Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada

Derecho al Olvido: Comparación de la legislación vigente para su aplicación en España, México y Costa Rica. El papel de la tecnología como protagonista en la aplicación del Derecho al Olvido.

Proyecto de graduación para optar por el grado académico de
Maestría en Ciberseguridad

Realizado por: Ing. Jose David Ibarra Quesada

Agosto, 2017



Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada

Derecho al Olvido: Comparación de la legislación vigente para su aplicación en España, México y Costa Rica. El papel de la tecnología como protagonista en la aplicación del Derecho al Olvido.

Proyecto de graduación para optar por el grado académico de
Maestría en Ciberseguridad

Realizado por: Ing. Jose David Ibarra Quesada

Agosto, 2017

Declaratoria de derechos de autor

Ninguna parte de esta tesis puede reproducirse o transmitirse bajo ninguna forma o por ningún medio o procedimiento, sin permiso por escrito del autor.

Dedicatoria

A:

Dios, por haberme dado la salud, el entendimiento, la paciencia y la perseverancia necesaria para poder concluir esta gran etapa. Sin sus bendiciones no habría sido posible concluir con éxito.

A mis padres, porque me han dado todo lo que ha estado a su alcance. Sus consejos, valores, amor y apoyo incondicional, han sido herramientas indispensables durante el recorrido. Los amo.

A todas aquellas personas que me impulsaron y brindaron un consejo o mensaje de apoyo.

Agradecimientos

En primer lugar a Dios, por darme las fuerzas necesarias para seguir adelante y cerrar un capítulo más de mi vida. A mis padres Judith Quesada y José Ibarra, hermano Jeffrey, tía Ruth y demás familiares que me han dado su apoyo incondicional durante el proceso.

Agradezco a mis profesores, que a lo largo de la carrera nos aportaron su conocimiento. En especial agradecimiento a los profesores LLM. Juan Ignacio Zamora Montes de Oca y Luis Naranjo, quienes permitieron que tuviese interés en el desarrollo del tema seleccionado para el proyecto de graduación, además por su gran colaboración durante el proceso.

Agradezco a la Universidad Cenfotec, a su personal administrativo quienes con su trabajo silencioso hacen posible que se lleve a cabo con éxito la culminación de esta etapa. Un especial agradecimiento a mis compañeros de carrera, quiénes hicieron posible levantar el ánimo y hacer los momentos de estrés y trabajo más agradables.

A mis compañeros de trabajo, en especial al Sr. Oscar Campos por sus constantes consejos de motivación y superación, por su apoyo incondicional.

Epígrafe

“No quiero vivir en un mundo donde todo lo que digo, todo lo que hago, todo lo que hablo, toda expresión de creatividad o de amor o de amistad queda grabada”

(Edward Snowden)

Índice General

Declaratoria de derechos de autor 1
Dedicatoria 2
Agradecimientos 3
Epígrafe 4
Índice General 5
Índice de figuras 8
Abreviaturas 9
Resumen 11
Palabras clave 12
1. Capítulo I: Generalidades 13
1.1 Antecedentes 13
1.2 Justificación 15
1.3 Objetivos 16
1.3.1 Objetivo General 17
1.3.2 Objetivos Específicos 17
1.4 Alcance 17
1.5 Limitaciones 17
2. Capítulo II: Estado de la cuestión 18
2.1 Planificación 18
2.1.1 Protocolo de revisión 18
2.2 Revisión de estudios seleccionados 20
2.3 Procesamiento y análisis de datos 23
2.3.1 Comparación 24
2.3.2 Juicio experto 24
2.3.3 Investigación documental 24
3 Capítulo III: Marco Teórico 25
3.1 Datos personales 25
3.2 Derecho al olvido 25

3.3 Derecho a la cancelación y oposición de datos 26
3.4 Autodeterminación informativa 26
3.5 Blockchain 27
3.6 Deep Web 27
3.7 Data Broker 27
4 Capítulo IV: Marco Metodológico 28
4.1 Tipo de investigación 28
4.2 Fuentes consultadas 30
4.2.1 Fuentes primarias 30
4.2.2 Fuentes secundarias 31
4.3 Metodología de investigación 32
4.4 Técnica de investigación 32
4.4.1 Análisis de datos 33
5 Capítulo V: Desarrollo 34
5.1 Apartado I ¿A qué se refiere el Derecho al Olvido? - Privacidad 35
5.2 Apartado II. La tecnología como elemento protagonista en el ejercicio del Derecho 39
5.2.1 Internet como herramienta en el ejercicio del Derecho 40
5.2.2 PageRank 45
5.2.3 Estándares publicados y controles técnicos 47
5.3 Apartado III. Retos tecnológicos para el cumplimiento del Derecho al Olvido 54
5.3.1 Blockchain o cadena de bloques 54
5.3.2 Data Brokers 61
5.3.3 Deep Web – Dark Web 69
5.3.4 Hacking 74
5.4 Apartado IV. Estado actual de los países en estudio 83
5.4.1 España 83
5.4.2 México 90
5.4.3 Costa Rica 100
5.4.4 Convenio de Budapest 114

5.4.5 Cuadro resumen: 116
6 Capítulo VI: Conclusiones 118
Referencias bibliográficas 122

Índice de figuras

Imagen 1 – Metodología del proyecto. Creada por el autor 32
Imagen 2 - Pilares de la Seguridad de la Información – Gráfico creado por autor 48
Imagen 3 – Sistema de Gestión de Seguridad de la Información, fuente PricewaterhouseCoopers 51
Imagen 4 – Gráfico proceso Blockchain (Fuente: PricewaterhouseCoopers) 56
Imagen 5 – Proceso de encripción de datos (Creada por el autor).....57
Imagen 6 –Comunicación cliente y servidor Web – Creada por el autor.....65
Imagen 7 – Contenido disponible para el acceso Web - PricewaterhouseCoopers.....70
Imagen 8 – Selección de nodos Tor – Tomado del sitio Web: www.tor.org.....72
Imagen 9 – Fases de hacking – Creada por el autor 81
Imagen 10- Porcentaje afectación por malware por país – Estudio EsEtLatam 2016.....82
Imagen 11 – Infografía caso obtención de información CCSS- Fuente Diario El Financiero 2017...114

Abreviaturas

AEPD: Agencia Española de Protección de Datos.

API: *Application Programming Interface*

BID: Banco Interamericano de Desarrollo

BSI: *British Standard Institution*

CBK: *Common Body of Knowledge*

CCSS: Caja Costarricense de Seguro Social

CVE: *Common Vulnerabilities and Exposures*

DDos: *Distributed Denial of Service*

DoS: *Denial of Service*

DRAE: Diccionario de la Real Academia Española

ECDSA: *Elliptic Curve Digital Signature Algorithm*

GPS: *Global Positioning System*

GSM/GPRS: *General Packet Radio Service*

HTTP: *Hypertext Transfer Protocol*

IEC: *International Electrotechnical Commission*

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

ISC2: *Certified Information Systems Security Professional*

ISO: *International Organization for Standardization*

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

MAC: *Media Access Control*

NIST: *National Institute of Standards and Technology*

PRODHAB: Agencia de Protección de Datos de los Habitantes

PII: *Personally Identifiable Information*

SHA1: *Secure Hash Algorithm*

SUGEF: Superintendencia General de Entidades Financieras

TCP, RLP: *Transmission Control Protocol*

URL: *Uniform Resource Locator*

VPN: *Virtual Private Network*

WWWW: *World Wide Web Worm*

Resumen

Este documento fue creado con el propósito de responder a la pregunta: ¿Cuál es el estado actual de Costa Rica en temas de Derecho al Olvido en Internet, en relación con Europa y Latinoamérica? Además de efectuar una revisión a los elementos técnicos que apoyan el ejercicio del Derecho al Olvido como tal, esta interrogante se ha planteado para brindar al lector un panorama actual y poder analizar a nuestro país desde una visión comparativa en términos de la ley vigente y además, comprender cómo es posible el uso de controles tecnológicos como apoyo en el ejercicio de tal Derecho.

Como uno de los elementos principales que forman parte del proceso de obtención y tratamiento de datos, se encuentra la implementación de elementos que conforman la seguridad de la información en las organizaciones, la misma se basa en el análisis y uso de una serie de controles que se han definido para proteger los datos expuestos al mundo por medio de la Internet.

Es importante considerar que estos controles, en función de proteger al ciudadano, pueden ser implementados desde el instante en que las soluciones tecnológicas expuestas a la Internet son desarrolladas y puestas en producción, es decir, durante el ciclo de vida de su gestión, sin embargo, se debe recalcar que no toda la responsabilidad de protección recae en la tecnología, además existen mecanismos legales en los que la sociedad (desde el lugar que ocupan los ciudadanos como usuarios de la tecnología) tienen a su disposición como un control de protección más, de forma metafórica “un escudo de protección”, pero que lamentablemente es desconocida por muchos.

A pesar de los controles disponibles para la aplicación, la tecnología pone en la palestra, gracias al desarrollo y la constante innovación, una serie de retos que darán batalla a la legislación y a los mismos controles definidos, al punto de hacer casi imposible desde el punto de vista técnico, el cumplimiento de los principios que el Derecho al Olvido establece.

Algunos de los retos tecnológicos que se resisten a mantener la seguridad de la información a un nivel aceptable son tecnologías como Blockchain, Data Brokers o corredores de datos, así como los constantes ataques por parte de hackers que mediante sus acciones maliciosas dejan fuera de control la información privada que le pertenece a los usuarios.

Asociado a lo anterior, las organizaciones basan sus aportes económicos en aspectos que les produce ganancias directas como una prioridad y dejan de lado la protección de la información que manejan, sin importar a quién pertenezca ésta y cuál es el tratamiento que se le da, sin considerar las regulaciones, derechos y deberes como custodios de esta información.

Para el desarrollo de esta investigación se efectuará una revisión de la documentación vigente de los países incluidos en el alcance, además se pretende dar una punto comparativo entre países que poseen un poco más de madurez en temas de Derecho al Olvido como España y México, así como describir el papel de la tecnología, mediante la intermediación de los motores de búsqueda Web, las redes sociales. Como complemento, describir algunas medidas de control que se puede aplicar con el objetivo de proteger al ciudadano en apoyo al ejercicio del Derecho al Olvido.

Palabras clave

Derecho al Olvido, Vulnerabilidad, Privacidad, Seguridad de la información.

1. Capítulo I: Generalidades

En este capítulo se detallan elementos iniciales para el desarrollo de la investigación, los antecedentes en relación con el tema así como los objetivos y la definición del alcance.

1.1 Antecedentes

En distintos países alrededor del mundo se han presentado casos relevantes en relación al Derecho al Olvido. Tal es el caso presentado con la compañía Google en Europa.

Europa, específicamente en España, desde hace algunos años se han desarrollado regulaciones específicas con grandes esfuerzos, como la promulgación de la Ley de Protección Orgánica de Protección de Datos, además en conjunto con los países que conforman la confederación, en la participación de convenios como el Convenio de Budapest.

En nuestro hemisferio, en concreto en América Latina y en relación con los países europeos, a pesar del rezago en temas de desarrollo, México ha sido uno de los pioneros en relación con el tema en estudio, la llamada “Ley Federal de Protección de Datos Personales en Posesión de los Particulares.” Para efectos del desarrollo de la investigación, ambos países mencionados se abordarán como objeto de estudio.

En Costa Rica los entes encargados de atender temas regulatorios a nivel nacional, se han visto influenciados, en el buen sentido de la palabra y han imitado algunas de las acciones exitosas que países europeos han adoptado en relación con la protección de datos personales; la presente investigación efectúa un análisis de la ley y compara e interpreta algunos de sus artículos.

En este sentido, en Costa Rica una de las medidas implementadas es la creación de regulaciones para la protección de los datos de las personas. Así mismo, se han

publicado decretos y legislación relacionada, las cuales se abordarán con más profundidad durante el desarrollo de la investigación.

Además de lo anterior, es importante mencionar que se han asignado responsabilidades a diversas instituciones con el objetivo de velar por el cumplimiento de la ley, en cuanto al uso de los datos personales.

Con el fin de ampliar la visión del campo que tiene el Derecho al Olvido y con el objetivo de mencionar de manera introductoria los antecedentes de las regulaciones, se describe a continuación uno de los casos más sonados y que abrió el camino para marcar el inicio de la discusión del tema en España, el mismo es conocido como caso Costeja vs. Google.

"Caso Costeja vs. Google"

Es posiblemente el caso más reconocido a nivel internacional, éste marca una línea entre el antes y el después en Europa, en relación con el tratamiento de datos privados en medios tecnológicos.

Su fundamento se basa en la interpretación de los artículos 2,letras b) y d), 4, apartado 1, letras a) y c), 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE[1]del Parlamento Europeo y del Consejo Europeo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[2] la cual lo describe el documento de "Sentencia del Tribunal de Justicia (Gran Sala)", publicado el 13 de mayo del año 2014. (Sentencia del Tribunal de Justicia, Gran Sala, 2014).

[1] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos (DO 1995, L 281, p. 31)

[2]La Unión Europea es una comunidad política de derecho constituida en régimen sui géneris de organización internacional nacida para propiciar y acoger la integración y gobernanza en común de los Estados y los pueblos de Europa.

En este caso Sr. Mario Costeja, ciudadano de España, presentó una solicitud de litigio entre Google Spain, S.L. (Google España), y Google Inc., ante la Agencia Española de Protección de Datos.

El hecho se remonta al año 2012 cuando el Sr. Costeja presenta una denuncia ante la Agencia Española de Protección de Datos en la cual se denuncia la compañía Google y el periódico La Vanguardia. Dicha acción se origina al descubrir que al buscar su nombre en Google, los resultados generados por dicho buscador muestra una serie de enlaces con información en la cual aparece una subasta de bienes inmuebles que se le habían embargado por falta de pago de las contribuciones a la seguridad social. El Sr. Costeja no cuestionaba la veracidad de la información enlazada, pero sí la consideró obsoleta e irrelevante, características que poseen los datos y como se podrá comprender, durante el desarrollo de la investigación, juegan un papel muy importante en el ejercicio del Derecho al Olvido.

Como resultado del proceso la Agencia Española acoge el reclamo del Sr. Costeja contra ambas entidades y ordenaba a Google Inc. que adopte o aplique las medidas necesarias para retirar los datos personales del Sr. Costeja de su índice e imposibilite el acceso futuro a los mismos. Es importante mencionar que en el proceso la AEPD (Agencia Española de Protección de Datos) desestimó la denuncia contra el periódico, esto por cuanto la Agencia indica en ese momento que la información que se publicó originalmente se consideraba que se había publicado de forma legal y que estaba protegida por el derecho a la información.

1.2 Justificación

El presente documento nace por la inmediata necesidad que tenemos de conocer la legislación vigente que pueda protegernos como individuos miembros de una sociedad con derechos y deberes, y que a la vez como ciudadanos nos vemos

expuestos a una serie de riesgos tecnológicos de los cuales no somos inmunes y que ponen en peligro nuestros datos, nuestra privacidad y nuestra vida.

La presente investigación se ha desarrollado tomando como referencia la regulación vigente de países con índices de desarrollo social más altos que Costa Rica. Tal es caso de España, la cual ha logrado educar a su población en el tema.

Sin duda alguna, el desconocimiento o la falta de cultura en términos de la privacidad en medios tecnológicos, permite ser una de las vulnerabilidades más aprovechadas por personas malintencionadas o por compañías que tienen el fin de lucrar con los datos, generando como consecuencia, que las personas sean víctimas de distintos hechos catalogados como no legítimos mediante el uso de la tecnología.

Es común que se escuche en medios de comunicación que las organizaciones y personas son víctimas de individuos mal intencionados, que han cometido algún tipo de delito en su contra. Cuando pensamos en estos hechos, vienen a nuestra mente pensamientos relacionados a diversas actividades ilícitas, como asesinatos, asaltos, estafas, etc. y dejamos de lado actos que de la misma forma a los hechos antes mencionados son ilícitos, con la diferencia directa que estos hechos son cometidos mediante la utilización de la tecnología.

Se pretende determinar además, si Costa Rica cuenta con los mecanismos legales necesarios para poder hacerle frente a los retos que la tecnología ha puesto con el paso del tiempo.

1.3 Objetivos

Los objetivos de esta investigación fueron definidos tomando como referencia la taxonomía establecida por Benjamin Bloom, su alcance de tiempos y conceptos permitirá abarcar temas precisos para la comprensión del objeto de estudio. Se tocarán los distintos niveles del modelo presentado para llegar de manera exitosa al objetivo general.

1.3.1 Objetivo General

- Establecer la situación actual del Derecho al Olvido en Internet en Costa Rica, mediante la comparación de la legislación vigente en los países de España y México, apoyada en la función que ejerce la tecnología.

1.3.2 Objetivos Específicos

1. Describir la función de la tecnología y sus componentes en el tratamiento de los datos de las personas físicas y la garantía de privacidad para los mismos.
2. Listar controles tecnológicos y algunos de los retos futuros para el ejercicio del Derecho al Olvido.
3. Determinar la situación actual de Costa Rica en temas relacionados con el Derecho al Olvido, mediante la comparación de la ley vigente en España, México y Costa Rica.

1.4 Alcance

Para el desarrollo de esta investigación se limitará el estudio comparativo a los países considerados en sus respectivas regiones geográficas, más desarrollados en el tema del Derecho al Olvido. Se efectuará una comparación en materia de legislación vigente en los países España, México y Costa Rica y se estudiarán además algunos de los controles tecnológicos que buscan el ejercicio del cumplimiento del Derecho y el papel que cumple el blockchain, DataBrokers y hacking como principales retos ante el ejercicio del Derecho al Olvido.

1.5 Limitaciones

Se ha identificado que las limitaciones para el desarrollo de este documento son:

- No se incluirá legislación de países no incluidos en el alcance.
- No se incluirá el estudio de la legislación que no ha sido aprobada oficialmente por le entidad correspondiente para cada país.

2. Capítulo II: Estado de la cuestión

En una investigación de esta magnitud, por el nivel de información disponible y por la complejidad de búsqueda, es necesario utilizar un proceso adecuado para el desarrollo de la misma. Pensando en esa premisa y con el objetivo de brindar un producto de calidad se ha utilizado la metodología planteada por Bárbara Kitchenham en relación con elaborar revisiones sistemáticas, por medio de su publicación “Procedures for Performing Systematic Reviews.”

2.1 Planificación

Con el objetivo de brindar un enfoque adecuado a la investigación y abordar el tema de forma amplia, es importante efectuar una revisión sistemática de las lecturas disponibles y que además tienen relación con el tema en estudio, de esta manera emitir un criterio basado en hechos reales y con bases académicas como respaldo.

2.1.1 Protocolo de revisión

Durante el proceso de búsqueda de los elementos utilizados en el desarrollo de la investigación se utilizaron una serie de parámetros, los cuales son:

Preguntas de investigación

Ante los antecedentes presentados y tomando en consideración el gran auge que ha tenido la tecnología mediante el uso de la Internet y la aparición de las redes

sociales, se pretende con el desarrollo de esta investigación, dar respuesta a la siguiente interrogante:

¿Cuál es el estado actual de Costa Rica en temas de Derecho al Olvido en la Internet, con relación a Europa (España) y Latinoamérica (México)?

Criterio de inclusión

Para la inclusión en las búsquedas efectuadas se tomaron en cuenta las siguientes lecturas relacionadas con los siguientes temas:

- Derecho al olvido
- Privacidad
- Legislación para la protección de los datos
- Protección de datos personales
- Motor de búsqueda
- *Right to oblivion*

Criterios de exclusión

Se han excluido documentos para el desarrollo de esta investigación con los siguientes criterios:

- Países fuera del alcance
- Legislación en desarrollo o no vigente

Criterios de calidad

La documentación consultada pertenece a bases de datos como ACM, ENSCOhost, VLEX, entre otras. La revisión se efectuó mediante búsquedas utilizando motores internos para esta función, tomando aspectos como el año de publicación, la relación del título con el tema en desarrollo.

2.2 Revisión de estudios seleccionados

Para la elaboración del Estado de la Cuestión se utilizaron algunos documentos que se identificaron durante la revisión de los mismos. A continuación se detalla una lista de los escritos que cumplieron con criterios de inclusión descritos:

Lista de los documentos que se utilizaron
Título: ***El derecho al olvido en Internet. Google versus España*** Autor: **Artemi Rallo Lombarte** Tipo: **Artículo** Descripción: **El documento trata de cómo fue que se desarrolló el polémico caso de Google y el tratamiento de los datos personales en España.**
Título: ***EL «DERECHO AL OLVIDO» COMO APORTACIÓN ESPAÑOLA Y EL PAPEL DE LA ABOGACÍA DEL ESTADO*** Autor: **Marta Silva de Lapuerta** Tipo: **Artículo** Descripción: **En este documento, la autora busca recalcar el papel de España para la regulación desarrollada por la Unión Europea, busca dar el debido reconocimiento desde el punto de vista legal a las acciones ejecutadas por este país.**
Título: **Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital** Autor: **Álvarez Caro, María** Tipo: **Libro**

Descripción: **Es una lectura desarrollada, desde el seno del caso España – Google, en apoyo con la Universidad San Pablo CEU y con la colaboración de Google. Se efectúa un repaso y descripción de los hechos presentados, así como los aspectos relevantes de la Constitución Española para darle frente a estos.**
Título: ***El derecho al olvido en internet. El fenómeno de los motores de búsqueda****   Autor: **Alejandro Platero Alcón**   Tipo: **Libro**   Descripción: **En esta lectura, se efectúa un análisis desde el punto de vista técnico y la función de los motores de búsqueda para el tratamiento de los datos personales.**
Título: ***sobre el derecho al olvido digital: una solución al conflicto entre la libertad de información y el derecho de protección de datos personales en los motores de búsqueda***   Autor: **Lorena Manzanero Jiménez**   Tipo: **Libro**   Descripción: **En este escrito, la autora pone al Derecho al Olvido por un lado como una herramienta jurídica presentada para el derecho del ciudadano, pero por otro lado, como una posible limitación para la libertad de información, desde el punto de vista de investigación periodística.**

Durante la revisión de los documentos se efectuó una lectura de los “abstracs” de documentos en los que se han desarrollado para ampliar el tema. Se efectuó una revisión sistemática para analizar el estado del tema en investigación.

Se desarrollará en paralelo a la definición de los términos clave para poder comprender el funcionamiento de la tecnología y cómo es implementada para el ejercicio del Derecho.

Los documentos utilizados fueron obtenidos de bases de información como ACM, ENSCOhost, VLEX, crcnetbase, entre otras, mediante el uso de una cuenta privada.

La búsqueda de la información se efectuó mediante la consulta a bases de información mencionadas, empleando palabras de búsqueda antes citadas.

El Derecho al Olvido mantiene relación con temas de carácter legal y tecnológico. El mundo se encuentra en la búsqueda constante de los mecanismos necesarios para llegar a la madurez apta y enfrentarse a las diversas situaciones presentadas en relación con la privacidad. Además de mecanismos técnicos que se ampliarán durante el desarrollo de la presente investigación, diversas leyes y reglamentos que se han desarrollado dan respaldo a la protección del ciudadano, tal como lo menciona el Sr. Luis Gervas de la Pisa, en el documento “Reglamento, en relación a la protección de los derechos fundamentales”:

> *“La protección de los derechos fundamentales en la red es cada día más necesaria. La sociedad de la información, basada cada vez en mayor medida en Internet, posibilita que cualquier contenido (aún perjudicial, inexacto u obsoleto), pueda ser objeto de una divulgación desproporcionada, accediéndose al mismo casi de forma inmediata a través de distintas plataformas (como los buscadores o redes sociales).*
>
> *En este ámbito el llamado "derecho al olvido", también denominado "derecho a vivir en paz", se ha convertido en una pieza clave para la defensa de las personas, ya sean anónimas o públicas.” (Gervas. L, 2016)*

Es por lo anterior que se puede afirmar que es necesario contar con mecanismos de defensa y proteger nuestra información, porque lejos de un capricho por parte de la sociedad, es sin duda, un derecho que va más allá de la tecnología.

Los ciudadanos y usuarios de medios tecnológicos nos encontramos bajo una sombrilla de riesgos relacionados al mal manejo o mal uso de nuestra información personal, los eventos que se han presentado en los últimos años han hecho que se despierten sentidos de defensa en relación con el tema.

Dicha preocupación y la presencia de los elementos tecnológicos ha generado que en temas como el tratamiento de los datos, entes Gubernamentales en los distintos países alrededor del mundo, se vean obligados a desarrollar legislación dirigida a este tema. Y es que la tecnología y su crecimiento aumentan la complejidad para el ejercicio de este derecho, tal como lo menciona Lorena Manzanero en su escrito:

> *"En los últimos años se ha popularizado el uso de las nuevas tecnologías de la información y la comunicación. Son herramientas que posibilitan nuevos modelos de negocio, formas de organización y paradigmas de comportamiento. Su rápida capacidad transformadora compromete los instrumentos vigentes de protección de las libertades y derechos de los ciudadanos, incapaces ya de dar una respuesta eficaz a los riesgos que genera el nuevo contexto y a los problemas jurídicos que conlleva: a esta erosión y degradación de los derechos fundamentales." (Manzanero. L, 2013)*

No es un secreto que la tecnología avanza a un ritmo impresionante, pues haciendo referencia al texto anterior, este hecho puede permitir que la complejidad para la creación de leyes, reglamentos y la burocracia para su promulgación nos lleve a la incapacidad para responder de forma eficaz. Por lo anterior es importante que los temas relacionados con la legislación, su avance en su proceso de diseño y su promulgación se efectúen a un ritmo adecuado y que se ajusten a la necesidad, de esta manera permitirá ser una herramienta o instrumento de defensa y prevención para los ciudadanos.

Palabras utilizadas para la búsqueda

Derecho al olvido, motores de búsqueda, datos personales, ley, regulación, privacidad

2.3 Procesamiento y análisis de datos

Para el desarrollo de esta investigación es fundamental aplicar una serie de técnicas, herramientas, o métodos, para recolectar información necesaria para poder realizar los entregables definidos. En el desarrollo se utilizaron las siguientes técnicas de investigación:

2.3.1 Comparación

Según lo define el autor Pérez (2016), la comparación es:

> *"En las técnicas de comparación se focaliza en grupos de individuos que están (estudios observacionales) o que se les sitúa (estudios experimentales) en diferentes condiciones que interesa comparar."*

En el caso de esta investigación, la comparación se realizará en el apartado IV con el estado actual de las regulaciones en los países incluidos en la investigación.

