PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

"ANÁLISIS DE LA PRIVACIDAD Y TRANSPARENCIA DEL INTERNET"

ANTONELA ESTEFANÍA SUÁREZ FLORES

DIRECTOR: ING. ALFREDO CALDERÓN SERRANO

QUITO, 2017

DEDICATORIA

A mis padres con mucho cariño les dedico el esfuerzo puesto para la realización de este trabajo de disertación de grado gracias a ustedes por los recursos empleados a lo largo de este camino.

A cada uno de los pequeños peluditos que han llegado a mis manos en distintas situaciones de abandono y que me han acompañado durante los años de estudios necesarios para llegar a la culminación de la carrera y que a la par, han encontrado su segunda oportunidad de vida.

También le dedico este proyecto a Erick, mi novio, con su compañía, confianza y escucha ha sido uno de las motivaciones más grandes para alcanzar esta meta.

AGRADECIMIENTO

Quiero agradecer a todas las personas que han compartido conmigo su conocimiento durante esta investigación, al grupo conformado por psicólogos y sociólogos que han motivado en la búsqueda de varios aspectos para el desarrollo de este trabajo.

A mis padres por su apoyo durante la carrera, a mis compañeros durante la realización de deberes y proyectos que han permitido la culminación de esta meta.

A mí querido amigo, Santiago por su ayuda, compañía y apoyo cuando el ánimo decaía.

A mi director por su dirección, opiniones, ideas y recomendaciones para el desarrollo del presente estudio.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La sociedad y el mundo en general, han dado un vuelco desde el que el internet estuvo disponible a nivel global a partir de 1980; la información y las actividades que se realizan durante un día se han trasladado hacia el mundo virtual con el paso del tiempo. Ha llegado tanto su auge que solo para 1992 ya existía alrededor de un millón de computadoras conectadas, ahora para el 2017 existen más de 2 billones de dispositivos conectados a internet entre dispositivos móviles y computadoras (WeAreSocial, 2017).

El internet se ha convertido en parte primordial de la vida de las personas, lo cual ha ocasionado la vinculación de toda actividad realizada en el mundo real con el virtual. Tanto ha sido este cambio que se ha modificado las relaciones personales del conocimiento cara a cara hacia un descubrir, de conocer, al otro a través de las actualizaciones de sus estados, fotos y frases provistas en distintos tipos de aplicaciones, redes sociales o sitios web disponibles en la red. Todas estas acciones en línea generan toneladas de información cada hora del día y las cuales deberán ser almacenadas para su uso posterior. Esto ha motivado a que la información se haya convertido en una de los recursos más valiosos e importantes tanto para uno mismo como para las diversas compañías desarrolladoras de tecnología, así como los distintos gobiernos que han encontrado en esta, un nuevo recurso para vigilar y controlar a sus ciudadanos.

Al momento que un usuario accede a internet e interactúa con los diferentes sitios disponibles; comienza a dejar una huella que contribuye a formar un perfil digital. El cual se construye a partir de todas las transacciones que va dejando en internet.

Los mensajes de WhatsApp, los likes, tweets, chats, compras mediante páginas como Amazon y eBay así como los pagos que realiza online, las búsquedas de información, tienen algo en común y es que llevan una serie de datos personales y geográficos que

contribuyen a la construcción de un registro del usuario, que quedará almacenado en grandes servidores, el cual nunca va a desaparecer, y del que ningún usuario común tiene el control.

Ante esta situación, las personas se pueden preguntar ¿hasta qué punto todos los datos dejados en internet preservan la privacidad del individuo?, ¿se realiza un correcto manejo de los datos para su almacenamiento y preservación?, ¿existe entidades que regulen el manejo de los datos? ¿Qué hacen los gobiernos para preservar la información frente amenazas externas? ¿Cuán transparente es el manejo de esta información?

JUSTIFICACIÓN

El internet es una herramienta que permite al público en general el acceso a la información desde cualquier parte del mundo y a cualquier hora del día. En él, se encuentra disponible la mayor diversidad de contenidos partiendo desde temas culturales, educativos, políticos, sociales hasta tópicos referentes a temas criminales o tabúes. Puede decirse que en cierto grado, este provee un ambiente de transparencia al presentarse de forma abierta a todos los ciudadanos del mundo. Sin embargo está limitado en muchos aspectos; ya que en ciertas partes del mundo el internet es considerado como una de las armas más peligrosas para generar rebelión contra sus gobernantes ya que pueden atentar contra el bienestar de un individuo. Además de proveer un sin número de artículos que atentan contra aspectos culturales de ciertas naciones por lo que sus mandantes han considerado regularlo y restringirlo, sacrificando la transparencia de por medio y con ella la libertad de expresión.

Hoy en día, a la Internet se puede utilizar en muchos ámbitos de la sociedad, por ejemplo la comunicación en general avanzó muchísimo por medio de esta herramienta, rompió fronteras y es el primer medio para la interacción entre personas. Por medio de las redes sociales ya no solo la sociedad puede comunicarse sino también informarse,

conocer sobre economía, política, antecedentes que marcan y marcaron la sociedad y las naciones, entre otras; pese a ello con la evolución de la tecnología la Internet no es solamente una herramienta de información y comunicación sino puede ser mal utilizada para fines que beneficien a unos pocos sin importar el perjuicio que esto pueda causar no solamente a unas pocas personas sino inclusive a naciones enteras.

ANTECEDENTES

En el año 2013, Edward Snowden ex contratista de la Agencia de Seguridad Nacional de los Estados Unidos (NSA) reveló información sobre el espionaje masivo realizado a millones de usuarios en el mundo por parte del gobierno norteamericano. Para lo cual se infiltró software espía en las aplicaciones móviles más populares como Angry Birds, Google Maps, etc. (Pastor, 2015) lo que provocó una intromisión en los sistemas operativos móviles más usados a nivel mundial (IOS y Android) y ocasionó en las personas un fuerte cuestionamiento acerca de su privacidad en Internet.

Anteriormente Julian Assange mediante WikiLeaks presentó múltiples artículos acerca de la entrega y venta de información de los usuarios pertenecientes a compañías tecnológicas poderosas como Google, Samsung entre otras. Mucha de esta información fue entregada a gobernantes de ciertas regiones.

Frente a esta situación, las personas de todas partes del mundo, usuarios de internet, comenzaron a tomar con énfasis la lucha en favor de su privacidad en medios digitales y aunque en un principio eran una minoría; poco a poco el conocimiento y la noción sobre este tema se extendió y ha llegado a captar la atención de algunos gobiernos acerca del manejo de datos sus ciudadanos por parte de medios externos. Estos a su vez han emitido leyes en favor de la protección de datos y almacenamiento dentro del país que maneja esta ley. Lo cual ha significado como un punto de lucha por la privacidad.

Al enfocar la situación de la privacidad y transparencia del internet en Ecuador, las leyes y decretos sobre el manejo en el mundo digital escasean. Además de a nivel cultural, la realidad sobre el manejo equivocado de los datos no es muy conocido localmente. Por lo que es fundamental que los usuarios de internet conozcan sobre la situación del país ante la privacidad y su abuso por parte de medios extranjeros.

Este trabajo partirá desde los acontecimientos que dieron origen a la preocupación sobre la privacidad del internet como las filtraciones realizadas por Snowden, las leyes impuestas sobre el internet en cada país, las WikiLeaks manejadas por su principal portavoz Julian Assange e incluso se realizarán encuestas para conocer la opinión y el conocimiento público sobre esta situación que afecta millones de personas en el mundo.

OBJETIVO GENERAL

Analizar la privacidad y la transparencia del internet a partir de opiniones de expertos, leyes, decretos que han sido impuestos en los últimos años en diferentes países del mundo, identificando la situación actual del Ecuador y la noción de sus ciudadanos en lo referente a este tema.

OBJETIVOS ESPECÍFICOS

- Identificar conceptos básicos acerca de privacidad, transparencia y neutralidad de la red.
- Conocer el estado del arte de la privacidad y transparencia del Internet.
- Analizar la situación de la privacidad y transparencia en el Ecuador.
- Determinar las diferentes herramientas que permitan poseer privacidad.
- Realizar un análisis y selección de herramientas que permitan poseer privacidad.

ALCANCE

Al tener en cuenta el conocimiento actual de los jóvenes, con respecto a la privacidad del internet, el proyecto culminará con la elaboración de una guía referencial respecto a herramientas tecnológicas que permitan a los usuarios la preservación de su privacidad en la red.

CAPÍTULO 1

En este capítulo se realizará una revisión de los principales elementos teóricos, sobre los cuales se fundamenta la presente disertación. Conceptos como Internet, privacidad, trasparencia y neutralidad de la red orientados hacia el ámbito tecnológico serán abordados para la comprensión de este trabajo.

