Universidad Tecnológica Ecotec

FACULTAD DE DERECHO Y GOBERNABILIDAD

Título del Trabajo:

ESTUDIO DE LAS INTERACCIONES EN LA RED COMO FUENTE DE VULNERACIÓN DE DERECHOS POR LA RECOLECCIÓN, USO Y COMERCIALIZACIÓN DE DATOS PERSONALES.

Línea de Investigación:

GESTIÓN DE LAS RELACIONES JURÍDICAS

Modalidad de Titulación:

PROYECTO DE INVESTIGACIÓN

Carrera:

DERECHO Y GOBERNABILIDAD

Autor:

ANDREA GABRIELA RODRÍGUEZ LÓPEZ

Tutor

AB. DAVID VERGARA SOLÍS MGTR.

Samborondón-Ecuador

2019

DEDICATORIA

Desde que nace hasta que muere, todo miembro del partido vive vigilado por la Policía del Pensamiento. Incluso cuando se encuentra solo no puede estar completamente seguro de estar completamente solo. Dondequiera que se encuentre, despierto o dormido, trabajando o descansando, en la cama o en el baño, puede ser inspeccionado sin que él sepa que lo están haciendo y sin previo aviso. (Orwell, 1949)

ANEXO N°16

CERTIFICACIÓN DE REVISION FINAL

QUE EL PRESENTE PROYECTO DE INVESTIGACIÓN TITULADO:

ESTUDIO DE LAS INTERACCIONES EN LA RED COMO FUENTE DE VULNERACIÓN DE DERECHOS POR LA RECOLECCIÓN, USO Y COMERCIALIZACIÓN DE DATOS PERSONALES.

ACOGIÓ E INCORPORÓ TODAS LAS OBSERVACIONES REALIZADAS POR LOS MIEMBROS DEL TRIBUNAL ASIGNADO Y CUMPLE CON LA CALIDAD EXIGIDA PARA UN TRABAJO DE TITULACIÓN, POR LO QUE SE AUTORIZA A: **ANDREA GABRIELA RODRÍGUEZ LÓPEZ,** QUE PROCEDA A SU PRESENTACION.

Samborondón, 06-07-2020.

AB. DAVID VERGARA SOLÍS, MGTR.

TUTOR

URKUND

Urkund Analysis Result

Analysed Document: Andrea Gabriela Rodríguez López.docx (D75079268)
Submitted: 6/16/2020 7:17:00 PM
Submitted By: mecoronel@ecotec.edu.ec
Significance: 4 %

Sources included in the report:

Cristina Arcos Mejía - Tesis Final.docx (D54383024)
Proteccion de datos Gabriel y Soledad.docx (D48961405)
TESIS.docx (D55652233)
PROYECTO DE INVESTIGACIÓN - ARQUI LLANGARI DAYANA KATERINE.docx (D63502112)
ENSAYO FINAL.docx (D63273821)
MORA MERCEDES-TITULACIÓN- MARZO 01-2020.docx (D64732519)
METODOLOGIA DE LA INVESTIGACION JOSE.docx (D54543496)
https://www.google.com/maps/timeline?gid=11540686536753669131 9&hl=es&pb=!1m2!1m1!1s2015-06-29
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ESProyecto

Instances where selected sources appear:

20

RESUMEN

El siguiente trabajo busca demostrar la realidad vulneradora de derechos que comprende el uso de las Tecnologías de la Información y Comunicación para las personas. El desplazamiento de las actividades humanas al mundo digital generó una nueva industria en el mercado, la llamada Economía de los Datos está basada en la recolección, el uso y la comercialización de datos y metadatos que se generan de las interacciones en la red con los usuarios. La falta de normativa regulatoria es aprovechada por las partes que comprenden la industria y por los gobiernos para recabar la información personal. Por esta razón, es una realidad que los datos personales, actualmente se encuentran desprotegidos.

El problema jurídico surge del carácter contractual que se le atribuye a las interacciones digitales, específicamente a las autorizaciones de los usuarios sobre el tratamiento de sus datos, sin considerarse la formación y el otorgamiento del consentimiento para el perfeccionamiento del contrato, que en algunas ocasiones implica la renuncia de algunos derechos de consumidor. Se ejemplifican los problemas existentes y se realizan encuestas direccionadas a explorar la falta de conocimiento y el desinterés del usuario en Internet.

Palabras clave: privacidad, vigilancia, datos personales, términos y condiciones, recolección de datos.

ABSTRACT

The following work seeks to demonstrate the reality of the infringement of rights that is involved in the use of information and communication technologies for people.

The displacement of human activities to the digital world generated a new industry in the market, the so-called Data Economy is based on the collection, use and commercialization of data and metadata that are generated from interactions on the network with users. The lack of regulatory standards is exploited by parties that comprise the industry and by governments to collect personal information. For this reason, it is a reality that personal data is currently unprotected.

The legal problem arises from the contractual nature that is attributed to digital interactions, specifically to the authorizations of users on the processing of their data, without considering the formation and granting of consent for the completion of the contract, which sometimes implies the waiver of some consumer rights.

Existing problems are exemplified and surveys are conducted to explore the lack of knowledge and disinterest of the user on the internet.

Key words: privacy, surveillance, personal data, terms and conditions, data collection.

ÍNDICE

Tabla de Ilustraciones

Tabla de Gráficos

Introducción

La creación de Internet y el uso de herramientas y servicios digitales generó un profundo impacto en la sociedad, cambiando radicalmente la vida de las personas. Nos encontramos frente a la necesidad de confrontar los problemas que surgen de las interacciones en la red y de las actividades como la recolección, el uso y la comercialización de datos personales, así como de la vigilancia y el rastreo que se realizan a través del empleo de medios tecnológicos.

La importancia radica en la protección que debe otorgar el Estado con relación a los derechos de las personas respecto del tratamiento de datos informáticos generados de las interacciones en la en la red, cuyo propósito es la creación de perfiles de comportamiento de los usuarios para actividades de publicidad o de vigilancia. En consecuencia y frente a la carente legislación nacional sobre la protección de datos de carácter personal, es apremiante que nos encaminemos con la corriente mundial, transformando y actualizando nuestro ordenamiento jurídico, cuyo fin debe ser la protección de los datos personales, en respeto y garantía de los derechos fundamentales.

Planteamiento del problema científico

La necesidad surge por la falta de normas que regulen y garanticen una efectiva protección, así como un adecuado tratamiento de datos informáticos de las personas en el país, al momento de realizar interacciones sociales y operaciones comerciales de toda clase y el desconocimiento de los derechos que corresponden a los usuarios y consumidores de Internet.

Para llegar a una situación óptima debe actualizarse el ordenamiento jurídico ecuatoriano, incluyendo nuevos conceptos de las tecnologías que promueven

la protección de las personas. Enfrentando la realidad de las compañías y corporaciones, sean nacionales o extranjeras que realizan actividades de recolección, uso y comercialización de datos personales.

Respecto a lo que se conoce hasta ahora, la legislación ecuatoriana contiene la definición del derecho de protección de datos personales, que se encuentra en el Art. 66 numeral 19 de la Carta Magna. No obstante, no existe una norma secundaria que desarrolle el contenido de este derecho fundamental. Sólo encontramos disposiciones dispersas que hacen relación a este derecho: el Art. 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el Art. 6 de la Ley Orgánica de Registro de Datos Públicos. En lo que respecta a la protección jurídica del derecho de protección de datos, existen dos vías: una constitucional, relativo a la acción de Habeas Data en el artículo 92 de la Constitución de la Republica del Ecuador y una penal, mediante la tipificación del delito de violación a la intimidad tipificado en el Artículo 178 del Código Orgánico Integral Penal.

El pilar fundamental para el uso de datos personales implica contar con el consentimiento del titular de los datos para que sean tratados por terceros. Este es el principal problema. Es necesario que el aprovechamiento del consentimiento por parte de terceros sea limitado, siendo esto el mecanismo idóneo para otorgar la protección debida al titular de los datos personales que se encuentran en forma de datos informáticos. Todos los servicios, sean privados o públicos, requieren datos personales de los consumidores y usuario, sin embargo, su acceso debería ser proporcional a la finalidad de su recogida.

Actualmente la Asamblea Nacional se encuentra discutiendo el Proyecto de Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales, que no ha sido aprobado por la apretada agenda legislativa, pues se le ha dado prioridad a otras normas “más urgentes”. Sin

embargo, es muy probable que sea aprobada la ley en este ultimo año de gestión del gobierno actual.

El resultado que se espera es exponer la vulneración de los derechos de las personas naturales producto del comercio indiscriminado de datos personales y el error de los conceptos que se utilizan al regular el tema. Se lo realizará a través de la sugerencia de medidas que promuevan la protección del usuario en la red.

Objetivo General

Demostrar la forma en que terceros recolectan, usan y comercializan datos personales, así como realizan actividades de vigilancia y rastreo a través del empleo de medios tecnológicos las malas prácticas de ciertos operadores promovidas por la falta de normativa nacional y de la vulneración de derechos.

Objetivo Específico

Analizar medios documentales, con los que se comprueba el tratamiento de datos de carácter personal.

Determinar el uso abusivo del concepto de consentimiento y de las prácticas contractuales que se generan en la red, en desmedro de los derechos fundamentales de intimidad y libertad.

Exponer medidas que promuevan la protección de datos y los derechos de las personas en la red, desde una posición en la que se considere al usuario como la parte vulnerable de las relaciones contractuales que se generan.

Justificación

Es necesario abordar este grave problema, por la velocidad con la que la realidad tecnológica toma parte en nuestras vidas, haciendo que la falta de normas frente al avance tecnológico facilite la vulneración de los derechos, por parte de quienes son responsables de la recopilación y tratamiento de datos personales.

Se espera como resultado la socialización de la información y el empleo de medidas que pretenden garantizar la inviolabilidad de los derechos de las personas naturales, mencionando que estas pueden implementarse de manera local como en las actividades que corresponden a la Universidad Ecotec. Para lograr esta protección es necesario que se refuercen, especifiquen y consideren los derechos de las personas por sobre quienes tratan y determinan el tratamiento de los datos de carácter personal, que, para aclarar, no son los legisladores del mundo.

Aspecto Novedoso

En cuanto a lo que se pretende transformar, dándole solución al problema emergente mediante el trabajo que incluirá el elemento de la creatividad e innovación, es necesario reconstruir, delimitar y actualizar conceptos primarios que deberán considerarse fuente de las sugerencias que tendrán por objeto impedir el menoscabo de derechos y garantizar el acceso eficaz a la protección jurídica de los datos informáticos.

CAPÍTULO I: MARCO TEÓRICO

Antecedentes

El uso de internet y las obligaciones que se contraen por parte de los consumidores

En Internet los usuarios realizan todo tipo de actividades ya sean comerciales, profesionales o aquellas relacionadas a la vida privada de éstos. Hoy, las comunicaciones interpersonales en su mayoría suceden mediante el empleo de dispositivos conectados a la red.

Para el año 1999, el número de usuarios en internet alcanzaba los 248 millones correspondiendo al 4.1% de la población mundial. Durante el año 2019 la cifra alcanzó los 4,536 millones equivalente al 58.8% de ésta (Miniwatts Marketing Group, 2019). En el Ecuador, el último informe sobre tecnologías de la información y comunicación del Instituto Nacional de Estadísticas y Censos, del año 2017, arrojó que el 58,3% de la población utiliza internet, que un 40,7% lo emplea en la búsqueda de información y el 31,0% en actividades de comunicación (Instituto Nacional de Estadisticas y Censos, 2017).

Este canal de transferencia masiva de información generó una nueva industria comercial, que tiene como materia prima a los datos que se generan de los rastros y registros informáticos por la navegación en la red, y que se da dentro de la llamada Economía de los Datos. Los gigantes tecnológicos oferentes de plataformas informáticas y la industria de la publicidad han visto incrementar sus ganancias con las prácticas comerciales que produce el tratamiento de datos.

Las compañías proveedoras de servicios en Internet imponen los requisitos para el uso de sus plataformas. Estos requisitos se encuentran establecidos en los llamados Términos y Condiciones, los cuales son

considerados como contratos de adhesión o condiciones generales de contratación, que tienen por objeto el tratamiento de los datos que se generan con el uso de cualquier servicio.

Así, mediante las cláusulas que establezca el propietario de la plataforma, se obtendrá la autorización para que toda la información que se pueda extraer sea cotejada. Menciona (Guerra Balic, 2017) que: “el elaborador electrónico goza de una verdadera autonomía respecto a la voluntad de las partes contratantes”. Ante la escasa legislación, los derechos de intimidad, libertad y confidencialidad de correspondencia se ven afectados.