2.3.2 Juicio experto

Con base en lo indicado en el artículo de Escobar (2008), el juicio experto se define como:

> *"una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones."*

Esta herramienta es de gran valor ya que las personas especialistas en Derecho, así como en temas relacionados con la seguridad técnica de los datos, conocen a profundidad el funcionamiento de la ley y la tecnología correspondientemente y por tanto el criterio que emitan es de gran valor.

2.3.3 Investigación documental

Se centra en la búsqueda e identificación de fuentes escritas o digitales que están a disposición para resolver el problema y cumplir con el objetivo general planteado. Por lo tanto, es de gran valor para esta investigación que se analice la documentación existente en bases de datos ya mencionadas, así como la documentación desarrollada por otros expertos en relación con el Derecho al Olvido y su relación con la tecnología.

3 Capítulo III: Marco Teórico

A continuación se detalla el marco teórico del proyecto, donde se describen los conceptos teóricos y prácticos que sustentan el desarrollo del presente proyecto.

3.1 Datos personales

La esencia del principio del Derecho al Olvido se encuentra estrechamente relacionado con el uso y tratamiento de los datos personales, el concepto como tal podría ser muy subjetivo desde la perspectiva de cada ciudadano, según lo que éste considere como personal, sin embargo, para efectos de la investigación, se considerará la siguiente definición brindada por la Ley de Protección a la Persona Frente al Tratamiento de sus Datos, la cual lo define como cualquier dato relativo a una persona física identificada o identificable. (Ley 8968, 2016) En relación con esta definición podría decirse que se incluyen datos como: el nombre, identificación.

3.2 Derecho al olvido

El Derecho al Olvido, tema central de la investigación, posee una serie de condiciones legales y técnicas cuyo objetivo es la protección del ciudadano, para comprender mejor el término, se utilizará como referencia la definición brindada por la Agencia Española de Protección de datos:

> *"El denominado 'derecho al olvido' es la manifestación de los tradicionales derechos de y cancelación y oposición aplicados a los buscadores de internet. El 'derecho al olvido' hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información)." (AEPD, 2016)*

Tal como lo indica la definición anterior, el Derecho al Olvido va de la mano con el uso de la tecnología, en este caso, mediante los navegadores o buscadores de Internet, es por este hecho que el presente documento contará con una breve explicación de cómo es que la tecnología juega un rol importante en el ejercicio del mismo.

3.3 Derecho a la cancelación y oposición de datos

En relación con la aplicación del Derecho al Olvido como tal, se aplican una serie de principios de los cuales se vale la legislación. El derecho a la cancelación y oposición son primordiales en el ejercicio del Derecho al Olvido como herramienta que legal que protege la privacidad, según informa la Agencia Española de Protección de Datos:

> *"La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas, transcurrido el cual deberá procederse a la cancelación" (AEPD, 2017).*

3.4 Autodeterminación informativa

La autodeterminación informativa es un concepto del cual se deriva la privacidad de los datos personales, según lo menciona

> *"El principio de autodeterminación informativa es un típico principio de reciente revelación, en el panorama normativo, y deconstrucción conceptual y jurídica. Éste ha encontrado en Alemania su origen o más bien su autonomía respecto a otro principio de origen angloamericano, es decir, el llamado derecho a la vida privada (right to privacy)." (Giulio Adinolfi, 2007)*

Además la "Ley 8968 Protección de la Persona frente al tratamiento de sus datos personales" en Costa Rica, en su artículo "4- Autodeterminación informativa":

> *"Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.*

> *Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias." (Ley 8968 Protección de la persona frente al tratamiento de sus datos personales, Costa Rica, 2011)*

Como lo referencia la cita anterior, es un derecho al cual tenemos acceso como ciudadanos, este derecho apoya el principio definido por el Derecho al Olvido, en la intención de mantener control sobre los datos y evitando un uso inadecuado o no informado de los mismos.

3.5 Blockchain

Es un término relativamente reciente en el ámbito de la tecnología y es usado en su mayoría para el registro transaccional de actividades bancarias, que utiliza una serie de algoritmos y elementos de procesamiento alrededor de una red, para poder proteger datos, evitando la alteración por un tercero.

3.6 Deep Web

La Web se encuentra conformada por una serie de "capas", que contienen sitios Web con información, la Deep Web o Internet profunda es un red de datos en la cual los sitios contenidos en ésta no poseen nombres de dominio como mecanismo de identificación, además para hacer uso de ésta, es necesario la utilización de herramientas que utilizan mecanismos de comunicación seguros para implementar el principio de anonimato durante la navegación de los usuarios, se caracteriza además, bajo este principio, por contener en ella una serie de transacciones y actividades que se consideran como ilícitas.

3.7 Data Broker

Son componentes que los sitios Web utilizan mediante técnicas de consumo de datos, para la recopilación de los mismos con el objetivo de personalizar la interacción del usuario con el sitio en que se encuentra. El proceso consiste en la instalación y uso de los mismos en el equipo del usuario que se encuentra navegando en un sitio Web.

4 Capítulo IV: Marco Metodológico

A continuación se define el marco metodológico utilizado en el desarrollo de esta investigación, en el cual se muestra el proceso que se ejecuta para lograr los objetivos inicialmente planteados. En esta sección se detallan elementos como: el tipo de investigación, las fuentes de información.

4.1 Tipo de investigación

Según Zorrilla, (1985) la investigación es considerada una actividad humana orientada a la obtención de nuevos conocimientos y su aplicación para la solución a problemas o interrogantes de carácter científico. El tipo de investigación que se utilizará se enfocará por la finalidad, criterio de medida y profundidad.

De acuerdo con la finalidad indicada por Echavarría (1999), la clasificación de la investigación se define en dos tipos:

- Investigación básica (pura): el autor (Barrantes Echavarría, 1999) indica textualmente lo siguiente:

> *"es aquella actividad orientada a la búsqueda de nuevos conocimientos y campos de investigación sin un fin práctico específico e inmediato. Su objetivo es crear un cuerpo de conocimientos teóricos en algún campo de ciencia." (Barrantes Echavarría, 1999)*

- Investigación aplicada: de igual forma el autor (Barrantes Echavarría, 1999), lo explica de la siguiente manera:

> *"su finalidad es la solución de problemas prácticos para transformar las condiciones de un hecho que nos preocupa. El propósito fundamental no es aportar al conocimiento teórico." (Barrantes Echavarría, 1999)*

Además, en relación con el carácter de la medida, la investigación se clasifica también como:

- Cuantitativa: se basa en elementos que se pueden cuantificar, se basa en una metodología empírica-analítica y utiliza la estadística.

- Cualitativa: se estudian los significados y utiliza la metodología de la interpretación. Se enfoca en el descubrir el conocimiento, la información se maneja cualitativamente.

De acuerdo con la profundidad, así se define el tipo de investigación a utilizar. Según el objetivo planteado, los tipos de investigación posibles se clasifican en cuatro tipos:

- Exploratoria.
- Descriptiva.
- Correlacional.
- Explicativa.

El autor Cazau, los explica de la siguiente manera:

> *"Según su alcance, las investigaciones pueden ser exploratorias, descriptivas, correlacionales o explicativas. Estos tipos de investigación suelen ser las etapas cronológicas de todo estudio científico, y cada una tiene una finalidad diferente: primero se 'explora' un tema para conocerlo mejor, luego se 'describen' las variables involucradas, después se 'correlacionan' las variables entre sí para obtener predicciones rudimentarias, y finalmente se intenta 'explicar' la influencia de unas variables sobre otras en términos de causalidad." (Cazau, 2006)*

Barrantes define un estudio exploratorio de la siguiente forma:

> *"Los estudios exploratorios sirven para preparar el terreno y por lo común anteceden a investigaciones con alcances descriptivos, correlacionales o explicativos." (Barrantes, 1999)*

Iniciando por la exploración inicial, se continúa con la investigación descriptiva, que según el autor (Arias, 2006) consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Es necesario analizar y describir esa realidad para poder desarrollar la propuesta de estrategia.

Esta investigación se realizó bajo la finalidad de una investigación básica porque no se hará aplicación alguna y un enfoque cualitativo desde este sentido, según Hernández (2010) esta conceptualización se define como:"...utilizar la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación", así como descriptiva porque se pretende explicar

las diversas perspectivas, interpretaciones, principios, normas y teorías contenidos en la doctrina, casos internacionales y jurisprudencia vigente. En ésta se describirán diferentes conceptos técnicos relacionados a la aplicación del Derecho al Olvido.

4.2 Fuentes consultadas

De acuerdo con el autor (Hernández Sampieri, 2010), citando al autor Danhke, el origen de la información para el desarrollo del proyecto se clasifica en tres tipos de fuentes de información, primarias, secundarias y terciarias.

Por medio de las fuentes de información es posible obtener datos e información útiles para el cumplimiento de los objetivos. Para la investigación se utilizaron dos tipos de fuentes de información, las cuales se detallan a continuación:

4.2.1 Fuentes primarias

La autora Susana Romanos (2000) define las fuentes primarias como las que "contienen información original, producto de una investigación o una actividad eminentemente creativa. Son fuentes destinadas a comunicar los resultados del conocimiento y de la creación." (Romanos de Tiratel, 2000) Algunas de las fuentes primarias para el proyecto son los las siguientes:

Bases consultadas para la toma de información
Motor de búsqueda: **ACM Digital Library** URL:**http://dl.acm.org/** Fecha de la consulta: **16 de julio, 2016** Otros parámetros: **se utilizó una búsqueda avanzada que incluyera documentos pdf.**
Motor de búsqueda: **IEEE**

URL:**https://www.ieee.org/index.html** Fecha de la consulta: **22 de julio, 2016** Otros parámetros: **se utilizó una búsqueda avanzada que incluyera documentos pdf.**
Motor de búsqueda: **Google Académico** URL:**http://scholar.google.com/** Fecha de la consulta: **22 de julio, 2016** Otros parámetros: **se utilizó una búsqueda avanzada que incluyera documentos pdf.**
Motor de búsqueda: **crcnetbase** URL:**www.crcnetbase.com** Fecha de la consulta: **16 de agosto, 2016** Otros parámetros: **se utilizó una búsqueda avanzada que incluyera documentos pdf.**
Motor de búsqueda: **ENSCOhost** URL:**https://www.ebscohost.com/** Fecha de la consulta: **16 de agosto, 2016** Otros parámetros: **se utilizó una búsqueda avanzada que incluyera documentos pdf.**

4.2.2 Fuentes secundarias

Como parte del proceso, se consultan fuentes de información secundarias, las cuales según Hernández (2010) son documentos, listas, compilaciones y resúmenes de referencias o fuentes primarias publicadas en un área de conocimiento en particular. Es decir, brindan información analizada por una fuente primaria o externa. Algunas de las fuentes secundarias que se utilizaron en este proyecto de investigación son:

- Leyes
- Reglamentos de las leyes
- Periódicos Digitales
- Artículos en relación al Derecho al Olvido

4.3 Metodología de investigación

El desarrollo de la investigación se realizará cumpliendo cada uno de los objetivos específicos planteados, donde a lo largo de su desarrollo, cada objetivo se irá profundizando. Los pasos a seguir durante la ejecución de la misma son los siguientes:

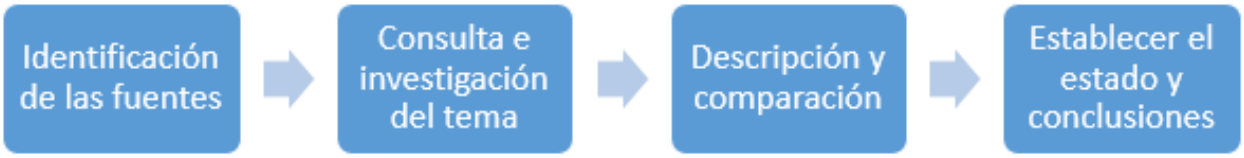


Imagen 1 – Metodología del proyecto. Creada por el autor

4.4 Técnica de investigación

Para el desarrollo de la investigación es fundamental aplicar una técnica, herramienta, o método, para recolectar información necesaria, para poder realizar las conclusiones finales. Durante la ejecución de la investigación se utilizó la siguiente técnica:

4.4.1 Análisis de datos

Esta técnica según Sampieri (2010), una vez que se cuenta con la información recolectada, lo primero que hay que realizar es una revisión para un posterior análisis en la cual se documente el proceso analítico y a partir de ahí definir los elementos referentes al Derecho al Olvido.

5 Capítulo V: Desarrollo

En la presente investigación, tal como se ha planteado en los objetivos de la misma, se busca brindar al lector, los aspectos necesarios para comprender el Derecho al Olvido digital, así como la relación con las herramientas tecnológicas que interfieren en el ejercicio del mismo y los retos a los que se enfrenta la legislación.

Además, mediante la comparación de las leyes aplicadas en los países en estudio, se espera dar el estado en que se encuentra Costa Rica, desde el punto de vista legal, qué institución da apoyo al cumplimiento de estas regulaciones y de qué manera es posible permitir el ejercicio del Derecho al Olvido.

En el primer apartado se establecen los conceptos principales para comprender a qué se refiere el Derecho al Olvido, se expondrá cómo algunos autores a nivel mundial se han referido al tema y la relación de éste con conceptos como la privacidad y la cancelación de los datos.

En el segundo apartado se espera describir el papel de la tecnología mediante la Internet y las redes sociales como protagonistas en el proceso del cumplimiento del Derecho.

En el tercer apartado se pretende presentar al lector, algunos de los principales retos tecnológicos que se espera enfrenten los ciudadanos y los entes responsables de garantizar la protección de los ciudadanos, retos relacionados a la aparición de nuevas tecnologías y que gracias a su tecnología desconocida por muchos, se han convertido en elementos de estudio para su correcta interpretación.

En un último apartado se establece la comparación de la legislación actual entre los países que forman parte del objetivo de estudio de esta investigación, es importante que el ciudadano conozca cómo otras naciones han trabajado desde hace algunos años, con el fin de dar protección y hacer valer los derechos esenciales que poseemos como tal.

Conocer todos estos elementos permitirá adquirir criterio para discutir sobre el tema y además para obtener un panorama del estado actual en que se encuentran las herramientas legales para el cumplimiento de nuestros derechos.

5.1 Apartado I ¿A qué se refiere el Derecho al Olvido? - Privacidad

El ser humano por naturaleza es capaz de retener datos e información por un período de tiempo definido, ya sea por enfermedad, falta de relevancia de ciertos eventos para una persona o por causas naturales, esta información deja de ser recordada. Sin embargo, con la tecnología, el olvido de información no ocurre de la misma manera, y a partir de este hecho, se busca ejercer los derechos al querer cancelar información de carácter personal a causa de circunstancias planteadas por el titular de los datos.

EL Derecho al Olvido es definido por el Superior Europeo de Protección de Datos como:

> *"El derecho al olvido puede entonces definirse como aquel principio según el cual los datos negativos deben ser eliminados de las bases de datos, una vez ha transcurrido el tiempo establecido para su tratamiento, con el fin de que la persona no quede "prisioner(a) de su pasado." (Supervisor Europeo de Protección de Datos, 2011)*

Según lo referencia la cita anterior, para la aplicación del Derecho, se consideran distintos elementos, en primera instancia se menciona la clasificación de los datos, al referirse a datos negativos y por otro lado considera una serie de características que poseen los datos, las cuales deben cumplir, refiriéndose a la relevancia y al tiempo (caducidad).

En relación con el origen al derecho al Olvido, se puede decir que forma parte de una serie de Derechos adquiridos por defecto al formar parte de la sociedad. Así lo menciona María García (2013), en referencia a los Derechos Humanos:

> *"En estos instrumentos se encuentran derechos que protegen: la personalidad jurídica, la vida, la integridad personal, la libertad personal, el debido proceso legal*

o garantías judiciales, la honra (también conocido como derecho al honor), la privacidad, la libertad de conciencia y religión, la libertad de expresión, la rectificación o respuesta, de reunión, la libertad de asociación, la nacionalidad, la circulación y residencia, los derechos políticos, el derecho a un recurso sencillo y rápido, etc.

El estudio de la privacidad, parte de un derecho pasivo proclamando la "no injerencia en la vida privada" del individuo y se sitúa en el catálogo de los derechos de primera generación. Este derecho llega a reivindicar un derecho de libertad informática o control de los datos personales incluidos en un fichero informático." (M. García, 2013)

Como lo indica la cita anterior, se encuentra la privacidad en una estrecha relación con el Derecho al Olvido, en el sentido del tratamiento de los datos. El objetivo que se promulguen leyes en relación con el tratamiento de los datos es hacer valer los derechos de los ciudadanos, así como limitar el accionar de entes intermediarios que administran y hacen uso de la información considerada como personal. Además desde la perspectiva del titular de los datos, se está irrumpiendo con sus principios de intimidad, honor. Según lo establece Manzanero (2015):

"Cabe recordar que el foco de atención está en la licitud del tratamiento de datos personales por el motor de búsqueda –indexar y difundir–, pues el ejercicio del derecho al olvido contra los buscadores solo entra en juego cuando el tratamiento de datos por el editor de la web fuente indexada es lícito y no cabe oponerse o solicitar la cancelación frente a él." (Manzanero, 2015)

Según lo indica la autora en la cita anterior, existe un proceso técnico que apoya el mal uso y tratamiento indebido de datos de los ciudadanos. Los motores de búsqueda y otras tecnologías que se encuentran implícitas en los mismos forman parte de estos elementos.

El Derecho al Olvido permite brindar los mecanismos para actuar ante la aparición de la tecnología y el uso de los datos, tal como lo menciona Higareda Magaña (2014):

"La contraposición entre el avance tecnológico y la tutela del derecho a la protección de datos personales, se resuelve en la medida en que el titular de los datos tenga el control efectivo para borrar el registro de su información que lo identifica o lo hace identificable en Internet a través del ejercicio del derecho al olvido, a fin de garantizar su seguridad jurídica en el tratamiento de su información

personal contenida en bases de datos a través de los motores de búsqueda en la red." (Magaña H., 2014)

Es claro que el Derecho al Olvido es una realidad y se establece bajo el sentido de la defensa ante ataques en contra de los datos de carácter personal, sin embargo, se encuentran disponibles también mecanismos inteligentes que pueden extraer información sensible de diversos bancos de datos y utilizarlos para fines múltiples, que podrían afectar los derechos de los ciudadanos y vulnerar así la protección de datos, sin que la persona se dé cuenta, limitando el ejercicio del derecho a la autodeterminación informativa.

En lo que respecta al ámbito privado en la sociedad tecnológica, se considera necesaria la protección de la información, que viene a recaer bajo la autodeterminación informativa como una potestad del control y manejo de información que tiene cada persona. El derecho a la autodeterminación informativa funciona como una defensa ante las intromisiones del Estado y de terceros así como ante los ataques tecnológicos que eventualmente trae consigo el uso de la Internet y de las redes sociales.

La autodeterminación informativa no le concede al ciudadano un poder absoluto para manejar los datos a su antojo, sino que el derecho se enfoca en la recepción de información acerca del uso de los datos, y a ejercer el derecho de defensa en caso de que se violenten sus garantías, mediante mecanismos jurídicos como las leyes promulgadas.

En ese sentido, como lo menciona Rodríguez (2016):

"la *autodeterminación informativa es una realidad, y funciona en el sentido de la defensa ante ataques en contra de los datos de carácter personal, existen, no obstante, mecanismos inteligentes que pueden extraer información sensible de diversos bancos de datos y utilizarlos para fines múltiples, que eventualmente afectan los derechos de la personalidad y vulneran la protección de datos, sin que la persona se dé cuenta, limitando así el ejercicio del derecho a la autodeterminación informativa." (Rodríguez 2016)*

Bajo la premisa establecida por la autora en la referencia anterior, el papel de la legislación ante la sociedad informática se encuentra limitado, esto se debe a que día a día se desarrolla nueva. Como resultado, es necesario un esfuerzo más profundo que lleve a la evolución en las leyes en este sentido.

En los medios tecnológicos, la gran cantidad de información contenida y su difícil rastreo es una tarea compleja, menciona Terwangne (2011):

> *"En el contexto de Internet, esta dimensión de la privacidad significa autonomía informativa o autodeterminación informativa. Internet maneja grandes cantidades de información sobre personas. Estos datos personales con frecuencia se tratan en el sentido de que se dan a conocer, se difunden, se comparten, se pueden seleccionar, descargar, registrar y usar de muchas maneras. En este sentido, la autonomía individual está en relación directa con la información personal. La libre determinación sobre la información significa tener el control sobre nuestra información personal, es decir, es el derecho de los individuos a decidir qué información sobre ellos mismos será revelada, a quién y con qué objetivo." (Terwangne C., 2011)*

El objetivo, no restringir la totalidad del uso de tratamiento de los datos, como lo indica el autor en la cita anterior, el fin es garantizar que esta cancelación se dé bajo las condiciones necesarias para garantizar la seguridad de los datos y el apego a las leyes y regulaciones establecidas.

Tener mecanismos de control para saber quién posee nuestros datos, a quién son transferidos y otras acciones relacionadas al tratamiento como tal, permitirá dar al ciudadano las herramientas, para que, en caso de solicitar la cancelación de dichos datos, el proceso sea exitoso.

El ejercicio del Derecho al Olvido no debe contemplar dentro de sus implicaciones la limitación de otros derechos, así lo establecen las mayorías de las leyes, uno de estos ejemplos es limitar el acceso a la información.

El acceso a la información es un derecho que se encuentra contemplado en el artículo 19 de la Declaración Universal de Derechos Humanos de las Naciones Unidas de 1948, el mismo establece en el artículo 19:

> *"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir*

informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión." (Declaración Universal de Derechos Humanos)

En nuestro país la Constitución establece en el artículo 30: "Se garantiza el libre acceso a los departamentos administrativos con propósito de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado."

Es por lo anterior que se debe efectuar un adecuado equilibrio y valoración de lo que pretende proteger desde el punto de vista técnico, pues se debe garantizar el cumplimiento al Derecho al Olvido, sin dejar de lado que existen principios fundamentales, los cuales no pueden ser incumplidos.

Es clara la importancia de la regulación sobre el tema, hoy se ha convertido en la herramienta de los titulares de los datos para proteger su intimidad, su dignidad, su buen nombre y la correcta utilización de sus datos personales, ya que de no existir, la información negativa mantenida en bases de datos de manera indefinida podría llegar a causar graves perjuicios para las personas y sus familiares.

5.2 Apartado II. La tecnología como elemento protagonista en el ejercicio del Derecho

En este capítulo se describirá de forma breve algunos elementos tecnológicos que se consideran como fundamentales en el ejercicio del Derecho al Olvido, parte de esta tecnología es la Internet como herramienta que ha generado todo un cambio radical en las personas, ya sea en beneficio o en perjuicio de las mismas. Es importante conocer de la existencia de mecanismos que han sido creados con el fin de dar protección a los ciudadanos y controlar el tratamiento que se da a sus datos personales por medio de la tecnología.

Como se podrá comprender en este apartado, la responsabilidad de garantizar qué datos no deben ser publicados de forma abierta no recae solamente en intermediarios como los navegadores Web o en las redes sociales.

La aparición de las nuevas tecnologías han producido que las compañías se adapten y con esto aparecen estándares de seguridad dirigidos a la protección de los datos y a la implementación de medidas para la protección de la información.

5.2.1 Internet como herramienta en el ejercicio del Derecho

La tecnología en la aplicación del Derecho al Olvido Digital, es representada mediante el uso de la Internet. Dicha herramienta se ha convertido durante el desarrollo de la historia en elemento fundamental para actividades como la generación de negocios, recreación, automatización, reducción de costos y un sinfín de actividades. Sin embargo, tal como se ha expuesto durante la presente investigación, a causa de hechos como el "caso Costeja" en España, el Tribunal de Justicia de la Unión Europea se ha pronunciado, por primera vez en un hecho histórico, sobre ejercicio del Derecho al Olvido contra estos servicios. Además de éste y otros precedentes han establecido una línea de restricción en el campo de acción del Derecho al Olvido en Internet para los llamados "motores de búsqueda", así como para las distintas redes sociales.

El ejercicio del Derecho se ve directamente influenciado por elementos tecnológicos. Mediante información obtenida del sitio Web de Google, se presentará la evolución que han desarrollado los motores de búsqueda a lo largo del tiempo.

Los "buscadores", se han visto obligados en adaptarse al crecimiento exponencial de la cantidad de sitios Web creados, tal como lo describe Google en su sitio Web:

> *"La tecnología de los motores de búsqueda ha tenido que escalar dramáticamente para mantenerse al día con el crecimiento de la web. En 1994, uno de los primeros motores de búsqueda web, el World Wide Web Worm (WWWW) tenía un índice de 110.000 páginas web y documentos accesibles en la web. A partir de noviembre de 1997, los principales motores de búsqueda afirman que el índice de 2 millones (WebCrawler) a 100 millones de documentos web (de Search Engine Watch). Es previsible que para el año 2000, un índice completo de la Web contenga más de mil millones de documentos. Al mismo tiempo, el número de consultas de motores de búsqueda de manejar ha crecido increíblemente también. En marzo y abril de 1994, el gusano de la World Wide Web recibió un promedio de unas 1500 consultas por día. En noviembre de 1997, Altavista afirmó que manejaba aproximadamente 20 millones de consultas por día." (Google, 2017)*

Además de las impresionantes cantidades de registros documentados por las compañías y según los datos referenciados, el número de consultas efectuadas por los usuarios ha crecido de forma exponencial, esto además es acompañado por la

necesidad de los usuarios por la obtención de información, así como de otros factores: la disminución de la brecha tecnológica y de acceso a la Web.

Como consecuencia de su función como intermediario en el suministro de información, el hecho ha obligado a las empresas administradoras de proveer el servicio de búsquedas Web a brindar mejores resultados en sus procesos tecnológicos, desde su rol en la intermediación, recopilación y presentación de enlaces a sitios relacionados con la búsqueda al usuario.

Los buscadores asumen un papel importante en el uso de la Internet mediante el re-direccionamiento a sitios Web que contienen la información de interés para los usuarios que efectúan una búsqueda.