CONCEPTOS FUNDAMENTALES

2.1. Internet

3.1.1. Definición

Internet es un neologismo del inglés que significa red informática descentralizada de alcance global; una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP (Caruso, 2005, pág. 2). Es decir, un sistema de redes informáticas interconectadas mediante distintos medios de conexión, que ofrece una gran diversidad de servicios y recursos**.**

En español, la palabra internet está considerada como un nombre propio. La Real Academia Española (RAE), en su diccionario, admite que se escriba con o sin mayúscula inicial. De allí que, preferentemente, se utilice sin artículo, aunque en caso de usarlo, se recomienda el uso femenino (la), ya que el nombre equivalente en español vendría a ser ‘red’, que es femenino.

Su origen data del año 1969, cuando una agencia del Departamento de Defensa de los Estados Unidos de América llamada ARPA desea darle un uso adicional a las computadoras para investigaciones científicas y académicas. Tres años después se realizó la primera demostración pública del sistema ideado, gracias a que tres universidades localizadas California y una en Utah lograron establecer una conexión conocida como ARPANET (Advanced Research

Projects Agency Network), bajo instalación de AT&T. Un año después se logra la primera intercomunicación internacional. (Licklider, 2002)

En 1989 ARPANET termina y Tim Berners-Lee crea WWW, una contraseña que permite difundir cualquier tipo de información.

Otros servicios y protocolos disponibles en la red de redes (Internet), son el acceso remoto a computadoras conocido como Telnet, el sistema de transferencia de archivos FTP, el correo electrónico (POP y SMTP), el intercambio de archivos P2P y las conversaciones online o chats.

El desarrollo de Internet ha superado ampliamente cualquier previsión y constituyó una verdadera revolución en la sociedad moderna. El sistema se transformó en un pilar de las comunicaciones, el entretenimiento y el comercio en todos los rincones del planeta. (Castells, 2001, pág. 15)

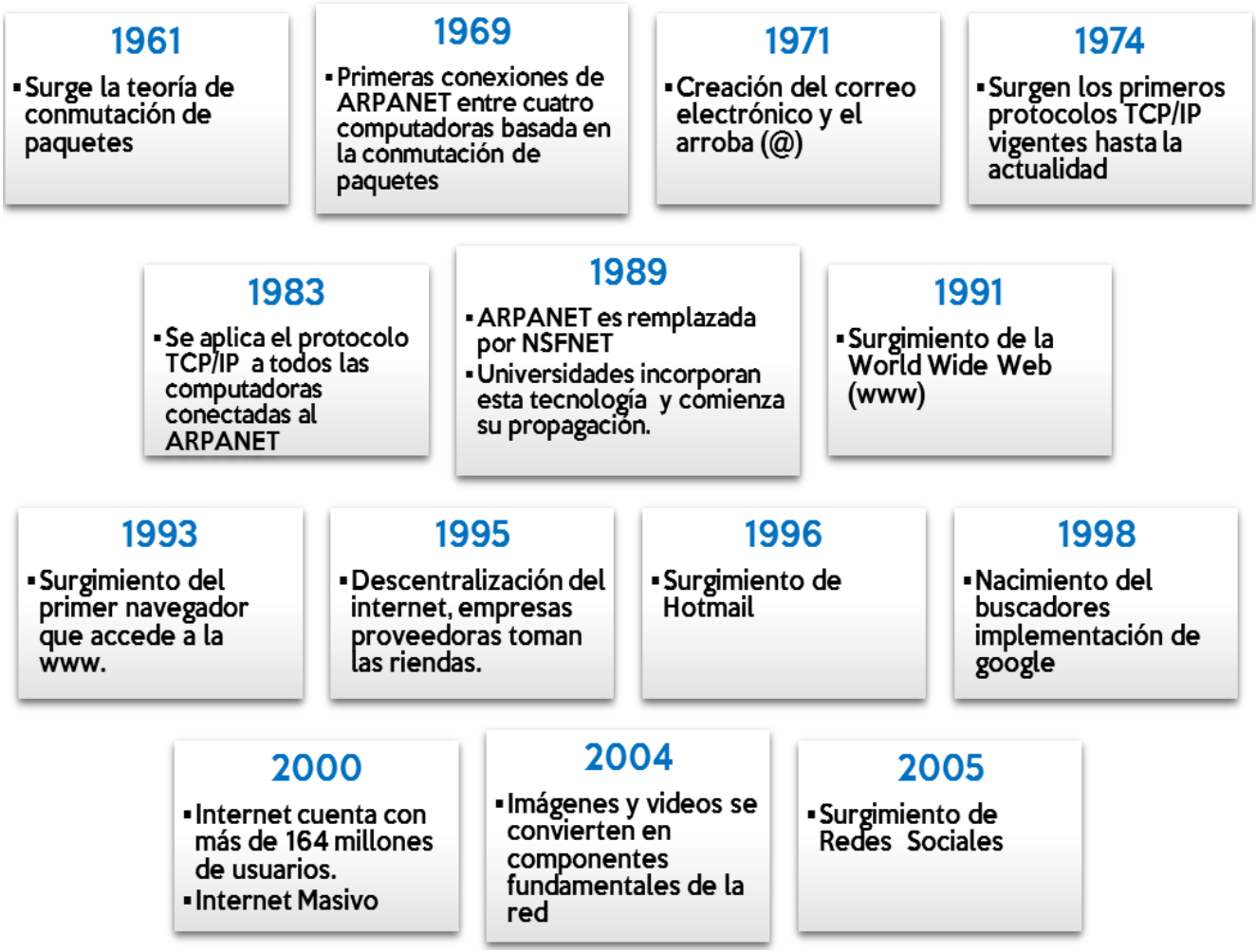
3.1.2. Evolución en el tiempo.

El desarrollo y la historia del ser humano han dado un vuelco desde que el internet se ha convertido en un elemento primordial que ha influenciado ampliamente el desarrollo tecnológico para su implementación en cada uno de los aspectos de la vida humana.

Desde su aparición, el internet ha pasado por varias fases que le han permitido su incorporación en diferentes tipos de dispositivos; pasando de ser una herramienta con fines específicamente militares a convertirse en un centro de comunicación continua entre individuos en todo aspectos cotidianos de toda índole, en cualquier horario y parte del mundo; su impacto ha sido tan fuerte, que ha sido implementado desde computadoras de escritorio hasta pequeños aparatos como tablets, smartphones, relojes, etc. que existen hoy en día y

permanecen conectados a la red durante días enteros, listos para compartir información a toda hora.

A continuación, se presenta los principales hitos a lo largo del desarrollo del internet:



Fuente: (Gonzáles, 2013)