Constituye sin duda un reto para los legisladores, encaminar sus esfuerzos por comprender los nuevos conceptos de la realidad digital que escapan de la regulación tradicional al simplemente no tener cabida en ella (Moreno Navarrete, 2016).

Los contratos electrónicos: términos y condiciones de uso

La celebración de contratos en Internet se da de manera incesante, todos los días los usuarios en la web autorizan el uso y tratamiento de sus datos personales con la aceptación de los términos y condiciones de una plataforma de servicios.

El contrato electrónico, siendo una variación del contrato general, implica el empleo de redes electrónicas por donde se transmiten mensajes de datos y es a través de éstos en donde las personas naturales o jurídicas, realizan actividades de distinta índole (Fernández Fernández, 2017). Así como lo establece la Ley de Comercio Electrónico, Firmas y Mensajes de Datos en su artículo 44, lo que implica una diferencia sustancial entre un contrato electrónico y los de otro tipo, es la forma en que este surge, es decir, que su perfeccionamiento se realiza a través del uso de los medios electrónicos, por mensajes de datos y redes electrónicas, para el envío de la oferta y la

aceptación (Ley de Comercio Electrónico, Firmas y Mesajes de Datos, 2014). La ley, les otorga la validez y perfeccionamiento con el cumplimiento de los requisitos que se establecen para los contratos en general.

Lo que interesa, a mas de las características técnicas que posibilitan la celebración de contratos a través de Internet, es el acto como tal, en donde se establecen las disposiciones del uso de los sitios o plataformas mediante cláusulas incluidas en los llamados contratos de Términos y Condiciones, que constituyen contratos de adhesión para el uso del servicio. Generalmente, éstos son autorizados por el usuario al realizar una acción afirmativa de *clic* sobre un mensaje de dato, de manera general su aceptación implica la cesión de ciertos derechos de los usuarios al propietario del sitio e inclusive a terceros, así como por ejemplo lo establecen las políticas legales de la red social *Facebook*.

> Cuando compartes, públicas o subes contenido que se encuentra protegido por derechos de propiedad intelectual en nuestros productos, o en relación con ellos, nos otorgas una licencia internacional, libre de regalías, sublicenciable, transferible y no exclusiva para alojar, usar, distribuir modificar, publicar, copiar, mostrar, o exhibir públicamente y traducir tu contenido. (Facebook, 2018)

Además de los contratos celebrados en las plataformas cuando se realiza la adquisición de un servicio, son importantes también aquellos que se refieren a la aceptación de términos y condiciones que tienen como fin el alojamiento de *cookies*, como los que surgen producto de la navegación de sitios en la web. Al aceptarse los términos y condiciones se entiende que el consentimiento del usuario es manifestado teniendo como resultado la validez del acto que se ha celebrado en la red (Guerra Balic, 2017).

Sin embargo, una de las características cuestionables de estos actos de aceptación de términos y condiciones está relacionada a la manifestación

del consentimiento sin que se configuren en éste las condiciones necesarias para que sea tomado como válido, pues el usuario generalmente no es informado con claridad sobre las implicaciones de dichos contratos, en lo relativo a sus derechos de imagen, privacidad, reputación, honor, buen nombre, etc.

El consentimiento

El consentimiento es una construcción jurídica que hace referencia a la exteriorización de la voluntad de un individuo frente a determinado acto u oferta, con el que se pretende se produzcan efectos jurídicos en el mundo real (Oviedo Albán, 2016). Al respecto (Garcés Vásquez, 2014) menciona que: “El consentimiento como manifestación de la voluntad que no deja lugar a dudas es una expresión autónoma del individuo constituido como parte dentro del negocio jurídico, es decir que tiene plenas competencias para ejercerla: tomar sus propias decisiones y asumir las consecuencias de sus actos”.

El artículo 1461 del Código Civil Ecuatoriano establece que: “Para que una persona se obligue a otra por un acto o declaración de voluntad es necesario: Que sea legalmente capaz; Que consienta en dicho acto o declaración, y su consentimiento no adolezca de vicio; Que recaiga sobre un objeto lícito; y, Que tenga una causa lícita (Código Civil, 2019).

Además, en el artículo 1456 del mencionado cuerpo legal, se dispone que el perfeccionamiento de los contratos consensuales se da específicamente por el solo hecho del consentimiento (Código Civil, 2019). Así también, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, en su artículo 46, que los contratos realizados a través de mensajes de datos por medios electrónicos se perfeccionan cumpliendo los requisitos de ley (Ley de Comercio Electrónico, Firmas y Mesajes de Datos, 2014) . En la misma línea el Código de Comercio en su artículo 228, considera que la realización de un hecho inequívoco de ejecución contractual implica la aceptación tácita de

alguna una oferta realizada y por tanto otorga el perfeccionamiento de éste (Código de Comercio, 2019).

Al ser el consentimiento uno de los elementos que le otorgan a los actos jurídicos validez y eficacia, denota que tan importante como la expresión de la voluntad es la construcción que se genera detrás de ella, es decir, en los procesos cognitivos que tienen lugar en el ser. Así, al ahondar en el desarrollo de la aceptación que se ocasiona posterior a una proposición u ofrecimiento es necesario mencionar la capacidad con la que debe contar una persona y que demuestre su habilidad deliberativa, además de la información de la que debe disponer en el momento de la reflexión.

Si suponemos que, durante el proceso deliberativo, una de las partes se comporte de manera poco auténtica en relación con aquello que es objeto de la oferta, entonces no podríamos hablar de comprensión adecuada, por lo que, quien delibera estaría asumiendo una postura deformada de la realidad. De la misma manera se dará cuando exista falta de información durante el referido proceso intelectual, y sobre este escenario también cuando estas deliberaciones impliquen la restricción, renuncia o cesión de un derecho a través de un contrato, como lo es en el caso en el que el usuario acepta los términos y condiciones de una plataforma o producto y que esta signifique la renuncia al derecho a la privacidad y sobre la confidencialidad de su información personal. Al respecto (Londoño Vásquez, Rendón Ángel, & Marín Muñoz, 2015) mencionan que: “En tanto que los deliberantes no se hagan lingüísticamente competentes y no estén anímicamente dispuestos a no caer en la tentación de la inescrupulosidad y la manipulación a través del discurso, la política deliberativa será tan utópica como su antecedente ilustrado”.

Como se mencionó anteriormente, al ser el consentimiento uno de los elementos primordiales para el nacimiento y la existencia de una obligación, la Ley de Comercio Electrónico hace mucho énfasis en su manifestación. El artículo 48 del mencionado cuerpo legal, habla sobre el consentimiento

informado, esto es la posibilidad que tiene quien recepta la oferta que se realiza de contar con los elementos necesarios para deliberar sobre la misma: “el consentimiento debe de ser informado y lo hará si se le hace saber de forma clara sobre lo que se requiere para acceder” (Ley de Comercio Electrónico, Firmas y Mesajes de Datos, 2014).

Entonces, podemos establecer que: los contratos electrónicos son considerados válidos siempre que estos cumplan con los requisitos establecidos en la ley ya que existe un marco normativo que los rige.

Sin embargo, ¿Pueden considerarse realmente como contratos válidos a aquellos que los usuarios contraen por el mero hecho del uso de un sitio web o de aquellos en los que el usuario no puede realizar una acción distinta que la de aceptar? Para contestar esta interrogante, primero se debe conocer la diferencia entre las formas de contrato electrónico que suceden habitualmente en la red.

Los contratos de click-wrap y de browse-wrap

Entre las formas en las que pueden presentarse los contratos electrónicos, se encuentra en primer lugar el contrato de *click-wrap*, es aquel en el que se requiere una acción afirmativa o *click* sobre algún mensaje por parte del usuario. Esta acción es considerada como manifestación expresa de la voluntad y por consiguiente aceptación inequívoca de los términos y condiciones, dotando así de validez el contrato suscrito (Kim , 2013).

Como ejemplo, en la página del Servicio Nacional de Derechos Intelectuales, en adelante SENADI, se puede observar que al ingresar aparece un recuadro en la parte inferior en donde explica que para continuar navegando la aceptación sobre los términos de la política al tratamiento de datos personales es necesaria.

Al revisar dicha política nos encontramos con la siguiente información:

> Uso de cookies: Este portal web utiliza cookies para mejorar la navegación y la calidad del sitio web. No compartimos sus datos personales. Cuando hace clic o interactúa con un anuncio o banner, existe la posibilidad de que el propietario de este recurso pueda colocar una cookie en su navegador con sus propias condiciones de uso. (Servicio Nacional de Derechos Intelectuales, 2019)

En segundo lugar, se considera como contrato de *browse-wrap* a aquel que por el mero uso del sitio se entiende como aceptado, no requerirá entonces que el usuario realice manifestación alguna explícita sobre su voluntad en consentir con la aceptación de este (Kim , 2013). Se podría considerar que el usuario que entra a un sitio jamás conocerá sobre la existencia de un contrato y menos que esté aceptando cualesquiera sean los términos y condiciones que se imponen en el mismo a través de las cláusulas, ya que se presume aceptado por el hecho de la navegación (Mann & Siebeneicher, 2015).

Se expone como ejemplo al portal web de la institución financiera Banco del Pichincha, cuando se accede a este no existe indicación alguna sobre el tratamiento de datos y las políticas de privacidad, por lo que el contrato existente correspondería a los de tipo *browse-wrap*, al buscar sobre las mismas se encuentra la siguiente información: “Al acceder a esta dirección electrónica y a cualquiera de sus direcciones y páginas anexas o conexas (en adelante, “la Web”) usted adquiere la calidad de usuario, y, por lo tanto, acepta las estipulaciones aquí contenidas” (Banco del Pichincha, 2020).

Al continuar con la búsqueda sobre las estipulaciones se encuentra la cláusula de declaración y utilización de información que menciona:

> El usuario, conoce y acepta que sus datos personales, a los que Banco Pichincha C.A. tenga acceso como consecuencia de consultas (…) y servicios que tengan lugar por cualquier medio, o de procesos

> informáticos, se incorporan a la información del usuario registrada en el Banco Pichincha C.A., autorizando a este al tratamiento de los que sean necesarios para el uso de sus datos en la oferta y contratación de productos y servicios, así como para el desarrollo de acciones comerciales, sean de carácter general o adaptado a sus características personales. (…) Autoriza la comunicación o cesión de los mencionados datos a las sociedades pertenecientes al Grupo Financiero Banco Pichincha con el mismo objeto indicado en los apartados anteriores (…) (Banco del Pichincha, 2020).

Al respecto de este punto y respondiendo a la interrogante, la doctrina ha debatido acerca del requisito del consentimiento y comprendemos que al silencio no se le otorga ningún tipo de valor de aceptación (Solar, 2015). También podemos observar la normativa, en el segundo inciso del artículo 46 de la Ley de Comercio Electrónico: “La apertura del mensaje de datos no implica aceptación del contrato” (Ley de Comercio Electrónico, Firmas y Mesajes de Datos, 2014). En concordancia con el artículo 243 del Código de Comercio: “La recepción, confirmación de recepción, o apertura del mensaje de datos no implica aceptación del contrato” (Código de Comercio, 2019). Se evidencia que la norma pretende entregar una protección para que no exista celebración de un contrato sin que el consentimiento sea manifestado inequívocamente pero solo en las actividades de transacciones comerciales convencionales, mas no de las que surgen a raíz de interacciones cotidianas por el uso de la red, ya que no podría afirmarse que para estos casos la ley pueda ser aplicada de manera directa.

En otras palabras, para que el consentimiento sea válido en los contratos tipo *browse-wrap*, debe existir una manifestación inequívoca de ejecución del contrato, como lo podría ser, crear una cuenta en la página web del banco para realizar las transferencias electrónicas. Sin embargo, no podría considerarse como consentimiento válido el sólo hecho de apertura de la

página o visitarla, pues no existe intención del usuario en contratar electrónicamente con la institución financiera ni usar sus servicios.

¿Qué se acepta cuando se autorizan los términos y condiciones al usar una plataforma en la red?