Desde una visión muy general y tratado el tema desde un análisis técnico, estas herramientas utilizan el proceso conocido como “indexación”, el mismo genera como resultado final una lista de elementos que ubica al usuario en los sitios que contienen elementos de mayor coincidencia a su búsqueda. Internamente el proceso se efectúa mediante el uso de mecanismos que utilizan una serie de algoritmos e inteligencia de datos que genera como resultado lo esperado por el usuario o información con un alto grado de satisfacción, en cuanto a similitud se refiere.

Desde el lugar que ocupan quienes utilizan este servicio para efectuar una búsqueda mediante un navegador Web, el proceso es de total transparencia y su expectativa será la misma: obtener la información esperada, rápida y con el mayor grado de coincidencia posible.

Según datos obtenidos por Google, en su servicio de buscador Web, para poder brindar al usuario los resultados con la información esperada o de mayor interés, el proceso inicia con la introducción de las palabras de búsqueda. Gracias a la tecnología utilizada por dichas compañías al día de hoy, su nivel de efectividad es tal, que es posible predecir las palabras que se utilizarán en la búsqueda, este proceso es producto del uso de tecnología, en la cual, mediante minería de datos y análisis de las bases de información que cada motor de búsqueda contiene.

El sitio Web de Google informa además, que las búsquedas no se ejecutan en la totalidad de la Web, si no que se aplica a un fragmento de sitios Web resumen creado por la compañía, este índice contiene más de 100.000.000 gigabytes y se ha necesitado más de un millón de horas de computación para su creación, por lo que el nivel de procesamiento de datos es impresionante; en la actualidad, gracias a la capacidad de hardware de los equipos que procesan tal información, esto no es un impedimento y es posible suplir dicha necesidad.

Continuando el proceso de búsqueda y como paso siguiente, gracias al diseño de la arquitectura tecnológica de la compañía (Google), mediante el uso de software denominado “Spiders” y con la utilización de algoritmos de búsqueda, es posible explorar los datos contenidos en los sitios Web disponibles, a su vez la búsqueda se vuelve a efectuar en los sitios a los cuales re direccionan los enlaces o “links” que se encuentran en estas páginas, este proceso es iterativo o repetitivo, su repetición se efectúa y permite indexar y ordenar millones de páginas o sitios Web contenidas en millones de equipos tecnológicos alrededor del mundo.

ELDRAE, Diccionario de la Lengua Española, define el concepto indexar como: “Registrar ordenadamente datos e informaciones, para elaborar un índice”, lo que permite afirmar que el proceso tecnológico mantiene como prioridad ordenar de forma digital y mediante el uso de un índice, considerando además el uso de criterios establecidos por las compañías encargadas de efectuar dicha función, los distintos enlaces de información, en referencia a lo anterior Google menciona:

> *La Web es como una biblioteca pública cada vez mayor con miles de millones de libros y sin un sistema de archivo. En resumen, Google recopila las páginas durante el proceso de rastreo y, a continuación, crea un índice, por lo que sabemos exactamente dónde tenemos que buscar. Al igual que el índice del final de un libro, el índice de Google incluye información sobre las palabras y dónde aparecen. Cuando haces una búsqueda, en el nivel más básico, nuestros algoritmos buscan los términos de consulta en el índice para encontrar las páginas adecuadas. (Google, 2017)*

Como lo describe la cita, el buscador se encarga de ordenar los distintos enlaces para que éstos puedan ser consultados por el usuario.

Los sitios Web indexados que se presentan en el índice final, se encuentran ahí porque la mayoría de éstos no poseen restricciones o condiciones de limitación en el proceso de rastreo por parte de los “Spiders” para ser mapeados y/o publicar contenido a la Internet, producto de este hecho es que se genera la posibilidad que la información contenida sea de fácil rastreo y acceso, por lo tanto presentada al usuario.

En otras palabras, sí existe la posibilidad que los dueños o encargados de dar mantenimiento a sitios Web (Web Manager) puedan limitar a los buscadores como el caso de Google a rastrear e indexar sus sitios, a través de distintos componentes del buscador, uno de éstos es mediante el uso de un archivo denominado "robots.txt".

Con este archivo, la restricción en la colocación de los sitios Web en los buscadores es posible, permitiendo en este sentido y como parte de la implementación de un control técnico, ejercer el Derecho al Olvido.

El archivo “robots.txt” es configurado con el fin de colocar información del sitio a disposición de los buscadores para facilitar su rastreo, según información obtenida del sitio Wikipedia, este archivo es:

> *(…)Robots.txt es un archivo de texto con extensión .txt, que creamos y subimos a nuestra página web, generando la URL www.midominio.com/robots.txt, y que utilizamos para impedir que ciertos rastreadores o bots, puedan agregar información que no deseamos en los resultados de búsqueda.*
>
> *Es decir, es un archivo público que usamos para indicar a esos rastreadores o arañas qué parte o partes no deben entrar a rastrear e indexar de nuestra página web. En él, podemos especificar de manera sencilla, los directorios, subdirectorios, URLs o archivos de nuestra web que no deberían ser rastreados o indexados por los buscadores.” (Human Level, 2017)*

Referenciando la información anterior, algunas de las características del archivo, es que éste permite informar al motor de búsquedas la información que puede ser presentada y limitar el acceso a la que debe mantenerse restringida como resultado de la búsqueda.

La estructura de este archivo es definida mediante el uso de la sintaxis establecida por el lenguaje técnico de programación en uso, éste permite que se establezcan una serie de restricciones. Sin embargo, la aplicación de este control no garantiza el cumplimiento o ejercicio del Derecho como tal, a pesar de sus configuraciones para la restricción en el mapeo Web, no es posible que se limite el acceso al sitio que se está protegiendo mediante el uso de otro sitio Web, es decir, no restringe el acceso al contenido.

En adición y como parte de las limitaciones del control aplicado mediante el archivo robots.txt es que las restricciones contenidas en éste pueden ser ignoradas por algunos motores de búsqueda generando que su control sea ineficiente.

Es importante mencionar, que al efectuar un proceso de implementación de controles, antes se debe establecer todo un proceso de identificación de riesgos y medir así el impacto que podría generar la aplicación de un control.

Según las mejores prácticas, se debe aplicar un estudio costo – beneficio que permita dar a conocer cuál opción es mejor, si asumir un riesgo y no implementar un control por los costos asociados a la implementación o ya sea en la implementación de las medidas correspondientes. Se dice que el valor del control no debe exceder el valor del activo que se está protegiendo. Además, dentro del mismo proceso de análisis de riesgo, debe existir una valoración de los mismos para obtener valores numéricos. Uno de las valoraciones efectuada en el proceso es la medición del riego inherente, es decir, el valor que posee el riesgo sin la aplicación de controles. Cuando ya se hayan aplicado los controles, el proceso debe repetirse, con la diferencia que ahora se obtendrá lo que se conoce como valor de riesgo residual. Se dice que un control es ineficiente al tener como resultado de las valoraciones antes mencionadas el mismo valor. En otras palabras, para que se pueda decir que la implementación de un control ha sido exitosa y que el mismo cumple la función de mitigación, el valor del riesgo residual debe ser menor al riesgo inherente.

Continuando con el papel de los motores de búsqueda, la labor principal al ejecutar la búsqueda, es saber cuáles de los sitios mapeados mediante el proceso de

indexación se deben presentar al usuario como resultado final y para esto además del proceso de revisión de archivos “robots.txt” se ejecutan distintas acciones, entre ellas están: el conteo de las palabras buscadas por cada sitio indexado, la ubicación de las palabras en los sitios. Adicionalmente, se analiza la cantidad de sinónimos de las palabras utilizadas, otra de las características principales es que estos elementos permiten que se brinde un posicionamiento mediante una calificación, proceso al que se le conoce como “pageRank”, el cual se describirá brevemente en la siguiente sección.

5.2.2 PageRank

El “pageRank” es el mecanismo en el cual se mide la importancia de una Web, el buscador clasifica el valor de los sitios en una escala del 1 al 10. Cuando una página Web enlaza a otra, esta transmite un valor, este valor depende del propio Page Rank de la página que enlaza.

La puntuación que brinda este proceso se puede definir de la siguiente forma, asumamos que la página Web A tiene las páginas T1 hasta Tn, que apuntan a ella (es decir, son citas contenidas en las páginas Web). El parámetro d es un factor de “amortiguación[3]” que se puede establecer entre 0 y 1. Por lo general, se fija d a 0.85. También C (A) se define como el número de enlaces que salen de la página A. El PageRank de una página A se da como sigue:

Fórmula: PR (T _ {1}) + PR (T _ {n}) / C (T _ {n}))

A= Página Web PR= PageRank T=Páginas C=Enlaces que se encuentran en A

Los PageRanks forman una distribución de probabilidad sobre páginas Web, por lo que la suma de todas las páginas web de PageRank será uno.

PageRank o PR (A) se puede calcular utilizando un simple algoritmo iterativo, y corresponde al vector propio principal de la matriz de enlace normalizado de la red.

[3]

Además, un PageRank para 26 millones de páginas web se puede calcular en pocas horas en una estación de trabajo de tamaño medio.

Esta actividad es efectuada en una cantidad de tiempo muy corto y por lo general se da como resultado una serie de enlaces o hipervínculos, los cuales podrían estar acompañados de información relevante como por ejemplo, una breve explicación del sitio con la cual el usuario puede definir si ingresa o no al mismo, información de sitios Web similares y recomendaciones de búsquedas que el usuario podría utilizar o podría tener algún tipo de interés.

El mecanismo de búsqueda dentro del proceso utiliza algoritmos matemáticos. Las compañías han trabajado durante años en la optimización de éstos con el objetivo mejorar los tiempos de respuesta y la calidad de la información resultante al efectuar una búsqueda. Google indica que los algoritmos son (…)"fórmulas y procesos informáticos que convierten las preguntas en respuestas." (Google, 2017) Considerando la definición anterior, se puede afirmar que estos elementos forman parte integral del proceso de búsquedas en la Web y que además su optimización permite brindar una respuesta cercana en cumplimiento con las expectativas que el usuario mantiene al efectuar una búsqueda.

En palabras más sencillas y teniendo como referencia lo dicho por el Sr. Alejandro Platero en su escrito "El derecho a ser olvidado":

> *Los motores de búsqueda son robots que desprenden sus tentáculos a toda la información existente en el universo web, con el objeto de facilitar al ciudadano información acerca de cualquier dato que resulte de su interés, sin que el ciudadano tenga que realizar más esfuerzo que hacer clic con el ratón de su ordenador o desde su móvil, tumbado en el sofá de su casa mientras, aburrido, hace zapping. Técnicamente, los motores de búsqueda pueden ser examinados como un "proveedor de contenidos, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado cada una de las empresas que poseen este tipo de servicio, han optimizado estos algoritmos de búsqueda. (Platenero, 2015)*

En ese sentido, del mismo modo que los buscadores, las redes sociales también forman parte del proceso en la aplicación del Derecho al Olvido, éstas se caracterizan por la gran cantidad de datos personales que contienen y además por

el tipo de información contenida. Sus sitios también pueden ser “indexados” o colocados por los mismos motores de búsqueda.

Es necesario que estas aplicaciones tecnológicas sean vistas como un arma de doble filo, por un lado con gran facilidad las personas pueden tener contacto con otras personas alrededor del mundo, efectuar contrataciones, ver fotografías; pero por otro lado y del cual se espera el ejercicio del derecho, ¿qué pasaría si esta información que se encuentra disponible en la Web es utilizada en contra de las personas? Tal como se ha informado en los últimos tiempos a través de los medios de comunicación, los resultados de esta actividad son sumamente agravantes para la integridad de las personas víctimas.

Las redes sociales, a diferencia de los motores de búsqueda, solicitan la aprobación del usuario para el uso de la información, se registra en éstas la responsabilidad, por lo tanto, recae en el usuario que acepta las condiciones propuestas por las redes sociales.

5.2.3 Estándares publicados y controles técnicos

La seguridad de la información, desde el punto de vista del manejo y uso de los datos, establece tres pilares fundamentales para el tratamiento de la misma, estos pilares son: confidencialidad, integridad y disponibilidad. La información hoy es uno de los activos más valiosos en las organizaciones, por lo cual debe ser protegida mediante la implementación y uso de controles técnicos, su nivel de protección se encuentra en un relación estrecha con los niveles que estos pilares contiene para cada tipo de dato.

Entes internacionales, considerando la realidad que vive el mundo en materia de la privacidad y el uso de los datos personales, han publicado una serie de documentos, que ofrecen a las organizaciones con el objetivo de implementar controles y estrategias para abordar el tema con buenas prácticas. En este apartado se mencionará en forma breve algunos de estos documentos. Así mismo se pretende dar una visión técnica con la definición de algunos de los controles técnicos que

pueden ser implementados con el objetivo de apoyar el ejercicio de Derecho al Olvido.

El ISC2, (International Information System Security Certification Consortium), Instituto a cargo de certificar profesionales en seguridad de la información a nivel mundial, define los pilares antes mencionados como:

Integridad: "Se refiere a efectuar esfuerzos para prevenir una modificación no autorizada o inapropiada de sistemas o de información."

Confidencialidad: "Se refiere a efectuar esfuerzos para prevenir acceso no autorizado a la información de personas que no tienen la necesidad o el derecho a consultarla."

Disponibilidad: "Se refiere a efectuar esfuerzos para prevenir la interrupción de servicios en producción." (ISC2, CBK Study 2009, p.4) El siguiente gráfico representa la relación de los principios antes mencionados y los datos:

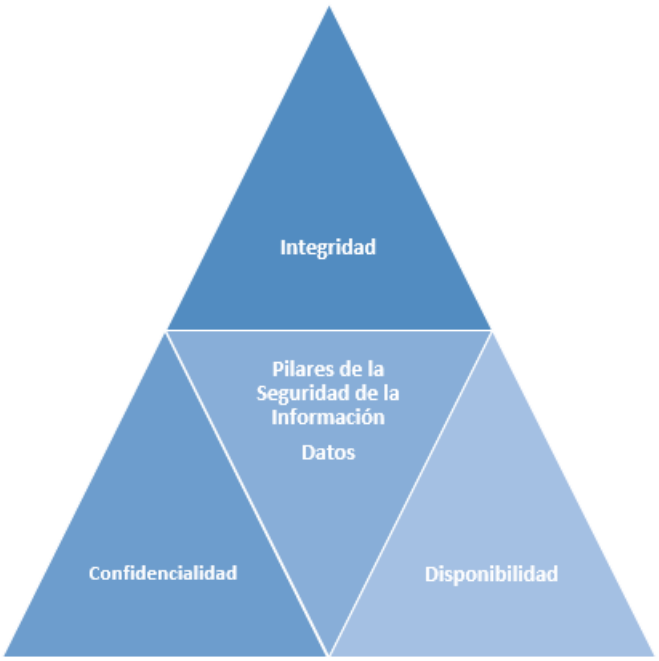


Imagen 2 - Pilares de la Seguridad de la Información – Gráfico creado por autor

Los pilares antes mencionados se ven aplicados en la información de forma proporcional, es decir, la mayoría de las veces, la implementación de un control que

permite mantener la disponibilidad de la información a un nivel alto, conlleva a que los niveles de confidencialidad disminuyan, lo que lleva a que se vean expuestos datos en cierta medida desprotegidos.

En relación con el Derecho al Olvido y el tratamiento de datos privados o de carácter personal, éstos se encuentran bajo los mismos principios, en otras palabras, la restricción del acceso a los datos personales o la cancelación de los mismos, por un lado garantiza el cumplimiento del principio de confidencialidad, pero por otro lado, limita la disponibilidad para su consulta, este hecho puede originar conflictos ante regulaciones relacionadas a la libertad de expresión o principios de acceso a la información.

El Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST por sus siglas en inglés), en la norma "800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", trata a la privacidad como:

> *(…) "La privacidad es mucho más amplia que la simple protección de la confidencialidad de las PII. Para establecer un amplio programa de privacidad que aborde el rango de asuntos de privacidad que las organizaciones pueden enfrentar, las organizaciones deben tomar medidas para establecer políticas y procedimientos que aborden todas las Prácticas Justas de Información. Por ejemplo, al proporcionar a los individuos aviso de nuevas recopilaciones de información y cómo su información personal será utilizada y protegida es fundamental para proporcionar protección a la privacidad y transparencia, no puede tener un impacto significativo en la protección de la confidencialidad de su información personal. Por otro lado, las Prácticas de Información Justa relacionadas con el establecimiento de salvaguardas de seguridad, especificación de propósito, limitación de uso, limitación de recolección y rendición de cuentas son directamente relevantes para la protección de la confidencialidad de la IIP. Como resultado, estos principios se ponen de relieve en todo este documento según corresponda." (…). (NIST Norma 800-122, 2017). (Traducido del idioma Inglés)*

Los entes encargados de la seguridad nacional en países como Estados Unidos, caracterizado por ser un país con gran inversión económica en este ámbito, han dado la importancia en la emisión de las pautas a seguir y han publicado una serie de mejores prácticas que tienen como fin principal dar el sentido para dirigir tratamiento de los datos personales de forma estándar.

En relación con la cita anterior, es importante recalcar cómo el ente establece acciones como la definición de políticas y procedimientos para el manejo de datos personales.

Por otro lado, el Instituto de Normas Británicas (BSI, por sus siglas en inglés) ha desarrollado el estándar internacional ISO/IEC: 29100, con su última publicación en el año 2011, nombrado como "Tecnologías de Información – Técnicas de Seguridad – Marco de Privacidad", dicha norma establece los parámetros necesarios para garantizar el nivel de protección y el tratamiento adecuado a datos sensibles, considerando elementos como las legislaciones vigentes y los controles tecnológicos correspondientes.

La norma se debe implementar bajo lo que se conoce como el ciclo de Deming[4] en el cual es necesaria una correcta planificación, incluyendo una serie de aspectos regidos por la norma (alcance, interesados, política, entre otros).

La implementación de los controles que esta norma dicta se encuentra estrechamente relacionados con los estándares internacionales ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información e ISO/IEC 27002: Control de Seguridad de la Información, que apoyan la gestión del Sistema. Estos estándares marcan la pauta en temas de seguridad de la información a nivel internacional y su implementación genera una serie de beneficios.

Es común ver como empresas se niegan a invertir en adquisiciones relacionadas a la seguridad de la información, principalmente, porque no pueden ver retorno de inversión o ganancias a corto plazo. A continuación se presenta mediante el uso de un gráfico, algunas de las clausulas incluidas en los estándares antes mencionados:

[4]El ciclo de Deming (de Edwards Deming), también conocido como círculo PDCA (del inglés plan-do-check-act, esto es, planificar-hacer-verificar-actuar) o espiral de mejora continua, es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhar

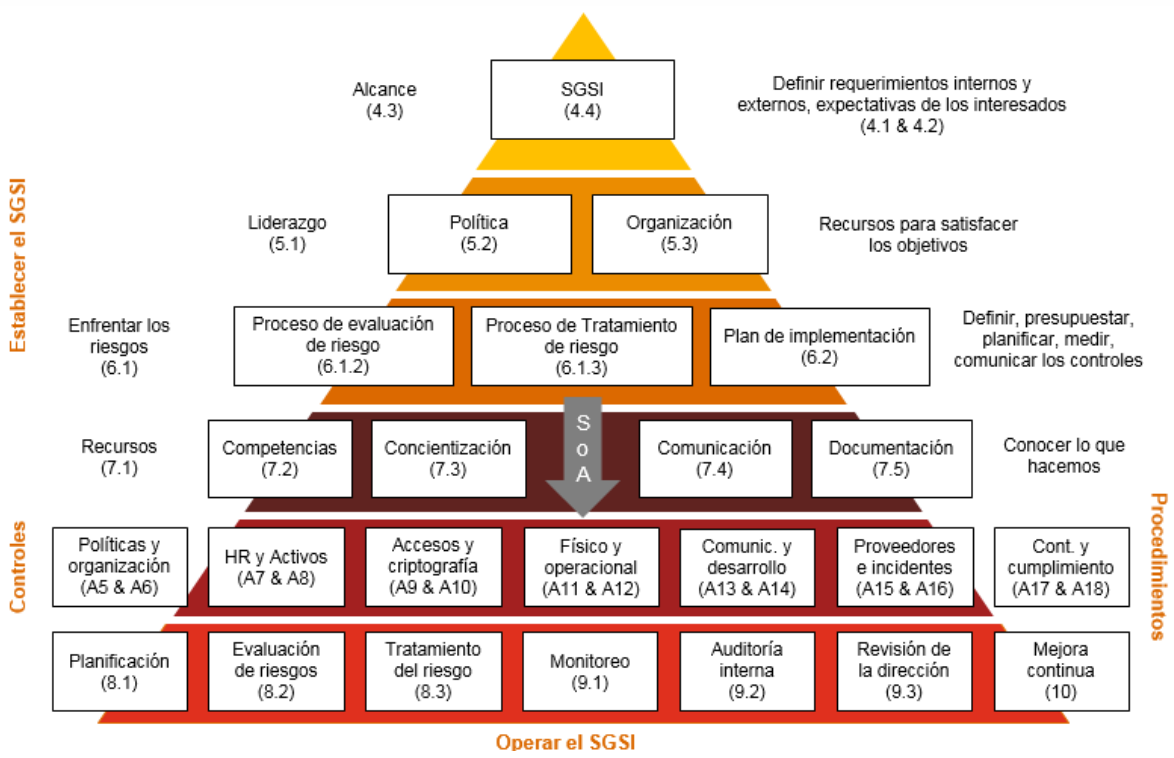


Imagen 3 – Sistema de Gestión de Seguridad de la Información, fuente PricewaterhouseCoopers

Por lo general las empresas cuentan con un modelo de seguridad poco maduro y se ve reflejado con el diseño de los procesos, no poseen un mecanismo de trabajo bajo normas de seguridad de la información y sus acciones son reactivas, en otras palabras, actúan bajo una situación presentada en la que sus datos se han expuesto producto a la explotación de vulnerabilidades o debilidades en su accionar.

Es importante recalcar que los documentos antes mencionados no pertenecen a una regulación o legislación de cumplimiento obligatorio como tal, son mejores prácticas que la industria ha desarrollado con el análisis del comportamiento y con la disponibilidad de los controles técnicos actuales.

Algunos controles técnicos

Como parte de los controles técnicos disponibles, además de todo el diseño de infraestructura basada en estándares que pueden ser utilizados para crear por parte de los administradores arquitecturas seguras y además del uso de restricciones técnicas definidas como ya se mencionó, en los archivos “robots.txt”, se encuentra la aplicación de medidas que tienen el mismo objetivo, limitar que la información

contenida en su sitio sea mapeada o indexada por los motores de búsqueda, dentro de las acciones se encuentra el uso de lo que se conoce como “Metadados” o “MetaEtiquetas.”

Metadatos

Estos componentes permiten, bajo la correcta configuración, que se efectúe una restricción de acceso a datos previamente definidos. Las meta etiquetas se encuentran disponibles, brindar instrucciones de protección de datos a los buscadores y que excluyan la información que se restringe de sus índices o bien hacer que la misma se encuentre disponible por un lapso de tiempo definido.

Desde la configuración técnica, las meta etiquetas puede ser utilizadas bajo la utilización de parámetros de restricción como lo son: “noindex” en la cual se restringe por completo la indexación del dato o bien mediante el uso del parámetro: “unavailable_after” (disponibilidad por tiempo) que permite establecer una fecha a partir de la cual un contenido determinado no debe aparecer enlazado en los resultados de los buscadores.

La mayoría de las etiquetas utilizadas se colocan en la sección head[5], elemento que forma parte del sitio Web y se encuentra programado bajo la sintaxis del formato HTML, de la siguiente manera: “<meta name="robots" content="noindex">”, éstas son configuraciones que se pueden implementar durante el desarrollo, si así lo considera el administrador técnico o bien durante la etapa de producción.

Además del estos elementos, existe la posibilidad de efectuar la implementación de otro control técnico adicional. Es factible efectuar un bloqueo de lo que se conoce en informática como URL. Google establece la siguiente indicación en relación a la implementación de este control:

> *“…si tienes contenido privado o confidencial que no quieres que se muestre en los resultados de Búsqueda de Google, la forma más sencilla y eficaz de bloquear URL privadas para que no se muestren es guardarlas en un directorio protegido con contraseña en el servidor del sitio. Ni el robot de Google ni el resto de*

[5]El elemento HTML <head> provee información general (metadatos) acerca del documento, incluyendo su título y enlaces a scripts y hojas de estilos. (Mozilla, 2017)

rastreadores web pueden acceder al contenido que se encuentra en directorios protegidos con contraseña." (Google, 2017)

Dicha protección se efectúa mediante la protección de los archivos que se encuentran en el servidor y que responden a las fuentes del sitio Web, específicamente en el file o carpeta en la que se almacena.

El hecho de que existan medidas de protección y que se encuentren disponibles una serie de mejores prácticas para la estandarización de los procesos, podría trasladar la totalidad de la responsabilidad para el ejercicio del derecho en los motores de búsqueda, sin embargo también como se ha presentado, hay una programación, configuración y administración por parte de los editores o encargados de administrar los sitios Web. En otras palabras, los responsables de administrar y dar mantenimiento técnico tienen a su disposición la opción de dar indicaciones a los buscadores en Internet de la información determinada para ser restringida en su indexación.

Según información obtenida de la firma internacional de consultoría PricewaterhouseCoopers, las organizaciones se encuentran en la tendencia de buscar mecanismos para proteger la privacidad y tratar este tema desde el ámbito de la seguridad con un alto sentido de prioridad, según esta compañía, las empresas se encuentran trabajando para adoptar medidas innovadoras de seguridad en temas de seguridad digital y de privacidad para manejar las amenazas con el objetivo de lograr ventajas competitivas, esto quiere decir que las consecuencias de incumplir con legislación puede generar pérdidas millonarias en sanciones, pero además, la pérdida de reputación al ser objeto de escándalo en los medios. Para ello, están pensando más ampliamente en la ciberseguridad y la privacidad como protectores y facilitadores para la empresa, socios y clientes.

Finalmente, las medidas de seguridad deben ser impulsadas por los responsables de mantener los archivos de datos y su tratamiento, para ello se debe adoptar medidas técnicas y organizativas que eviten el mal uso y/o alteración de los datos.