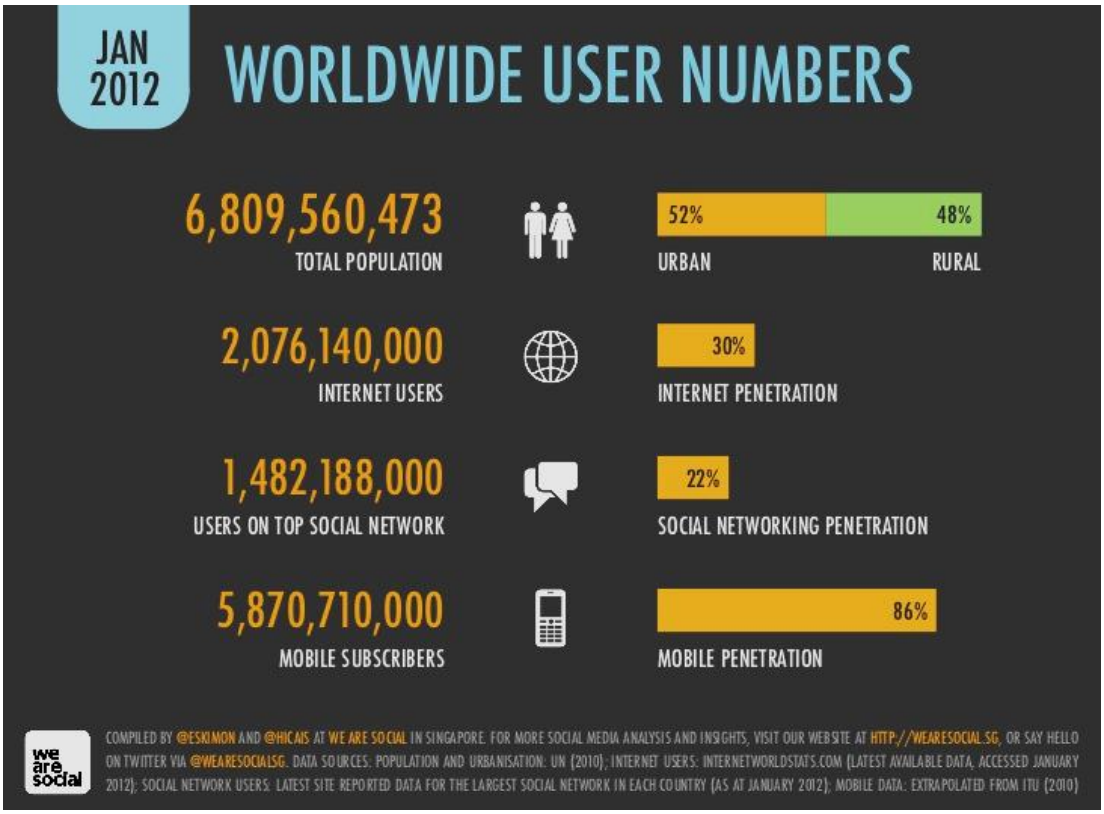
Elaborado por: Antonela Suárez

Fig. 1 Principales hitos de la historia del internet

Cabe recalcar que para el año 2000 - 2001, Japón da un vuelco a lo conocido e implementa la primera red 3G, lo que dota a los dispositivos móviles de nuevas capacidades de conectividad y da un empujón para que el internet pueda llegar a ser parte de estos nuevos artefactos. La experiencia de usuario, se vuelve algo primordial por lo que la apariencia de las páginas web como su interactividad se potencia para brindar una mayor satisfacción al consumidor y promover su uso con mayor frecuencia. Es aquí, cuando el término “Web 2.0” aparece y se considera a los blogs y redes sociales como los principales habitantes de este nuevo mundo virtual. Siendo así para el 2004, llega una de las más grandes empresas consolidadas hoy en día; Facebook surge y gracias a la evolución de la trasferencia de información y multimedia dota de capacidades a este sitio para permitir el desarrollo de uno los principales lugares para el compartir libremente, donde las fotografías, transmisión de videos, música, plasmado de ideas y nuevas formas de comercio se evidencian. Con esto, sitios como: YouTube, Twitter, Wikipedia, MySpace van pareciendo, popularizándose y gracias al constante uso el tráfico de datos comienzan a aparecer en la red. (Licklider, 2002)

El crecimiento del internet en los últimos quince años se ha dado en forma exponencial desde que surgió la capacidad de expansión de la red gracias la extensión de cables submarinos por todo el globo terráqueo que permitió extender esta conectividad de todos los usuarios al internet (Piscitelli, 2005). Tanto ha sido su crecimiento e impacto que solo en los últimos años el nivel de penetración a la red ha crecido a pasos agigantados a la par del desarrollo tecnológico en algunas regiones y ha sido considerado como política pública. Según estudios, para enero del 2012 la penetración del internet a nivel global era de apenas del 30%; número que con el pasar de los años ha ido en

incremento al igual que la presencia de terminales móviles que se conectan a la internet como se evidencia en la Figura 2.

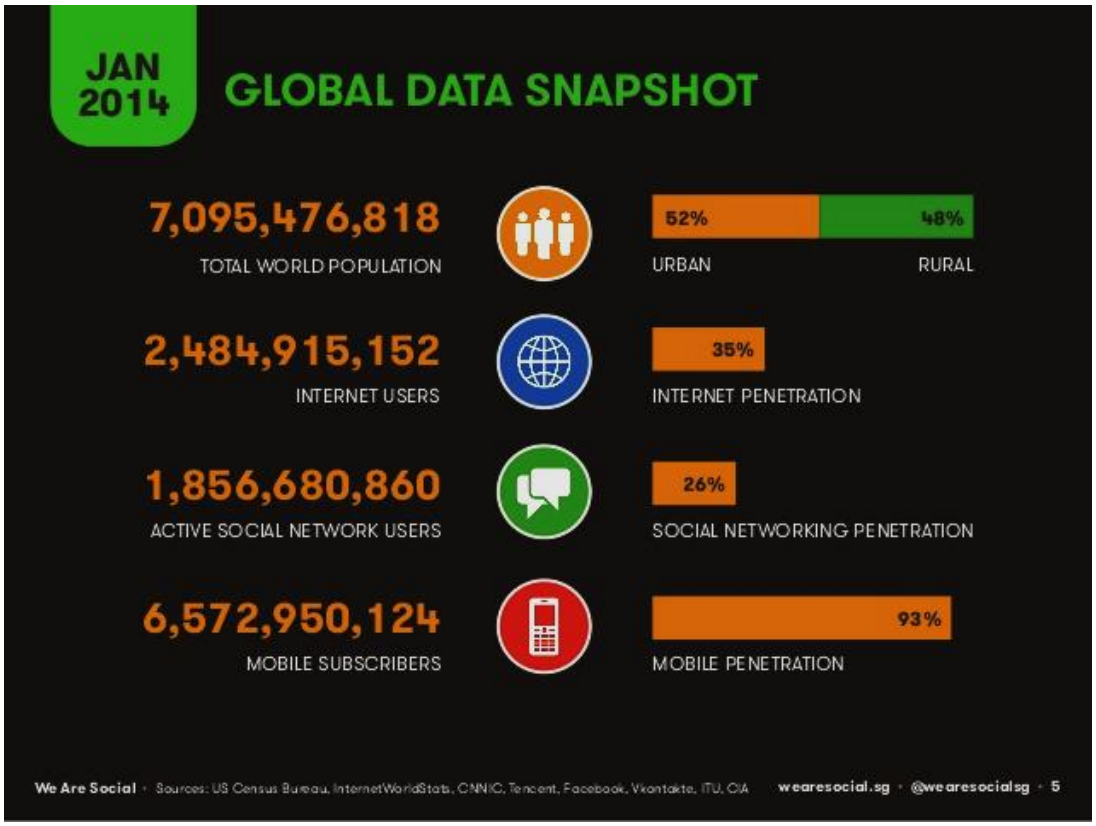


Fuente: (WeAreSocial, 2012)

Elaborado por: WeAreSocial

Fig. 2 Uso del Internet en 2012

Para el 2014, se evidencia un crecimiento del 5% con respecto a lo expuesto en el 2012.La tasa de penetración por parte de dispositivos móviles alcanza el 93%, en la Figura 3 se evidencia este incremento del 7% en este indicador.

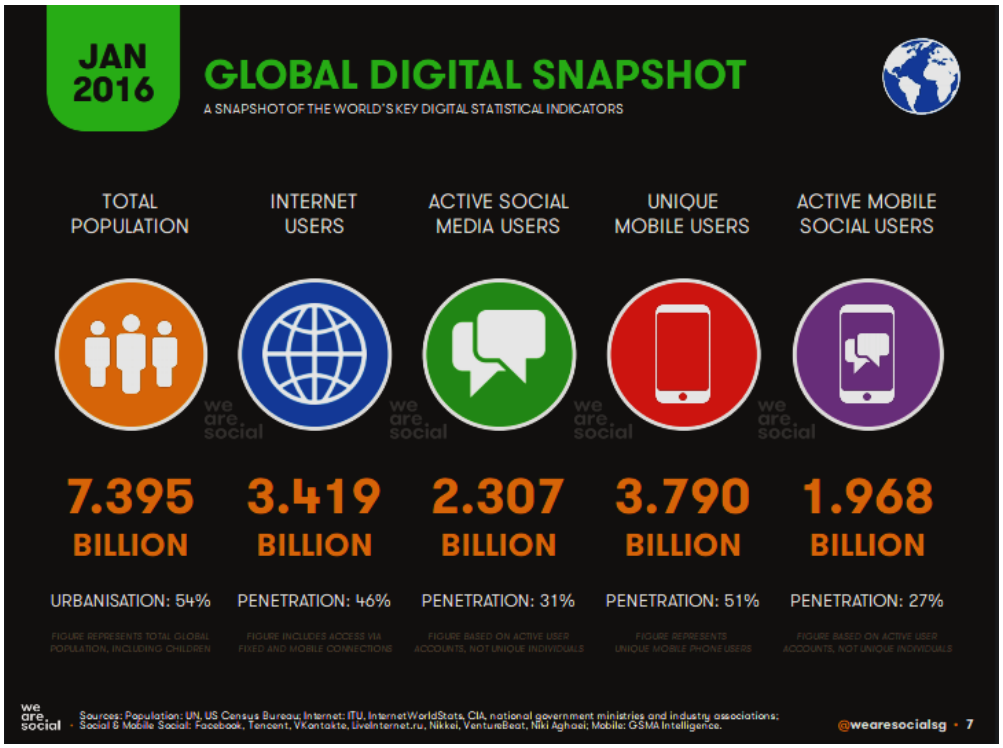


Fuente: (WeAreSocial, 2014)

Elaborado por: WeAreSocial

Fig. 3 Uso del Internet en 2014

Mientras que para el 2016, el acceso a internet incrementa a un 45% donde cabe poner énfasis que el acceso móvil tienen un crecimiento mucho más acelerado con respecto a años anteriores. Al igual que el porcentaje de penetración a redes sociales que evidencia un crecimiento al 31% como se puede ver en la Figura 4.



Fuente: (WeAreSocial, 2016)

Elaborado por: WeAreSocial

Fig. 4 Uso Del Internet en 2016

Por otro lado, en el primer mes del 2017 se denota que existen más de tres billones de usuarios de internet y que la penetración del internet alcanza un 50% a nivel mundial. Las redes sociales son más comunes que nunca contando con una penetración del 37%. Al momento se refleja que el uso de internet y redes sociales se da mediante terminales móviles.