Como se ha mencionado, el uso de sitios y dispositivos electrónicos implica la aceptación a las estipulaciones de los términos y condiciones, que tienen como objetivo la autorización para recopilar, usar y procesar los datos que generan los usuarios en dichas plataformas; como los de contenidos, interacciones, búsquedas, comunicaciones o de canales de mensajería y también el de los metadatos -los datos de los datos- que se refiere a aquellos de los que se obtiene características contextuales descriptivas de cierta información, como las de geolocalización, la identidad de quienes se comunican, el tiempo de comunicación, etc., convirtiéndose cada plataforma en propietaria de esta información y que en su conjunto ofrece un conocimiento ilimitado del usuario de internet. Se promueve el tratamiento de estos datos como base para la optimización de las plataformas con el objetivo de ofrecer un servicio personalizado basado en las preferencias del usuario como resultado del análisis de su comportamiento y también para actividades de publicidad (Golbeck, 2015).

Otras condiciones de uso incluyen el alojamiento de archivos – cookies- en los dispositivos electrónicos con el fin de extraer información correspondiente a la localización, los proveedores de pago, a las redes de proveedores del servicio de internet e inclusive a la información de fecha y hora.

El alojamiento de cookies

Las cookies, son pequeños fragmentos de información que se alojan en los ordenadores de los usuarios cuando visitan un sitio web, lo que se espera con su descarga, es el almacenamiento de datos del usuario para su posterior recuperación por parte del responsable de su instalación. Estas pueden ser propias o de terceros cuando los sitios han permitido incluirlas, también pueden ser activadas por una sola ocasión, como las llamadas cookies de sesión, utilizadas para almacenar datos de acceso o ser activadas de manera permanente, como las llamas cookies persistentes, cuya utilización puede implicar años. Se promueve su necesidad alegando la funcionalidad de las plataformas, pero las cookies no solo sirven para ayudar a mejorar la experiencia del usuario en el sitio, recordando las acciones de este en él, sino, también para almacenar direcciones IP, rastrear y obtener datos sobre los hábitos de navegación (Martínez Pastor & Muñoz Saldaña, 2016).

La finalidad de la obtención de datos es su tratamiento. Los tipos de cookies que existen tienen relación con los propósitos de procesamiento de información especifica, así tenemos a:

1. Las cookies técnicas, que tienen relación con el uso de la plataforma y la utilización de opciones dentro de ella.
2. Las cookies de personalización, que se refieren a los criterios del tipo por el que se accede al servicio, como el navegador, la información regional, el idioma, etc.
3. Las cookies de análisis, que están enfocadas al estudio y medición del comportamiento del usuario en la plataforma cuyo objetivo es la creación de perfiles de navegación.
4. Las cookies de publicidad, que se encargan de administrar los espacios de anuncios incluidos en la plataforma y de los elementos relacionados a la presentación de publicidad en base a los perfiles de navegación.

Como se mencionó anteriormente, una de las funciones que tiene el uso de cookies es obtener información, como la correspondiente a direcciones IP. La *internet protocol address*, es una secuencia de números que atañe a la dirección de un dispositivo. Su función es identificar un espacio o punto de conexión entre la red y un *host*, éste último se refiere a dispositivos que proveen y utilizan servicios en la red. Este protocolo permite diferenciar e identificar a todos los ordenadores conectados (Verdejo Alvarez , 2018).

A continuación, a manera de ejemplo veremos la información que puede obtenerse de la dirección IP. En la página web gratuita *Ultratools*, fueron ingresando los dígitos que corresponden al IP de un teléfono móvil, automáticamente el programa muestra la información correspondiente a la identificación en la red, incluyendo longitud y latitud de la ubicación del dispositivo.

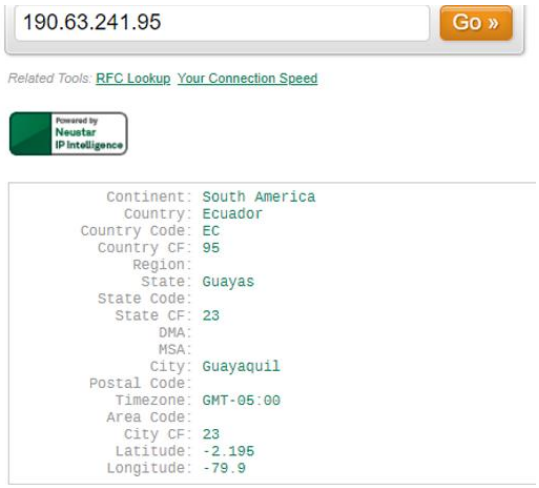

Ilustración 1

Fuente: Pagina Web http://www.ultratools.com/

Con el uso de la página *mapadirections* en donde pueden revisarse coordenadas geográficas con la información de latitud y longitud, en segundos se estableció en donde se encontraba el dispositivo móvil.

Ilustración 2

Fuente: Pagina Web http://mapadirections.info/

Con la aceptación de los términos y condiciones que realiza un usuario al ingresar en un sitio web, permitiendo el alojamiento de cookies en el ordenador o dispositivo móvil y su posterior captación y envío de información, compañías como Google, posee registros inequívocos sobre ubicaciones, lugares visitados, medios de transportes usados y horarios de permanencia de cualquier usuario.

De manera rápida es posible para el usuario saber sobre los datos que guarda Google al respecto. Con el empleo de una cuenta de Gmail, buscando en la opción *location.* Lo primero que se observa al ingresar es el siguiente mensaje: “El dispositivo móvil informa la ubicación” (Google, s.f.)

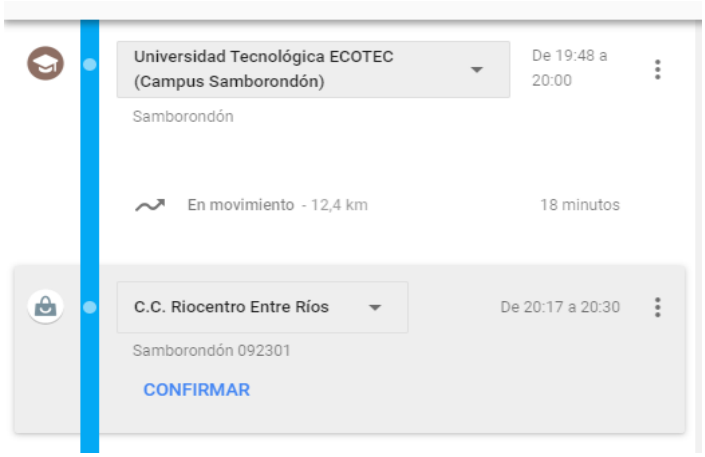

Ilustración 3

Fuente: Página Web de Google, ubicaciones de usuario Gmail https://www.google.com/maps/timeline?gid=11540686536753669131 9&hl=es&pb=!1m2!1m1!1s2015-06-29

La información presentada ofrece datos de actividades y hábitos de una persona, que se encuentran disponible para diversas industrias al no existir norma alguna que prohíba el uso de *cookies*.

Con el ánimo de proteger la privacidad de los usuarios en la red (Apple, 2017) implementó en su buscador Safari un programa Inteligente de Prevención de Rastreo. Su funcionalidad consiste en borrar la o las *cookies* de cualquier dispositivo 24 horas después de que esta estuvo alojada impidiendo así que esta pequeña pieza de información continúe recolectando datos. Este ejemplo evidencia que existen herramientas que pueden ayudar a la protección de cierta información en distintos dispositivos.

Los datos personales en el internet

A consecuencia del uso de distintas plataformas, servicios y productos informáticos, sean gratuitos o de pago, sus usuarios al aceptar los términos y condiciones ceden los derechos de la información que se incluye o que se genera en éstos, indiscutiblemente esta corresponde a información personal. Debemos establecer las características de los llamados datos personales, la protección que la ley debe otorga a éstos y la importancia que tienen como base en la nueva Economía de los Datos.

Los datos personales

Al hablar de datos personales, nos referimos a toda información de carácter personal o íntimo, con la que se puede identificar a una persona y que es materia de protección en la legislación. La cual no está sujeta al principio de publicidad pues se entiende como aquella que se deriva de los derechos personalísimos y fundamentales consagrados en la constitución.

El articulo 4 del Reglamento General de Protección de Datos de la Unión Europea define a los datos personales como:

“Toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo el nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física” (Comisión Europea, 2016)

En este contexto y considerando las actividades que las personas realizan a través de las plataformas en Internet. (Gozaíni, 2018) refiere que la información que se producen en éstas son datos personales y que inclusive presuponen en su conjunto la identidad digital de cada usuario, incluyéndose aquellos que no necesariamente surgen con el uso de internet, sino que se cotejan a través de éste o del empleo de sistemas como sucede con los datos biométricos.

Los datos biométricos comprenden el registro de imágenes, voz, huellas o iris de personas, sobre éstos se aplican técnicas de extracción de características particulares cuya finalidad es la relación a una identidad específica.

La relevancia que los datos tienen en el mundo actual proviene del volumen que se producen de las interacciones y que pueden ser cuantificados por las empresas de procesamiento de información, que encontraron en este gran conjunto de datos - *big data* - una nueva industria que se ha ido desarrollando en los últimos diez años de internet. “Las compañías como Google y Facebook, vieron la oportunidad de construir modelos de negocios basados en la captura de los datos personales de los usuarios” (Assange, 2016)

El derecho a la Intimidad como base del derecho de protección de datos

Antes de la existencia del derecho de intimidad como lo conocemos hoy. Los derechos de la propiedad y de la libertad, protegían los bienes y a las personas. La revolución industrial y la aparición de instrumentos de comunicación y reproducción masiva, como la fotografía y la imprenta, produjeron cambios drásticos en la sociedad contemporánea. Es así como el uso indiscriminado de dichas herramientas, invadieron las esferas de desarrollo de las personas, provocando un malestar generalizado en ciertos sectores de la población. (Peces-Barba, 2016)

Los primeros vestigios que se tienen sobre el derecho como tal a la privacidad dentro de la edad moderna los podemos encontrar en una obra de 1890, de quienes construyeron y defendieron el derecho a la privacidad, al respecto podemos ver que mencionan:

> La intensidad y complejidad de la vida, atendido los avances de la civilización, han hecho necesario un cierto apartamiento del mundo, y

> el hombre, bajo el refinado influjo de la civilización, ha llegado a ser más sensible a la publicidad; de modo que la soledad y privacidad han llegado a ser más esenciales para el individuo. Pero las empresas e inventos modernos, invadiendo su privacidad le han producido un sufrimiento mental y angustia mayor que las que se les podrían infringir por una mera lesión corporal. (Warren & Brandeis, 1890)

En América latina la mayoría de las legislaciones adoptaron por asimilar y establecer a la intimidad como derecho no incluyendo así la palabra privacidad de manera explícita, aunque evidentemente refiriéndose a la protección que se le procura dar a la esfera personal de la vida de los seres en sociedad, es así el caso de nuestra legislación como podemos observar en el artículo 66 de la Carta magna, correspondientes a los derechos de libertad, en su numeral 20: “el derecho a la intimidad personal y familiar”; numeral 21. “El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual”; 22. “El derecho a la inviolabilidad de domicilio” (Constitución de la República del Ecuador, 2008) y en cuanto a las acciones que tiene el ciudadano para acudir ante la autoridad correspondiente, cuando quiera conocer sobre los datos que otros poseen se tiene la garantía jurisdiccional de Habeas Data en el artículo 92.

En el sentido de legislación comparada vemos el caso argentino, en donde se recoge explícitamente el término derecho a la privacidad, establecido en su Constitución en el artículo 19: “Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados” (Constitución de la Nación Argentina, 1994).

Si bien existe una similitud en cuanto al empleo de los términos tanto en la comparación de legislaciones como en el ámbito doctrinal, es acertado traer la división que realiza el autor Carlos Santiago Nino, sobre la diferencia y el complemento que existe entre los conceptos. En cuanto a la privacidad,

tenemos como a las acciones que se encuentran fuera del escrutinio, aunque se produzcan en público siempre que no dañen a terceros; y a la intimidad, como aquella reserva de circunstancias personales que realiza un sujeto para que ciertos aspectos no sean conocidos por otros (Nino, 2017).

El derecho de protección de datos en la legislación ecuatoriana

El derecho a la protección de datos se entiende como la suma de principios, derechos y garantías establecidos a favor de las personas para proteger su información, se fundamenta en el derecho a la intimidad y en la facultad que éste entrega a su titular para exigir la reserva de sus acciones. (Gozaíni, 2018). La diferencia sustancial entre el derecho a la intimidad y el derecho a la protección de datos personales es que el primero refiere el poder que otorga la ley a una persona sobre su esfera intima mientras que el segundo al poder sobre los datos que la persona genere independiente de si son íntimos o no. En esencia, consiste en la facultad del titular para decidir sobre el acceso y uso de sus datos personales por terceros.