5.3 Apartado III. Retos tecnológicos para el cumplimiento del Derecho al Olvido

Como parte de la tecnología que se encuentra disponible y producto de la adaptación de la misma en la suplencia de necesidades han surgido nuevas tecnologías que ponen a prueba como un reto más a la regulación y a los controles tecnológicos que se han diseñado con el fin de garantizar el ejercicio del Derecho al Olvido. Se describirán los siguientes desafíos tecnológicos, debido a que éstos son de influencia directa, además, se su poco conocimiento por parte de la población.

5.3.1 Blockchain o cadena de bloques

Uno de los retos que la tecnología ha interpuesto por las características que posee, denominado “BlockChain” o en castellano “Cadena de Bloques.” El tema aún sigue dando de qué hablar, ya que su aparición en el medio sigue siendo relativamente reciente.

Para comprender de una mejor manera tal afirmación, a continuación se presentará una breve descripción del funcionamiento de dicha tecnología, así como su papel en un futuro próximo en relación con el Derecho en estudio. El blockchain es una tecnología que nace en el año 2009, a partir de la red utilizada para acuñar y efectuar transferencias mediante la moneda virtual “BitCoin[6]”, es la combinación de una serie de principios matemáticos, criptográficos y económicos que tiene como fin mantener una base de datos con participación de múltiples participantes sin la necesidad de ningún tercero validador o reconciliación, dichas características serán ampliadas.

Su mecanismo de seguridad es tal, que se han registrado bancos a nivel mundial que han empezado a utilizarla para poder asegurar sus transacciones virtuales. Es decir, esta tecnología es utilizada para distintas actividades pero en su mayoría por

[6]Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. (Bitcoin.org, 2017)

el sector financiero, con el objetivo de verificar que los movimientos bancarios a través de medios tecnológicos o virtuales, son o hayan sido alterados.

La plataforma sobre la cual se construye el principio de esta tecnología, se encuentra diseñada de manera tal que permite a los usuarios escribir con seguridad la información mientras se mantiene una historia constante de la información previamente registrada y de las interacciones que se efectúan durante el proceso. En ese sentido, su principio es, y de forma metafórica, “escribir en piedra”, dado que lo que se incluye en esta cadena, no puede ser modificado, incluyendo datos personales.

Esta tecnología se compone de una red de equipos que trabajan de manera colaborativa, la misma cumple con características que permiten que su utilización sea segura, una de éstas es que es “descentralizada”, debido a que no existe un repositorio central ni se encuentra ejecutando sus procesos en equipos físicos (hardware) centralizados, esto permite que exista una interacción entre los miembros de una red sin que se presenten inconvenientes como retrasos en la comunicación.

La red antes mencionada se encuentra compuesta de lo que se han denominado “Nodos” y corresponden a programas o sistemas informáticos que se encuentran ejecutando en equipos de cómputo, cada uno de estos nodos, tiene la responsabilidad de verificar que la información nueva sea válida, la estructura está diseñada para permitir que exista comunicación entre ellos y que cuando se presente un ingreso de información nueva, sea analizada, así cuando no es aceptada por uno de los elementos, sea conocido por todos los demás, este proceso se caracteriza por la ausencia del ser humano para su ejecución, es decir, es automático.

El Blockchain posee además, la característica de ser “inmutable”, es decir, una vez escrita, no se sobre-escribe. En todas las plataformas blockchain, se toman medidas para asegurar este principio. Es por esta característica precisamente, que se ha establecido esta investigación como un reto para el cumplimiento del ejercicio al Derecho al Olvido.

Además, dicha tecnología cumple el principio de ser “transparente”, esto quiere decir que los nodos que componen la tecnología contienen un registro completo de las transacciones registradas.

El siguiente gráfico representa las características mencionadas:

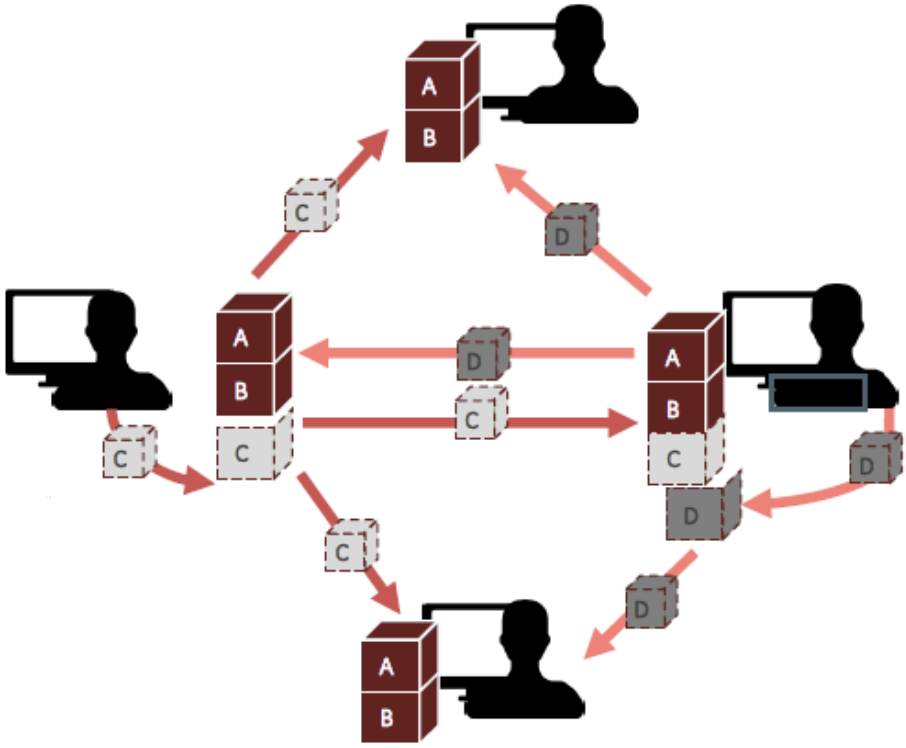


Imagen 4 – Gráfico proceso Blockchain (Fuente: PricewaterhouseCoopers)

Tal como se puede apreciar en el gráfico anterior, los participantes de la red (nodos) contienen la misma información (transparencia), al ejecutarse una nueva modificación de la cadena de datos, incluyendo a “C” y a “D”, esta nueva información es validada y replicada al resto de miembros.

Funcionamiento de los nodos

En el funcionamiento interno de los nodos participan una serie de elementos, entre éstos los “Key”, los cuales representan el identificador único para cada usuario del blockchain y se utilizan en las transacciones efectuadas para agregar información a la cadena.

Los nodos poseen funciones que permiten la correcta ejecución del proceso, estos componentes tienen la capacidad de crear los “Key” antes mencionados, mediante la utilización de algoritmos matemáticos, dichos algoritmos se encuentran basados en lo que se conoce como función “hash”, existen varios tipos de funciones hash, algunos de los más utilizados son: SHA1, Md5. Este proceso permite convertir los datos puros o en texto plano en una serie de letras y números que no son posibles de leer por un ser humano. Se caracteriza porque cuando se utiliza un mismo tipo de función hash, por ejemplo SHA1, el resultado al aplicar esta función a un dato, siempre será el mismo, esto permite identificar cuando hubo o no una alteración en un dato a lo largo de la cadena, este proceso se aplica a cada dato que se pretende registrar. Este proceso se puede representar de forma gráfica de la siguiente manera:

El funcionamiento de las llaves o keys, se efectúa mediante el uso de

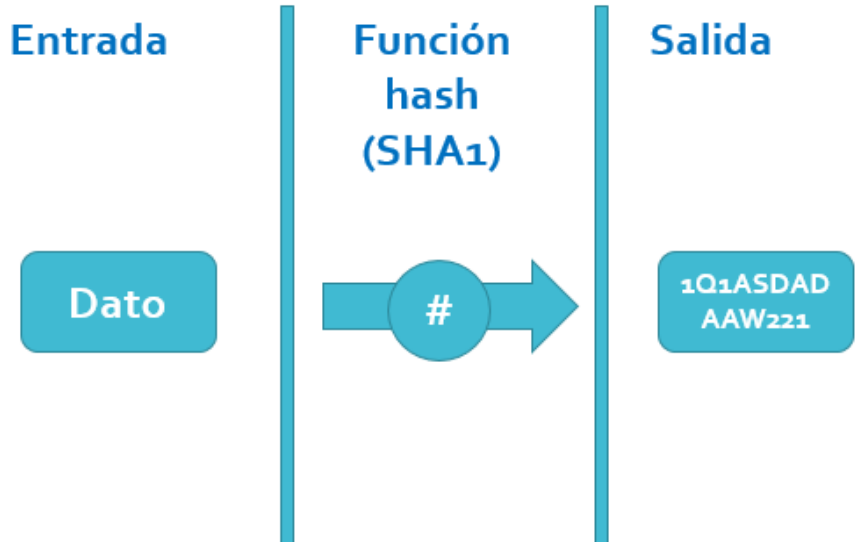


Imagen 5 – Proceso de encripción de datos (Creada por el autor)

algoritmos de encripción y el uso de lo que se conoce como llaves públicas y privadas, esto permite que se efectúe un intercambio de datos entre pares y la lectura de datos entre éstos, sea confiable. A esta estructura se le denomina cifrado

de llave pública por su funcionamiento. El objetivo principal de este mecanismo es la creación y uso de certificados firmados digitalmente con estas llaves.

En el proceso se utilizan dos tipos de llave o clave, la primera es la pública, llamada así porque es compartida de forma pública y por otro lado se encuentra la llave privada que sólo conoce el emisor o creador de la información. El inicio del proceso consiste en aplicar un algoritmo de encripción a la llave privada para generar la llave pública, posterior a este paso, se vuelve a aplicar otro proceso de encripción para generar una dirección, ésta funciona como una forma abreviada de un identificador único, unido a la clave pública y privada.

Es importante mencionar que debido al proceso recién descrito, la seguridad Blockchain se basa en la fuerza o robustez de la llave privada, por lo que su protección es sumamente importante, si esta está comprometida, es posible que un atacante pudiese actuar como si fueran un usuario autorizado.

Otro componente del blockchain son las transacciones, las cuales forman parte de las entradas del proceso, es por eso que se dice que dicha tecnología posee una estructura transaccional, es en este paso en el cual se efectúa un registro de los datos en la cadena, se efectúa además una firma digital de la transacción y una marca de tiempo. El proceso de firma se efectúa mediante uno de los algoritmos más comunes para tal fin, el algoritmo se llama firma digital de la curva elíptica (ECDSA[7]). Las implementaciones de ECDSA aceptarán la clave privada del usuario y un hash de sus datos para crear el mensaje firmado. Posteriormente, este mensaje firmado se utiliza para verificar que el mensaje fue enviado a la cadena de bloque por el usuario adecuado.

Los nodos además poseen la importante función de validar la información, a este proceso se le denomina “Consenso y Verificación”, en esta paso cada nodo debe comprobar para asegurarse de que la información está bien y verificar que los otros nodos están de acuerdo con el registro.

[7]Elliptic Curve Digital Signature Algorithm es una modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA (problema del logaritmo discreto). (Wikipedia, 2017)

La comunicación entre nodos es esencial durante el proceso, éstos se comunican a través de protocolos de red relativamente estándar (TCP, RLP, etc.). Transmiten transacciones firmadas o bloques como parte del protocolo de consenso antes mencionada.

Con las transacciones firmadas, se está enviando lo que se necesita para el proceso de verificación (clave pública, mensaje hash, mensaje firmado) y con los bloques se están enviando el conjunto de transacciones y otros “metadatos” utilizados para el protocolo de consenso. Los nodos tendrán una lista de direcciones IP de nodos en su red desde la que enviarán y recibirán transacciones y bloques, esto como medida de protección.

Los nodos de la red reciben transacciones de todos los demás nodos miembros. El nodo receptor deberá comprobar que las transacciones recibidas están firmadas por la clave privada asociada con la dirección del remitente de la transacción.

Sin embargo, el nodo receptor no tiene acceso a la clave privada del firmante. Aquí es donde se utilizan las propiedades de la firma de clave pública. Para comprobar la validez de la firma, el nodo necesita los siguientes elementos:

1- El hash de los datos sin procesar del mensaje
2- La clave pública que se derivó de la clave privada del remitente
3- El mensaje firmado, producido en el paso de firma digital por la el remitente. Estos tres elementos se pasan al algoritmo de verificación (paso de verificación ECDSA). El algoritmo indicará si la firma ha sido firmada correctamente o firmada incorrectamente. Si está firmada correctamente, la transacción se agregará a la lista de transacciones que el nodo desea agregar al siguiente bloque.

Esta breve descripción del funcionamiento del blockchain ha sido para poner sobre la mesa un reto importante que tendrán los entes encargados de velar por el cumplimiento del Derecho, esta tecnología vuelve casi imposible la cancelación de los datos una vez registrados en los bloques o cadenas de información, desde esa

perspectiva y como se ha establecido en este documento, el ejercicio del Derecho va más allá que la promulgación de una ley.

Desde el punto de vista técnico y tomando como referencia el funcionamiento de esta tecnología es casi imposible hacer valer el principio aplicado por el Derecho al Olvido, en caso de tener que eliminar información o datos privados, los credenciales usados para el uso de una cadena de datos podrían verse vulnerados por atacantes.

Existen dos caminos posibles para estos efectos, en primer lugar corresponde a la eliminación de las cuentas de acceso a la cadena, dicho paso sería vulnerado mediante la identificación de los datos utilizando lo que en informática se conoce como ataques de fuerza bruta o de diccionario.

Por otro lado, se podría diseñar un proceso de cadenas de datos editables, perdiendo el sentido de protección y de rastreo que ofrece hoy el blockchain.

Finalmente, y según lo indica la Agencia de Protección de Datos de Costa Rica, el Derecho al Olvido no puede ser garantizado utilizando sólo medios técnicos es importante que se efectúen otro tipos de esfuerzos, el ser humano por naturaleza mantiene ciertos comportamientos, el control de los datos privados en medios tecnológicos como la Internet es casi una tarea imposible, por lo que el cumplimiento o ejercicio del Derecho se ve en riesgo, tal como le menciona Javier Mieres en su escrito “El derecho al olvido digital”:

> *“Ante la insuficiencia de las soluciones tecnológicas, el debate sobre cómo impedir “la configuración de una historia lineal e ininterrumpida de la persona” en la red o, al menos, facultar al individuo para controlar el grado de trazabilidad de su vida en línea se ha articulado bajo el nombre de derecho al olvido. La denominación puede resultar equívoca, por excesiva. La limitaciones humanas para recordar no son trasladables a un entorno tecnificado como el mundo digital. Como ha advertido ENISA, en un sistema abierto y global como Internet es técnicamente imposible eliminar todas las copias que pueden existir de una información o unos datos (ENISA, 2011:8). Sin embargo, aunque el olvido digital no sea totalmente practicable, mantener la denominación de derecho al olvido tiene la ventaja de que, por la carga emotiva que conlleva la palabra, es capaz de atraer la atención de la opinión pública sobre los intereses subyacentes merecedores de protección.” (Mieres. J, 2014)*

En otras palabras y haciendo referencia a la cita anterior, a pesar de que se implementen los controles necesarios desde el punto de vista tecnológico, es necesario complementar y desarrollar una legislación apta, tal como lo veremos en el siguiente apartado, se han establecido acciones legales que protegen al ciudadano en pro del ejercicio del Derecho.

5.3.2 Data Brokers

En estrecha relación con los navegadores Web, se presenta a continuación una breve descripción de la tecnología denominada “Data Brokers” o también conocidos como corredores de datos. En la actualidad es común ver cómo tecnologías como los navegadores Web y las redes sociales nos “bombardean” con publicidad que es dirigida con el objetivo de que podamos acceder y consumir o adquirir un servicio. Es impresionante como esta información se encuentra tan estrechamente relacionada a búsquedas, compras, enlaces, a los que hemos efectuado con anterioridad.

Las compañías que se encargan de brindar servicios y utilizan la Internet como medio para su distribución y publicidad buscan conocernos, quieren saber cuáles son nuestros gustos y preferencias. A partir de este hecho, es por medio del uso de la tecnología que nacen las empresas recolectoras de datos o conocidas como Data Brokers, las cuales por medio la utilización de algoritmos y herramientas tecnológicas recopilan datos que producimos con la interacción y el uso de medios digitales como lo son los navegadores Web, sitios de compra y además mediante las redes sociales.

Según el periodista Alberto Luna, del periódico digital El Confidencial, Data Broker se puede definir como:

> *“Los llamados data brokers son compañías que se dedican a recabar y vender información personal, generalmente sin consentimiento ni conocimiento de los usuarios. Lo saben prácticamente todo. Sin embargo, no sabemos nada de ellas.” (Luna A., El Confidencial, 2014)*

Como se referencia en la cita anterior, la misión de estas compañías es la recopilación de datos y buscan además lucrar, mediante la venta de los mismos. Se

debe recalcar de esta definición, que la mayoría de las veces el proceso de recolección de estos datos se efectúa sin el debido consentimiento de los usuarios que utilizan la tecnología intermediaria, este punto viene a incumplir requerimientos establecidos por la legislación desarrollada con el objetivo de proteger el uso y tratamiento de datos personales, mismo que será ampliado con la descripción de las leyes y su reglamento en el apartado siguiente de este documento.

Desde el punto de vista tecnológico, en el proceso de recolección de datos participan distintos elementos, según lo establece la siguiente definición, aportada por el periodista Muñoz 2014:

> *"son los grandes beneficiados del negocio de las bases de información en internet. Su trabajo consiste en conocer la vida de los navegantes sin que ellos se enteren- o al menos sin que les importe, ¿cuántas veces ha cerrado la pestaña de que dice nueva política de cookies o ha ignorado las condiciones y términos de uso?- para luego venderlos." (Muñoz, 2014)*

En primera instancia, hay que considerar que detrás de esta actividad hay un negocio, una forma de buscar ganancias económicas con nuestros datos. En relación a las ganancias que podrían generarse, el periódico digital El País, en uno de sus artículos, menciona:

> *Un equipo de investigadores de Amnistía Internacional (AI) revela la oferta por parte de una de estas empresas, Exact Data, de los datos de 1,8 millones de musulmanes por 138.380 dólares (126.851 euros), es decir, a razón de 7,5 centavos (7 céntimos de euro) por persona. La compañía en cuestión, "presume de tener una base de datos total de 200 millones de contactos de Estados Unidos que se pueden filtrar mediante 450 categorías, tales como religión y etnia", detalla el informe y ha podido comprobar este periódico en la propia web. (El País, 2017)*

La mayoría de estas compañías no informan de su actividad, por lo que es muy probable que conozcan mucha de nuestra información personal y nosotros no conozcamos en absoluto lo que está sucediendo.

Bajo esta premisa y considerando el uso de lo que se ha denominado como "cookies", es un código permanente colocado en un archivo en el disco duro de una computadora por un sitio web que el usuario de la computadora ha visitado. El

código identifica de forma exclusiva, o "registra", a ese usuario y se puede acceder a él por el número de fines de marketing y seguimiento de sitios.

En términos generales, las cookies o galletas por su traducción en español, son archivos pequeños que se instalan en el navegador del computador o en el medio tecnológico utilizado para el ingreso a un sitio Web en Internet. Una de sus funciones es almacenar información relacionada a las sesiones del usuario en un sitio determinado o los artículos en un carro de compras utilizado en un sitio de compras. Se dice que este componente facilita la interacción del usuario con el sitio Web en el que se encuentra navegando, ya que su utilización reduce en manera considerable los tiempos de respuesta y procesamiento de datos que se produce por defecto. Por otro lado, su creación permite que se brinde un servicio personalizado a cada usuario, las configuraciones y gustos o preferencias son distintos entre los mismos.

Desde el punto de vista técnico, existe un proceso de comunicación entre los protagonistas denominados cliente (la persona que consulta un sitio Web) y el servidor (equipo que hospeda el sitio Web). La comunicación se efectúa por medio de protocolos de comunicación, como el uso del protocolo HTTP (Hypertext Transfer Protocol). En el momento usuario acceder al sitio se están utilizando cookies de manera automática y casi de manera transparente al usuario. La petición o solicitud de acceso del cliente al servidor activa de inmediato un parámetro en una de las cookies. Tal como lo define el Sr. Ramón Saquete (2013):

> *"Una cookie está formada por una clave que le da nombre y un valor asociado, que se puede crear, modificar o borrar tanto en el cliente como en el servidor y que una vez creada se envía en cada petición HTTP, de cada archivo, como parámetro de este protocolo. El nombre de cookies se deriva del término informático magic cookie, que define a la información que se envía y se devuelve igual en cada petición." (R, Saquete, 2013)*

Las cookies se encuentran asociadas a un usuario mediante la asignación de identificadores que permiten garantizar al sitio Web que se encuentra

interactuado con él. Según la referencia anterior, el proceso se efectúa mediante el uso del protocolo HTTP, el cual se define por CISCO[8] como:

> *El Protocolo de transferencia de hipertexto (HTTP) es un protocolo común que rige la forma en que interactúan un servidor Web y un cliente Web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor Web implementan el HTTP como parte de la aplicación. HTTP se basa en otros protocolos para regular la forma en que se transportan los mensajes entre el cliente y el servidor. (CISCO, 2017)*

Durante el proceso, como lo establece la compañía CISCO, existe un intercambio de información, desde el cliente (usuario), efectuando una petición a un sitio Web, mediante el uso de un dominio. En este intercambio de datos se da la instalación de las cookies que la página Web va a utilizar.

El siguiente gráfico representa mediante un ejemplo de acceso a un sitio Web, la comunicación existente entre cliente y servidor:

[8]Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

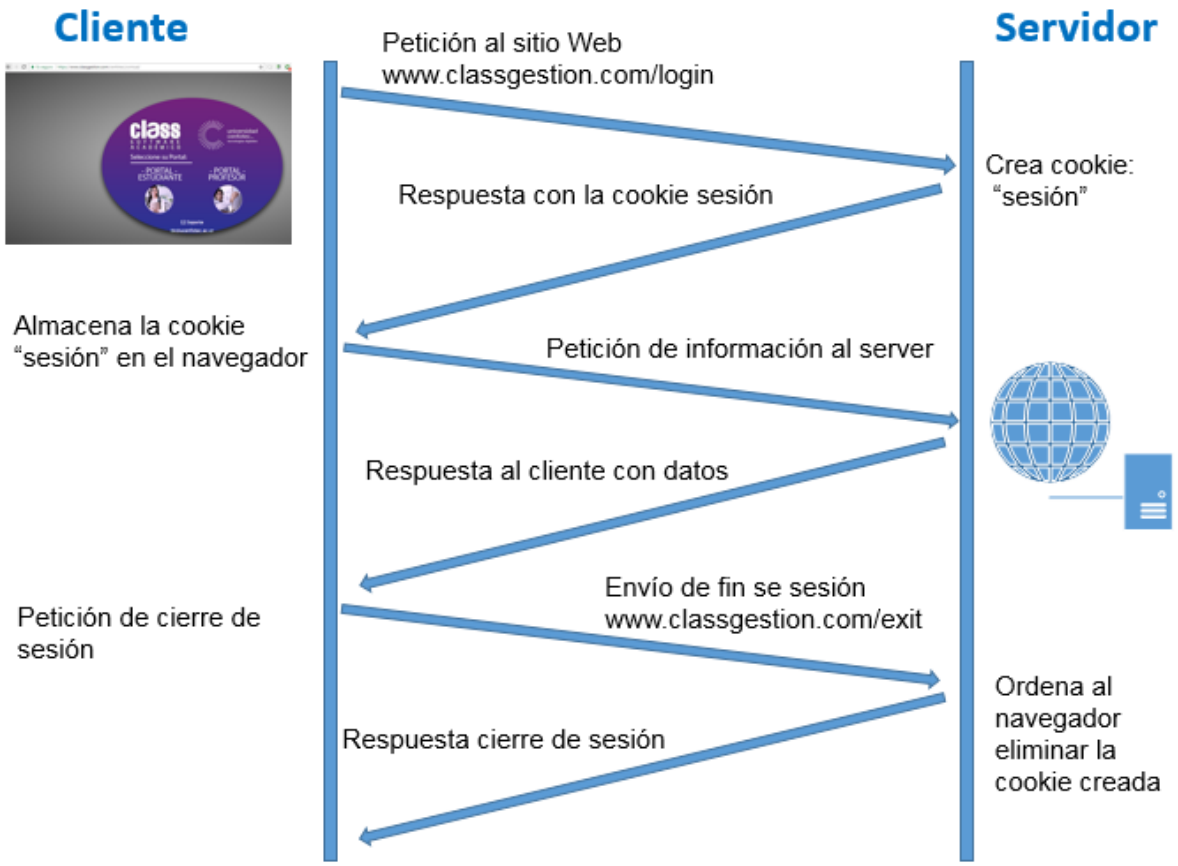


Imagen 6 –Comunicación cliente y servidor Web – Creada por el autor

Las cookies se encuentran separadas además en dos grandes categorías, por un lado las persistentes y por otro lado las no persistentes. Se les llama persistentes, si poseen tiempo de expiración y si no lo tienen, se borran en el momento en que se cierra el navegador. Las no persistentes son las que se utilizan para mantener la sesión del usuario abierta, ya que el equipo que funciona como servidor y gracias al identificador de la cookie, a qué usuario pertenece cada sesión abierta en memoria.

Los sitios que utilizan esta tecnología, por lo general poseen mecanismos de registro y de sesiones, en el cual el usuario de registra o ingresa a una cuenta previamente creada, con el fin de identificarse ante el servicio Web, de esta manera, si tuviese que ingresar a una sección restringida en el mismo sitio Web, evita que tenga que ingresar nuevamente sus datos de acceso, del mismo modo, en caso que por el tipo de perfil se encuentre utilizando en un momento

específico, se podría encontrar con zonas restringidas, de esta manera se bloquearía su acceso, adicionalmente, Google utiliza este tipo de tecnología para obtener datos estadísticos y poder brindar datos procesados a los dueños del sitio al que se ha ingresado.

En la teoría, cada sitio Web genera sus propias cookies y por lo tanto el acceso y uso de las mismas solamente es permitido que se ejecute por el creador, a pesar que en el navegador utilizado se encuentren almacenadas cookies de otras páginas Web o servicios.

Existen dos tipos de cookies, las propias y las de terceros, las cookies de terceros se originan cuando el sitio Web que estamos utilizando necesita información que es brindada por otra página Web, éstas son utilizadas por lo general, para efectuar un registro de la actividad del usuario en el momento de navegar, son las que recopilan los datos necesarios para posteriormente brindar recomendaciones basadas en nuestros hábitos de navegación además de otras actividades como registros estadísticos, entre otras.