Fuente: (WeAreSocial, 2017)

Elaborado por: WeAreSocial

Fig. 5 Uso del internet en los pocos meses de 2017

El internet se ha convertido en parte integral del diario vivir de la mayoría de las personas que conforman la población mundial. La transmisión y el envío de datos desde dispositivos móviles, son acciones comunes realizadas a toda hora del día. La información se está convirtiendo en la herramienta primordial para el desarrollo de artículos tecnológicos nuevos, cada vez más capacitados y ajustados al estilo de la vida de cada persona. En donde lo habitual para estas es realizar más del 70% de actividades (REDACCIÓN PERU21, 2015) desde estos terminales móviles además de la notoria preferencia de los usuarios por realizar transacciones económicas en línea. Toda esta transición de las actividades cotidianas hacia la “nube” es lo que está marcando el desarrollo del internet a futuro.

3.1.3. Proyección hacia el futuro

Existen diversas proyecciones sobre lo que podría llegar a ser el internet con el transcurso de los años, pero todas estas concluyen en que el futuro de la red no será más que un reflejo de lo que la especie humana está cultivando (Baraniuk, 2014).

Uno de los avances más mencionados es el internet de las cosas, donde cada objeto como: electrodomésticos, autos, casas, entre otros estén dotados de acceso a la red y componentes de domótica que le sirvan para solventar problemas sencillos como por ejemplo: el desabastecimiento, desgaste de las piezas del artefacto, manejo y adecuación de su temperatura; con la finalidad de mantener un lugar confortable para el usuario, que faciliten su convivencia y reduzca el tiempo que se emplea para la realización de tareas del hogar. (Jiménez Cano, 2011)

Por otro lado, se espera que por la red circulen miles de datos relacionados a la vida de las personas, sus horarios laborales y de ocio, sus preferencias e incluso sus historiales médicos, así como el de sus familiares y amigos es decir que toda esta información asociada a una persona circule libremente y se encuentre disponible para que miles de aplicaciones y objetos gestores de actividades del usuario y que le envíen a este recomendaciones de todo tipo, así sea algo tan simple como la compra de un regalo. La idea del internet en todo lugar y para todos, promete usuarios que siempre estén conectados a la red y almacenen información en la nube a cada segundo impulsando la conectividad total y la digitalización global; permitiendo consigo una comunicación más sencilla y eficiente para todas las personar, sin importar el lugar en donde este y donde la única limitación para que las personas no se encuentren conectados sea su voluntad propia. (Sarmiento, 2017)

Aspectos como la publicidad, las redes sociales y la necesidad de saber que está pasando en la vida de los otros serán explotados para solventar la demanda de los usuarios; ya que se contará con la cultura “On Demand” (Sarmiento, 2017) en donde el contenido será explícitamente desarrollo para el usuario que lo solicite a un costo igualmente diseñado para ese usuario.

Todas estas visiones y expectativas sobre la red tienen un punto en común, los datos, como tal la información se convertirá en una herramienta clave, lo que nos vinculará con artefactos y mantendrá monitoreada la vida de los ciudadanos en todos los sentidos. Lo que genera una gran preocupación para la sociedad de hoy. Debido a que surge la pregunta de quién y de qué forma se asegurará que estos datos se mantengan privados y seguros de los otros, y que grupos de poder, así como gobernantes no se apropien de ellos para ejercer control sobre los ciudadanos. Si bien algunos artículos mencionan que esto ya no será una preocupación y que se desarrollara leyes y alternativas para un manejo óptimo de la información además de la aceptación de la gente que no todo es tan inseguro como dicen (Baraniuk, 2014).

1.1. Privacidad

3.1.4. Definición

La privacidad, como término general se lo puede definir como una necesidad que tienen todos los individuos para preservar su existencia, en donde haya la mínimo intromisión por parte de los otros. (Rotenberg, 2015) Es decir, la privacidad mantiene un espacio metafórico en el cual se da el desarrollo del ser humano en forma libre; cuyos beneficios constituyen: el manejo de relaciones sociales en todos sus diferentes grados, el surgimiento de la creatividad, el pensamiento independiente, el desarrollo personal además de asegurar la salud mental.

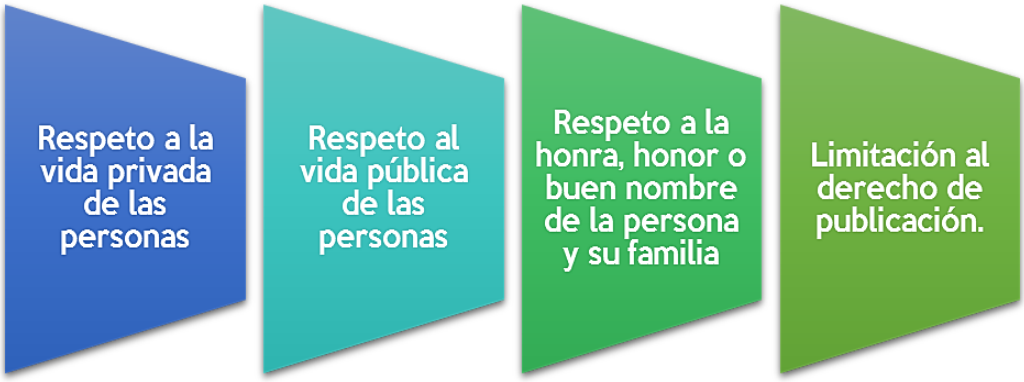
La privacidad provee de seguridad y relajación, ya que le permite al individuo constituir una “zona libre” de miradas externas en donde se pueda realizar todas aquellas actividades que, por pudor, temor a los otros, miedo al fracaso y a la discriminación pública se abstiene de realizar pero que son necesarias para el desarrollo futuro como individuos de una sociedad. (Lynch, 2012)

A un nivel mayor, es necesario de la presencia de la privacidad dentro de las sociedades para que resguarde a quienes la conforman de sus propios gobiernos y altos mandos pues “la libertad política requiere que los ciudadanos tengan el derecho de mantener en secreto su voto, sus asociaciones, y sus ideas políticas” (Véliz, 2014); algo que sin privacidad quedaría permanentemente revocado.

Siendo así, la privacidad pasó a ser considerado como un derecho. El cual salió a relucir desde el momento que apareció “la inquietud por preservar la intimidad de las personas y la conciencia por concederles esa facultad” (Mendoza, 2017). Este derecho se definiría como aquel que los individuos tienen para separar aspectos de su vida íntima de la indagación pública, por lo que, sin

diferenciación, todos los seres humanos tienen derecho a ella (Mendoza, 2017) además de que forma parte de la Declaración Universal de los Derecho Humanos establecida en 1948.

Este derecho asegura:



Fuente: (Falconí, 2008).

Elaborado por: Antonela Suárez

Fig. 6 Derecho a la privacidad

Las primeras admisiones de este derecho fueron establecidas en Estados Unidos a finales del siglo XIX, por el surgimiento de las fotografías instantáneas. De acuerdo a la tecnología que utilizaban para su revelación se consideró que quebrantaban la "vida doméstica" ya que las imágenes podían ser difundidas en forma masiva por lo que se consideró primordial definir un derecho a mantener la vida íntima de las personas, en ese entonces este derecho a la privacidad fue nombrado como el derecho a no ser molestado.

"Posteriormente, el concepto de privacidad incorporó otros elementos destacables como la facultad que toda persona posee para determinar la manera, el momento y la información personal que podía ser comunicada con otras personas. En otras palabras, esta idea ofrecía la posibilidad y el derecho a controlar la información propia, incluso luego de que fuese compartida." (Mendoza, 2017)

El derecho a la privacidad, se encuentra establecido para ser ejercido en espacios físicos, en el convivir diario de las personas, sus familias y el manejo de su correspondencia asimismo buscan garantizar la dignidad del individuo, con lo cual nadie puede ser considerado objeto-sujeto de injerencias arbitrarias o ilegales en los distintos desenvolvimientos de su vida (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 3).

A su vez este derecho brinda la condición de permanecer libre del ámbito del Estado en la esfera privada, al mismo tiempo, permite determinar quién posee su información personal y como es usada. Cabe recalcar que la privacidad se encuentra estrechamente relacionada con la seguridad personal.

“El Estado es el agente prioritario para proteger y respetar el Derecho a la intimidad o privacidad y por tanto, abstenerse de incurrir en actividades que amenacen o lesionen la integridad personal que es un bien jurídico protegido” (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 4).

En el Ecuador, sobre todo, la Constitución ecuatoriana reformada en 2008 reconoce y garantiza el derecho a la intimidad personal y familiar en su Artículo 66 numeral 20 (Falconí, 2008) asegurando las mismas garantías de su concepción original. Conjuntamente con este derecho se suma el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual para cualquier tipo de comunicación remarcado en el numeral 21 del mismo artículo.

Más allá de ser un derecho universal, la privacidad se deberá encontrar protegida por distintas formas de legislaciones nacionales. Comenzando por una ley que resguarde los datos personales de cada individuo, sus comunicaciones, sus documentos privados y su imagen. Con la presencia de la tecnología y el internet, varias legislaciones han sido modificadas para proteger

la privacidad en las nuevas formas de comunicación como lo es el correo electrónico.