La ley, le otorga protección a la información restringiendo a otros su acceso, como a aquellos mencionados en el artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos que establece:

> Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. (Ley Orgánica del Sistema Nacional de Registro de Datos Públicos , 2017)

Sin embargo, este concepto no es absoluto y a pesar de la protección brindada por la carta magna, también permite que el titular de la información pueda consentir en la utilización respecto de terceros, así como se encuentra dispuesto en el artículo 66 de la Constitución de la República del Ecuador, que en su numeral 19 menciona:

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

Al analizar lo establecido en la ley, la problemática radicaría entonces en la autorización de la utilización de información correspondientes a datos personales, como los anteriormente nombrados, debido a que esta se encuentra protegida por los principios de confidencialidad y reserva, que emanan del derecho mismo a la intimidad, por ello es de especial atención velar por el cumplimiento de dicho requisito para cumplir con las normas expedidas para su protección. Así como lo indica el artículo 9 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos que establece:

> La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución política de la Republica y esta ley, los cuales podrán ser utilizados o transferidos con autorización del titular u orden de autoridad competente. (Ley de Comercio Electrónico, Firmas y Mesajes de Datos, 2014)

Comprendemos que el acopio de estos datos no autoriza al tercero a hacer uso de un manera libre e ilimitada de la información recogida, es deber del mismo detallar junto a los fines específicos del acopio, las futuras formas

de utilización de la información, las reglas destinadas a garantizar la claridad de la operación y el conocimiento de ésta por los titulares.

La Economía de los Datos y la industria de la publicidad

La publicidad, su función persuasiva y la relación entre los productos informáticos y la influencia en el comportamiento humano

En el contexto del desarrollo del presente tema, la industria de la publicidad tiene un papel protagónico dentro de la Economía de los Datos, el tratamiento de éstos junto al empleo exitoso de medidas de influencia mediante las plataformas le permitió reinventar su modelo de negocio convirtiéndose actualmente en una de las actividades comerciales más lucrativas en la Era Digital, es por esto que, debemos resaltar su importancia y considerar los efectos que produce y producirá en la realidad moderna.

La publicidad, es una actividad de promoción de ideas, bienes y servicios realizados por una marca, grupo e inclusive por un gobierno. Se encuentra asociada a la forma de influir sobre un objetivo a través de mensajes que pueden utilizar distintos tipos de comunicación (Kotler & Armstrong, 2017).

En palabras de (Ferrer, 2015) sobre la persuasión de la publicidad:

> Si el lenguaje es un arma de convencimiento y sugestión entre los humanos, el lenguaje de la publicidad es el instrumento para alcanzar aquel objetivo hasta sus últimas consecuencias.

Uno de los grandes objetivos de la publicidad ha sido promover el consumo de bienes y servicios masivos a través de técnicas de persuasión que las industrias han fomentado con el empleo de discursos retóricos en temáticas explícitas como en el de los ideales fantásticos de belleza, lo cuestionable de este tipo de situaciones es que los publicistas han dejado de lado los valores éticos que deberían tener (Spurgin, 2003).

> Cuanto más atractivo visualmente sea el producto para su público objetivo, más probabilidades tendrá de ser persuasivo. El diseñador puede revisar las revistas que lee el público y la música que escuchan, observar la ropa que usan, determinar que tendencias son populares entre ellos y buscar otras pistas sobre lo que les puede resultar atractivo. (Fogg, 2016)

Hasta hace unos años, la publicidad en la red llegaba indiscriminadamente, es decir, que quien pretendía promover una idea o un producto debía elaborar un único mensaje que llegaría a todos los usuarios de una plataforma por igual. Hoy el mensaje publicitario está adecuado al receptor basado en las preferencias que se obtienen con la recolección y tratamiento de los datos de su comportamiento en la red. Como así lo establece *Facebook* en su política de datos.

> Usamos la información que tenemos (incluida la actividad que realizas fuera de nuestros productos, tal como los sitios web que visitas y los anuncios que ves) para ayudar a los anunciantes y otros socios a medir la eficacia y distribución de sus anuncios y servicios, así como a entender que tipo de personas los usan. (Facebook, 2018)

Considerando la influencia que produce lo que vemos y oímos a través de la publicidad, ¿Es posible encontrar una relación entre su función persuasiva, los productos tecnológicos – que van desde páginas webs hasta dispositivos electrónicos- y los cambios en el comportamiento humano? Para contestar esta interrogante empezaremos reconociendo la cantidad de tiempo a la que las personas de manera general le dedican al uso de la tecnología.

Counterpoint research, es una compañía de análisis de la industria de la tecnología, los medios y de las telecomunicaciones, que en el año 2017, publicó un estudio sobre el tiempo que los usuarios de los *smartphones* destinaban para el uso diario de los dispositivos, en él encontramos que el

29% de manera global pasaba entre 3 a 5 horas diarias, mientras un 26% utiliza más de 7 horas su teléfono móvil (counterpointresearch.com, 2017).

El desarrollo de esta relación tan íntima que tienen hoy los seres humanos con los productos informáticos, se debe a que en la creación de éstos se han implementado técnicas educativas de comportamiento establecidas por las mentes más brillantes del mundo de la psicología como las de Edward L. Thorndike y de Burrhus F. Skinner y que hoy son adaptadas por científicos modernos como Brian Jeffrey Fogg, quien es el fundador y director del laboratorio de tecnología persuasiva de la Universidad de Stanford en Estados Unidos, además del mentor de muchos de los creadores de las plataformas más populares con sede en Silicon Valley.

En su obra (Thorndike, 2017) menciona que cuando existe una recompensa positiva para ciertos actos, estos tienen mas posibilidad de repetirse, si una rutina es repetida lo suficiente acaba transformándose en un hábito. (Skinner, 2015) por su parte consideraba que, si una organización pretendía imponer el control, este podría surgir al sistematizar ciertos actos en las personas, que a su vez generarían cambios deliberados en pequeñas partes del entorno social, proporcionando así el diseño cultural requerido.

Siguiendo esta línea, B. J. Fogg crea un método para el diseño del comportamiento humano, que ha sido adaptado en el desarrollo de muchas de las plataformas que las personas usan hoy en día, como *Instagram*. “El comportamiento ocurre cuando la motivación, la habilidad y un aviso se unen en el mismo momento” (Fogg, 2016).

Así también (Fogg, 2016) refiere que los productos tecnológicos pueden diseñarse para que sean persuasores, incluyendo en sus dinámicas presencia-social como la dotación de características físicas que producen en las personas respuestas-sociales; un ejemplo de esto es el empleo del concepto de “atractivo” sobre un dispositivo, sabiendo que como efecto, los usuarios

además de quererlo asumirán que éste también es confiable. Otro es el uso extensivo del lenguaje para influir en la compra de productos, como en el caso de Amazon, que personaliza los mensajes y el contenido que ve el usuario basado en sus preferencias. Las plataformas buscan que el *engagement* –compromiso o enganche- se genere a partir de actos repetitivos del usuario, que terminan configurándose como rutinas inconscientes, logrando que el usuario permanezca la mayor cantidad de tiempo usando un producto o plataforma.

Una vez establecido que la mecanización de actos crea hábitos y que puede por ende modificar la conducta de las personas, es válido asegurar que ésta en combinación con la publicidad y el uso de productos tecnológicos, producirán las reacciones que puedan querer de las personas y por consiguiente de la sociedad quienes los que controlen.

Un ejemplo de la efectividad en el control es el experimento de contagio emocional que realizó el departamento de comunicación y ciencias de la información de la Universidad Cornell en Estados Unidos. Con el uso de la red social *Facebook* se pretendía comprobar si las emociones pueden transferirse a través de redes sociales, así como sucede durante las interacciones personales de los humanos en el mundo real.

El experimento consistió en observar los efectos sobre los usuarios al presentárseles únicamente publicaciones que referían a un tipo de emoción como aquellas que contenían expresiones negativas. Como consecuencia las publicaciones posteriores de estos usuarios en la red social tendieron a ser menos positivas de lo habitual. Esta situación se constituye como evidencia experimental de que las emociones expresadas por otros en las plataformas de redes sociales influyen en las emociones de quienes están siendo expuestos a ese contenido (Cornell University, 2014).

“La manipulación deliberada de la cultura es en sí misma una característica de muchas culturas” (Skinner, 2015)

Los ganadores en la nueva Economía de los Datos con la segmentación de la información y los perfiles de personalidad

El empleo de cookies por las grandes plataformas en el entorno digital, sumado a la recopilación de la información, les permite a éstas y a sus aliados las asociaciones comerciales de marketing y las compañías de investigación de mercado, desarrollar sus negocios en la llamada Economía de los Datos. Esto consiste en un modelo de negocio basado en la explotación de la información de los usuarios en la red. El autor (Berners-Lee, 2011) en su obra *there`s gold to be mined from all our data* mencionó que: “los datos son la nueva materia prima del siglo XXI”.

La forma en la que se da esta explotación de datos comprende el acceso a los mismos y su tratamiento mediante herramientas tecnológicas como la Inteligencia Artificial, estas *machine learning*, son sistemas desarrollados para el procesamiento y análisis de información del que se extrae conocimiento y cuyo fin en el caso particular de la publicidad comprende la segmentación o categorización de actitudes, el desarrollo de perfiles de personalidad y la predicción del comportamiento humano (Golbeck, 2015).

Imitando ciertas funciones humanas la Inteligencia Artificial desarrolla de manera general, técnicas para la resolución de problemas mediante una programación definida por un algoritmo -conjunto de reglas e instrucciones establecidas para completar una acción- de aprendizaje de datos, que está orientado al desarrollo del razonamiento. En esta programación se incluyen conceptos como los de la inferencia o el de la planificación, así el campo de aprendizaje automático de las redes neuronales artificiales se centra en el reconocimiento de patrones con el objetivo de descubrir características discriminatorias de la información procesada. Como cuando los seres

humanos realizan ejercicios mentales de agrupación de similitudes y marginación de diferencias (Rosebrock, 2017).

Al respecto de la segmentación que se refiere a la agrupación de información basada en características especificas, tenemos por ejemplo la que realiza la compañía Global Web Index con la información que obtiene de distintas plataformas que incluye redes sociales, instituciones bancarias, marcas reconocidas de más de 50 países, y la de distintos tipos de servicios. Este acceso a la información le permite investigar el mercado para desarrollar su plataforma de uso de datos, que comercializa a quienes la requieran. En su sitio web consta lo siguiente: “Los datos de clic y la ubicación geográfica simplemente no son suficientes. Para tomar buenas decisiones comerciales, necesita más piezas del rompecabezas” (Globalwebindex.com, 2019).

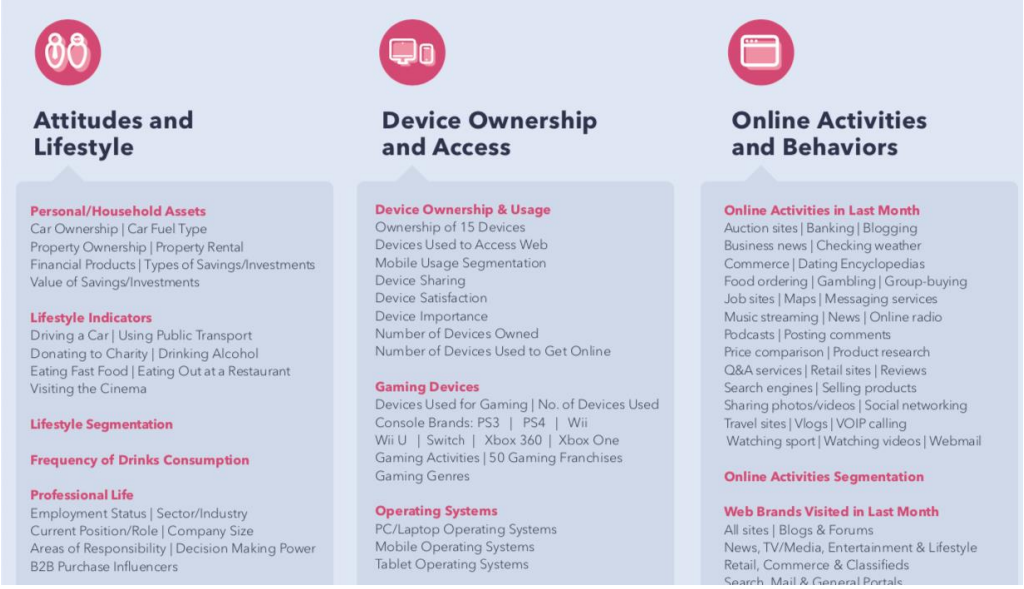

Ilustración 4

Fuente: Global Index Web, data coverage 2019 https://www.globalwebindex.com/reports/trends-19

Vemos a continuación, tres ejemplos de esquemas de segmentación de la información: el que se refieren al estilo de vida, el del comportamiento en la

actividad online y al del acceso a dispositivos. En el primero se observa una subclasificación que corresponde a la de los indicadores del estilo de vida, y en ella tenemos el del uso de transporte público, el consumo de alcohol y de comida rápida. Este resultado es el producto del análisis de la información recopilada y del uso de las *machine learning*, así las personas son clasificadas dentro de estas categorías que le permite a su vez a otras empresas descubrir nuevas oportunidades comerciales basándose en las preferencias y el comportamiento de las personas.