Es posible implementar acciones para bloquear el consumo de nuestros datos, mediante las cookies de terceros. Los navegadores poseen mecanismos de configuración de la privacidad. Dichas configuraciones difiere según el proveedor del servicio de navegación (Google Chrome, Mozilla FireFox, Explorer, entre otros) y no se encuentra configurada por defecto, por lo se recomienda al usuario aplicar las configuraciones necesarias, con el fin de mantener los niveles de privacidad correspondientes.

Es importante mencionar que los datos obtenidos por medio de las cookies se consideran de carácter personal, eso significa que se aplican las medidas de legalidad correspondiente.

Alguno de los sitios Web que utilizan este tipo de mecanismos para la obtención de información, utilizan políticas para el uso de cookies y el consentimiento informado, de esta manera el usuario puede habilitar a dicha tecnología a cumplir con su función. Al aceptar este consentimiento, el usuario habilita a qué

sitio pueda obtener su información. Es importante mencionar que el simple hecho de continuar en el sitio que ha solicitado aprobar el uso de cookies, aún sin haber aceptado la política, confirma que se está de acuerdo y que por lo tanto se puede obtener la información.

Las cookies no son el único mecanismo para la recolección de datos por parte de los data brokers, además se utiliza la información recopilada mediante los dispositivos móviles, datos como los lugares que se frecuentan, mediante la geolocalización, comportamientos del usuario por el tipo de aplicación utilizada entre otros, forman parte de la información que puede ser recopilada por estas compañías. Los indicadores abarcan la posición GPS (Sistema de Posicionamiento Global), las aplicaciones instaladas, el sistema operativo, el movimiento del usuario por la web, sus amigos en las redes sociales, etc.

El objetivo es recrear un perfil incluso de quienes no tienen una historia financiera, el tipo de cliente al que la banca tradicional deniega créditos y ofrece tipos de interés más bien altos.

Cada vez que utilizamos un sitio que pretende obtener información mediante este tipo de mecanismos, es sumamente importante conocer las políticas y leerlas para comprender cuál será el uso de los datos obtenidos por esta tecnología, así lo establece:

> *"Para fortalecer estas funciones es oportuno que los avisos legales incluyan formatos en los que de forma visual se facilite la información a los usuarios de los proyectos digitales sobre el alcance de las diversas cláusulas del aviso legal.*
>
> *Actualmente, bajo la etiqueta de aviso legal o condiciones de uso se engloban aspectos muy diversos que incorporan cláusulas relativas al contenido de la página web, a la calidad de la información difundida y su reutilización, a la protección de los datos personales y, en particular, al uso de galletas o cookies, a la responsabilidad por los servicios prestados, a la propiedad intelectual o a la seguridad."(Alguacil M., 2017)*

La necesidad de conocer por parte de las compañías permite ofrecer servicios dirigidos a grupos de la sociedad, ya sea por edad, personas de una región demográfica o como parte de la solución a un problema, como es el caso del sector salud.

No hay duda de que los riesgos asociados con la protección de datos es una tarea complicada y aún más cuando existen grandes cantidades de información personal. Un desafío adicional en el mundo que se presenta actualmente son las sofisticadas soluciones tecnológicas analíticas las cuales en combinación con Big Data y la falta de conciencia por parte de los usuarios incrementan los riesgos relacionados al uso y tratamiento.

Esta es otra dimensión de *Big Data,* concepto que no formará parte de esta investigación*,* es su uso para el descubrimiento de conocimiento mediante la aplicación de técnicas de minería de datos. El descubrimiento del conocimiento, permite obtener nuevos datos que no se conocían previamente. Cuando este descubrimiento involucre información acerca de una persona y esa información se usa con un propósito no previamente identificado y sin consentimiento surge, como ya se ha planteado, un problema de privacidad. El descubrimiento del conocimiento puede ser problemático debido al hecho que la persona no puede saber que la información existe, mucho menos que está siendo analizada y utilizada por otros.

Para concluir con esta breve descripción, Gartner, en su sitio Glosario de términos, establece que una data bróker es:

> *"… es un negocio que agrega información de una variedad de fuentes; Lo procesa para enriquecerla, limpiarla o analizarla; Y las licencias a otras organizaciones. Los intermediarios de datos también pueden licenciar los datos de otra empresa directamente o procesar los datos de otra organización para proporcionarles mejores resultados. Normalmente se accede a los datos a través de una interfaz de programación de aplicaciones (API), y con frecuencia implica contratos de tipo de suscripción. Normalmente, los datos no se "venden" (es decir, se transfiere su propiedad), sino que se autoriza para usos particulares o limitados. (Un intermediario de datos también se conoce a veces como un intermediario de información, un corredor de datos sindicado o una compañía de productos de información)." (Gartner, 2017)*

Si las compañías utilizan datos que han sido recolectados de fuentes que no conocemos, qué mecanismo les garantiza a estas compañías que toda esta información es actual y desde nuestro actuar, de qué forma puedo corregir la información en caso que no sea real.

Es impresionante la gran cantidad de información que se espera recopile esta tecnología, como lo ha descrito el periódico Libertad Digital:

> *Llegará un momento en que alguien registre cada foto que uno tome, cada libro que lea, cada texto que escriba y cada compra que haga. Habrá empresas almacenando datos sobre la actividad física de las personas gracias a los wearables e infiriendo conclusiones sobre su salud; proliferarán las bases de datos de genomas personales y los teléfonos móviles podrán calcular cuándo una persona está deprimida, si podría desarrollar una incipiente diabetes y si comienza a mostrar síntomas de alzhéimer. Harán falta gran dosis de transparencia y sólidas garantías de la privacidad.*
>
> *Este mundo está empezando a tomar forma. Mapfre ya comercializa un seguro para jóvenes que utiliza un dispositivo GSM/GPRS para evaluar su estilo de conducción. El sistema envía diariamente información de los tipos de vía por los que el joven transita, los horarios, los kilómetros recorridos, los excesos de velocidad... Según la compañía, un estilo seguro se traduce en una prima de hasta el 40 por ciento en el precio de la póliza. Es una buena oportunidad para los jóvenes, cuyos seguros son caros, y para la aseguradora, que puede ofrecer mejores precios que la competencia. (Diario Web Libertad Digital, 2015)*

Sin duda el desconocimiento por parte de los usuarios apoya el objetivo de esta tecnología, es importante que se efectúe la lectura de las políticas de uso de cookies de los sitios Web a los que se accede y estar de acuerdo con las mismas, considerar las consecuencias que puede tener el mal uso de los datos.

5.3.3 Deep Web – Dark Web

Ambas son tecnologías que han dado de qué hablar en la actualidad, en primera instancia por el sentido de desconocimiento en la población en general y en un segundo plano por la falta de control o regulación que se mantiene sobre las mismas.

La primera nombrada como la **Deep Web** o Internet profunda por su traducción al castellano, es definida por María Bautista, en su artículo “Aproximaciones a la ciber irresponsabilidad”:

> *“La Deep web o Hard web es una parte gigantesca de las plataformas virtuales indetectables donde ocurren ciberacciones que tienen como precedente el ocultamiento de la identidad del usuario y han dado pie a la tergiversación del concepto de persona y a la utilización de la web de una manera irresponsable —*

en algunos casos— para causar desazón, para perseguir o a veces hackear bancos, entidades y cuentas privadas." (D, Bautista)

Como bien lo referencia la autora en la cita anterior, al hablar de esta tecnología, lleva a pensar en hechos ilícitos, los cuales no poseen monitoreo y control por las entidades encargadas en los distintos países. En este nuevo mundo se encuentran, en relación con el ejercicio al Derecho al Olvido, datos de cada uno de los ciudadanos, posiblemente lucrando con los mismos o efectuando algún tipo de actividad de la cual no se tiene idea.

La segunda, denominada como **Dark Web**, usa pequeños repositorios que forman parte de la Deep Web y además transmite sus comunicaciones encriptadas para asegurar el principio de privacidad y oscuridad en las mismas. Es el ambiente ideal para personas mal intencionadas como terroristas y hackers que se encuentran a la espera de un descuido para cometer sus actos.

La siguiente imagen, tomada de la compañía PricewaterhouseCoopers, representa mediante el uso de un iceberg o isla de hielo, la proporción que puede ser accedida en referencia al contenido Web:

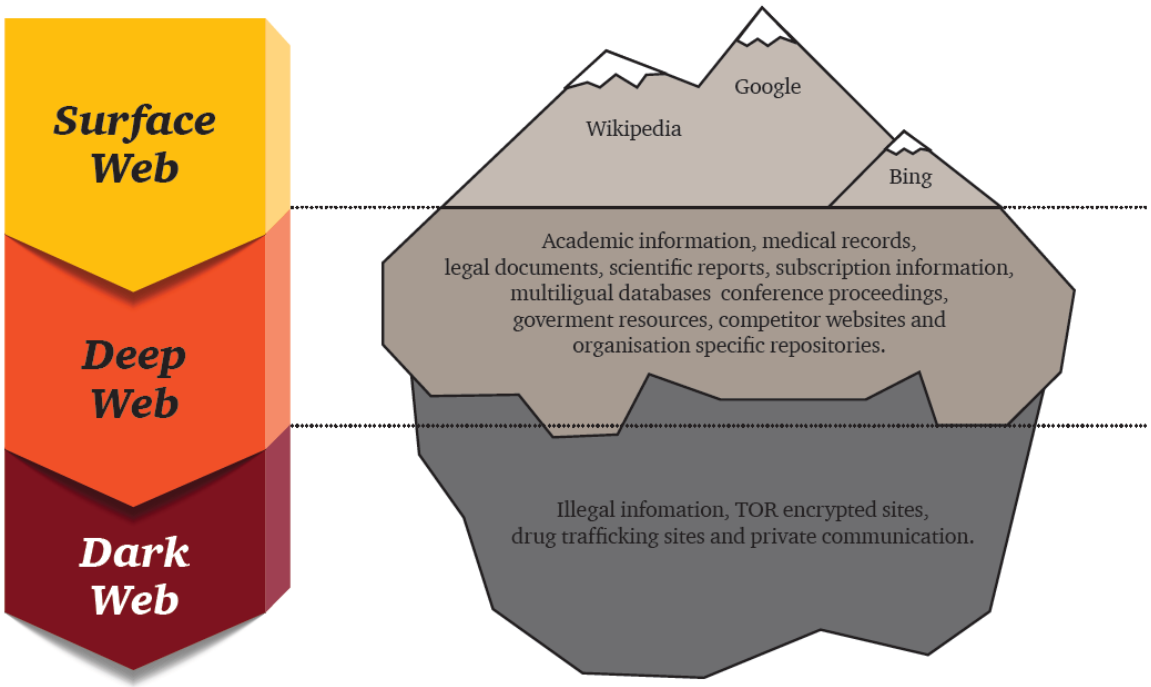


Imagen 7 – Contenido disponible para el acceso Web - PricewaterhouseCoopers

Como lo muestra la imagen anterior, la proporción de contenido Web para el acceso con herramientas conocidas como Google, Yahoo, Bing, entre otras, puede ser de aproximadamente 4% - 96%, siendo el porcentaje más bajo el de acceso público o indexado. La Deep Web y Dark Web comparten el resto del porcentaje. En la Deep Web se dice que se pueden encontrar archivos o documentos correspondientes a historial médico de las personas, suscripciones, recursos gubernamentales, entre otros. Por otro lado la Dark Web mantiene dentro de su contenido información que se ha clasificado como ilegal, uso de herramientas para la encripción de la información, actividades ilícitas.

Hoy uno de los riesgos que se pueden identificar, es que muchas personas intentan acceder a estas desconocidas redes de datos. Existen sitios en Internet o en la red superficial que publican contenido para guiar al uso de estos contenidos desconocidos. Una de las herramientas disponibles para el acceso y uso abierto es el navegador denominado "**Tor."**

En otras palabras, los riegos y actividades ilícitas que se encontraban en estas redes ocultas se encuentran en este momento en proceso de expansión y de publicación a lugares de mayor acceso para el usuario en general. Como se ampliará adelante, en esta misma sección, una de las características de este navegador (Tor) es que ofrece anonimato para la navegación en estas redes ¿De qué manera se ofrece anonimato? A continuación, se describirá brevemente cómo es que ejecuta técnicas distribuidas de procesamiento hasta alcanzar los sitios Web de interés.

Para iniciar, es importante considerar Tor no es solamente una herramienta que se encuentra disponible para la descarga y uso, va más allá. Se define como una red de servidores operados por voluntarios que permite a las personas mejorar su privacidad y seguridad en Internet. Los usuarios de Tor utilizan esta red conectándose a través de una serie de túneles virtuales, también conocidos como VPN, en lugar de establecer una conexión directa, lo que permite compartir información sobre redes públicas sin comprometer su privacidad. Según información brindada en el sitio Web de esta herramienta, los usuarios utilizan esta red para

evitar que los sitios web los rastreen y los miembros de su familia, o para conectarse a sitios de noticias, servicios de mensajería instantánea o similares cuando éstos son bloqueados por sus proveedores de Internet.

Tor ha definido una solución a esta vulnerabilidad, en lugar de que los datos tomen una ruta directa desde la fuente hasta el destino, los paquetes de datos en la red Tor toman una ruta aleatoria a través de varios nodos que además cubren sus pistas de modo que ningún intermediario pueda decir de dónde vienen los datos o hacia dónde van. Este proceso se crea a través de una red privada de comunicación, el software o cliente del usuario construye de forma incremental un circuito de conexiones cifradas a través de nodos en la red, ninguno de estos conoce la ruta completa que ha tomado un paquete de datos. De esta manera cada cliente negocia un conjunto separado de claves de cifrado para cada salto a lo largo del circuito y para asegurarse de que cada salto no pueda rastrear estas conexiones a medida que pasan. Una vez que se ha establecido un circuito, se pueden intercambiar muchos tipos de datos y se pueden desplegar varios tipos diferentes de aplicaciones de software a través de la red Tor. A continuación se presenta un gráfico obtenido del sitio oficial de Tor que representa la selección de los nodos de la red:

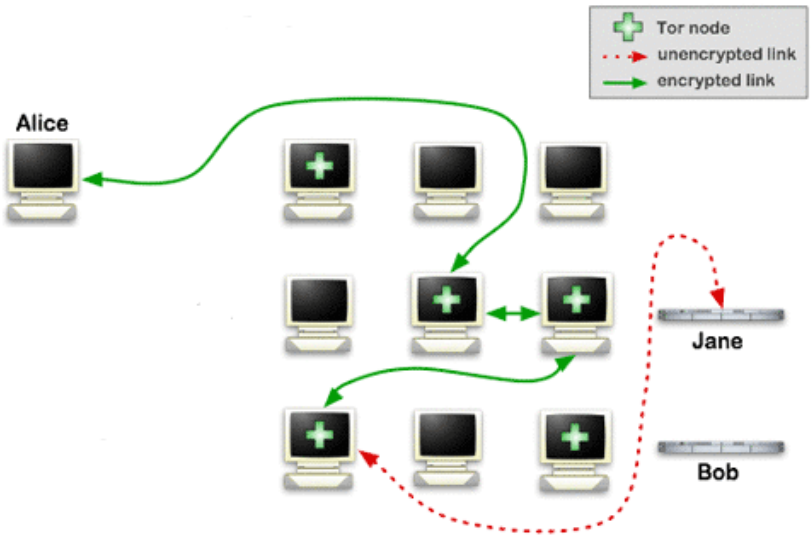


Imagen 8 – Selección de nodos Tor – Tomado del sitio Web: www.tor.org

Como se puede observar en la imagen, la selección de la ruta para efectuar la comunicación, en este caso Alice – Jane, la herramienta que utiliza Alice, selecciona

a los nodos de la red previamente creados y encripta la comunicación, los datos viajan a través de los nodos seleccionados y que forman parte de la red de Tor, hasta llegar a Jane, la línea punteada y de color rojo, representa que este canal de comunicación no se encuentra encriptado.

Por el tipo de mecanismo de comunicación que utiliza la herramienta, una de las ventajas que se obtiene con el uso de ésta, es que se protege contra una forma común de ataques en la red como lo es la vigilancia en Internet conocida como "análisis de tráfico." El análisis de tráfico se puede utilizar para conocer quién está hablando con quién a través de una red pública, una de las herramientas utilizadas se denomina “Wireshark”. Los paquetes de datos que viajan a través de Internet tienen dos partes: una carga de datos y una cabecera utilizada para el enrutamiento (mecanismo que establece la manera en qué se comunican los dispositivos en Internet). La carga de datos es lo que se envía, puede ser un mensaje de correo electrónico, una página web o un archivo de audio. Incluso si cifras la carga de datos de las comunicaciones. Eso se debe a que se centra en el encabezado, que revela la fuente, el destino, el tamaño, el tiempo, etc.

A pesar de la seguridad que se ofrece mediante la encripción de los canales de comunicación y el anonimato, Tor, en referencia a éste último, informa:

> *“Tor no puede resolver todos los problemas de anonimato. Se centra sólo en la protección del transporte de datos. Es necesario utilizar el software de soporte específico del protocolo si no desea que los sitios que visite identifiquen su información de identificación. Por ejemplo, puede utilizar el Navegador Tor mientras navega por la Web para retener información sobre la configuración de su computadora.*
>
> *Además, para proteger su anonimato, sea inteligente. No proporcione su nombre u otra información reveladora en formularios web. Tenga en cuenta que, al igual que todas las redes de anonimato que son lo suficientemente rápidas para la navegación web, Tor no proporciona protección contra ataques de sincronización de extremo a extremo: Si su atacante puede ver el tráfico que sale de su computadora y también el tráfico que llega a su Elegido destino, puede utilizar el análisis estadístico para descubrir que son parte del mismo circuito.”(Tor.org, 2017)*

Tal como lo informa la propia herramienta, proteger la privacidad y el anonimato no es necesariamente una tarea de la tecnología, es importante que se tomen acciones

para poder apoyar los controles técnicos implementados. Dichas acciones son aplicadas por parte del usuario que utiliza este tipo de medios para el acceso a contenido Web.

Hoy la protección y mitigación de riegos, en relación con el tratamiento de datos se ha convertido en una difícil tarea, tanto desde el punto de vista tecnológico como desde la visión de la ley y las regulaciones, principalmente, porque es casi imposible identificar todas la vulnerabilidades, amenazas que ofrece este nuevo mundo, así como por la limitación que se encuentran al mantener a las herramientas utilizadas para el acceso de modo disponible para la descarga y uso.

Uno de los elementos que caracterizan a esta tecnología es la dificultada para la navegación. En la Web superficial, la que cotidianamente utilizamos, se encuentra diseñando para que podamos acceder a los sitios Web mediante lo que se ha llamado dominios.

En estas redes con contenido desconocido, los dominios se encuentran cifrados y en constante cambio, esto quiere decir, lo que conocemos hoy al navegar mediante la Web, por medio de navegadores como Google, Yahoo, Bing, etc., lo estamos haciendo en sitios que se encuentran indexados, registrados para presentar al usuario al efectuar una búsqueda específica.

5.3.4 Hacking

Otro de los grandes retos desde el punto de vista técnico para enfrentar la regulación en términos de privacidad y del ejercicio del Derecho al Olvido es el “hacking”, una de las actividades ilícitas que más pérdidas económicas ha generado en las compañías a nivel mundial. Según datos publicados por el periódico digital El Financiero, cálculos recopilados por el Banco Interamericano de Desarrollo (BID) estiman que los delitos cibernéticos cuestan a América Latina y el Caribe alrededor de $90.000 millones por año, recursos que podrían cuadriplicar el presupuesto que se destina a investigadores científicos de la zona. Entre el 2011 y 2014, los gobiernos de la región reportaron un incremento promedio de un 12% en el número de incidentes de este tipo.

En los últimos tiempos se ha presentado casos de hackeo a compañías de gran renombre mundial y de la cuales por la magnitud que representan sus marcas no se esperaría un evento como éstos. Uno de los casos más sonados ha sido el sitio de citas por Internet Ashley Madison. En el año 2015 un grupo de hackers denominado "Impact Team", vulneró los sistemas de la compañía obteniendo de forma ilegal datos como los nombres de los clientes y los números de sus tarjetas de crédito, pensando en el tipo de sitio Web y en el servicio que éste brinda, es muy probable que además obtuvieran información relacionada con sus gustos, preferencias, zona residencial, etc. Posterior al incidente, los datos fueron publicados en lo que se conoce como en la Deep Web. Se estima que la cantidad de usuarios afectados mediante este hecho fue de aproximadamente 37 millones y la cantidad de datos adquiridos rondaban en aproximadamente 9 Gb (Gigabytes).

Como este hecho se han presentado una gran cantidad alrededor del mundo. Los datos de estas personas usuarias del servicio, ahora han perdido el control de sus datos, sin duda el hacking irrumpe en el ejercicio del Derecho.

Desde el ejercicio del Derecho al Olvido y la privacidad, el hacking puede convertirse en una actividad que evite la correcta ejecución de los principios establecidos por las legislaciones. El robo de los datos, así como el uso y tratamiento de los mismos no son controlables cuando se habla de este tipo de acciones ilícitas.

El hacker se define por McAfee como:

> *"…es una persona (hombre o mujer) que utiliza sus habilidades de programación y conocimientos técnicos para crear y modificar software y hardware encontrando sus debilidades y explotándolos.*
>
> *Los hackers pueden ser motivados por una serie de razones, tanto positivas como negativas. Por ejemplo, los hackers criminales pueden crear malware para cometer crímenes, como robar información y dinero…" (McAfee, 2017)*

Los ataques son ejecutados por hackers, en el ámbito de ciberseguridad, se ha establecido una categorización de éstos, según sean sus objetivos, esta clasificación es:

- Sombrero blanco: También conocidos como White Hat Hackers, ejercen el control a la hora de vulnerar sistemas, sin embargo ellos lo hacen para estudiar y fortalecer los fallos encontrados.
- Sombrero gris: Este es el tipo de Hackers que usan sus habilidades para traspasar los niveles de seguridad y luego ofrecen sus servicios como administradores de seguridad informática para corregir dichos errores.
- Sombrero negro: Conocidos como sombreros negros son aquellos que realizan actividades para vulnerar la seguridad de sistemas, violentar y extraer información restringida con un fin monetario. Entre otras actividades también son creadores de virus, spywares y malwares. Dentro de esta categoría, se incluirían aquellos atacantes que obtengan información personal sin el debido consentimiento. (McAfee, 2017)

El proceso para el hacking incluyen cinco fases, las mismas se presentan en forma cíclica, con el objetivo de tomar posesión de un sistema o de datos, según sea el objetivo del atacante, estas fases se describirán a continuación:

Como fase 1 o inicial, denominada como “Reconocimiento”, en esta se ejecuta la obtención de información, el atacante necesita y busca recaudar información que le sirva de ayuda para poder llevar la operación. La fase de reconocimiento puede conseguirse de dos maneras, conocidas como pasivo y activo. En el método pasivo el atacante recopila la información sin la necesidad de interactuar con el objetivo, puede indagar por medio de buscadores, información por medio de los DNS, dominios, etc. Existen en Internet una serie de herramientas Web, que permiten al atacante obtener información, uno de estos es el conocido sitio whois.icann.org, el cual brinda información relacionada al dueño o responsable de un dominio Web, además de otros datos. Otro de los mecanismos utilizados bajo esta técnica, se encuentra lo que se ha denominado como “Google Hacking”, en la cual mediante el uso de sintaxis en el buscador Google, se puede obtener como resultado de una búsqueda específica, datos como contraseñas, nombres de usuario, información relacionada con bases de datos, etc.

Método Activo: Aún en la fase inicial, este método permite la obtención de información, el atacante recauda información mediante la interacción con el objetivo, haciendo uso de la **ingeniería social**, en esta técnica, los atacantes buscan obtener información ejecutando una serie de actividades que se encuentran dirigidas a vulnerar a un individuo como tal, es decir, se aprovechan de la falta de conocimiento o de cultura en términos de seguridad de la información, entre las técnicas más utilizadas se encuentran:

- Phishing: Método que se ejecuta para efectuar una suplantación de identidad, mediante el uso de ésta, los atacantes hacen creer a un usuario que se encuentra navegando en un sitio Web original, cuando en realidad han accedido a uno falso, creado por el atacante. Mediante esta técnica se pueden obtener datos como los credenciales de acceso a una plataforma Web. Se puede aplicar la misma técnica con el uso de correo electrónico. Según datos aportados por la compañía EsEt, en uno de sus estudios, los porcentajes en América Latina de casos que se dieron por país bajo este tipo de ataque corresponden: Al analizar los resultados de las encuestas, es posible ver que los países más afectados por casos de Phishing son Ecuador (24%), seguido por Perú (22%) y Guatemala (20%); y los países menos afectados son Honduras con 12%, Costa Rica con 10% y El Salvador con el 9%.
- DumpsterDiving: Uno de los lugares que más información sensible contiene, son los basureros o lugares de desecho de las organizaciones, la falta de políticas para la correcta destrucción de la información, así como no contar con el conocimiento por parte de los empleados, permiten que los atacantes encuentren en estos lugares, además de basura, una serie de información que puede ser clasificada como confidencial, además datos que se obtienen de esta técnica pueden dar pistas para que los atacantes establezcan el ingreso.

Continuando con las fases de hacking, se encuentra la fase número 2 denominada como fase de escaneo: En ésta el atacante realiza el análisis de la información

recopilada en la fase inicial y termina de recopilar datos relacionados a posibles vulnerabilidades técnicas para posteriormente ser explotadas. En esta fase se utilizan una serie de herramientas, entre éstas se encuentran:

- Wireshark, el cual es un analizador de tráfico Web, en el cual se puede capturar información que no cuente con los mecanismos de defensa correspondiente, como lo puede ser certificados de seguridad, canal seguro de comunicación con el uso de redes privadas virtuales (VPN), entre otros.
- Metasploit: Esta es una base de datos de exploits, los cuales son utilizados mediante mecanismos dirigidos a vulnerabilidades específicas para intentar ocasionar un daño.
- Nmap o ZenMap: Herramientas que se encuentran diseñadas para hacer un reconocimiento en una red de datos y es capaz de brindar información como la cantidad y los puertos abiertos en equipos, el nombre de los equipos, direcciones IP, identificadores MAC, entre otros.
- Armitage: Es una herramienta que se utiliza para la aplicación de exploits de forma gráfica, es decir, mediante la utilización de una interfaz, lo que facilita el uso de la misma.