La privacidad es un término cuya definición es subjetiva ya que factores como el tiempo, las costumbres, las generaciones y aspectos como la tecnología cambian la manera en cómo es percibida y contribuye a que sea un concepto difícil de consensuar. Hoy en día, la privacidad podría necesitar de una nueva definición dado el auge e imponencia que continúa surgiendo con el internet y los aparatos tecnológicos dotados con mayores capacidades inteligentes que contribuyen a formar un aspecto fundamental de la vida de los usuarios y sobre los cuales, los consumidores generan dependencia.

3.1.5. Enfoque hacia el internet.

"El hecho de estar en una red global quiere decir que no hay privacidad"

(Castells, 2001)

En la actualidad las personas se encuentran inmersas en un sinfín de componentes tecnológicos, cuyas capacidades son cada vez más desarrolladas y potenciadas para "facilitar" la vida de los usuarios de estas a costos relativamente aceptables. Terminales que permiten tomar fotografías, grabar y reproducir audio, así como facilitar la comunicación en segundos en cualquier parte del mundo han sido las herramientas digitales que mayor impacto han tenido durante años gracias a la presencia del internet. A la par del surgimiento de las redes sociales; lugares donde conocer lo que está haciendo el otro es lo primordial; todo esto ha contribuido a que las personas expongan sus actividades cada vez más, con total consentimiento de lo que realizan, pero partiendo desde el desconocimiento de lo que en realidad está pasando dentro

de los componentes digitales y que muchas veces están transgrediendo lo que era definido como privacidad y el derecho a la misma.

Al hablar de privacidad en el mundo de la red, se entendería “como el control que ejerce una persona sobre su información para limitar la cantidad de personas autorizadas a verla. Esto incluye datos personales, fotografías, documentos, etc.” (ESET, 2015); componentes que contribuyen a la construcción del perfil digital, es decir información relacionada a las actividades realizadas por los usuarios en el ciberespacio en función de la interacción con otros usuarios, organizaciones o servicios en Internet (Mendoza, 2017) y de los cual sin el manejo apropiado serán entregados a terceros para darle todo tipo de usos, lucrar de ellos y venderlos al mejor postor e incluso muchos de estos datos serán examinados exhaustivamente para conocer su contenido promulgando la vigilancia continua. En la actualidad muchos servicios de internet conocen la gran parte de actividades que realizan los usuarios desde gustos, preferencia, datos personales y ubicaciones geográficas; varios de estos datos son usados para fines comerciales y han transformado a la información en algo valioso tanto para el desarrollo de productos para la venta, como la apertura para la realización de todo tipo de actividades ilícitas. Por lo tanto, la protección de los datos contribuye a la preservación de la intimidad del sujeto.

“En el año 2013, la Asamblea General de Naciones Unidas reafirmó el derecho a la privacidad y reconoció la naturaleza global y amplia del internet como un factor coadyuvante hacia el desarrollo en sus distintas formas, alertando a los países la necesidad de proteger los derechos de las personas en internet” (Usuarios Digitales & Fundación 1000 Hojas, 2016) y sobre todo de los datos que abundan en internet.

La protección de datos como base de la Privacidad en Internet

"De la misma manera que protegemos nuestros bienes materiales para evitar que estos sean robados y utilizados por terceros, ¿por qué razón no debemos hacer lo mismo con nuestra información?"

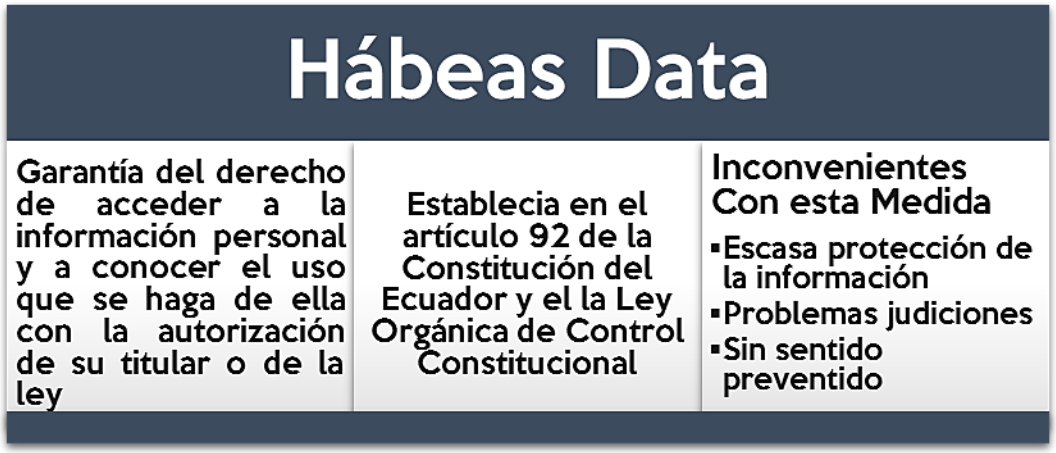
David Puron, Vicepresidente de Ingeniería BlackPhone, 2017

La protección de datos personales no abarca todos los aspectos de la privacidad, pero aun así se ha convertido en una pieza fundamental ya que busca la protección de lo denominado como identidad digital.

En algunos países existen normas jurídicas que regulan el tratamiento de los datos por ejemplo: España cuenta con la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) cuyo objetivo es "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar" (Ley Orgánica de Protección de Datos de Personales, 2007).

Por su parte, en Ecuador su Constitución reconoce y garantiza el Derecho a la protección de datos de carácter personal en su artículo 66 numeral 19. Este incluye "el acceso y la decisión sobre información y datos de carácter personal así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o por mandato de la ley." (Jaramillo, 2014)

A la vez se optó por proteger los datos mediante el Hábeas Data.



Fuente: (Jaramillo, 2014)

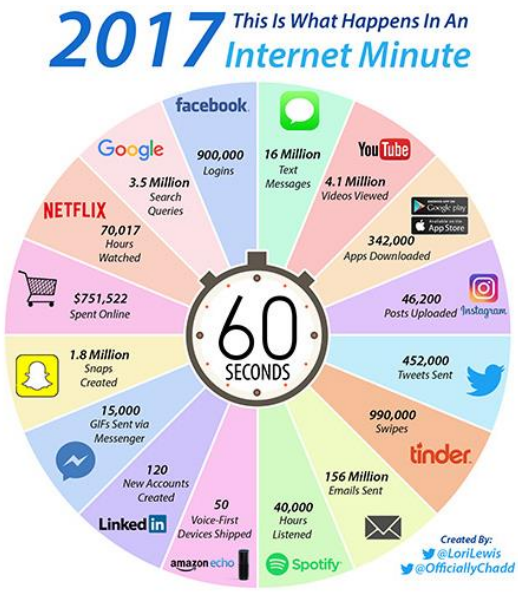
Elaborado por: Antonela Suárez

Fig. 7 Definición de Hábeas Data resumen Ecuador

El Big Data y la Privacidad

Hoy por hoy, el tráfico de datos que circulan por el internet es cada vez más denso; el uso frecuente del internet para realizar transacciones comerciales y de toda índole es el pasar cotidiano de las personas y más aún de los jóvenes.

El paso de las actividades económicas, comerciales y del entretenimiento al ciberespacio han abierto un sinfín de posibilidades para ver y realizar dentro de la red y muchas veces permiten a los usuarios realizar cualquiera de estas actividades de forma gratuita a simple vista, en donde el único requisito es la identificación y entrega de parte de su información personal con el consentimiento de aquella persona que accede a estas. Sin embargo, el precio que se paga por los lugares gratuitos es el precio de la información, de los datos y muchos de estos se van almacenando en grandes bases de datos según los lugares accedidos generando grandes volúmenes de datos al día.



Fuente: (Lewis & Callahan, 2017)

Elaborado por: Loris Lewis

Fig. 8 Lo que pasa en internet en un minuto

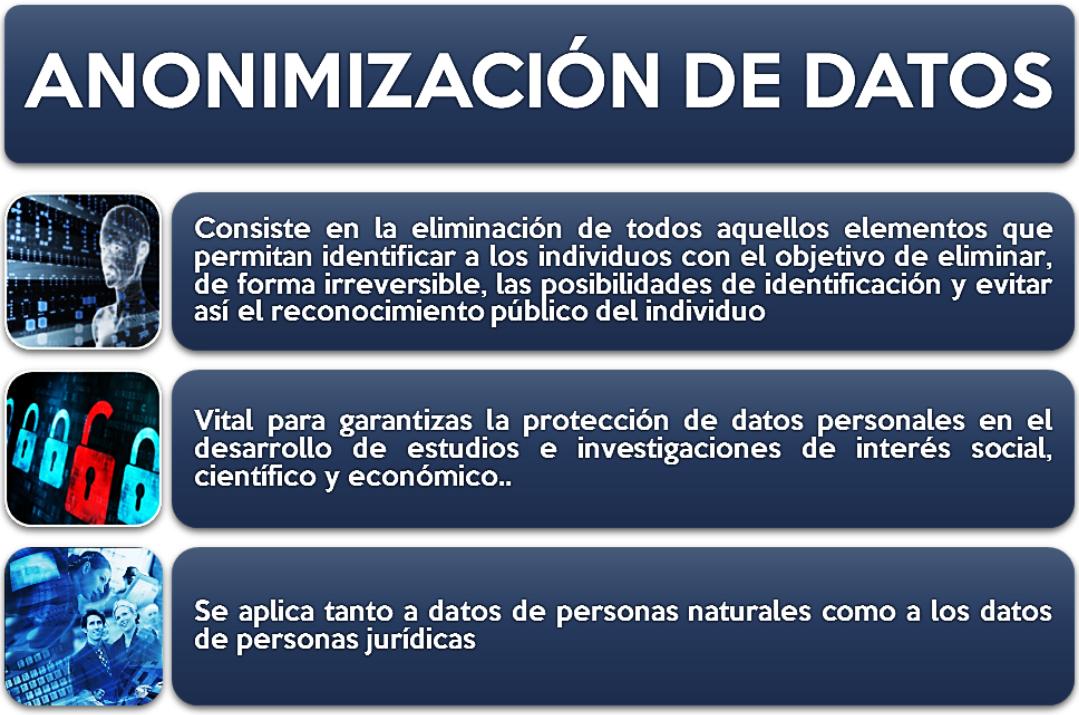
La Figura 8 muestra la densidad de datos enviados en un minuto dentro del internet (¿Qué sucede en internet cada minuto? , 2017). Esta información es valiosa para las empresas dado que su análisis y tratamiento permite la toma de decisiones de forma más asertivas y permite ser aplicada en múltiples campos como: en la comercialización, la salud, la gestión del tráfico, las comunicaciones móviles, detección de fraudes, el deporte, entre otros.