Para cuantificar el crecimiento de este modelo económico, de la publicidad personalizada, revisaremos la información proporcionada por una de las asociaciones comerciales de publicidad más grandes del mundo, La *Interactive Advertising Bureau*, que posee alianzas estratégicas con las plataformas de interacción social, como *Facebook*, *Google*, *Twitter*, entre otros, y que tiene como fin impulsar el desarrollo de la publicidad y la comunicación digital (IAB, s.f.).

En noviembre de 2018, emitieron un reporte sobre los ingresos de la publicidad por internet, y en él podemos apreciar sus cifras en cuanto al cambio que presentó la sociedad a través de los años en relación con los dispositivos en donde se consume la publicidad y el porcentaje de los ingresos económicos. Solo durante la mitad del año 2018, los ingresos por publicidad móvil representaron el 62.5%, como puede observarse el en contraste con el año 2012 cuando apenas representaban el 7%.

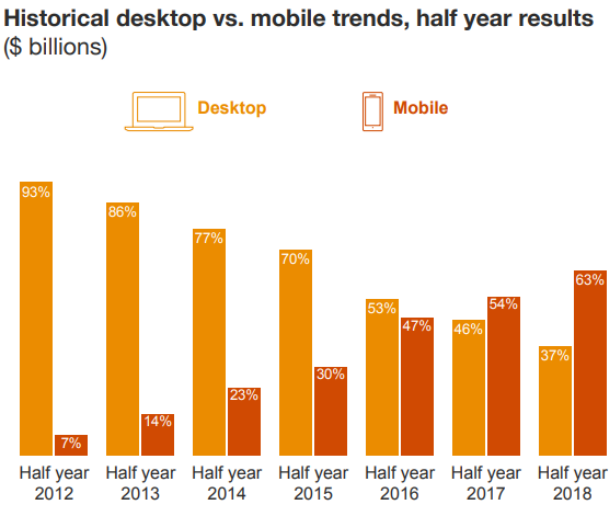

Ilustración 5

Fuente: IAB internet advertising revenue report 2018 https://www.iab.com/wp-content/uploads/2018/11/REPORT-IAB-Internet-Advertising-Revenue-Report-HY-2018.pdf

Así también, se encuentra el desarrollo de los ingresos por trimestre entre años 1996 al 2018. Vemos como los ingresos durante los primeros seis meses del año 2018, alcanzaron los $25.6 mil millones de dólares.

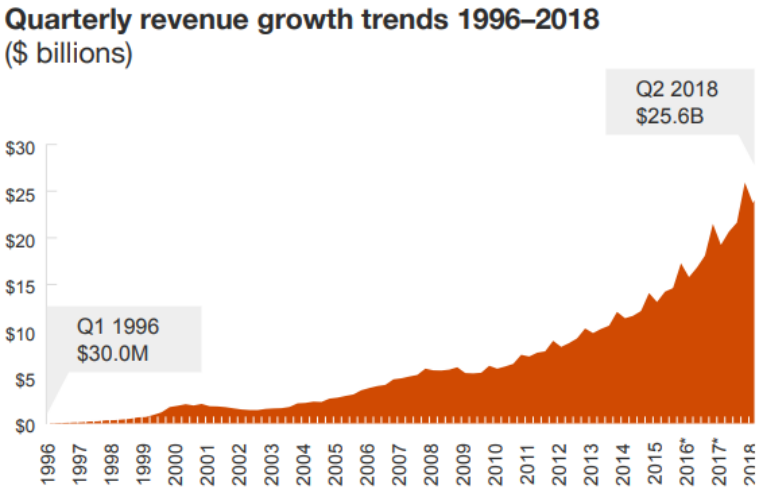

Ilustración 6

Fuente: IAB internet advertising revenue report 2018 https://www.iab.com/wp-content/uploads/2018/11/REPORT-IAB-Internet-Advertising-Revenue-Report-HY-2018.pdf

La forma en la que se desarrolla la elaboración de perfiles, el empleo de la Inteligencia Artificial de la mano con la publicidad dirigida y su influencia en el contenido que es redirigido a los usuarios en internet representa para las grandes industrias no solo enormes ingresos sino también una oportunidad de control social, que como se conoce ya es usada por varios gobiernos del mundo, cuyo origen es la recolección y el tratamiento de datos. Ante la indiferencia de la ley, la estructura de la Economía de los Datos se erige sobre la violación a los derechos fundamentales de los seres humanos.

Proyecto de Ley de Protección de Datos Ecuador 2019

El 19 de septiembre del año 2019, se presentó ante la asamblea el Proyecto de Ley de Protección de Datos. A continuación, los temas más relevantes relacionados al presente trabajo:

En la exposición de motivos del proyecto, se alude a la existencia de un mercado negro del que la información de los usuarios es parte. “Los sujetos se enfrentan a una realidad en donde su información forma parte de un mercado negro, del que nadie habla pero que es innegable” (Proyecto de Ley de Protección de Datos Personales, 2019) .

Sin embargo, y como hemos expuesto, el mercado que representa los mayores riesgos de vulneración a los derechos fundamentales es el que se da de manera legal y el que precisamente corresponde a las actividades domésticas, es importante resaltar este término ya que el proyecto hace una excepción de la aplicación de la normativa a las actividades familiares o

domésticas como se menciona en el artículo 3. No es claro a qué tipo de actividades corresponden dichos términos, podría considerarse a la comunicación como tal, y por ende quedando fuera de la protección que se le pretende dar a las relaciones suscitadas en la red.

En cuanto al consentimiento, la redacción del artículo 14 del referido proyecto de ley establece que:

> Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular de hacerlo.
>
> El consentimiento será válido, cuando la manifestación de la voluntad sea: libre, es decir, que se encuentre exenta de vicios del consentimiento(…); expresa, que de manera indubitable el responsable pueda demostrar que el titular manifestó su voluntad a través de una declaración o acción clara, afirmativa o se deduzca de una acción del titular. (Proyecto de Ley de Protección de Datos Personales, 2019)

Aunque se trata de definir cuales son las consideraciones que deben de tenerse para que el consentimiento dado sea estimado como válido, es sin lugar a duda el principal problema, no se propone nada distinto a lo que ya se encuentra establecido en la normativa existente, se destaca la idea de que el consentimiento debe de ser informado para que sea válido, y poder así generar las obligaciones que se pretenden con las suscripciones de contratos. Pero, no se considera la posibilidad de que el titular de los datos rechace la oferta de tratamiento de sus datos personales, es decir, no podría hablarse de un real consentimiento si el usuario debe elegir entre aceptar los términos y condiciones o no usar los servicios que requiere, como por ejemplo el del acceso a una página web de una institución financiera nacional o de una entidad gubernamental.

A pesar de la inclusión del derecho de oposición que consta en el artículo 28 y que menciona: “el titular tiene el derecho a oponerse o negarse

al tratamiento de sus datos personales, en especial para fines de mercadotecnia, valoración o decisiones automatizas incluida la elaboración de perfiles" (Proyecto de Ley de Protección de Datos Personales, 2019). En contraste, el artículo 14, deja abierta la posibilidad de que la declaración del consentimiento se tenga como manifestada con el solo hecho de que el titular de los derechos deduzca una acción afirmativa, lo que podría interpretarse como la que se realiza al entrar a una página web y navegar en ella, cediendo automáticamente ante las cláusulas incluidas en los términos y condiciones.

Por ende, y a efectos prácticos mientras no se obligue al proveedor del servicio a incluir necesariamente la opción de la negativa en la aceptación y que se elimine el concepto de acciones afirmativas como elemento suficiente para la suscripción de un contrato, el derecho de oposición incluido en el artículo 28 del referido proyecto de ley no podrá lograr los efectos pretendidos.

Aquello que tiene relación con la conservación de los datos, se encuentra en el artículo 17 numeral dos y se menciona que serán conservados: "hasta cuando cumplan con la finalidad para la cual fueron recogidos o tratados" (Proyecto de Ley de Protección de Datos Personales, 2019). Surge entonces la duda de que si la finalidad de quienes realizan la recolección de los datos personales se encuentra sobre los derechos fundamentales de la privacidad y la libertad. De ser cambiado el artículo sobre la conservación, podría constituirse como un precedente positivo limitando las facultades que poseen quienes tratan la información, incluyéndoles la obligación de conservar ésta por tiempos cortos y determinados.

La aplicación del reconocimiento facial y su relación con el Proyecto de Protección de Datos Personales en El Ecuador

El reconocimiento facial es un sistema que emplea a la Inteligencia Artificial como un identificador, procesando la información proporcionada por dispositivos de captación de imágenes y una base de datos previamente enlazada. Esta herramienta es empleada en varias plataformas de redes sociales, en páginas webs, en *smartphones* y también es aprovechado por al menos 75 gobiernos de países en el mundo, entre ellos Ecuador (Carnegie Endowment, 2019).

Durante los últimos años este tipo de tecnologías han sido promocionadas por los gobiernos como símbolo de seguridad y de lucha frente al crimen. Latinoamérica no deja de ser la excepción y en varios países del continente ya funcionan sistemas de detección facial y de recolección de datos biométricos; así tenemos el caso colombiano, en donde estas tecnologías son fuertemente empleadas por instituciones públicas y privadas. Llegando inclusive a ser sancionadas algunas empresas privadas por no contar con la autorización para la recolección de datos por el uso de sistemas biométricos (Superintendencia de Industria y Comercio , 2018).

Apropósito del terreno ganado por el empleo de las tecnologías de vigilancia masiva, el Ministro de Telecomunicaciones y de la Sociedad de la Información, Andrés Michelena Ayala, desde el año 2019 se ha encargado de impulsar la política llamada Ecuador Digital, en ella se busca que el país se convierta en un referente de tecnología. Entre una de sus propuestas se encuentra la implementación del sistema de reconocimiento facial en Quito y Guayaquil.

En una declaración en el mes de junio durante la firma de este convenio expresó que: “Estamos en el proceso de digitalización de cédulas y pasaportes para que las cámaras que están distribuidas en las ciudades puedan realizar

un reconocimiento facial y así, brindamos mayor seguridad a los ecuatorianos" (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019).

Mediante una entrevista oficial, a el Diario el Universo, el ministro manifestó que:

> Hay sistemas que permiten leer el rostro para saber si tiene molestia, dolor, o un tema que se pueda prevenir. Si tenemos 40 grados con sol y alguien usa chompa, capucha, esa cámara me identifica y me genera alertas, eso se conecta al sistema de video vigilancia. Cuando esté el sistema de autentificación fácil ya podemos saber quién es esa persona, donde trabaja, que hace y prevenir si tiene antecedentes. (Michelena, 2019)

Continuando con la ejecución de la política de impulso digital en el país, en el mes de diciembre del año 2019 fueron instaladas en la ciudad de Quito 78 cámaras con el sistema de reconocimiento facial (El Comercio, 2019). Mediante el proceso número SIE-EMS-003-2019 de subasta inversa electrónica se le adjudico el contrato de adquisición e instalación del mencionado sistema a la compañía ANDEANTRADE S.A., que para cumplir con las especificaciones del proyecto implementó tecnología desarrollada por la empresa pública HIKVISION del Gobierno de la República Popular China. Que, a propósito de su política de privacidad, la compañía establece que recopila información de los productos conectados a sus servicios para entre otras cosas realizar análisis e investigaciones de clientes (Hikvision, 2020).

Así también, durante el mes de marzo del presente año la alcaldesa de Guayaquil, Cynthia Viteri, hizo un llamado a las distintas instituciones públicas del país para que transfirieran sus bases de datos con el fin de poner en marcha el plan de instalación de cámaras con reconocimiento facial en la ciudad (El Universo, 2020).