Estas son algunas de las herramientas disponibles, la mayoría de las mismas son de uso libre y se ejecutan a través de uno de los sistemas operativos diseñados para hacking, denominado como Kali Linux, éste es una distribución de Linux y proviene del ya desaparecido BackTrack.

Uno de los riesgos en relación con estas herramientas, es que las mismas son de libre descarga y uso, además, con el pasar de los años, las mejoras efectuadas por los fabricantes, han permitido mejorar la interacción de las mismas para una mayor facilidad de uso. Este hecho permite que personas que no cuenten con mayor preparación técnica pueda hacer uso de las mismas y ocasionar un impacto en dónde haga uso de éstas.

De esta fase, se obtiene como parte de los resultados, la lista de vulnerabilidades técnicas que contiene una infraestructura tecnológica. En el mundo existen bases de datos de información de estas vulnerabilidades para que las herramientas

tecnológicas la consulten y puedan dar resultados posteriores a un proceso de análisis de vulnerabilidades. Uno de estas bases de datos es el CVE - CommonVulnerabilities and Exposures (CVE), la cual puede ser consultada a través del sitio Web https://cve.mitre.org/. Las vulnerabilidades poseen un identificador, así como una serie de información que permite dar a conocer a los profesionales en seguridad, elementos como el impacto que puede ocasionar aprovecharse de la misma, la categoría a la cual pertenece, en ese sentido, la categoría permite indicar su nivel de criticidad para las compañías, quiere decir que si por ejemplo se identifica una vulnerabilidad como altamente crítica, es más probable que el impacto sea mayor que una que se ha clasificado como moderada. Esta información funciona en ambos sentidos, por un lado para el atacante, el cual se encuentra en una etapa de encontrar por dónde puede efectuar un acceso sin ser detectado y por otro lado, para que los profesionales que tienen a cargo mantener el nivel alto de seguridad de una infraestructura tecnológica, pueda implementar los controles correspondientes.

En la fase 3, denominada como obtención de acceso: Una de las fases clave, en ésta se ejecutan técnicas para el ingreso, tomando como base la información recopilada en las fases anteriores. El hacker efectúa maniobras para explotar o aprovechar las vulnerabilidades identificadas e ingresa a la red o al sistema que se encuentre vulnerando. En ésta se ejecutan acciones que pueden poner en peligro la disponibilidad de un servicio, se presentan ataque conocidos como DoS o DDos.

El ataque DoS, denegación de servicio, es cuando del cual una persona puede hacer que un sistema sea inutilizable para usuarios legítimos al sobrecargar el sistema. La carga es tal, que los niveles de estrés a los que se ven expuestos los componentes tecnológicos sobrepasan su máximo nivel de capacidad y se ven en la obligación de detener el servicio. A diferencia del DDos, ataque de denegación de servicio distribuido, en este último, se establece el ataque mediante la utilización de una red llamada “Botnet” de equipos esclavos, a los cuales se les denomina “Zoombies” y ejecuta de forma distribuida, ejecutando una serie de código malicioso en estos equipos, para que en forma conjunta se pueda efectuar la interrupción del servicio al cual va dirigido el ataque.

En la fase número 4, mantener acceso: El hacker se asegura mediante la ejecución de ataque y uso de herramientas, la descarga de archivos e información. Además identifica los mecanismos de acceso para volver a ingresar sin ser detectado. En esta fase se hace uso de una serie de elementos denominados códigos maliciosos, algunos de los más reconocidos por el gran impacto que generan al ser utilizados son:

- Virus, los cuales corresponden a Programas con código malicioso que se propaga por archivos.
- Worms: Son programas que se auto-replican y que no necesitan pegarse a otro programa como el virus. Algunos son auto ejecutables y se propagan por la red. Normalmente usan mucho ancho de banda y saturan las redes.
- Troyanos: Es un programa que no se auto-replica, que aparenta ser un programa legítimo. Normalmente buscan desarrollar una tarea específica como robar passwords o destruir archivos específicos.
- Scareware: Es software que pareciera legítimo (Anti-Virus), asusta, hace pensar al usuario que tiene un problema, ejecuta cosas visuales para entretener al usuario, mientras hace otras cosas maliciosas.

Como última fase se encuentra, limpiar las huellas: En esta fase, el hacker analiza las acciones que ha ejecutado y cuáles son los posibles rastros que ha dejado durante el proceso. El objetivo de esta fase es que se pueda borrar la evidencia de que estuvo dentro de una infraestructura y en primer lugar, garantizar que va a poder ingresar de nuevo por el mismo camino por el cual llegó y por otro lado para que, en caso de una investigación policial, no sea incriminado por los delitos cometidos.

A continuación se presenta de forma gráfica, el proceso de hacking y sus fases:

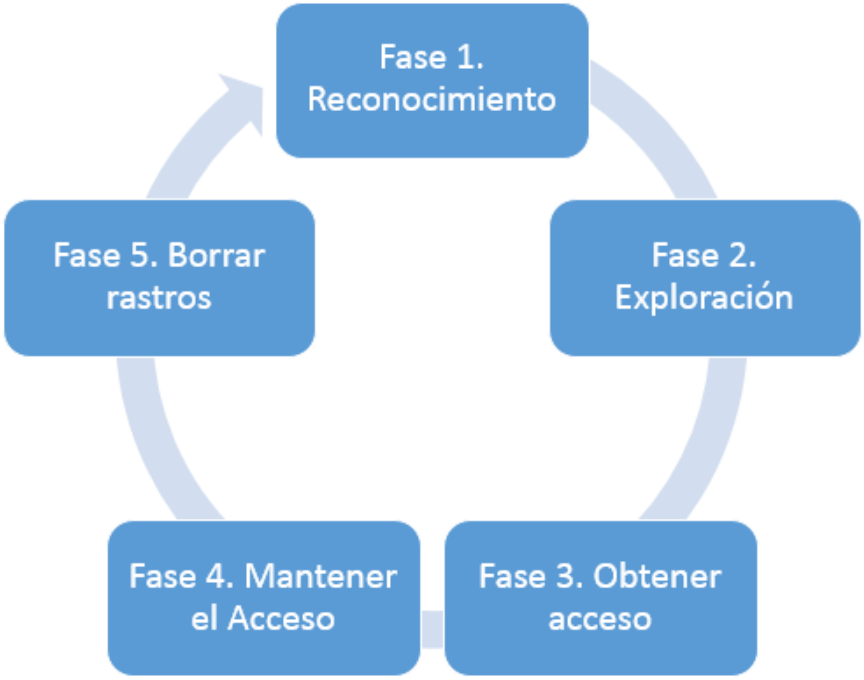


Imagen 9 – Fases de hacking – Creada por el autor

Posiblemente uno de los códigos maliciosos que más ha dado de qué hablar en los últimos días corresponde al Malware, según lo define Norton en su sitio Web:

> *"Es el término que describe cualquier software colocado en una computadora sin el conocimiento o permiso del propietario (o usuario). Malware puede ser tan simple como una broma que coloca una línea de texto dentro de algunos de la codificación de la computadora, a los programas intrusivos que causan daños a millones de ordenadores de todo el mundo, el trabajo de los cibercriminales profesionales." (Norton, 2017)*

Costa Rica no se encuentra inmune a los ataques, uno de estos es mediante los denominados "Malware", según un estudio realizado por la empresa EsEt, se presenta a continuación un gráfico con el porcentaje de ataques a los países de la región:

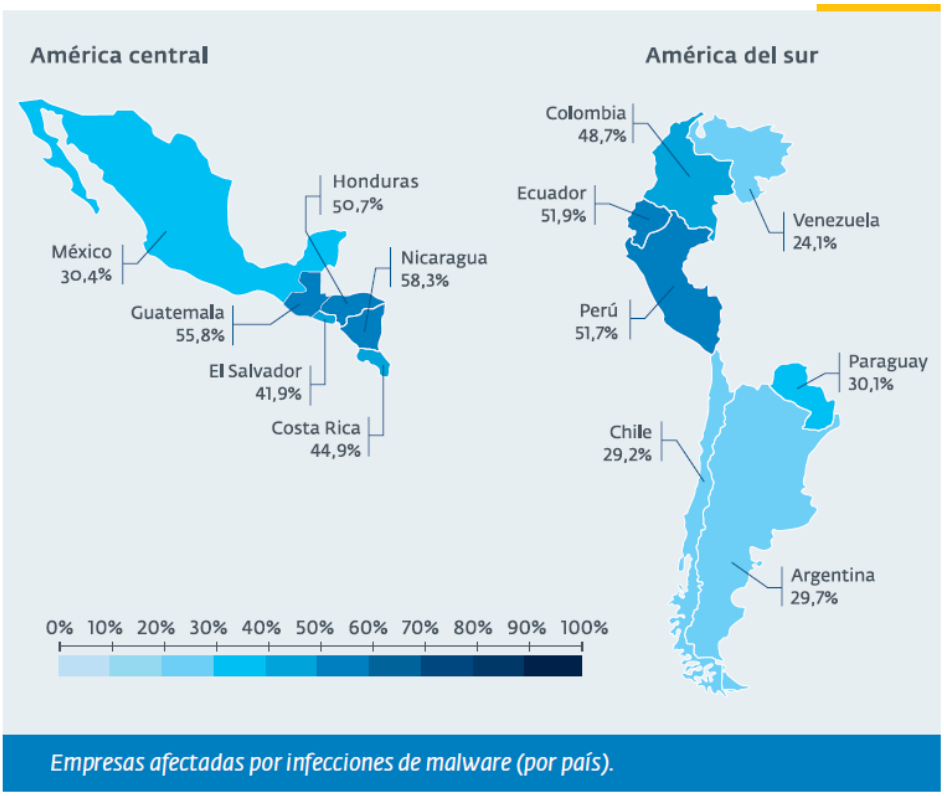


Imagen 10- Porcentaje afectación por malware por país – Estudio EsEtLatam 2016

En Costa Rica, como apoyo legal para evitar este tipo de acciones ilícitas, se cuenta con la "Ley de Delitos Informáticos". Sin embargo, una de las mejores prácticas para evitar formar parte de las estadísticas relacionadas a la cantidad y tipos de ataque es plantear un adecuado mapa de ruta, en cuanto seguridad corresponde. Las organizaciones deben implementar políticas que marquen las pautas a seguir por su personal e incluir dentro de su gestión, acciones como una valoración de riesgos periódica, una correcta gestión de vulnerabilidades, un adecuado inventario de activos de información y principalmente invertir en materia de seguridad. La concientización y la preparación a los usuarios es una de las acciones inmediatas, las cuales podrían acudir las empresas y entidades de Gobierno. Las leyes y los entes creados para la protección forman parte de un trabajo en conjunto con las autoridades, es por eso que en el siguiente capítulo se efectuará un análisis de las leyes vigentes de los Estados que forman parte del objeto de estudio del presente documento.

5.4 Apartado IV. Estado actual de los países en estudio

En este capítulo se mencionará y brindará una breve descripción y los antecedentes de la legislación vigente en los países en estudio. Regular adecuadamente actividades relacionadas a medios electrónicos o digitales es una tarea complicada, tal como lo expone:

La regulación de la administración digital presenta ciertas particularidades respecto a la regulación del régimen jurídico de las Administraciones públicas desde una perspectiva tradicional porque debe dar respuesta a problemas que no existen en el mundo físico y a situaciones que presentan una dimensión diferente respecto al mundo físico. Asimismo, esta regulación se lleva a cabo a través de diferentes instrumentos que van más allá de la tradicional reglamentación de la actividad y el funcionamiento de las Administraciones públicas a través de leyes y reglamentos.

Como se ha expuesto a lo largo de la investigación, es sumamente importante que la tecnología sea apoyada por la presencia de leyes y regulaciones.

5.4.1 España

En Europa, específicamente en España, país de estudio para el desarrollo de esta investigación, a raíz de una serie de casos en los cuales se han visto involucrados personas que poseen interés en que su información no se encuentre disponible para consulta abierta, se han publicado legislaciones que permiten el ejercicio del Derecho para sus ciudadanos. El principio, como la mayoría de las regulaciones relacionadas a la protección de los datos personales, mantienen en cierto sentido su origen en materia de secreto bancario, en este país se incluye este tipo de tratamiento desde el año 1999 en su Ley Orgánica 15/1999 definida el 13 de diciembre de “Protección de Datos de Carácter Personal y señala que existe un plazo definido para la conservación de datos referente a la condición económica de una persona.

La Ley 15/99 de protección de datos de carácter personal (LOPD) sustituye a la LORTAD (Ley Orgánica para la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal), ésta exige la inscripción obligatoria de las bases de

datos con información personal en el Registro de la Agencia Española de Protección de Datos, este principio, como se podrá comprender más adelante, también aplica tanto en México como en Costa Rica, por medio de las leyes correspondientes de cada país.

En ese sentido nace lo que se denominada “autodeterminación informativa”, este concepto corresponde al derecho a la protección de los datos personales, el mismo ha sido reconocido y protegido.

El Tribunal Europeo de Derechos Humanos ha justificado la privacidad en el artículo 8 del Convenio europeo de Derechos Humanos. El Convenio 108 del Consejo de Europa establece desde 1981 el derecho a la protección en lo que respecta al tratamiento automatizado de los datos personales.

Como fundamento de la normativa emitida, la Carta de los Derechos Fundamentales de la Unión Europea menciona el derecho a la protección de datos como un derecho autónomo, protegido como tal. En su artículo 8.1 establece que: “Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.” Además, la Directiva 95/46 de la Unión Europea relativa a la protección de las personas respecto al tratamiento de datos personales y a la libre circulación de dichos datos ofrece un régimen jurídico muy detallado. La ya mencionada Directiva 95/46/CE corresponde a una promulgación efectuada por el Parlamento Europeo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos. El Tribunal Constitucional de España en el año 2000 a través de las sentencias 290/2000 y 292/2000, reconoce que del artículo 18.4 de la Constitución Española se desprende un derecho fundamental a la protección de datos que es distinto, en su finalidad, objeto y contenido, del derecho a la privacidad reconocido en el artículo 18.1 de la norma suprema mediante la expresión:

> *“…la peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la privacidad radica, pues en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.”*

Los objetivos de esta promulgación corresponden a proteger al ciudadano, tal como lo trata la misma directiva:

> *"…consisten en lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el progreso económico y social, eliminando las barreras que dividen Europa, fomentar la continua mejora de las condiciones de vida de sus pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones Y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos." (Directiva* 95/46, 2012)

Su jurisdicción permite la aplicación del Derecho en países miembros (Alemania, Austria, Bélgica, Bulgaria, Chipre, República Checa, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, Rumanía y Suecia), fomentando la estandarización y la protección para los ciudadanos miembros.

Es importante mencionar que a raíz de una serie de cambios en la legislación Europea relativos al tratamiento y uso de los datos, el Parlamento Europeo y del Consejo, como resultado de trabajos que parten desde el año 2012, el 27 de abril de 2016 ha derogado la Directiva 95/46/CE. El reglamento, a diferencia de las directivas, tiene como principal efecto ser de directa aplicación en toda Europa, sin necesidad de incorporación por los Estados miembros a su ordenamiento interno. No obstante, debido al calado y trascendencia de las nuevas normas y derechos regulados, será aplicable a partir del 25 de mayo de 2018. Así, durante los dos próximos años, cada Estado y todas las empresas y administraciones públicas podrán realizar las modificaciones y ajustes necesarios para garantizar su cumplimiento. Dicha derogación tendrá efecto a partir del 25 de mayo de 2018, para permitir la plena adecuación de Estados, administraciones públicas y empresas.

Como parte de estos cambios, es importante mencionar que en este nuevo reglamento no sólo se reconocen los ya clásicos derechos de acceso, rectificación,

cancelación y oposición, sino que se regulan dos nuevos derechos: el derecho al olvido, como efectivo derecho de supresión, y la portabilidad de los datos.

España además se encuentra regida bajo el "Reglamento General de Protección de Datos de la Comisión Europea", con el cual busca poner la regulación al día con los cambios que se han producido en la tecnología de la información y las comunicaciones, y en consecuencia una protección más efectiva frente al tratamiento internacional de datos, en especial en los grandes sistemas, como los motores de búsqueda.

En esta propuesta, contrario a lo que pasaba en la Directiva *95/46/CE*, donde sólo se establecía el derecho de supresión, se regula con rigor el derecho al olvido haciendo recaer la responsabilidad de la supresión del dato en quien lo haya publicado en Internet y no en los buscadores, lo que realmente es la aplicación de los derechos arco en esta red.

En España existe la Agencia Española de Protección de Datos la cual es un ente con presupuesto propio y plena autonomía funcional. Esta Agencia se creó en 1992 y comenzó a funcionar en 1994.

En análisis del comportamiento y la justificante del Derecho como tal, se puede establecer una serie de fases que se ven involucradas en el ejercicio del mismo, la primera fase está relacionada con el pasado judicial o penal de un individuo.

En comparación con Costa Rica, desde el 13 de enero del año 2017, entra en vigencia la última modificación efectuada a la ley 6723 nombrada "De registros y archivos Judiciales", según información obtenida del Diario La Prensa Libre, en un artículo publicado el 14 de enero del año 2017, esta reforma data desde noviembre del año 2011 cuando se iniciaban los esfuerzos para su preparación, pero no es hasta el 2 de junio del 2016, que 38 diputados lo aprobaron en segundo debate. Anteriormente, los ex privados de libertad que hayan cumplido sus penas por delitos menores [9]debían esperar 10 años para que los antecedentes fueran borrados, con

[9] Para efectos laborares, se cancela inmediatamente después de cumplir la pena, excepto para los siguientes delitos: Crimen organizado, Terrorismo, Homicidio calificado, Delitos sexuales contra menores de edad, Delitos contra los deberes de la función pública, Femicidio.

la reforma se busca que, aquellos ex reclusos con condenas de 3 años o menos tendrían el beneficio de inmediato mientras que los que cumplieron penas de más de 5 años deberán esperar uno.

La ley española se encuentra diseñada bajo 7 grandes titulares. El primer título establece elementos como su alcance y su propósito, siendo este último:

> *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar." (LODAP, 2017)*

Es importante recalcar como desde la misma ley se hace mención a los principios de honor e intimidad. Este capítulo incluye una sección que establece los conceptos para comprender y aplicar lo estipulado por la misma correctamente.

En el título 2, se efectúa la definición de los principios de protección de datos con que cuentan los ciudadanos, entre estos principios se encuentra lo relacionado a la recolección y tratamiento de los datos, indicando en referencia a los datos de carácter personal, éstos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Además, establece que los mismos no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario.

Otro de los principios indica que se prohíbe la obtención o recolección de datos por medios fraudulentos, desleales o ilícitos, en ese mismo sentido, como se detallará más adelante, Costa Rica, establece este mismo principio. En el artículo 6 de este mismo título se establece en relación con el consentimiento del afectado, éste se necesita para poder realizar el tratamiento de los datos personales de un sujeto. Sin embargo, este no es indispensable cuando se recabe la información por parte de la administración pública (por el desempeño de sus funciones), por ser parte en un contrato determinado, dicho tratamiento sea para proteger los intereses de su titular procurando siempre que no se vean afectados los derechos del titular. El artículo 9 establece la responsabilidad de quien es el responsable de archivos o ficheros para mantener seguros los mismos mediante la implementación de medidas ya sean organizativas o técnicas. El título 3 establece los derechos por parte del titular de

los datos, en relación con este tema, se define como uno de los derechos la consulta de los datos y el acceso correspondiente sin algún tipo de costo por parte del titular. En este título, específicamente en el artículo número 16 se definen los derechos de cancelación y ratificación de los datos, mismos que forman parte de los principios establecidos por el Derecho al Olvido. Dicho artículo menciona que el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días, estableciendo un mínimo de días para la resolución de la solicitud como tal.

El artículo 21 del título 4, en relación con la transferencia de datos personales entre entidades de gobiernos establece:

> *"21- Comunicación de datos entre Administraciones públicas.*
>
> *1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*

En referencia al artículo anterior, existen dos elementos importantes, por un lado la colaboración entre entidades del Estado al compartir datos, pero condicionada esta acción a fines que ya se han mencionado en el artículo. Es decir, a pesar de que es una misma Nación en la que se encuentra los datos, el tratamiento no es a la libre. Y por otro lado el fin con que sí se autoriza esta transferencia de datos.

El título número 5 hace referencia a lo que concierne a movimiento de datos internacionales, llama la atención que como se podrá apreciar, este apartado aparece solamente en la legislación Española y vincula a la Agencia de Protección de datos como responsable de evaluar la legislación en temas de tratamiento de datos del país al que se van a transferir.

En relación con la Agencia de Protección de Datos, el título 6 en el artículo 35, ítem 1:

> *"Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena*

independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno."

En relación con los países en estudio, al igual que España, se ha creado una entidad para hacer valer lo estipulado por la presente Ley. Además de esta Agencia, la ley hace referencia a un Registro General de Protección de Datos, el cual es parte de esta Agencia y tiene como objetivo contener la información general sobre los ficheros públicos y privados, las autorizaciones que indique esta legislación.

Costa Rica ha imitado, en el buen sentido de la palabra, algunas de las disposiciones que la ley establece para con la Agencia, una de éstas es el registro de bases de datos y publicando en su sitio Web las bases de datos ya registradas.
El resto de este título establece las responsabilidades de miembros que conforman a la Agencia.
En el título 7 infracciones y sanciones, se establecen que las infracciones se calificarán de leves, graves o muy graves, dependiendo en cuál de estas faltas concuerde la situación presentada, así será la multa a imponerse. Este apartado también es contenido en la regulación mexicana y costarricense.
El reglamento a esta ley se crea en Madrid a partir del real decreto número 1720/2007, del 21 de diciembre de 2007 y publicado en el Boletín Oficial Español, el 19 de enero de 2008 y se componen de 158 artículos. Este reglamento tiene como fin:

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo. (Real Decreto 1720/2007 de 21 de diciembre, 2008)

Como se ha expuesto a lo largo de este breve repaso por la ley española, se recalca el apoyo que el Estado mantiene sobre el cumplimento de las garantías y principios que los ciudadanos españoles poseen, ahora es turno de efectuar el mismo proceso para una zona en el que el desarrollo en relación con este tipo de legislación es un

poco más rezagado, en las siguientes secciones se podrá observar algunas diferencias, mucho menos que las similitudes entre estas leyes.

En el caso de España, se encuentra a disposición de los ciudadanos sitios por parte de los motores de búsqueda para efectuar la solicitud de aplicación del derecho, a continuación se adjunta el enlace de acceso al formulario Web que cada uno pone a disposición:

- Google - Retirada en virtud de la ley de privacidad de la UE: https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636390636989855852-2439546048&hl=es&rd=1
- Bing - Solicitud para bloquear resultados de búsqueda en Bing en Europa: https://www.bing.com/webmaster/tools/eu-privacy-request
- Yahoo - Solicitudes para Bloquear resultados de búsqueda en Yahoo Search: Recursos para Residentes Europeos: https://io.help.yahoo.com/contact/index?y=PROD_SRCH&token=w5FCchB1dWGbc2RE0kcjij0u65u86GoeqUkmqtTbcuO%2BLU%2FUQgc3BzwNZtXp6XEXn5YwJ6Wu6A9MCYnw7SzQy5BySKiGUpoj0xug9Sr7JfZdSQjOyA5v2Of2mZTMotlsehDS1xQqu1g%3D&locale=es_ES&page=contactform&selectedChannel=email-icon&isVip=false

5.4.2 México

Es importante que tengamos visión de nuestra región, como se pudo comprender con el estado actual de España, la legislación diseñada para la defensa y la protección del ciudadano es amplia. Ahora en México, uno de los países más desarrollados será parte del siguiente análisis, en el que se efectuará una revisión de su actual regulación y del ente encargado de velar por su cumplimiento.

En Latinoamérica, específicamente en México, la protección de los datos personales nace como un principio Constitucional, así lo establece su Constitución en el artículo número 16:

> *"Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (…)" (art. 16 Constitución Política de los Estados Unidos Mexicanos de 05 de febrero, 1917)*

En relación con el propio tema del Derecho al Olvido digital, posterior a la declaración del principio constitucional antes mencionada, este pasó a ser un derecho fundamental dentro de México y se protege mediante lo que se conoce como "hábeas data." El cual es un recurso legal que permitía llenar los vacíos que dejaba la ausencia de una ley específica.

En el año 2011, El Pleno de la Suprema Corte de Justicia de la Nación, mediante la promulgación de resoluciones establece y defiende el Derecho y define como parte de la misma algunas limitaciones:

> *El derecho de protección de datos personales no es absoluto, en tanto admite excepciones por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (Pleno de la Suprema Corte de Justicia de la Nación 699/2011 de 9 y 10 de julio de 2012*

Cabe mencionar que todos estos hechos han marcado la base para que se desarrollen esfuerzos legales orientados al ejercicio del Derecho al olvido como tal. Se han promulgado leyes como la "Ley Federal de Protección de Datos Personales en Posesión de Particulares", ésta fue publicada el 5 de julio del año 2010 en el Diario Oficial de la Federación, periódico oficial del Estado Mexicano, bajo el mandato del presidente Sr. Felipe Calderón, el cual ejerce su mandado el año 2006 al año 2012. La ley tiene como uno de sus objetivos asegurar los derechos de privacidad y autodeterminación informática de los ciudadanos mexicanos, dentro de sus artículos, algunos de los más significativos y en relación al Derecho al Olvido. La ley se conforma por 6 capítulos y un artículo transitorio los cuales se detallarán a continuación.

Se procederá a efectuar un breve repaso por la ley, para comprender e interpretar los esfuerzos que se encuentran disponibles para le defensa del ciudadano.

El primer capítulo “Disposiciones Generales”, establece una serie de artículos que permite la comprensión de la misma en su aplicación, en el artículo 1 de ésta se establece:

> *“La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.” (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)*

Tal como lo establece el artículo anterior, la ley enmarca desde su inicio el alcance en cuanto a datos personales en posesión de particulares, así mismo, define su objetivo de regulación en el adecuado tratamiento de los datos y garantizar la privacidad.

Uno de los artículos a recalcar en el primer capítulo, es el artículo 5, éste establece que a falta de disposición expresa de la presente ley, se acuda al Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo. Del mismo modo, este hecho se presenta en la legislación de Costa Rica, la misma se ampliará en el análisis correspondiente, en relación con la ley General de Administración Pública.