El tratamiento, análisis y estadísticas realizadas con grandes volúmenes datos se conoce como Big Data. Es una de las herramientas de inteligencia de negocios que alcanzó gran importancia con las proyecciones a futuro sobre distintos temas en diversas áreas de la industria.

El Big data representa un gran reto al momento de hablar de la privacidad, dado la presencia de datos personales en la multitud de información a analizar y que podrían transgredir las leyes de protección de datos, dejando como afectados

a los usuarios directamente. Sin embargo, si estos datos no hacen identificable a una persona, es decir “se hacen anónimos a través de técnicas de anonimización, se convierten en datos no personales, la privacidad de los individuos queda protegida, de modo que no es necesario aplicar ninguna norma sobre protección de datos” (González E. G., 2016).

Conjuntamente con la creación de datos pseudónimos (disociación) y la anonimización se cuenta con mayores garantías para la privacidad de los usuarios. La anonimización se define como:



Fuente: (Mediano, 2016)

Elaborado por: Antonela Suárez

Fig. 9 Definición de Anonimización de Datos

La privacidad a nivel tecnológico ha sido uno de los aspectos que mayor preocupación genera en la actualidad y donde su pronunciamiento ha salido a luz gracias a los escándalos presentados por la vigilancia continua por parte de

los gobiernos a sus ciudadanos y en especial por parte de la Agencia de Seguridad Nacional de Estados Unidos, así como la evidencia de la comercialización de datos por parte de empresas tecnológicas poderosas.

Si bien es un tema que afecta a todos los usuarios de internet, varios de ellos no tienen un conocimiento al respecto ni toman las medidas necesarias para hacer respetar su derecho a la privacidad.

1.2. Transparencia

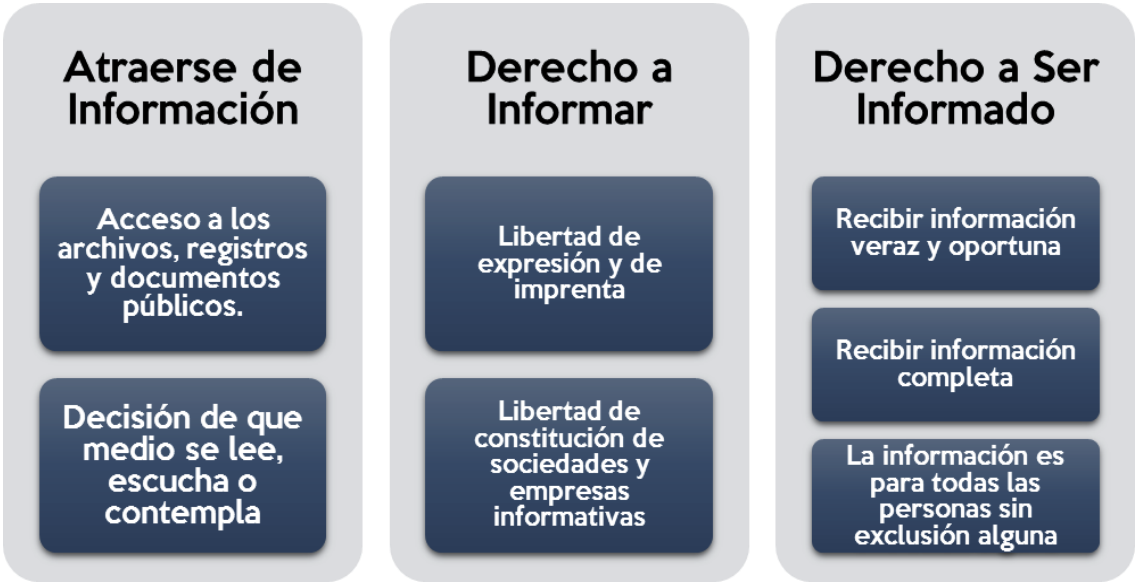
3.1.6. Definición

El aseguramiento de la democracia y la participación ciudadana es una de las herramientas más poderosas que puede tener un gobierno para mantener a sus ciudadanos conformes acorde a su gestión. Más aún, cuando los mantiene informados y brinda el libre acceso a conocer que es lo que están realizando en diferentes periodos de tiempo. Todas las personas esperan que sus gobernantes realicen sus tareas de la mejor forma posible, sin embargo, la presencia de la corrupción, de los actos injustificados puede ocasionar la inconformidad total de sus ciudadanos y repercutir en enfrentamientos innecesarios. Es por eso que la transparencia es fundamental para asegurar un buen convivir entre el estado y sus gobernados.

El término transparencia es difícil de definir dado que aborda diferentes dimensiones como son: “una dimensión jurídica, una dimensión económica, y una dimisión política, además de una asociación con la moral y en donde sus acciones repercuten en varios ámbitos de la vida social; lo que implica que sea tratada de forma interdisciplinaria” (Villaescusa, 2012).

La transparencia asociada a la moral se la ve como un valor aplicado a la conducta humana que permite el entendimiento total de lo que se desea expresar, sin ambigüedades que facilite la interpretación por parte de los demás y es considerado como un valor esencial para la democracia. (Ucha, 2010)

Desde el punto de vista del derecho, la transparencia se encuentra estrechamente ligada al derecho a la información, el cual garantiza que toda persona pueda “atraerse información, informar y a ser informada” (Carpizo, 2000).



Fuente: (Carpizo, 2000)

Elaborado por: Antonela Suárez

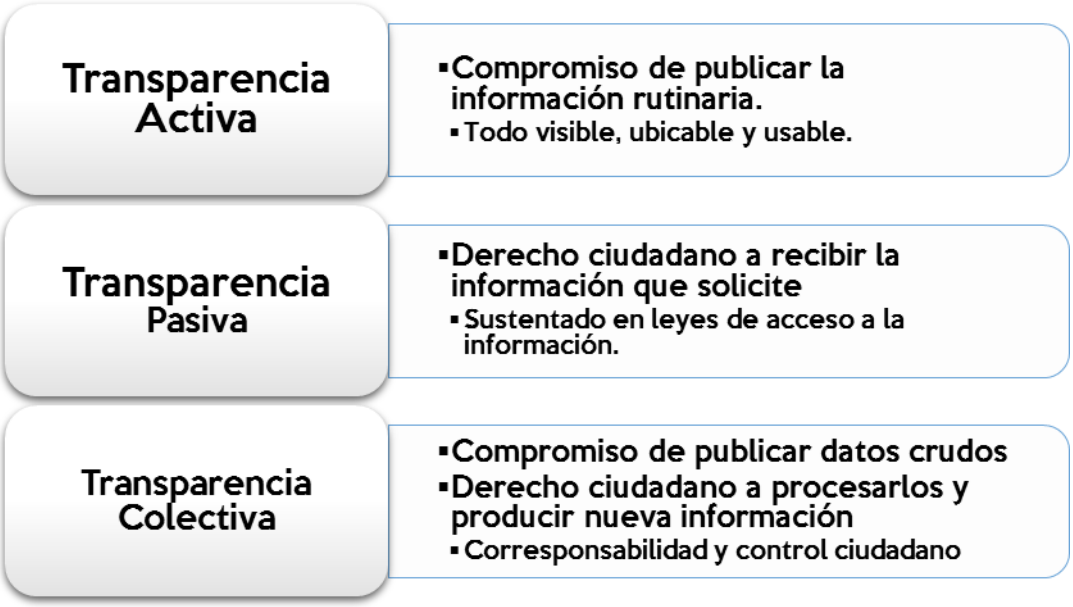
Fig. 10 Garantías del derecho a la información

Para lograr que se haga efectivo este derecho humano se lo realizará mediante el reconocimiento del derecho de acceso a la información pública.