La promoción y el empleo de estas políticas gubernamentales se desarrollan en un escenario en el que no existe en el país una ley que garantice la protección a los datos de los ciudadanos y tampoco que establezca limites a las prerrogativas estatales. Ante esta arrolladora realidad surgen las interrogantes: ¿Quién tendrá acceso a estos datos?, ¿En dónde serán almacenados?, ¿Cómo serán tratados?, ¿Quién es el propietario de esta tecnología? y ¿Por qué el propietario de este sistema puede tratar datos sensibles?

Se debe considerar que para el funcionamiento de estos sistemas es necesario el tratamiento de los datos biométricos de toda una población, siendo uno de los efectos de su aplicación la producción de otros miles de datos y metadatos de los ciudadanos que serán vigilados. El almacenamiento y control de esta información escapa del poder de cualquier estado que emplee sistemas desarrollados por empresas o gobiernos extranjeros cuya infraestructura no se encuentre dentro de su jurisdicción. Ante la indiscutible transnacionalización de datos, las leyes locales se enfrentan a la escaza o nula posibilidad de proteger los datos personales de los ciudadanos de un país fuera de sus fronteras.

Al revisar el Proyecto de Ley de Protección de Datos, vemos como muchos de los principios y nociones establecidos en éste otorgarían la legitimidad necesaria para el empleo de un sistema de reconocimiento facial en el país.

- El articulo 10 numeral 7 del proyecto de manera explícita indica que el tratamiento de datos será legitimo: “para proteger intereses vitales, del interesado de otra persona natural, como por ejemplo su vida, salud o integridad” (Proyecto de Ley de Protección de Datos Personales, 2019).
- En cuanto al derecho de rectificación, actualización, eliminación, oposición anulación y portabilidad, el artículo 31 menciona que el interés publico se constituye como una de sus excepciones, así como

cuando sean necesarios para investigación científica, histórica o estadística por parte del Estado.

- La ley establece que solo se podrán hacer transferencia de datos transnacionales cuando previo al acto, la autoridad de protección de datos personales nacional haya emitido un informe sobre los niveles adecuados de protección, sin embargo en el articulo 69 se enumera una lista de excepciones a esta regla general, numeral 2: “cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales”; numeral 7 “Cuando la transferencia sea necesaria por razones de interés publico”; y numeral 10: cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados” (Proyecto de Ley de Protección de Datos Personales, 2019).

El empleo de herramientas tecnológicas que identifica y monitorea a los ciudadanos de un país procurando mitigar la inseguridad en el mismo, puede constituir una amenaza a los derechos fundamentales de las personas. Estos medios deberán ser ampliamente revisados, su sola existencia constituye un conflicto en la ponderación de derechos, sin considerar que sus efectos aún son incalculables (Cordero Vega, 2015).

CAPÍTULO II: ASPECTO METODOLÓGICO

Enfoque del tipo de investigación

Al ser un trabajo de investigación, fueron utilizadas fuentes bibliográficas y material legislativo nacional e internacional como las de la Unión Europea, para el desarrollo y explicación de los conceptos. Además, se aplicaron encuestas a abogados de la ciudad de Guayaquil, de la que se obtuvo información cuantitativa.

Métodos y técnicas para la investigación

En el presente trabajo se utilizaron los siguientes métodos de investigación:

1. Método Analítico: Proceso cognitivo que implica la descomposición de un objeto de estudio para su análisis individual. Este método fue aplicado a lo largo del trabajo, al analizar por separado los elementos que componen el escenario global del tratamiento de datos que se originan desde las interacciones en la red y cuyo efecto es la vulneración de derechos.

2. Método Descriptivo: Proceso que busca una investigación sistemática, que estudia la realidad educativa y su desarrollo, con las que se describe y analiza las condiciones por las que puede darse una situación. Este método fue aplicado al analizar el origen de las consecuencias del tratamiento de datos.

3. Método Deductivo: Proceso de razonamiento con el que se llega a explicar particularidades de conclusiones generales. Este método fue aplicado al analizar los distintos principios, postulados y la legislación.

La técnica utilizada fue la encuesta, se hicieron preguntas tendientes al uso y de las prácticas en internet, los deberes del estado y sobre derechos fundamentales. Las personas que participaron de la entrevista anónima fueron 103 jóvenes abogados, graduados entre el 2012 y el 2019. La intención fue medir el conocimiento de los usuarios sobre las prácticas de manera general de los proveedores de servicios en Internet y su percepción sobre la vulneración de derechos fundamentales.

Resultados

Primera pregunta: ¿Tiene alguna idea de la estructura de negocio con que operan los servicios que se ofrecen a través de Internet? (Google, Spotify, Instagram)

El NO, tiene el 69,7% correspondiente a 70 respuestas.

El SI, tiene el 30,3% correspondiente a 33 respuestas.

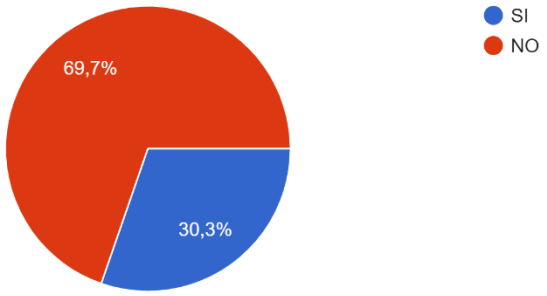

Gráfico 1

Segunda pregunta: ¿Alguna vez ha leído los términos y condiciones de los servicios que adquiere o utiliza en Internet?

El NO, tiene el 51,5% correspondiente a 52 respuestas.

El SI, tiene el 48,5% correspondiente a 51 respuestas.

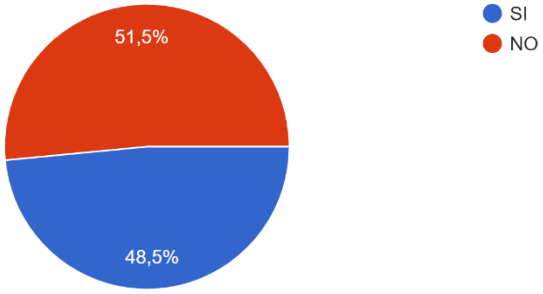

Gráfico 2

Tercera pregunta: ¿Sabía usted que, al aceptar los términos y condiciones, está compartiendo su información personal (de identificación, multimedia, ubicación, etc.) con la empresa que le otorga un servicio y autorizando para que esta realice con ellos lo que estime conveniente?

El NO, tiene el 24,2% correspondiente a 27 respuestas.

El SI, tiene el 75,8% correspondiente a 76 respuestas.

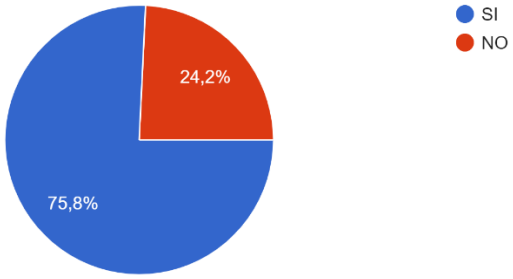

Gráfico 3

Cuarta pregunta: ¿Sabía usted que, todas las comunicaciones realizadas con el uso de servicios a través de Internet son guardadas y monitoreadas con objetivos de análisis para publicidad?

El NO, tiene el 45,5% correspondiente a 47 respuestas.

El SI, tiene el 54,5% correspondiente a 56 respuestas.

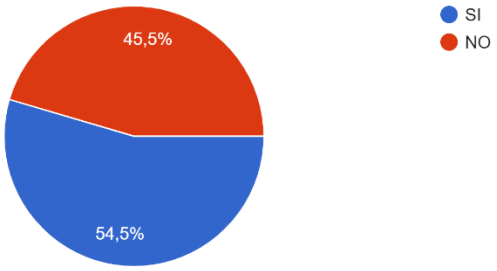

Gráfico 4

Quinta pregunta: ¿Le parece aceptable que recolecten, usen y comercialicen su información personal?

El NO, tiene el 81,8% correspondiente a 83 respuestas.

El SI, tiene el 1% correspondiente a 1 respuestas.

El ME ES IRRELEVANTE, el 15,2% correspondiente a 19 respuestas.

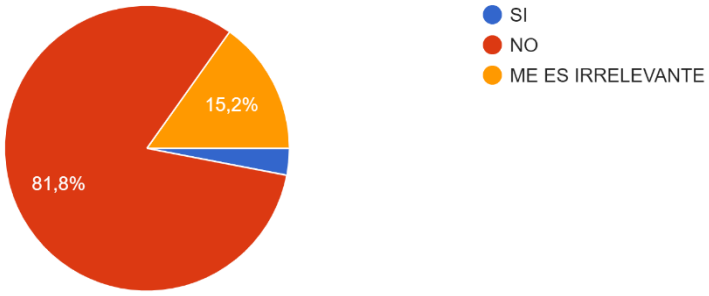

Gráfico 5

Sexta pregunta: ¿Cree usted que el Estado debería iniciar campañas y proyectos de enseñanzas sobre tecnología y los derechos de los usuarios en la red?

El NO, tiene el 6,1% correspondiente a 9 respuestas.

El SI, tiene el 90% correspondiente a 90 respuestas.

El ME ES IRRELEVATE, el 3% correspondiente a 4 respuestas.

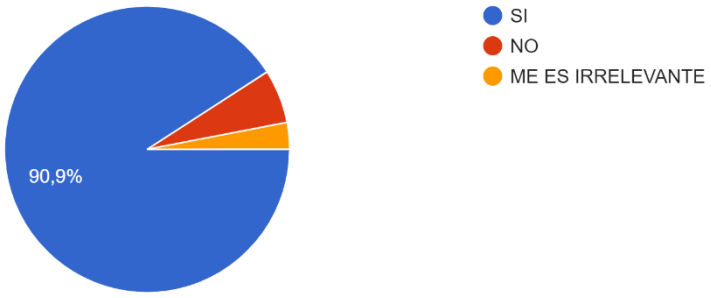

Gráfico 6

Séptima pregunta: ¿Cree usted que el Estado debería limitar el comercio de datos personales?

El NO, tiene el 6,1% correspondiente a 7 respuestas.

El SI, tiene el 57,6% correspondiente a 59 respuestas.

El NO, PORQUE ES EL USUARIO QUIEN DECIDE ACEPTAR LOS TÉRMINOS Y CONDICIONES, el 36,4% correspondiente a 37 respuestas.

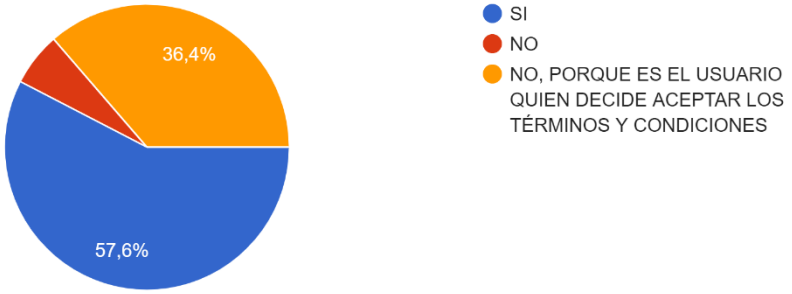

Gráfico 7

Octava pregunta: ¿Alguna vez había escuchado los términos, ciberseguridad, VPN o encriptar?

El NO, tiene el 33,3% correspondiente a 35 respuestas.

El SI, tiene el 66,7% correspondiente a 68 respuestas.

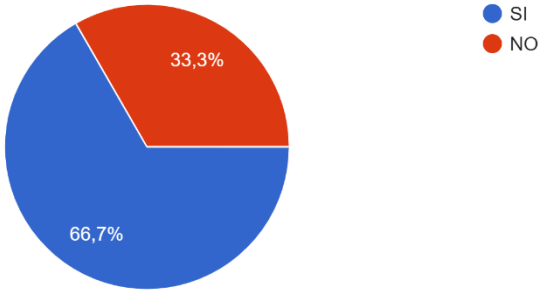

Gráfico 8

Novena pregunta: ¿Cree usted que el Estado debería promover el uso de herramientas que impulsen la seguridad de los usuarios en la red?

El NO, tiene el 3% correspondiente a 4 respuestas.

El SI, tiene el 87,9% correspondiente a 89 respuestas.

El ME ES IRRELEVANTE, el 9,1% correspondiente a 10 respuestas.