En el capítulo 2 “De los Principios de Protección de Datos Personales”, se definen una serie de artículos correspondientes a los procesos de recolección y tratamiento de los datos, definiendo en el artículo 6 características que deben poseer los datos, entre estos se puede mencionar: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En relación con la obtención o recolección de los datos, el artículo 7 del mismo capítulo establece:

> *“… La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.*
>
> *En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos*

por esta Ley." (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)

Es importante recalcar, tal como la ley lo establece, la delimitación en el proceso de obtención de los datos, en ese sentido, regula e indica que dicho proceso debe contar con las medidas necesarias y no permite el uso de actividades fraudulentas o engañosas. En la actualidad, lamentablemente los mecanismos utilizados para la recolección de los datos no cumplen definitivamente con lo estipulado por este artículo, ya que los usuarios no son notificados o forman parte de las estadísticas relacionadas a delitos informáticos. Además es importante que en términos de datos personales, además del proceso de recolección, se debe verificar el proceso de traslado y uso de los mismos, en otras palabras, que quién se encargue de dar tratamiento a dichos datos implemente los controles técnicos necesarios para asegurarse que no se incumple con lo establecido por la ley.

En el artículo 8 se establece que el uso y tratamiento de los datos personales se encuentra en estrecha relación al consentimiento del titular de los mismos. En ese sentido el artículo establece que existen dos tipos de consentimiento, por un lado el expreso y por otro el tácito.

En primer lugar, el consentimiento expreso es cuando se acepta mediante medios establecidos por la ley, ésta indica medios como: verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Además, se encuentra el tácito, este consentimiento hace referencia a lo que se conoce como "Silencio positivo", quiere decir, que si no hay una respuesta por parte del ciudadano usuario a una solicitud de consentimiento de uso y tratamiento de datos, la entidad interpreta este hecho como si el usuario aceptara las condiciones propuestas. El artículo además menciona, que dichos consentimientos, considerando los dos antes descritos, pueden ser revocados en cualquier momento sin que se le atribuyan efectos retro-activos. Para aplicar tal revocación, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos correspondientes.

La ley establece un trato diferencial para los datos que se han considerado como personales sensibles e indica, en el caso del consentimiento, que el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. Además, en relación con las bases de datos, si las mismas contienen datos personales sensibles, las mismas no podrán crearse sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos, lo que regula en gran sentido a compañías que buscan lucrar con dicha información. Se plantea demás una serie de excepciones relacionadas al consentimiento, en la que se citan puntos específicos, relacionados a situaciones de emergencia, atención médica, entre otros.

Se encuentra el artículo 11, desde el punto de vista de la vigencia de la información:

> *"El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.*
>
> *Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.*
>
> *El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento." (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)*

El artículo anterior hace énfasis en primer lugar al fin por el cual se están recopilando los datos y por otro lado a la responsabilidad de quién administra la base de datos en la cual se almacena la información privada, otro aspecto a considerar en el artículo es la temporalidad, elemento que marca uno de los principios para el ejercicio del Derecho, dando como indicación la eliminación del dato.

En relación con el papel que ocupan los terceros, éstos deben procurar que los primeros cumplan de igual manera con los principios que se imponen en esta normativa. Asimismo, el aviso de privacidad se debe respetar también por el tercero.

Este aviso de privacidad debe contar con algunos requisitos a los que hace mención la ley en su artículo 16, en el cual se señala que este debe contemplar: la identidad y domicilio del responsable de los datos, las finalidades del tratamiento de datos, las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos, los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en la Ley, así como las transferencias de datos que se efectúen, y el procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

Según lo establece el artículo 17, en relación con los avisos de privacidad, éstos deben ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, recalcando el ítem 2 que menciona:

> *"Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad."(Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)*

Como lo referencia la cita anterior, se limitan en relación con los avisos de privacidad y en estrecha relación con el ejercicio del Derecho al Olvido, la obligatoriedad por parte de las empresas que brindan un servicio mediante medios como la Internet, a brindar de inmediato la información correspondiente al uso y tratamiento de los datos así como de las infracciones que pueden aplicar en caso de incumplimiento. Este elemento es importante que sea considerado para la debida promulgación y capacitación a las personas, como ya se ha establecido a lo largo de la investigación, no es solamente trabajo de la tecnología y de las leyes para permitir el ejercicio al Derecho al Olvido.

Es importante que los ciudadanos tomen las medidas correspondientes y es precisamente mediante la lectura de los avisos de privacidad y de la aceptación o rechazo de los mismos, para permitir el uso y tratamiento de los datos.

En el artículo 19 se define la responsabilidad de quien lleve a cabo tratamiento de los datos, éste, según lo establece el artículo, deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Asociado a esto, el artículo 20 de la ley establece que las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares deben ser debidamente comunicados para tomar las medidas correspondientes.

Lamentablemente, hoy, la cantidad de riesgos a los cuales se ven expuestos los responsables de mantener y dar tratamiento a los datos, es impresionante. Éstos tienen sobre sus hombros una gran responsabilidad, las técnicas y herramientas para cometer delitos en contra de la información sensible aumentan, así como los motivos por parte de las personas maliciosas.

Continuando con el análisis, en el capítulo 3 de la ley, denominado “De los Derechos de los Titulares de Datos Personales” se establece mediante sus artículos algunas de las funciones por parte del titular de los datos, haciendo énfasis en los artículos 24 y 25, por un lado se establece el derecho que posee el titular a rectificar sus datos en caso de que sean inexactos o incompletos.

El ejercicio del Derecho al Olvido es apoyado además por el artículo 25 el cual establece:

> *“El titular tendrá en todo momento el derecho a cancelar sus datos personales.*
>
> *La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.*

Una vez cancelado el dato se dará aviso a su titular.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también."(Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)

La cancelación, principio que forma parte en el ejercicio del Derecho al Olvido, es detallada en capítulo IV de la Ley, además, los requisitos para poder solicitar dicha acción se encuentran en el artículo 29, algunos de éstos son: el nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud, los documentos que acrediten la identidad, en dado caso, la representación legal del titular, la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados y cualquier otro mecanismo que permita la localización del titular (Ley Federal).

Es importante, que la cancelación de los datos no aplica en todos los casos y para ello la ley establece en su artículo 34, los casos en los cuales no procede la aplicación de este derecho. Dichas excepciones son:

I. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;

II. Cuando en su base de datos, no se encuentren los datos personales del solicitante;

III. Cuando se lesionen los derechos de un tercero;

IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y

V. Cuando la rectificación, cancelación u oposición haya sido previamente realizada. (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)

En el capítulo 5 de la ley se establecen indicaciones para la transferencia de los datos, en el cual brindan las pautas necesarias para efectuar la debida comunicación al titular de los datos en caso de que éstos sean transferidos, ya sea dentro del territorio Mexicano como fuera de éste.

Asimismo, se definen excepciones que permiten que este proceso de comunicación con el titular no se ejecute, las razones recaen principalmente en la no interrupción de procesos judiciales, en caso de tener relación con investigaciones y demás.

La ley asigna responsabilidades a entidades de Gobierno que tienen como parte de sus funciones la protección de este tipo de información en beneficio de sus ciudadanos, dichas entidades son definidas en el capítulo VI "De las autoridades" y en primera instancia, en la sección I se establece el Instituto Federal de Acceso a la Información y Protección de Datos Personales, el cual, según lo establecido tendrá como responsabilidad:

> *"…difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento…" (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)*

Dichas funciones antes descritas, corresponden en cierta medida, y como se detallará adelante en este documento lo que en Costa Rica es ejercido por la Agencia de Protección de Datos de los Habitantes (Prodhab).

Al instituto Mexicano se le conoce además como Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI).Dicho instituto tiene como misión:

> *"Garantizar en el Estado mexicano los derechos de las personas a la información pública y a la protección de sus datos personales, así como promover una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales para el fortalecimiento de una sociedad incluyente y participativa."(INAI, 2017)*

La creación de entes que se encarguen de permitir el cumplimiento de la legislación en beneficio del ciudadano siempre será significado de esfuerzos para este fin.

Otro de los entes con responsabilidades asignadas mediante la ley es la Secretaría de Economía, principalmente con actividades como la promulgación de las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

En el capítulo VII Del Procedimiento de Protección de Derechos, la ley establece que el reclamo para la protección de datos se efectuará por parte del titular de los

datos o mediante el representante legal y se define un plazo de 15 días para que exista respuesta de parte del responsable hacia el titular de los datos. En cierta medida este punto permite la agilización del proceso y no se demore una cantidad de tiempo y entrabe el proceso. Asimismo, el Instituto tiene la potestad por ley de sobreseer o desechar la solicitud de protección de datos por improcedente, o confirmar, revocar o modificar la respuesta del responsable.

Cuando se presente la solicitud de datos en el Instituto, se le da audiencia al responsable para que presente pruebas y manifieste lo que considere pertinente. Por terminada la recopilación de la prueba, el Instituto notificará al responsable para que presenten los alegatos que estime necesarios en el plazo de 5 días. El Instituto resuelve después de esto sobre la solicitud y el Reglamento expone los demás detalles de este proceso. Los detalles que debe contener dicha solicitud se encuentran en el artículo 46, entre éstos se puede mencionar: el nombre del titular, el nombre del responsable del tratamiento de datos a quien se le presentó previamente una petición ya sea de acceso, rectificación, cancelación u oposición, un domicilio para las notificaciones, la respuesta del responsable, los motivos que lo mueven para presentar la diligencia y todos aquellos elementos que considere indispensables para el proceso.

Uno de los artículos que más llaman la atención, se encuentra en el capítulo XI “De los Delitos en Materia del Tratamiento Indebido de Datos Personales”, principalmente porque las sanciones establecidas en los artículos contenidos en éste, corresponden a imposición de medidas carcelarias y el tiempo sancionado lo define el tipo de delito cometido.

Esta ley es apoyada con la publicación efectuada el 21 de diciembre del 2011 del Reglamento de la Ley Federal de Protección de los Datos Personales en Posesión de los Particulares, en el cual y para mencionar de forma general su contenido, establece algunas definiciones relacionadas al proceso de transferencia de información desde el punto de vista territorial. En su artículo 1 define su objetivo como: “El presente ordenamiento tiene por objeto reglamentar las disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.”

(Reglamento Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010)

Además, en cuanto a su aplicación, geográficamente establece que cuando el responsable no se encuentre ubicado en territorio mexicano, pero el encargado lo esté, este último le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III del mismo Reglamento. Dicho capítulo trata temas relacionados a las medidas de seguridad en el tratamiento de datos personales.

Desde el punto de vista de controles y medidas que pueden tomarse para evitar el uso inadecuado de los datos, el reglamento es claro, éste establece acciones como la ejecución periódica de análisis de riesgos y verificación de vulnerabilidades técnicas que puedan ser aprovechas y cometer actos ilícitos. En ese mismo sentido define las responsabilidades por parte del responsable de los datos para garantizar que los datos se encuentran protegidos y dichas vulnerabilidades hayan sido mitigadas.

Es importante mencionar que no existen instrumentos globales jurídicamente vinculantes en materia de protección de datos El derecho al olvido debe dar prioridad a las exigencias del derecho a la información cuando los hechos que se revelan presentan un interés específico para su divulgación. Sin embargo, existen herramientas de defensa para la colaboración entre Estados, uno de éstos es el convenio de Budapest, del cual se ampliará en la presente investigación, cabe mencionar que México no se ha adherido a este convenio.

5.4.3 Costa Rica

A continuación se procederá con una breve descripción de la legislación vigente para Costa Rica, partiendo de la Ley de Protección de Datos y su relación con el Derecho al Olvido.

En Costa Rica, en relación con el tratamiento de datos y la privacidad de los mismos, se establecen hechos históricos que permiten definir su fundamento. Desde hace

años, antes de la emisión de leyes dirigidas al tratamiento de los datos personales se emite mediante la promulgación de la Sala Constitucional:

> *"Por el solo atributo de su humanidad, todo individuo debe ser protegido en sus derechos, independientemente de su género, color, origen étnico, religión, educación, condición económica, nacionalidad, etc.; debe estar desvinculado totalmente de discriminación alguna contraria a su altísima condición, cualesquiera que sean las circunstancias en las que se desenvuelva o se haya desenvuelto. Precisamente, de la argumentación elaborada es que se deriva el llamado derecho al olvido, "a tenor del cual ciertas informaciones deben ser eliminadas de los archivos oficiales transcurrido un determinado lapso desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede prisionero de su pasado." (Sentencia número 2004-04626 2004, Sala Constitucional 7937-2011 de 17 de junio)*

En referencia con el extracto anterior de la Sala Constitucional, es importante recalcar como defensa de los derechos de los ciudadanos e interpretando la Constitución se orientan los primeros esfuerzos en relación con el Derecho al Olvido con acciones como la limitación en el accionar del tratamiento y uso de datos con elementos como el tiempo y la importancia o el tipo de dato para los ciudadanos.

Como parte de esta historia, la primera Constitución se estableció en 1821, es llamada "Pacto de Concordia o Pacto Social Fundamental Interino de Costa Rica", la misma rigió hasta 1824. Posterior a este hecho y luego de una serie de hechos históricos presentados, según Pochet, el 22 de noviembre de 1824, se establece la República Federal Centroamericana y con esto surge la legislación. Dentro de ésta se mantienen los derechos fundamentales adquiridos por medio de la Carta Magna. Más tarde, en 1841 aparece mediante un golpe Estado el Sr. Braulio Carrillo, quién mantiene dentro de sus prioridades frente al país, proteger las garantías de los ciudadanos.

En el año 1844 nace una nueva Constitución y posee como una de sus características principales el voto o sufragio, ampliando aún más el sentido democrático que caracteriza al país. No es hasta el año 1848, en la que aparece la normativa que contiene los derechos de propiedad y secreto de las comunicaciones, dicha carta fue emitida el 29 de diciembre de 1859. Los temas relacionados a la privacidad de los datos son considerados bajo el artículo 27- "En ningún caso se

podrán ocupar, ni menos examinar, los papeles privados de los habitantes de la República." (Art. 27 Constitución Política de Costa Rica de 29 de diciembre de 1859)

El cambio que ha experimentado nuestro país para adaptarse a la realidad nacional, se ha reflejado principalmente en cambios en las constituciones y lo establecido por las distintas Cartas Magna, la primera fue establecida desde el reconocimiento de Costa Rica como una República en 1821. En este importante documento se tratan temas relacionados a la protección de la privacidad, abordándose desde el concepto de "propiedad privada". Actualmente, Costa Rica se encuentra regida para lo establecido por la Constitución Política del 7 de noviembre de 1949, la misma fue realizada por la Junta Fundadora de la Segunda República y tal como lo menciona Araya, contempla:

> *"… entre sus más relevantes logros, el desarrollo del Estado Social Democrático de Derecho, así como, una importante mejora en el sistema electoral y una mayor participación ciudadana en el poder. Asimismo, esta se divide principalmente en tres derechos fundamentales: las garantías individuales, las sociales y las políticas." (Araya Pochet 2005, 137)*

De la presente Carta Magna es importante mencionar la relevancia que tiene el artículo 24, el cual establece, en relación al tratamiento de los datos personales:

> *Artículo 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. (…)(Art. 24 Constitución Política de Costa Rica de 07 de noviembre de 1949)*

En Costa Rica, además dentro de las instituciones que permiten establecer medias en relación con el tratamiento de datos, existe el Tribunal Contencioso Administrativo, esta entidad establece principios que buscan establecer medidas para uso y tratamiento los datos personales de las personas, con éstas, se pretende que el tráfico y tratamiento de datos de carácter personal, se vea disminuido así como, protegido. Además, que las empresas sepan de la existencia de estos principios que deben respetar en Costa Rica.

La Sala Constitucional también ha permitido establecer medidas en relación con la protección de los datos mediante resoluciones, una de estas es la resolución "8996 del año 2002".

Como ya se ha mencionado, la tecnología ha permitido la interacción entre personas alrededor del mundo, la automatización ha permitido además generar muchos beneficios económicos a las empresas, pero además trae implícitas una serie de repercusiones que pueden ser causa de violación de derechos fundamentales tales como la intimidad, el secreto de las comunicaciones y la libertad, la desaplicación de lo que en principio debería ser el consentimiento informad. Es por estas razones que el derecho es sumamente importante, ya que actúa a través de la legislación, además de la ley antes mencionada, en nuestro país se encuentran otros esfuerzos como la ley N° 9135“reforma de los artículos 196,196 bis, 230, 293 y 295, y adición del artículo 167 bis al Código Penal”, la misma fue aprobada el 26 de abril del año 2013 y trata temas relacionados al tratamiento de datos personales, algunos de los artículos más relevantes para la presente investigación corresponden a los artículos siguientes:

> *"Artículo 230.-Suplantación de identidad. Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información."*

Refiriendo la cita anterior, se sancionará lo que en informática se conoce como “Phishing” o suplantación de identidad, según CISSP, el término corresponde una modalidad de ataque:

> *“…en la que un atacante intenta obtener información confidencial de un objetivo, incluyendo nombres de usuario y contraseñas, información de identificación personal o información de tarjeta de pago. Esto suele hacerse a través de correo electrónico, pero también puede ampliarse para incluir ataques de agujeros de riego, donde un atacante planta enlaces de aspecto inocuo en lugares como foros de discusión para atraer a las víctimas a hacer clic.”(CISSP, CKB, 2013)*

Tal como lo establece la definición anterior, esta técnica o modalidad de ataque cibernético, consiste en hacerse pasar por una persona o entidad cuando en realidad se está engañando a una persona para que acceda e ingrese al sitio Web falso con el objetivo de capturar datos de carácter personal y luego cometer acciones ilícitas en contra de las mismas. La ley considera sanciones en caso de que se presente este ataque en medios digitales como lo son las redes sociales.

Otro de los artículos a mencionar desde el objeto de estudio de esta investigación es el artículo 196 bis, el cual establece:

> *"Artículo 196 bis.-Violación de datos personales. Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos."*

La importancia del artículo 196, radica en que se sancionan hechos que van en contra del ejercicios del Derecho al Olvido. Se consideran en la misma, elementos como la privacidad por un lado y por otro las acciones en el uso o tratamiento de datos, específicamente cuando no se cuente con la autorización del titular de los datos.

La ley como ya se ha definido en algunos de sus artículos, establece sanciones a quién cometa los delitos tipificados, las sanciones son períodos de cárcel, este factor puede marcar un precedente para los delitos informáticos, así como para el ejercicio al Derecho al Olvido. Las sanciones económicas podrían no ser un impedimento para el uso de datos personales, sin embargo estas medidas carcelarias podrían dar un apoyo al objetivo de la legislación.

Uno de los esfuerzos más significativos en materia Jurídica para Costa Rica y con relación al tratamiento de los datos personales es la publicación de la "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales". Esta ley se origina el 7 de julio del año 2011, Ley N° 8968 de 7 de julio del 2011 y publicada en el Diario Oficial La Gaceta No. 170 del 5 de setiembre del 2011, la misma tiene como objetivo:

> *"… garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes." (Ley 8968, 2011)*

Estableciendo desde su definición el principio de autodeterminación y la relación de la actividad privada, incluyendo el concepto de automatización.

Esta ley contiene dentro de su contenido 34 artículos distribuidos en 6 capítulos. A continuación, se expondrá de forma breve algunos de los capítulos, considerados como de influencia directa en el ejercicio al Derecho al Olvido desde el objeto de estudio de esta investigación.

En el capítulo 1 “Disposiciones Generales”, se especifica mediante el planteamiento de sus artículos, el alcance de aplicación de la ley, además, tal como ya se expuso, se presenta su objetivo, en el artículo 2, se define su ámbito de aplicación, refiriéndose a los datos como:

> *“:.. será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.” (Ley 8968, 2011)*

Tal como se lo se establece en su alcance, se consideran datos almacenados en bases de datos sin importar su mecanismo utilizado para procesarlos, además recalca que no hay importancia si los propietarios o dueños de dichas bases de datos pertenecen a entidades públicas o privadas. Con respecto a las bases de datos, en ese sentido, se consideran desde archivos en formatos utilizados por las organizaciones en las que se almacena información hasta bases de datos complejas o relacionales basadas en motores de almacenamiento dedicados a esta función.

El artículo 3 “Definiciones”, establece una serie de conceptos que permitirá efectuar la correcta interpretación de la misma en su aplicación, uno de los términos que pueden relacionarse de forma directa con el ejercicio del Derecho al Olvido, es el “Tratamiento de datos personales”, el cual se define como:

> *“… cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.”(Ley 8968, 2011)*

La ley es clara al referirse al tratamiento de datos personales, desde el mecanismo utilizado en el proceso de recolección de los mismos hasta la utilización o difusión, es importante mencionar que la destrucción, bloqueo o supresión son acciones que se consideran como parte del tratamiento que se le puede dar a los datos, estas últimas consideradas como acciones para la aplicación del Derecho al Olvido.

En este mismo artículo, la ley define la diferencia entre los conceptos de datos personales:

> *b) Datos personales: cualquier dato relativo a una persona física identificada o identificable.*
>
> *c) Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.*
>
> *d) Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.*
>
> *e) Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.(Ley 8968, 2011)*

Es importante considerar que no todos los datos personales tienen igual nivel de protección jurídica. Como lo define la ley y en referencia a las definiciones antes citadas, se encuentran disponibles categorías de datos, por lo tanto existen datos que se encuentran distribuidos éstas, como por ejemplo, datos sensibles, los cuales son los que se encuentran directamente relacionados con la religión, salud, identidad sexual, socioeconómicos y políticos, y deben contar con un mayor grado de protección. Esto se debe que se encuentra en relación con la intimidad y privacidad, por lo que deben ser custodiados con mayor recelo.

En el capítulo “2 Principios y derechos básicos para la protección de datos personales” se establecen los principios y conceptos como el de autodeterminación informativa, de los principios de refiere como:

- Principio de consentimiento informado, considerando aspectos como la obligación de informar: “Cuando se soliciten datos de carácter personal será

necesario informar de previo a las personas titulares o a sus representantes, de modo expreso…" y otorgamiento del consentimiento: "Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo."

- Principio de calidad de la información: "Solo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados."

En relación con el principio de calidad de información, tal como se ha expuesto durante el presente documento, éste es parte de los elementos que permiten el ejercicio del Derecho al Olvido, la considera una serie de características para establecer la calidad de los datos. La importancia de este artículo recae en el fundamento que el ciudadano presenta para hacer valer la cancelación de los datos, aspectos como la veracidad de los datos, actualidad:

Actualidad

Los datos de carácter personal deberán ser actuales. El responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados. En ningún caso, serán conservados los datos personales que puedan afectar, de cualquier modo, a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otra cosa. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular.

Veracidad

Los datos de carácter personal deberán ser veraces.

La persona responsable de la base de datos está obligada a modificar o suprimir los datos que falten a la verdad. De la misma manera, velará por que los datos sean tratados de manera leal y lícita.

Exactitud

Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o

incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

Si los datos de carácter personal registrados resultan ser inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados. Igualmente, serán eliminados si no media el consentimiento informado o está prohibida su recolección.

Adecuación al fin

Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley.

Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública. (Ley 8968, 2011)

Tal como lo establece la ley, es responsabilidad del encargado de la base de datos de efectuar el tratamiento correspondiente para eliminar de los registros la información que no cuente con los parámetros necesarios desde el punto de vista de la calidad de los datos.

En el artículo 7 de la ley se definen los derechos con respecto a los datos, para los ciudadanos, dentro de éstos se encuentra el acceso a la información, refiriéndose a que no importa el mecanismo utilizado para el registro de los datos, éste debe permitir el acceso de la persona interesada, además define las garantías como las facultades del interesado. Se establece adicionalmente el derecho a la rectificación, del cual se extrae:

"Todo titular puede solicitar y obtener de la persona responsable de la base de datos, la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales." (Ley 8969, 2011)

La cita anterior apoya y confirma la responsabilidad del encargado de la base datos, en cuanto al tratamiento y uso de datos, así como las garantías que posee el titular como dueño de dicha información. En el artículo 8 se establecen los límites mediante las excepciones, recalcando que se consideran aspectos como la

seguridad del Estado, investigaciones y la aplicación de otras regulaciones para el debido tratamiento de los datos

En la segunda sección, mediante el artículo 9 se establecen las “Categorías espaciales para el tratamiento de datos”, dicho numeral amplía lo establecido en las definiciones brindadas en el artículo 2. Mediante el artículo 10 de la tercera sección, “Seguridad y Confidencialidad del tratamiento de los datos” La ley confirma y establece que el responsable de la base de datos debe:

> *El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.(Ley 8968, 2011)*

El responsable debe considerar los mecanismos necesarios para mantener la seguridad de los datos a un nivel considerable y tomando como referencia la clasificación a la que pertenecen éstos.

El artículo 13, establece el derecho administrativo que posee el ciudadano, con el fin de ser protegido contra actos que violen sus derechos fundamentales reconocidos en la ley, dicho proceso es efectuado por medio de la Agencia de protección de datos (Prodhab, 2017).

En el capítulo 3,”Transferencia de Datos Personales” establece en el artículo 14:

> *“Los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley.”(Ley 8968, 2011)*

Mediante la definición de este artículo se confirma por un lado la responsabilidad que posee el responsable de la base de datos y por otro lado el derecho que posee el titular de los datos a efectuar las autorizaciones correspondientes mediante consentimiento informado. En este sentido es importante considerar que la aplicación del Derecho al Olvido en medios tecnológicos necesita el apoyo de este tipo de medidas. Hoy el uso de aplicaciones ya sea para dispositivos móviles o mediante el uso de navegadores, así como la proliferación de las redes sociales

permiten que los datos personales sean recolectados de forma sencilla y asociado a esto y desde la visión del ciudadano usuario de dichas soluciones tecnológicas, se acepte un contrato que posee cláusulas y términos que trasladan el tratamiento y uso de los datos a las compañías fabricantes, dejando de lado el control y seguimiento de dicha información.