En el ámbito político, este término es usado para expresar la honestidad que caracteriza la gestión de los gobernantes. Es decir “es el deber de todo Gobierno de informar, dar cuentas y poner a disposición de sus ciudadanos la

información pública" (¿qué es y para que sirve la transparencia gubernamental?, 2012). Sin exponer aquella información que pueda "comprometer la seguridad pública, dañar la estabilidad financiera del país, poner en riesgo una negociación internacional o la persecución de delitos, por lo que este tipo de información se reconoce como confidencial." (¿qué es y para que sirve la transparencia gubernamental?, 2012)

Tipos de transparencia

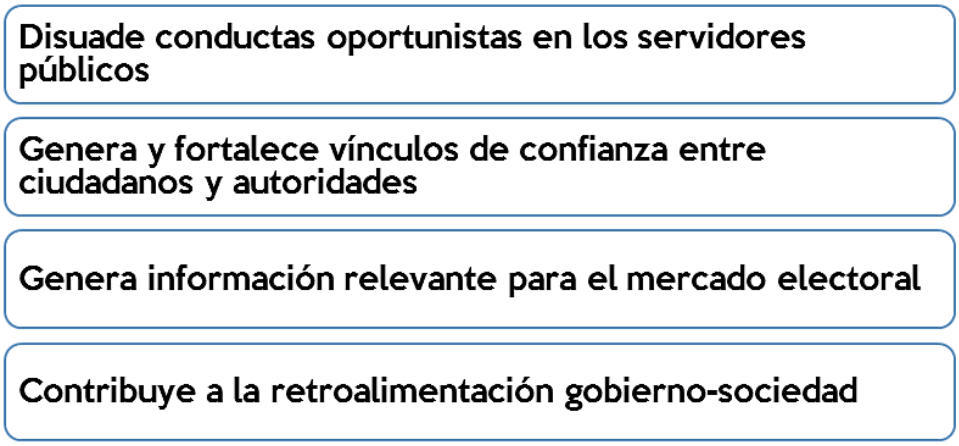


Fuente: (Alorza, 2013)

Elaborado por: Antonela Suárez

Fig. 11 Tipos de Transparencia

Beneficios de la transparencia



Fuente: (Gutiérrez, 2008)

Elaborado por: Antonela Suárez

Fig. 12 Beneficios de la Transparencia

3.1.7. Enfoque hacia el internet.

Con la llegada del internet, y gracias al aumento de la tasa de penetración de a la red en diferentes estados democráticos, la transparencia se ha impulsado ya que mediante el uso del internet facilitó el acceso gratuito a toda la "documentación del gobierno y a la formulación de políticas" (MARGETTS, 2011); cientos de sitios webs de casi todos los gobiernos proveen enlaces de redes sociales y otros medios, lo cual permite una mayor posibilidad de desarrollo de interacciones que cultiven las relaciones gobierno - ciudadano.

Estas aplicaciones proporcionan a los ciudadanos una fácil comprensión de los cambios que suceden en los procesos de gobierno como por ejemplo la publicación de procesos gubernamentales para la toma de decisiones hasta relevaciones más dramáticas con respecto a las acciones, palabras y pensamientos políticos que pueden ser leído en páginas como Twitter o incluso

a través de WikiLeaks generando nuevas fuentes de confianza, del sentirse aliado. En otras palabras, el internet es una herramienta que ha permitido que se dé un proceso de libertad de información donde los ciudadanos tienen “un potencial mucho mayor para observar y entender lo que está sucediendo en el gobierno, desdibujando las fronteras entre los ciudadanos y el estado y abriendo procesos de escrutinio” (MARGETTS, 2011). El poder leer, entender, analizar y compartir con otros ciudadanos esta información permite que ellos puedan tomar la transparencia en sus propias manos, confiando en ellos mismos y pudiendo expresar su opinión con mayor relevancia.

El paso de la tecnología contribuye a que al debilitamiento de la capacidad de los tribunales y otras instituciones del Estado para bloquear la transferencia de información. Dado que en la red todo puede ser expuesto con tan solo un clic y una serie de algoritmos.

En algunos casos, la ganancia de transparencia implica enormes cantidades de datos o la traducción de documentos mediante procesos en código de computadora, realizado por ciudadanos comunes que conocen acerca del manejo de tecnología; esto implicará confianza en nuevos actores cuya confiabilidad aún no ha sido demostrada y que no están sujetos a ninguno de los controles y que a su vez equilibra los sistemas gubernamentales creados y manejados actualmente.

Open Data

Los datos abiertos son uno de los medios que contribuyen a la búsqueda de la transparencia en la actualidad. Estos se definen según la “definición de la apertura” la cual consta de tres puntos fundamentales que son:

Fuente: (El manual de Open Data, 2016)

Elaborado por: Antonela Suárez

Fig. 13 Definición de apertura

Se puede decir bajo las premisas anteriores que “Los datos abiertos son datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen.” (El manual de Open Data, 2016)

Al contar con datos abierto es fundamental la presencia de la interoperabilidad, lo que quiere decir la habilidad para integrar diferentes conjuntos de datos y que se mantengan trabajando juntos. Esto permite la construcción de sistemas complejos y grandes.

“La esencia del manejo de datos compartidos es que una parte del material abierto pueda ser mezclado con otro material abierto. Esta interoperabilidad es absolutamente fundamental para entender los principales beneficios prácticos de la apertura: el incremento dramático de la habilidad de combinar distintas bases de datos o conjuntos de datos y así desarrollar más y mejores productos y servicios”. (El manual de Open Data, 2016)

Los datos abiertos están conformados por información no personal, es decir que no contiene datos sobre algún individuo en específico. Siendo así, también excluye algunos datos gubernamentales que pueden ser de riesgo para la nación, véase la Figura 14 para conocer algunos de los datos abiertos disponibles y los indicadores que utilizan los investigadores para evaluar la transparencia de un país. Estos datos “pueden ser utilizados, reutilizados y libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen.” (Taiwán primer lugar en el mundo en acceso a datos abiertos del gobierno, 2017)

Fuente: (Taiwán primer lugar en el mundo en acceso a datos abiertos del gobierno, 2017)

Realizado por: Antonela Suárez

Fig. 14 Tipos de datos abiertos y sus indicadores de calidad

La importancia de los datos abiertos recae en el desarrollo de aplicaciones en todo tipo de áreas y es un campo extenso de explotación. Por ejemplo, hasta el momento existen algunas aplicaciones creadas por usuarios comunes gracias al acceso a datos abiertos. “Find Toilet” es una aplicación desarrollada por una mujer en Dinamarca que muestra todos los baños públicos daneses, para personas que tuviesen problemas de vejiga. Otras aplicaciones como “Mapumental” y “Mapnificent” permiten encontrar lugares donde vivir considerando el tiempo de duración del viaje contribuye con precios de vivienda y el tipo de área que es; estas aplicaciones fueran realizadas mediante datos abiertos en Reino Unido y Alemania respectivamente.

1.3. Neutralidad de la Red

3.1.8. Definición

La neutralidad de la red nació como un principio fundador de internet, donde todos los datos que se encuentre circulando a través de la red, sean tratados por igual sin importar su procedencia, tipo o contenido y es fundamental para la conservación de un Internet no discriminatorio, diverso, innovador y libre. Un lugar donde sea primordial fomentar y mantener las libertades de acceso y distribución de información.

Fuente: (El Telegrafo, 2017)
Realizado por: Antonela Suárez

Fig. 15 Principal Ideal de la Neutralidad de la Red

“La neutralidad de la red también garantiza el ejercicio de derechos humanos: favorece el acceso al conocimiento de las personas, la pluralidad de discursos y favorece la libertad de expresión, al no permitir la discriminación de contenidos. Incluso protege la privacidad, al no brindar ninguna razón legítima a los proveedores de conexión para vigilar el tráfico en Internet.” (HOTT, 2014)

Desde el punto de vista técnico, el protocolo aplicado para la generación de internet fue diseñado de forma que no discrimine según los contenidos que viajen mediante la red, más bien que sean tratados por igual, salvo que exista algún inconveniente con la gestión de tráfico donde se aplicara medidas puntuales, de todas formas, todos los datos deben ser tratados de forma imparcial.

Hoy en día, la neutralidad de la red no cuenta con regulaciones en algunos países alrededor del mundo lo que implica que las compañías y diferentes proveedores de servicio, quieran controlar y establecer tarifas para el uso de distintos servicios provistos en la red, afectando directamente a usuarios con estas medidas. Es por eso que grandes empresas como Google, Amazon, Yahoo, Netflix entre otras ven fundamental la lucha por la neutralidad de la red y han presentado fuertes quejas. (González M. , 2014)

Fuente: (González M. , 2014)
Realizado por: María González

Fig. 16 Priorización de tarifas por uso de servicios de internet

El internet sin neutralidad destruye completamente lo que es conocido como ciberespacio, todos los proyectos de innovación que han surgido gracias a la amplia libertad de navegación y la fácil obtención de datos para estudio quedarían sujetos al criterio de empresas de telefonía y cable que decidirán que aplicaciones y sitios web en futuro tendrían éxito. Sumado a la exclusión de un

sin número de personas que serán discriminadas de su uso convirtiendo a la red en una división de estratos sociales. Desde otro punto de vista, los grupos de activistas que se expresan para la defensa de diferentes causas, así como pequeños negocios que empiezan a establecer su mercado, gracias a su accionar en la red quedarán relegados y perderán su espacio si no cuenta con los fondos necesarios para pagar su establecimiento en el mundo virtual.