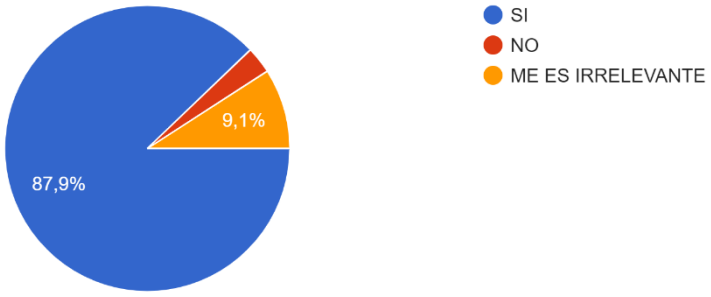

Gráfico 9

Décima pregunta: Luego de lo leído, ¿Considera que las prácticas que surgen de las interacciones en la red vulneran sus derechos a la intimidad y a la libertad?

El NO, tiene el 12,1% correspondiente a 14 respuestas.

El SI, tiene el 84,8% correspondiente a 85 respuestas.

El ME ES IRRELEVANTE, el 3% correspondiente a 4 respuestas.

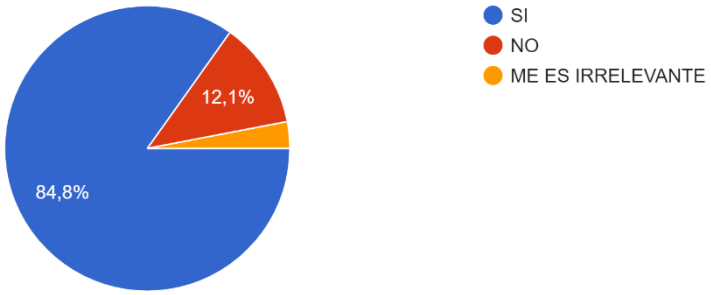

Gráfico 10

CAPÍTULO III: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

Análisis de las encuestas

El objetivo de las entrevistas fue poder determinar el nivel de información y conocimiento que posee una persona, de entre 25 a 30 años, de un segmento de la población Guayaquileña, con un nivel de instrucción académica superior, y específicamente por desarrollar sus actividades profesionales en el área del derecho.

Del análisis de los porcentajes con relación a sus respuestas, en términos generales podemos concluir lo siguiente:

La mayoría de los entrevistados un 69,7%, no tiene conocimiento de cómo las compañías que ofrecen servicios en internet generan ganancias. Independiente de si estos servicios son o no gratuitos para el usuario.

El 51,5% de los entrevistados no ha leído los términos y condiciones que acepta cuando adquiere un servicio, cualquiera sea su tipo a través de la red. Esto evidencia una conducta de desinterés. Es claro que la mayoría de los usuarios no se cuestionan de qué manera pagan por aquello que aparentemente es gratuito.

El 48,5% de los entrevistados, señaló haber leído los términos y condiciones de los servicios en la red. Sin embargo, en comparación con el porcentaje de respuesta de la pregunta número uno, respecto a tener conocimiento de cómo estas compañías generan ganancias, que corresponde al 30,3%, si realmente el usuario estuviese informado sobre los Términos y condiciones, el porcentaje personas que comprenden la estructura de este tipo de negocios sería más alta. Con lo que se determina que el usuario ha mentido en las respuestas de la pregunta número 2.

El 75,8% de los entrevistados comprende que comparte información sensible y datos personales con el uso de estos servicios, esto refuerza el punto sobre el desinterés del usuario. Así también vemos como el 24,2% de los entrevistados no tenía conocimiento sobre la información que compartía con estas compañías al hacer uso de sus herramientas, lo que nos muestra que no existe al menos para una parte de los usuarios consentimiento informado sobre los términos y condiciones, esto es claramente atribuible a la dificultad de la disponibilidad de las cláusulas de estos contratos que se celebran al navegar en la red, sobre todo con aquellos denominados *browse-wrap*.

El 54,5% de los entrevistados saben que las comunicaciones que mantienen con el uso de estas herramientas son monitoreadas, sin embargo, continúa haciendo uso de ellas. Esta situación es atribuible a más del desinterés del usuario, a la necesidad existente del empleo de estas soluciones tecnológicas en la realidad del siglo XXI.

Al 81,8% de los entrevistados le parece inaceptable que se realicen actividades comerciales con sus datos, y el 90% considera que el Estado debería impulsar la educación sobre aspectos tecnológicos, así como de proteger y garantizar los derechos de los usuarios en el país.

El 36,4% de entrevistados en la pregunta 7 sobre limitar el comercio de datos personales, piensan que mientras el usuario acepte los términos y condiciones, el Estado no debería interferir. Es interesante comprender esta visión de los usuarios de internet, al mismo tiempo que consideran en su mayoría inaceptable las prácticas comerciales, comprenden que no tienen otra opción, sin duda un punto relevante sobre este concepto es que entienden la vulneración de derechos que implica, conforme al porcentaje determinado en la pregunta diez que corresponde al 84,8%, y que a su vez no se sientan atraídos en cambiar sus hábitos en la red. Sin duda, dicho comportamiento es

atribuible a que no se sienten vigilados. Entonces tienen conocimiento de estas prácticas porque lo presumen, pero no les interesa porque no lo ven.

CAPÍTULO IV: CONCLUSIONES

Son conclusiones a esta investigación las siguientes:

I. El contrato electrónico y el carácter contractual de los Términos y Condiciones

El consentimiento que debe construirse posterior a una oferta y que constituye un elemento inequívoco de la voluntad que legitima la contratación generando obligaciones para ambas partes, no es informado y en la mayoría de los casos no se da de manera legal. Otorgarle naturaleza contractual a estas autorizaciones que se dan en la red solo debería suceder en la medida en la que se el consentimiento no se vea condicionado, no pueden considerarse como contratos válidos a aquellos que surgen de las autorizaciones de los términos y condiciones cuando es imposible verificar la manifestación inequívoca de la voluntad como elemento condicionante para el surgimiento de una obligación. En la mayoría de las paginas que encontramos en Internet, no se exige revisar el contenidos de los Términos y Condiciones; al contrario, se aplican los contratos tipo browse-wrap, en los que por la simple actividad del usuario en la pagina web, se asumo su consentimiento sobre todas las condiciones del servicio, incluyendo aquellas clausulas que implican vulneración a sus derechos.

Esto se debe a la forma en la que el consentimiento esta concebido dentro del ordenamiento jurídico, permitiendo que estos actos que involucran el tratamiento de información personal sean considerados como contratos válidos siempre que cuenten con la autorización del titular del derecho. Si embargo, esta concepción no puede estar más alejada de la realidad digital, la autorización y el consentimiento que involucra ésta debe ser examinado y desarrollado desde una perspectiva proteccionista, considerando que nos encontramos en un escenario en que las personas deben ceder sus derechos para hacer uso de plataformas o productos tecnológicos y que los datos

personales tratados posterior a la cesión, representan un conocimiento inequívoco de la esfera más íntima del ser humano.

Aunque las autorizaciones que se otorgan a los términos y condiciones se encuentran fuera de la regulación de la ley, si se aplicara el carácter subsidiario de las normas para enfrentar la problemática que surge a raíz de la valoración del consentimiento dado, se concluiría que en el Ecuador las empresas nacionales y sus plataformas en línea incumplen con la legislación local. Por lo tanto, en vista de dicho incumplimiento, se concluye que la ausencia de regulación específica sobre este tipo de contratos ocasiona que los usuarios digitales sufran constantes violaciones a su derecho a la intimidad, por la indebida utilización de sus datos personales.

II. Los datos

Los datos que se recopilan son almacenados en servidores ubicados en países en donde se encuentran domiciliadas las empresas dueñas de las plataformas, bajo el actual sistema de descentralización y transnacionalización de datos. Por este motivo, el titular de éstos jamás podrá saber quien tiene sus datos ni para que los usan. Por ende, se deja a éstos fuera de la protección de la legislación nacional.

Cuando los datos son entregados por los gobiernos a compañías extranjeras que gestionan sistemas dentro de una nación como por ejemplo el de reconocimiento facial, se termina privatizando la información de los ciudadanos, esto sucede debido a la imposibilidad técnica de la mayoría de los estados para desarrollar y controlar de manera local las herramientas tecnológicas, sumado a los bajos costos que estos sistemas tienen en comparación con lo la inversión que tendría que hacer un país para desarrollarlos.

Si bien la ley actualmente regula las transacciones comerciales que se realizan a través del servicio de redes y de internet, como así lo menciona la Ley de Comercio Electrónico en su considerando: “se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil.” Podría pensarse que ésta le otorgaría protección al usuario de internet sobre las prácticas que surgen de la interacción en distintas plataformas, no es menos cierto que dicha relación no está considerada dentro de la realidad comercial, es por esto que las plataformas de las empresas del país no se ven obligadas a cumplir con lo establecido en la ley, a pesar de que la información que recopilan de los usuarios y que es obtenida como producto de una celebración contractual en la que el usuario cede los derechos de sus datos personales, tenga indiscutibles fines comerciales.

III. La economía de los datos y la industria de la publicidad

Al llevarse prácticas indiscriminadas de recolección, uso y comercialización de información de usuarios de distintas plataformas con la aceptación de términos y condiciones, se comprueba el comercio de datos personales, con lo que se establece que existen vulneraciones de derechos fundamentales. El desarrollo de perfiles de personalidad basado en preferencias tiene como objetivo convertir a los usuarios de las plataformas en mejores consumidores, y también tienen la posibilidad de modelar e influir en su comportamiento en el mundo real, es por esto que hoy se habla de la Economía de los Datos, que está basada en el tratamiento de los mismos y que genera millones de dólares a los pequeños grupos de gigantes tecnológicos y de la publicidad.

Del empleo de técnicas de control y creación de hábitos con el fin de generar más interacciones con los dispositivos, depende de la extracción del mayor volumen de información de un usuario. El conocimiento que obtienen tras el tratamiento de los datos y metadatos que recolectan las empresas propietarias de las plataformas en la red o que los gobiernos entregan con el

empleo de herramientas tecnológicas en la prestación de servicios públicos, les posibilita descubrir e implementar nuevas estrategias de atención y control que son aplicadas a los mismos usuarios, la existencia de estos datos les permite mercantilizar todas las áreas de la vida de los seres humanos, lo que a su vez les procura popularidad y hegemonía en el mercado, teniendo como consecuencia lógica el monopolio de la red y de los datos en ella.

Uno de los escenarios que produce el tratamiento de información para quien los posee es la mejora en la toma de decisiones, y no solo en el ámbito de la publicidad se podrá establecer sobre quien o quienes se debe influir de cierta manera u otra promoviendo el consumo de un producto, sino también en distintas actividades sociales, así como vemos el sistema de crédito social de la Republica Popular China, en el cual a sus ciudadanos al perder puntuación debido a comportamientos incorrectos se les priva de por ejemplo acceder al transporte público. Con el conocimiento que tienen las corporaciones sobre la mayoría de los ciudadanos del mundo y que comercializan a negocios de otras industrias como a las aseguradoras, es fácil inferir que en un futuro no muy lejano se le prive a alguien la posibilidad de ser asegurado o solicitar un pago más elevado de lo generalmente costaría uno de sus servicios, al tener por ejemplo ciertos hábitos alimenticios que pueden ser traducidos por los algoritmos de los sistemas de inteligencia artificial que cotejan datos, en futuras enfermedades o de complicaciones en la salud.

IV. Proyecto de Ley de Protección de datos en el Ecuador

El proyecto de Ley Orgánica de Protección de Datos Personales de Ecuador responde a una realidad de la que los ciudadanos están conscientes como lo es la venta de bases de datos de su información correspondiente a identidad, números telefónicos, historial crediticio, etc., por parte del sector de la banca, de las empresas de créditos y de las telecomunicaciones. Sin embargo, no contempla la problemática que actualmente se discute en otras naciones, que corresponde a una realidad imperceptible para la mayoría de

los ciudadanos del mundo como es el tratamiento de sus datos personales por el uso de internet ni la importancia que estos tienen en el ámbito comercial. Este proyecto tampoco trata de manera distinta el concepto del consentimiento como elemento fundamental de las autorizaciones, ni promueve la regulación de cookies o la inclusión de todas las actividades que suceden en la red para el ámbito de aplicación de la normativa, por ende y posterior a su aprobación continuará el tratamiento indiscriminado de los datos personales de todos los ciudadanos en el país, que se da producto de las actividades cotidianas en el uso de la red.

Las prácticas de rastreo que son aprovechadas por los gobiernos sustentan su empleo en el interés y la seguridad nacional, al no existir normas que impidan o limiten las prerrogativas estatales de vigilancia y tratamiento de información personal de los ciudadanos de una nación por el empleo de sistemas de los que aún no se pueden calcular sus efectos, como el de reconocimiento facial y de inteligencia artificial. Resulta indiscutible considerar que nos encontramos frente a una práctica de poder autoritaria, que nos hacer cuestionar la existencia de la democracia cuando se comprueba que el modelo de mercado tiende a la manipulación poblacional, transformando a la red en un facilitador de totalitarismo.