La ley además establece en el apartado 4 de esta ley, la definición de la Agencia de Protección de Datos de los Habitantes, el cual es un órgano de desconcentración máxima, adscrito al Ministerio de Justicia y Paz, dentro de sus responsabilidades y según lo estipulado por la ley en el artículo 16 debe cumplir una serie de estipulaciones, entre ellas se incluye:

- Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.
- Poner las sanciones establecidas, en el artículo 28 de esta ley, a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito.
- Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional. (Ley 8968)

Dicha entidad, en relación con lo estipulado por la ley, establece en su Misión y Visión organizacional:

> *Misión: La Agencia de Protección de Datos de los Habitantes es una entidad pública, que garantiza a toda persona su derecho fundamental a la autodeterminación informativa y demás derechos de la personalidad, la defensa de su libertad e igualdad con respecto al tratamiento de la información correspondiente a sus datos y al de sus bienes.*

> *Visión: Ser una organización pública reconocida a nivel nacional e internacional, con una cultura de transparencia y de buenas prácticas en la protección de los datos de la persona y los de sus bienes. (Prodhab, 2017)*

Como se lo plantea la misma Agencia, su Misión organizacional va dirigida a las garantías que poseen los ciudadanos en relación con la autodeterminación, información, y además en el tratamiento de los datos que le pertenecen como tal.

Las organizaciones, con el objetivo de brindar o mejorar el servicio a sus clientes mediante la tecnología, así como con acciones relacionadas a la venta de los datos, han creado bases de datos con información que puede clasificarse como personales y que por lo tanto deberían de mantener el nivel de protección adecuado, este tipo de escenarios se presentan actualmente con entidades financieras, las cuales se ven regidas mediante la Superintendencia General de Entidades Financieras (SUGEF). Desde la promulgación de la ley y con la creación de la Prodhab se ha desarrollado un procedimiento para que estas organizaciones efectúen del debido registro a esta institución.

En relación con el tema, mediante las nuevas reformas al Reglamento mediante el Decreto Ejecutivo No. 40008-JP del 19 de julio del 2016 y publicación No. 287 del Diario Oficial La Gaceta del 6 de diciembre del 2016, se establece en su artículo 2:

> "(…) Las bases de datos de entidades financieras que se encuentren sujetas al control y regulación por parte de la Superintendencia General de Entidades Financieras (SUGEF), no requerirán inscribirse ante la Agencia de Protección de Datos de los Habitantes. Sin perjuicio de lo anterior, la Agencia tendrá plena competencia para regular y fiscalizar la protección de los derechos y garantías cubiertos bajo la Ley nº 8968 y ejercer todas las acciones que se conceden al efecto, sobre dichas bases de datos. El régimen de protección de los datos de carácter personal que se establece en este Reglamento tampoco será de aplicación a los datos que se refieran a personas físicas en su calidad de profesionales siempre y cuando ello se realice para fines propios de la profesión o en cumplimiento de disposiciones legales." (Decreto Ejecutivo No. 40008-JP, 2016)

En la segunda sección del capítulo 4 de la ley, se establece la estructura interna, en relación con la Prodhab.

El capítulo 5 “Procedimientos”, dicta las pautas, son necesarias para establecer las sanciones correspondientes distribuidas en tres secciones: Intervención, Procedimientos Internos, Cánones. Cabe señalar que la ley establece como referente, a la Ley General de Administración Pública como respaldo legal, quiere decir que lo que no se contempla en ésta, puede ser consultada la ley que respalda.

Lamentablemente, en dicha en la ley 8968 no existen artículos que hagan referencia al Derecho al Olvido explícitamente, sin embargo en su reglamento llamado: “Reglamento a ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales” creado mediante Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012 y publicado en el Alcance No. 45 del Diario Oficial La Gaceta del 5 de marzo del 2013, se subsana en cierta medida la brecha en relación con el tema que la ley dejaba, el reglamento en su artículo 11 menciona:

> “Artículo 11. Derecho al olvido. La conservación de los datos personales que puedan afectar a su titular, no deberá exceder el plazo de diez años, desde la fecha de terminación del objeto de tratamiento del dato, salvo disposición normativa especial que establezca otro plazo, que por el acuerdo de partes se haya establecido un plazo distinto, que exista una relación continuada entre las partes o que medie interés público para conservar el dato.” (Reglamento ley 8968, 2011)

Como parte de las modificaciones efectuadas mediante el Decreto Ejecutivo No. 40008-JP antes mencionado, sufrió además modificaciones, el artículo 11. El anterior establecía:

> Artículo 11. Derecho al olvido. La conservación de los datos personales, que puedan afectar a su titular, no deberá exceder el plazo diez años, desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o porque el acuerdo de las partes haya establecido un plazo menor. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular. (Reglamento ley 8968 v1)

Como se puede apreciar, parte de las modificaciones efectuadas mediante el decreto, corresponden al momento en que empiezan a regir los plazo establecidos para la conservación de los datos personales, además se efectúa un cambio en la necesidad de la conservación del dato, por un lado en el artículo original, se menciona la des-asociación del dato con el titular y por otro, mediante la reforma

efectuada, se menciona que el mismo se conserva considerando la normativa vigente.

En este reglamento además viene a dar herramientas a la Prodhab, en la definición de cánones y dar el apoyo necesario para el cumplimiento de la ley, así, como en el caso del Derecho al Olvido, cerrar las brechas que la ley no contempla.

El procedimiento de registro de las bases de datos, es aún confuso para muchas compañías e instituciones, al parecer la interpretación de lo estipulado en la ley y sus reglamentos no es una tarea sencilla. A pesar de la publicidad que se ha difundido por distintas redes sociales y medios de comunicación tanto impresa como televisiva, es importante que se ejecuten acciones más específicas, con el objetivo de esclarecer las dudas en relación con el tema.

Uno de los casos más sonados en Costa Rica, en los últimos tiempos, en relación con el uso y tratamiento de los datos personales, se presentó en una de las entidades públicas más grandes del país. El hecho se presentó en la Caja Costarricense de Seguro Social (CCSS) en el año 2015, al denunciar haber sido víctima de un hackeo que comprometió los datos de 500.000 registros del Sistema de Recaudación Centralizada (SICERE). Esta solución tecnológica lleva el registro de los afiliados de la CCSS, y controla los aportes del Régimen de Invalidez, Vejez y Muerte, pensiones complementarias, enfermedad y maternidad, fondos de capitalización laboral y las cargas sociales, por lo que los datos contenidos en las bases de datos que soportan su funcionalidad contienen una gran cantidad de datos personales de los ciudadanos, su contenido podría ser considerado como sensible, por el tipo de datos que se encuentran registrados. En la siguiente infografía, tomada del sitio Web del periódico digital El Financiero, se puede comprender gráficamente lo sucedido en este hecho:

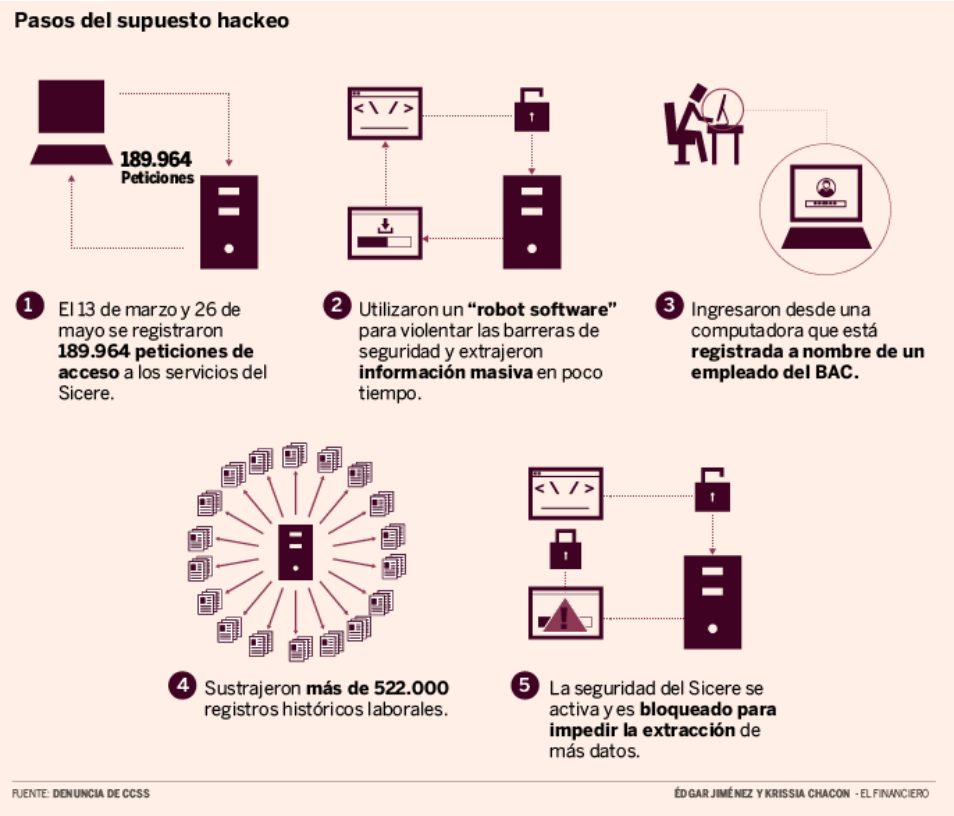


Imagen 11 – Infografía caso obtención de información CCSS- Fuente Diario El Financiero 2017

La denuncia de este hecho fue presentada al Ministerio Público para la debida investigación, así mismo se interpuso ante la Agencia de Protección de Datos de los Habitantes. Este evento ha planteado y abierto la discusión entra las compañías y las personas en relación con el uso de los datos, así como el estado de la seguridad que poseen las Instituciones Estatales. La discusión se centra principalmente en el cuidado especial que debe de darse a este tipo de datos, el país cuenta con profesionales y compañías que se encuentran en la capacidad de proveer las técnicas y herramientas para asegurar a un nivel técnico aceptable estas soluciones tecnológicas. Se pierde información que probablemente sea comercializada y al final se obtendrá una entrada desde el punto de vista económico, pero se pierda aún más al tener un evento de éstos y dar a la población una imagen de descuido o de falta de capacidad. La pérdida de la imagen y reputación podrían no ser elementos de fácil recuperación.

5.4.4 Convenio de Budapest

El Convenio es el único instrumento internacional vinculante sobre ciberseguridad. Sirve de guía para cualquier país que desarrolle una legislación nacional integral contra el Delito Cibernético y como marco para la cooperación internacional entre los Estados que forman parte del tratado.

El Convenio de Budapest se complementa con un Protocolo sobre Xenofobia y Racismo cometido a través de sistemas informáticos. Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China. El Convenio de Budapest es un convenio que se estableció en el año 2001.

Costa Rica, el 9 de mayo del año 2017, los diputados aprobaron en segundo debate unirse al Convenio de Budapest, 5 años después de ser presentado ante la Asamblea Legislativa, siendo el primer país de la región en unirse. España ya formaba parte de este convenio y México no se ha adherido, se encuentra en discusión por algunos miembros del Parlamento.

La unión tiene como uno de sus objetivo complementar la ley actual 9048 de Delitos Informáticos y conexos del título VI del Código Penal para mejorar la lucha contra la ciberdelincuencia y se protegerán actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como datos personales, la identidad y los derechos de los niños y niñas.

Según informa la Presidencia de la República mediante su sitio Web, el Sr. Luis Paulino Mora, Ministro de Estado, indica:

> “Con este proyecto se busca hacer frente en general a los delitos informáticos, de Internet, e incluso de propagación de mensajes racistas o xenófobos, mediante la armonización de las leyes de los Estados parte. Esperamos que este impulso en pro de la seguridad ciudadana continúe, y podamos tener pronto dentro de nuestro legislación otras herramientas, como la Extinción de Dominio, que se constituirían en verdaderos hitos en la lucha contra el narcotráfico, el terrorismo, el crimen organizado y el blanqueo de capitales.” (P, Mora, 2017)

Entre las consideraciones que este convenio establece, se indica:

> “Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia,

en particular mediante la adopción de una legislación adecuada y a la mejora de la cooperación internacional.” (Convenio Budapest)

Este hecho rectifica la preocupación del Estado por garantizar la seguridad de los ciudadanos costarricenses. Es sumamente importante que se pueda compartir información relacionada a los crímenes que se ejecutan a través de medios digitales del mismo modo, la colaboración entre Estados para poder llevar de forma estándar a un nivel de seguridad a la población.

5.4.5 Cuadro resumen:

País	Ley o regulación	Fecha de creación de la ley	Entes encargados	Otros aspectos
España	Ley 15/99 de protección de datos de carácter personal (LOPD)	13 de diciembre de 1999	La Agencia Española de Protección de Datos	Forma parte del Convenio de Budapest
México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares	05 de julio de 2010	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	No forma parte del Convenio de Budapest
Costa Rica	Ley 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales	05 de setiembre de 2011	Agencia de Protección de datos de los Habitantes	No hay sanciones División de incumplimiento por niveles a diferencia de México.

Al culminar este breve repaso por cada una de las regulaciones vigentes, es posible tener visión de cómo se encuentra cada uno de estos Estados en materia regulatoria. Sin duda, se han efectuado esfuerzos por parte de las autoridades, la creación de entidades para la protección del ciudadano en materia de privacidad y del uso y tratamiento de sus datos han venido a crear un sentido de respaldo. Es

importante que se pueda difundir de forma correcta a la población y que éstos conozcan que el país cuenta con las herramientas legales para su defensa.

Una de las grandes diferencias entre México y Costa Rica, es que ni la ley ni el reglamento Mexicano contienen definiciones o apartados en defensa explícita del Derecho al Olvido. Otra, entre estos dos Estados, es el mecanismo de financiamiento, en México, se estipula mediante la ley, que se dispondrá de un rubro en las partidas nacionales para el mantenimiento y protección de los ciudadanos.
En términos generales, podría decirse que el costarricense se encuentra en un estado de seguridad que se ajusta gracias a la legislación vigente a los cambios que la tecnología ha implementado con el paso de los años. Las leyes de protección, llámese de comercio, delitos informáticos, protección de datos personales, entre otras, brindan ese soporte necesario para que los ciudadanos puedan hacer uso de estas herramientas legales en el ejercicio de sus derechos. Es importante mencionar que desde el punto de vista de tecnología, también se encuentra en vigencia una serie de regulaciones que establecen los requerimientos mínimos para ciertas entidades, según sea su nicho de negocio. Una de estas regulaciones es la norma SUGEF 14-09 Reglamento sobre la Gestión de la Tecnología de Información, SUGEF 14-09 en relación con mecanismos para la gobernanza de las Tecnologías de Información en entidades financieras.

Por otro lado, la Contraloría General de la República, establece de carácter mandatorio para las entidades Gubernamentales, la implementación de la regulación denominada Normas Técnicas para la Gestión y Control Interno de las Tecnologías de Información, incluye en ésta, temas relacionados a la seguridad de la información y continuidad de negocio. Las leyes establecidas en países anglosajones, España, ha permitido que se imite en cierta medida este comportamiento, con la adhesión al convenio de Budapest, se confirma la preocupación que tiene el Estado por garantizar el bienestar de todos los ciudadanos.

6 Capítulo VI: Conclusiones

- Se concluye que es sumamente importante que las empresas desarrollen y actualicen sus metodologías o procesos para la administración de datos respetando siempre el principio de la privacidad y el cumplimiento legal o regulatorio, así como implementar o actualizar un marco de gobierno de uso de datos, aplicación de estándares de seguridad en las cuales se consideren realizar análisis de riesgos mediante técnicas que permitan implementar sistemas de gestión. Muchos pueden beneficiarse de la consolidación segura de infraestructuras y tecnologías para hacer frente a las necesidades que el mercado y los ciudadanos exigen. Es importante valorar que el cumplimiento con las regulaciones que se definan será un desafío para muchos incluyendo a las organizaciones y a los ciudadanos. A las empresas se les puede requerir la ejecución de evaluaciones de riesgo exhaustivas e implementar nuevas mejoras de seguridad, pero muchos tendrán que rediseñar las estrategias de gestión de datos e implementar procesos y tecnologías lo que representa costos económicos y de tiempo.

- Después de repasar la información descrita en los capítulos anteriores, se puede concluir que en materia relacionada al Derecho al Olvido, cada vez cobra una mayor importancia en las regulaciones sobre protección y tratamiento de datos personales, especialmente por el auge de las nuevas tecnologías que han permitido el uso de los datos y tratamiento de los mismos, lo que a su vez dificulta el control de los usuarios sobre sus datos personales.

- Se concluye que los países que se analizaron en esta investigación cuentan con características muy similares, considerando que poseen regulaciones que limitan el tratamiento de los datos, así como la búsqueda de la autodeterminación informativa, incluyendo además principios de

rectificación, acceso, oposición y cancelación. Además los tres países cuentan con entidades que se encargan de velar por que se efectúe la debida aplicación de las leyes emitidas, mismas que promovieron la creación de estos entes.

- Se concluye que hoy, debe ser prioridad para las organizaciones considerar cuidadosamente el tipo de información que se recopila sobre los ciudadanos y garantizar la que la recolección, almacenamiento y tratamiento de los datos cuenten con los principios de seguridad necesarios bajo la implementación de los controles técnicos correspondientes, desde su recolección hasta su almacenamiento. Los beneficios del negocio deben superar el riesgo.

- Producto de la promulgación de nuevas regulaciones, es probable que muchas de las empresas se vean afectadas por acciones como demandas por el mal uso o el uso sin consentimiento de los dueños de los datos. Por ejemplo, se espera que en Europa se efectúe uno de los cambios más grandes en el Reglamento General de Protección de Datos de la UE, que entrará en vigor en abril de 2018. Con la aplicación de dicho cambio se presentarán demandas de privacidad que necesitarán una atención renovada a la privacidad de datos para las empresas que ofrecen bienes y servicios a los ciudadanos de la UE. Las empresas que no cumplen con GDPR se enfrentan a multas de hasta el 4% de los ingresos anuales globales de la compañía.

- La necesidad de conocer y compartir en un mundo virtual ha permitido que las personas no midan las consecuencias de publicar información personal en sitios Web o redes sociales y de los cuales no podrán tener el control. La tecnología ha incluido, de eso no hay duda, sin embargo, es algo ya se encuentra en nuestro diario vivir, por lo tanto no podemos quitarlo de la noche a la mañana. Es importante que además de los elementos técnicos disponibles y de las leyes promulgadas para la defensa, se tomen las

medidas correspondientes por parte de los ciudadanos. El Estado tiene que encontrar los mecanismos correspondientes para generar ese sentido de protección, prevención y conciencia en la población.

- El ejercicio del Derecho al Olvido no debe permitir la intromisión o el incumplimiento de otros principios fundamentales como el acceso a la información, es decir, debe existir claridad para la definición de los datos que se buscan proteger, considerando la proporcionalidad.

- La implementación de controles técnicos para el debido tratamiento de los datos no debe verse como un gasto para las organizaciones o para el propio Estado, lo correcto es que sea vista como una inversión que permitirá por un lado evitar pérdidas por sanciones emitidas por los entes correspondientes, el bienestar del ciudadano.

- Costa Rica se encuentra en un estado aceptable desde la perspectiva de legislación sin embargo, nos encontramos en un estado de asimilación del cambio tecnológico y de los controles impuestos por la legislación, tal como lo establece el abogado costarricense Juan Diego Castro:
  "El impacto de la informática en el derecho costarricense, obliga a que nuestro ordenamiento jurídico se ajuste a estas novedosas tecnologías. La proliferación de bases de datos, tanto a nivel público como privado, exigen eficaces regulaciones que protejan los derechos fundamentales de los ciudadanos." (Castro, J.) Esfuerzos por parte de entes nacionales, en este caso, mediante el código de ética del Colegio de Profesionales en Bibliotecología de Costa Rica, capítulo XII "con respecto al acceso abierto y propiedad intelectual", Ítem D:
  "Los Profesionales en Bibliotecología deben procurar las condiciones más favorables para el acceso a los recursos de información, en nombre de sus usuarios y tratar de garantizar que el acceso no se vea afectado por las leyes de propiedad intelectual y que las licencias no anulen las excepciones que para las bibliotecas figuran en la legislación internacional." (COPROBI, 2017)

Referencias bibliográficas

Alguacil M., Cerrillo A., González S., Moro A. (2012). A las puertas de la administración digital: Una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015. España.

Adinolfi, Giulio. (2007). Autodeterminación informativa, consideraciones acerca de un principio general y un derecho fundamental. Cuestiones constitucionales, (17), 3-29. Recuperado de:http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932007000200001&lng=es&tlng=es.

Barrantes Echavarría, R. (1999). Investigación un camino al conocimiento. San José: Editorial UNED.

Bautista M. (2014). Deep Web: aproximaciones a la ciber irresponsabilidad. Revista Latinoamericana de Bioética1, pp.26-37.rev.latinoam.bioet. Obtenido de: http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S1657-47022015000100003&lng=e&nrm=iso

Castro. J. El Habeas Data en Costa

Cazau, P. (2006). Introducción a la investigación en ciencias sociales. Buenos Aires.

Convenio ciberdelincuencia Costa Rica. (19 de mayo de 2017).Costa Rica se adhiere a Convenio contra Ciberdelincuencia. Presidencia de la República.

Recuperado de: http://presidencia.go.cr/comunicados/2017/05/costa-rica-se-adhiere-a-convenio-contra-ciberdelincuencia/

Chacón, K. (20 de setiembre de 2015). Hackeo en CCSS enciende alarmas en seguridad de datos personales. *El Financiero*. Recuperado de: http://www.elfinancierocr.com/tecnologia/CCSS-hackeo-extraccion_de_datos-BAC_San_Jose-seguridad_informatica_0_813518666.html

Datos Personales Brokers. (15 enero del 2015). Así hacen dinero los 'data brokers' con tus datos en Internet. Libertad Digital. Obtenido de: http://www.libertaddigital.com/ciencia-tecnologia/internet/2015-01-15/asi-hacen-dinero-los-data-brokers-con-tus-datos-en-internet-1276538231/

DE Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. En: VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet. Revista de Internet, Derecho y Política. N. º 13, pág. 53-66. España. Universidad Oberta de Cataluña.

EsET.(2016) SET Security Report 2016. Obtenido de: https://www.welivesecurity.com/wp.../2016/04/eset-security-report-latam-2016.pdf

Ferrari, V., Schnidrig, D. (2015). Responsabilidad de intermediarios y derecho al olvido, aportes para la discusión legislativa en Argentina. (Argentina). Centro de Estudios en Libertad de Expresión y Acceso a la Información.

Garriga A. (2010).Tratamiento de datos personales y derechos fundamentales: desde Hollerith hasta Internet. España. Universidad de Vigo.

Galeano A. (2017). Reforma para borrar antecedentes de ex reos ya está funcionando. La Prensa Libre. Obtenido de: https://www.laprensalibre.cr/Noticias/detalle/100035/reforma-para-borrar-antecedentes-de-exreos-ya-esta-funcionando-

Guzmán M. (2013). El derecho fundamental a la protección de datos personales en México. Análisis desde la influencia del ordenamiento jurídico español. España. Universidad Complutense de Madrid.

Hernández, R., Fernández, C., & Baptista, P. (2010). Metodología de la Investigación. México D.F.: McGraw-Hill Interamericana.

Hernández Sampieri, R. (2010). Metodología de Investigación. Mexico: McGraw Hill Internamericana.

Higadera. (2014). El derecho a la protección de datos personales y la configuración del derecho al olvido. México. Universidad de Colima.

Hwangbo, H., Seckman S. (2016) *Blockchain Playbook- A technical primer on blockchain platforms*. Estados Unidos. PricewaterhouseCoopers.

ISC2. (2015). CBD Study CISSP. Estados Unidos. AuerbachPublications.

Escobar- J.Á. C.-M. (2008). humanas.unal.edu.co. Obtenido de humanas.unal.edu.co:

http://www.humanas.unal.edu.co/psicometria/files/7113/8574/5708/Articulo3_Juicio_de_expertos_27-36.pdf

Luna A. (21 de mayo de 2014). Data brokers: las empresas que no conoces pero que lo saben todo de ti. El Confidencial. Recuperado de: https://www.elconfidencial.com/tecnologia/2014-05-31/data-brokers-las-empresas-que-no-conoces-pero-que-lo-saben-todo-de-ti_138785/

McCallister E. (2010).Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).USA. National Institute of Standards and Technology.

Manzanero L. (2015). Sobre el derecho al olvido digital: una solución al conflicto entre la libertad de información y el derecho de protección de datos personales en los motores de búsqueda. España: Universidad Autónoma de Madrid.

Mieres J. (2014). El derecho al olvido digital. España: Fundación Alternativas.

Muñoz. F. (4 de agosto del 2014). «Data Broker»: cómo las empresas de datos controlan toda tu vida. ABC Tecnología. Recuperado de: http://www.abc.es/tecnologia/informatica-software/20140713/abci-comercio-datos-internet-data-broker-cookies-201407111531.html

Pochet A. (2005). Historia del derecho constitucional costarricense. Costa Rica, San José: Editorial Universidad Estatal a Distancia.

Platero, A. (2016). El derecho al olvido en internet. El fenómeno de los motores de búsqueda. Colombia. Universidad de Extremadura (España).

Pérez S. (2017) Tus datos se venden por 7 céntimos de euro. El País. Recuperado de: https://elpais.com/tecnologia/2017/05/03/actualidad/1493835469_309268.html

Rallo A. (2014). El derecho al olvido en internet: Google versus España. España. Centro de Estudios Políticos y Constitucionales.

Rodríguez, G., y Gil, J. (1996). Metodología de la Investigación Cualitativa. Granada: Aljibe.

Rodríguez, S. (2016). Los derechos de intimidad y protección de datos personales (Tesis de Licenciatura). Universidad de Costa Rica, Costa Rica.

Romanos de Tiratel, R. (2000). Guía de Fuentes de Información Especializadas. Humanidades y Ciencias Sociales. Buenos Aires: GREBYD.

Santín, Marina (2017). "The problem of the right to be forgotten from the perspective of self-regulation in journalism". El profesional de la información, v. 26, n. 2, pp. 303-310. La problemática del derecho al olvido desde la perspectiva de la autorregulación periodística. Universidad Rey Juan Carlos. Facultad de Ciencias de la Comunicación http://www.elprofesionaldelainformacion.com/contenidos/2017/mar/17_esp.pdf

Saquete, R. (8 octubre 2013). ¿Qué son y cómo funcionan las cookies? Human Level Coomunications. Recuperado de:

https://www.humanlevel.com/articulos/desarrollo-web/que-son-y-como-funcionan-las-cookies.html

Zorrilla Arena, S (1985) Introducción a la metodología de la investigación .México. Edit. Océano.