95/46/CE*. Recuperado el 2 de Julio de 2016, de <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046>
- Piñar Maña, J. L. (2009). *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio*. Fundación Alternativas.

- Posicionamiento web. (2013). *Posicionamiento web*. Recuperado el 14 de junio de 2015 de <http://www.posicionamientoswebs.org/que-es-un-buscador-o-motor-de-busqueda>
- Puente de la Mora, X. (2007). *La Sociedad de la Información y la Necesidad de Protección de Datos Personales en la Gestión Pública Estatal*. *Revista de Derecho Informático*(105). Recuperado el 12 de Noviembre de 2016, de http://www.alfa-redi.com//apc-aa-alfaredi/img_uplo
- Real Academia de la Lengua Española. (s.f.). *Diccionario de la Lengua Española*. Recuperado el 10 de septiembre de 2016 de <http://dle.rae.es/?id=RBfDug8>
- Real Academia de la Lengua Española. (s.f.). *Diccionario de la Lengua Española*. Recuperado el 29 de Septiembre de 2016, de Decidir: <http://dle.rae.es/?id=BwLsxjt>
- Revista Fortuna vs INAI, 74/2012 (Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región 7 de Julio de 2016).
- Rodríguez Palchevich, D. (2008). *Nuevas Tecnologías WEB 2.0: Hacia una real democratización de la información y el conocimiento*.
- Rosas, I. (2014). *El derecho al olvido pone en riesgo a la libertad de expresión*. Recuperado el 15 de mayo de 2014 de <https://www.fayerwayer.com/2014/05/el-derecho-al-olvido-pone-en-riesgo-a-la-libertad-de-expresion/>
- Rubio, F. (2016). *Euronews La Justicia Italiana Investiga el Suicidio de una Joven Italiana que Protagonizó Videos Sexuales*. Recuperado el 14 de septiembre de 2016 de La justicia italiana investiga el suicidio de una joven italiana que protagonizó vídeos sexuales: <http://es.euronews.com/2016/09/14/la-justicia-italiana-investiga-el-suicidio-de-una-joven-italiana-que>
- Ruiz Miguel, C. (1994). En Torno a la Protección de los Datos Personales Automatizados. *Revista de Estudios Políticos (Nueva Época)*(84)..
- Secretaría de Protección de Datos Personales. (2014). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Ciudad de México: Instituto Federal de Acceso a la Información y Protección de Datos.
- Serrano, M. (2003). *El derecho fundamental a la protección de datos. Derecho español y comparado*. Madrid: Arazandi, p. 380.

- Silva, M. (2014). *El Derecho al Olvido*. Cáceres: Universidad de Extremadura.
- Smith, Graham J. H. (2007). *Internet Law and Regulation*. Lóndres: Sweet & Maxwell, p. 342.
- Solove, D. (2004). *The Digital Person. Technology and Privacy in the Information Age*. New York, EE.UU.: New York University Press.
- Touriño, A. (2014). *El derecho al olvido y a la intimidad en internet*. Madrid: Catarata.
- Tribunal Constitucional del Ecuador, (2008). *Sentencia de la Sala Primera sobre el Caso 0049-2008-HD*. Registro Oficial, Edición Especial No. 85.
- Tribunal constitucional del Ecuador, (2009). *Sentencia de la Sala Tercera sobre el Caso 0065-2008-HD*. Registro Oficial, Edición Especial No. 100.
- Tribunal de grande instance de Paris. (16 de Septiembre de 2014). *Legalis*. Recuperado el 2 de julio de 2016, de M. et Mme X et M. Y / Google France: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291
- Tribunal de Justicia de la Unión Europea, (2014). *Sentencia del Tribunal de Justicia (Gran Sala) del caso Costeja y AEPD vs Google INC y Google Spain SL., C-131/12 del 13 de mayo de 2014*. Recuperado el 14 de septiembre de 2016 de <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=229183>
- Tribunal Supremo de España, (2016). *Sentencia sobre caso RJ\2016\1525 Costeja y AEPD vs Google INC y Google Spain SL., RJ\2016\1525 del 14 de Marzo de 2016*. Recuperado el 17 de marzo de 2016 de www.nreg.es/ojs/index.php/RDC/article/download/163/159
- Xalabarder Plantada, R. (2006). *La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios*. *REVISTA DE INTERNET, DERECHO Y POLÍTICA*, 7.