El reconocimiento facial, se contrapone a los principios y derechos establecidos en tratados, constituciones y en legislaciones de todo el mundo. Su implementación en Ecuador constituye una vulneración directa a la vida privada, libertad de tránsito, libertad de asociación, inviolabilidad del hogar, así como del principio de presunción de inocencia.

CAPÍTULO V: Propuestas

I. A través de la implementación de programas especiales, el gobierno, centros educativos, colegios y universidades, deben invertir recursos en la educación para toda la población del país, en cuanto a los medios, uso y consecuencias del empleo la tecnología. Así como de políticas dirigidas al empleo de herramientas de seguridad y protección de la información de los usuarios y en el debate sobre los riesgos existentes sobre los datos personales.

II. Las autorizaciones que se suscriben en la red deben contar con un régimen especial de regulación dentro de la ley de protección de datos, para que puedan ser consideradas jurídicamente relevantes se debe comprobar la manifestación inequívoca de la voluntad de consentir en el acto mediante una acción afirmativa de aceptación, como el caso de los contratos de *click-wrap*. Así como de imponer a los proveedores de servicios de internet, proveedores de plataformas tecnológicas y demás servicios que se realizan en la red, la obligación de contar con pestañas que señalen el tipo de información que será recolectada y que la recolección únicamente podrá corresponder a aquella que es necesaria para la navegación de la página y no ser tratada con el fin de crear perfiles de preferencia, incluyéndose la posibilidad de que el usuario pueda rechazar la recolección de datos y el alojamiento de cookies con el fin de promover la confidencialidad de la información que se envía y que se genera por el uso de las plataformas.

III. A través de la Ley de Protección de Datos Personales, disponer la Prohibición de la recolección, uso y comercialización de datos dentro del territorio para fines de publicidad, rastreo u otros que vulneren los derechos fundamentales de los usuarios de internet, sobre todo de aquellos servicios que corresponden a las telecomunicaciones, banca, salud, educación y a los de aseguradoras. Imponiendo además para quienes poseen información, que sea eliminada en un tiempo determinado no mayor a 24 horas desde que los datos son almacenados.

IV. Que el Estado previo a la implementación de políticas que pueden resultar nocivas respecto de los derechos de los ciudadanos, como el uso de sistemas de reconocimiento facial, o de otras que puedan ser desarrolladas en el futuro realice estudios pertinentes, en los que se tome la opinión de expertos en las materias que corresponda en las áreas de informática y derecho. Así como de limitar las facultades del estado en relación con el uso de tecnología que permite la identificación, localización y rastreo de los ciudadanos.

V. Que se promuevan políticas públicas enfocadas en la disposición de distribución de datos anonimizados por parte de quienes controlan los datos a otras empresas o personas naturales que las requieran, implicando que estos no serán comercializados, sino, compartidos para el análisis y aplicación de tecnologías beneficiosas para el entorno y desarrollo de una sociedad, como aquellas de medición de smog, ruido, o de detección de enfermedades.

VI. Que se promueva la soberanía tecnológica del país, entendiéndose que la inversión y el destino de recursos en el desarrollo de sistemas e infraestructura propia, contribuye a la ejecución de procesos dentro del país, impidiendo que se contraten monopolios extranjeros para el tratamiento de datos cuando se requiera la prestación de servicios públicos, limitando así el flujo de datos transnacionales ya que éstos serían almacenados de manera local servidores nacionales.

VII. Que se promueva la celebración de acuerdos internacionales en donde el objetivo primordial de éstos, sean la promoción de la protección de datos y el compromiso de los países en donde se encuentran ubicadas las compañías de tratamiento de datos**.** En consecuencia, los países suscriptores deberían tener regímenes similares de protección de datos, con el propósito de que los ciudadanos de ambos estados se encuentren igualmente protegidos, sin perjuicio de que sus datos se transfieran fuera del territorio.

Bibliografía

Warren, S., & Brandeis, L. (1890). *The Right of Privacy.* Hardard Law Review 4.

Constitución de la República del Ecuador. (2008). *Lexis.* Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=PUBLICO-CONSTITUCION_DE_LA_REPUBLICA_DEL_ECUADOR&query=constitucion#I_DXDataRow0

Constitución de la Nación Argentina. (1994). *Casa Rosada.* Obtenido de https://www.casarosada.gob.ar/nuestro-pais/constitucion-nacional

Española, R. A. (s.f.). *RAE*. Obtenido de https://dej.rae.es/lema/dignidad-de-la-persona

Garcés Vásquez, P. A. (2014). *El Consentimiento: su Formación y Vicios.* Institucion Universitaria de Envigado.

Código Civil. (2019). *LEXIS.* Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=CIVIL-CODIGO_CIVIL&query=codigo%20civil#I_DXDataRow0

Kim , N. (2013). *Wrap Contracts.* Oxford: Oxford University Press.

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos . (2017). *LEXIS.* Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=PUBLICO-LEY_ORGANICA_DEL_SISTEMA_NACIONAL_DE_REGISTRO_DE_DATOS_PUBLICOS&query=la%20ley%20del%20sistema%20nacional%20de%20registro%20de%20datos%20p%C3%BAblicos#I_DXD

Ley de Comercio Electrónico, Firmas y Mesajes de Datos. (2014). *LEXIS.* Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=MERCANTI-LEY_DE_COMERCIO_ELECTRONICO_FIRMAS_Y_MENSAJES_DE_DATOS&query=ley%20de%20comercio%20electr%C3%B3nico#I_DXDataRow0

Lessig, L. (2015). *Code: And Other Laws of Cyberspace, Version 2.0 .* California: Basic Books.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). *Access Denied: The practice and Policy of Global Internet Filtering.* London: MIT PRESS.

Varon Ferraz, J. (2012). Filtrado de contenido en América Latina: razones e impacto en la libertd de expresión. En E. Bertoni, *Hacia una Internet libre de censura Propuestas para América Latina* (pág. 181). Buenos Aires: Universidad de Palermo.

IAB. (s.f.). *IAB*. Obtenido de https://www.iab.com/our-story/

Google. (s.f.). *Google*. Obtenido de https://myaccount.google.com/activitycontrols/location

Apple. (2017). *Apple developer*. Obtenido de https://developer.apple.com/documentation/safari_release_notes/safari_12_release_notes

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). *telecomunicaciones*. Obtenido de https://www.telecomunicaciones.gob.ec/quito-sera-la-primera-ciudad-inteligente-del-pais/

Michelena, A. (15 de septiembre de 2019). Con autentificación facial podemos saber si esa persona tiene antecedentes. (A. Bajaña, Entrevistador)

Orwell, G. (1949). *1984.* Caracas: Lucemar.

Cordero Vega, L. (2015). Videovigilancia e Intervencion administrativa: las cuestiones de legitimidad. *Revista de Derecho Publico*, 359-376.

Guerra Balic, J. (2017). La Conclusion de contratos por medios informáticos. *Informática y Derecho*, 63-132.

Código de Comercio. (2019). *LEXIS.* Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=MERCANTI-CODIGO_DE_COMERCIO&query=codigo%20de%20comercio

Código Orgánico Integral Penal. (2019). *LEXIS.* Obtenido de http://www.silec.com.ec/Webtools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=PENAL-CODIGO_ORGANICO_INTEGRAL_PENAL_COIP&query=derecho%20a%20la%20intimidad#I_DXDataRow6

Miniwatts Marketing Group. (2019). Obtenido de https://www.internetworldstats.com/emarketing.htm

Instituto Nacional de Estadisticas y Censos. (2017). *Ecuador en cifras.* Obtenido de INEC: https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2017/Tics%202017_270718.pdf

Banco del Pichincha. (2020). *Banco del Pichincha*. Obtenido de https://www.pichincha.com/portal/Informacion/Informacion-legal

Servicio Nacional de Derechos Intelectuales. (2019). *Servicio Nacional de Derechos Intelectuales*. Obtenido de https://www.derechosintelectuales.gob.ec/politica-datos-personales/

counterpointresearch.com. (12 de octubre de 2017). Obtenido de Counterpoint: https://www.counterpointresearch.com/almost-half-of-smartphone-users-spend-more-than-5-hours-a-day-on-their-mobile-device/

Ferrer, E. (2015). El lenguaje de la publicidad. Tezontle: Fondo de cultura economica.

Kotler, P., & Armstrong, G. (2017). *Principles of Marketing.* New York: Pearson .

Fogg, B. (2016). *Persuasive Technology.* California: Morgan Kaufmann Publishers.

Thorndike, E. L. (2017). *Animal Intelligence.* London: Forgotten Books.

Skinner, B. F. (2015). Science and Human Behavior. En B. F. Skinner, *Science and Human Behavior* (pág. 427). Massachusetts: The B. F. Skinner Foundation.

Spurgin, E. W. (2003). What`s wrong with computer-generated images of perfection in advertising. *Journal of Business Ethics 45*, 257-268.

Berners-Lee, T. (2011). There`s gold to be mined from all our data. *The Times*.

Globalwebindex.com. (2019). Obtenido de Global Web Index: https://www.globalwebindex.com/data-coverage

Golbeck, J. (2015). *Analyzing the social web.* Massachusetts: Morgan Kaufmann.

Moreno Navarrete, M. A. (2016). *Contratos Electrónicos.* Madrid: Derecho Civil Hoy.

Fernández Fernández, R. (2017). *El Contrato Electrónico.* Barcelona: Jose María Bosch Editor.

Mann, R., & Siebeneicher, T. (2015). Just One Click: The Reality of Internet Retail Contracting. *University of Texas: Law and Economics Research*.

Oviedo Albán, J. (2016). *La Formación del Contrato.* Bogotá: Temis S.A.

Londoño Vásquez, D. A., Rendón Ángel, J. E., & Marín Muñoz, G. S. (2015). *Revista Virtual de la Universidad Católica del Norte.* Obtenido de https://www.redalyc.org/pdf/1942/194218961014.pdf

Facebook. (19 de abril de 2018). *Facebook.com*. Obtenido de Facebook: https://www.facebook.com/about/privacy/update

Facebook. (2018). *Facebook.com*. Obtenido de Facebook: https://www.facebook.com/legal/terms

Solar, L. C. (2015). *Explicaciones de derecho civil chileno y comparado.* Santiago: Editorial Juridica de Chile.

Martínez Pastor, E., & Muñoz Saldaña, M. (2016). En busca del equilibrio entre la regulación y la autorregulación de la publicidad comportamental en línea. *Estudios Sobre El Mensaje Periodístico*, 289-297.

Verdejo Alvarez , G. (2018). *Seguridad en Redes IP.* Barcelona: Universitat Autónoma de Barcelona.

Peces-Barba, G. (2016). *Curso de Derechos Fundamentales.* Madrid: Universidad Carlos III de Madrid.

Gozaíni, O. A. (2018). *Habeas Data: Protección de datos personales.* Buenos Aires: Rubinzal-Culzoni.

Assange, J. (2016). *Cypherpunks.* New York: OR Books.

Comisión Europea. (27 de abril de 2016). Obtenido de ec.europa.eu: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Proyecto de Ley de Protección de Datos Personales. (2019). *Asamble Nacional.* Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/pp-pro-dat-lmoreno-t379637-19-09-2019.pdf

Nino, C. S. (2017). *Fundamentos del Derecho Constitucional.* Buenos Aires: Astrea.

Cornell University. (25 de marzo de 2014). *Proceedings of the National Academy of Sciences of the United States of America.* Obtenido de PNAS: https://www.pnas.org/content/pnas/111/24/8788.full.pdf

Rosebrock, A. (2017). *Deep Learning for Computer Vision with Python.* New York: PyImageSearch.

Carnegie Endowment. (2019). *Carnegie Endowment for International Peace.* Obtenido de carnegieendowment.org: https://carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf

Superintendencia de Industria y Comercio . (2018). *Superintendencia de Industria y Comercio .* Obtenido de sic.gov.co: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2018055405.pdf

El Comercio. (9 de diciembre de 2019). *El Comercio*. Obtenido de elcomercio.com: https://www.elcomercio.com/actualidad/camaras-reconocimiento-facial-quito-marin.html

El Universo. (9 de Marzo de 2020). *El Universo*. Obtenido de eluniverso.com: https://www.eluniverso.com/guayaquil/2020/03/09/nota/7774155/cynthia-viteri-espera-base-datos-institucionales-efectividad