3.1.9. Enfoque hacia la privacidad y transparencia

La neutralidad del internet es un componente fundamental para poder hablar sobre transparencia y privacidad a nivel tecnológico. Por un lado, la red ha permitido el intercambio de información a gran escala lo que ha permitido dar lugar a un pequeño camino de transparencia gracias a la posibilidad de colocar contenido de forma gratuita, más aún la privacidad ha surgido en una virtualidad sin límites y control donde exponer los datos es algo implícito en sus transacciones.

Si la neutralidad de la red es eliminada, todas las políticas de protección de datos que están surgiendo, así como la posibilidad de acceder a todo tipo de información libremente sin importar fronteras quedara completamente relegada convirtiendo al ciberespacio en un objeto comercial, tarifado por la competencia entre compañías que buscan establecer su mercado, y donde la información de los usuarios formaría parte de los proveedores de internet y telefonía móvil.

Resumen

Internet, fue el resultado de un experimento del Departamento de Defensa de Estados Unidos, en el año 1969, que se materializó en el desarrollo de ARPAnet, una red que enlazaba universidades y centros de alta tecnología con contratistas de dicho departamento. Tenía como fin el intercambio de datos entre científicos y militares. A la red se unieron nodos de Europa y del resto del mundo, formando lo que se conoce como la gran telaraña mundial (World Wide Web). En 1990 ARPAnet dejó de existir.

Desde su aparición, el internet ha pasado por varias fases que le han permitido su incorporación en diferentes tipos de dispositivos; pasando de ser una herramienta con fines específicamente militares a convertirse en un centro de comunicación continúa entre individuos en todo tipo de aspectos cotidianos, en cualquier horario y parte del mundo.

El internet se ha convertido en parte integral de la vida cotidiana de la mayoría de la población mundial. La transmisión y el envío de datos desde dispositivos móviles, es de lo más común a toda hora del día. La información se está convirtiendo en la herramienta primordial para el desarrollo de artículos tecnológicos nuevos, cada vez más capacitados y ajustados al estilo de la vida de cada persona.

La idea del internet en todo lugar y para todos, promete usuarios que siempre estén conectados a la red y almacenen información en la nube a cada segundo impulsando la conectividad total y la digitalización global; permitiendo consigo una comunicación más sencilla y eficiente para todos, sin importar el lugar en donde este, donde la única limitación para no estar conectados sea la voluntad propia.

Aspectos como la publicidad, las redes sociales y la necesidad de saber qué está pasando en la vida de los demás es otro aspecto que será explotado y desarrollado con énfasis para los dispositivos móviles y aparatos pequeños que se desarrollen a futuro mediante nanotecnología.

Hoy por hoy, el tráfico de datos que circulan por el internet es cada vez más denso; el compartir de las actividades que se van realizando a lo largo del día se ha vuelto algo casi natural para la sociedad y más aún para los jóvenes. El paso de las actividades económicas, comerciales y del entretenimiento al ciberespacio han abierto un sinfín de posibilidades para ver y realizar dentro de él y muchas veces permiten realizar cualquiera de estas de forma gratuita a simple vista, en donde el único requisito es el del identificarse y entregar parte de la información personal con el consentimiento de quien accede. Sin embargo, el precio que se paga por los lugares gratuitos es el precio de la información, de los datos y muchos de estos se van almacenando en grandes bases de datos según los lugares que se vaya accediendo, generando grandes volúmenes de datos al día.

El internet es una herramienta que ha permitido que se dé un proceso de libertad de información donde los ciudadanos tienen un potencial mucho mayor para observar y entender lo que está sucediendo en entidades primordiales como los gobiernos, desdibujando las fronteras entre los ciudadanos y el estado y abriendo procesos de escrutinio.

En algunos casos, la ganancia de transparencia implica enormes cantidades de datos o la traducción de documentos mediante procesos en código de computadora, realizado por ciudadanos comunes que conocen acerca del manejo de tecnología; esto implicará confianza en nuevos actores cuya confiabilidad aún no ha sido demostrada y que no están sujetos a ninguno de los controles y que a su vez equilibra los sistemas gubernamentales creados y manejados actualmente.

La neutralidad del internet es un componente fundamental para poder hablar sobre transparencia y privacidad a nivel tecnológico. Por un lado, la red ha permitido el intercambio de información a gran escala lo que ha permitido dar lugar a un pequeño camino de transparencia gracias a la posibilidad de colocar contenido de forma

gratuita, más aún la privacidad ha surgido en una virtualidad sin límites ni control, donde exponer los datos es algo implícito en sus transacciones.

Si la neutralidad de la red es eliminada, todas las políticas de protección de datos que están surgiendo, así como la posibilidad de acceder a todo tipo de información libremente sin importar fronteras quedara completamente relegada convirtiendo al ciberespacio en un objeto comercial, tarifado por la competencia entre compañías que buscan establecer su mercado, y donde la información de los usuarios formaría parte de los proveedores de internet y telefonía móvil.

CAPÍTULO 2

Este capítulo, tiene como objetivo obtener una visión sobre la privacidad y transparencia del internet a nivel mundial, así como las regulaciones correspondientes. Situaciones expuestas por parte de WikiLeaks y la realidad presentada por Edward Snowden serán abordadas.

ESTADO DEL ARTE

2.2. La Privacidad del Internet en el Mundo

> "Para una sociedad abierta, en la era electrónica la privacidad es necesaria. La privacidad no es un secreto. Un asunto privado es algo que uno no quiere que todo el mundo sepa, pero un asunto secreto es algo que alguien no quiere que cualquiera sepa. La privacidad es poder revelarse uno mismo al mundo en forma selectiva"
>
> *Eric Hughes,1993*

3.1.10. Informes electrónicos WikiLeaks

Wikileaks es una organización formada por periodistas, disidentes, matemáticos y programadores de todo el mundo. Cuya misión consiste en publicar en varios sitios de internet, incluida su página web, informes filtrados por fuentes anónimas sobre comportamientos poco éticos y delitos de gobiernos, ejércitos y grandes corporaciones de todo el mundo. WikiLeaks fue creada en diciembre del 2006 por Julian Assange. Y su página web se encuentra alojada en servidores suecos desde enero del 2007 ya que en este país se mantienen leyes que protegen el anonimato.

No obstante, WikiLeaks no alcanzó un impacto mundial hasta el año 2010 cuando concretó una alianza con algunas empresas informativas de gran importancia en el mundo para revelar los documentos secretos que poseía.

Durante sus primeros años, Wikileaks presentó una serie de revelaciones de información secreta; entre ella se encontraba: un informe sobre el expresidente keniano Daniel Arap Moi, quien saqueó a su país para apropiarse 1.500 millones de euros. El manual de procedimiento militar en el Campamento Delta de la base de Guantánamo de Estados Unidos. También realizaron “la difusión de fotografías y extractos de correos electrónicos personales de la gobernadora ultraderechista de Alaska y candidata a la vicepresidencia de Estados Unidos en 2008, Sarah Palin; o más de 3.000 mensajes de correos electrónicos intercambiados por algunos de los climatólogos más influyentes del mundo” (Quian, 2013).

En el 2010, WikiLeaks alcanza un impacto mundial con la publicación sobre un video en el que se ve cómo soldados estadounidenses acribillan al fotógrafo de la agencia Reuters Namir Noor-Eldeen, a su ayudante y a nueve personas más desde un helicóptero Apache estadounidense en Irak. Su difusión fue realizada mediante Collateral Murder y presentada por National Press Club de Washington en una conferencia de prensa. Distintos medios de comunicación como The Washintong Post, The New York Times, CNN, The Guardian continuar con la difusión de la noticia luego de que esta tomara fuerza al ser transmitida por la cadena árabe Al Jazeera y el canal Rusia Today.

Luego de la creación de alianzas estratégicas con diferentes medios de comunicación y su acuerdo para la protección de las fuentes de las revelaciones miles de archivos con información secreta comenzaron a salir a la luz, según la ética “hacker” de Assange estos debían ser presentados de tal y como estaban sin suprimir ningún tipo de información así demuestra la identidad de una persona; esto causó distintas disputas entra la ética profesional de los periodistas.

A continuación, un resumen de las revelaciones más importantes que han dado a conocer a WikiLeaks:

Diciembre de 2007	Publicación acerca de un compendio para los soldados de la Armada de Estados Unidos que se ocupaban de los prisioneros de la Bahía de Guantánamo.
Septiembre de 2009	Revelación acerca de la empresa Transfigura sobre el vertido tóxico realizado en las costas de Marfil y su afectación a más de 100 000 personas.
Abril de 2010	Publicación de un video militar clasificado donde muestra a un helicóptero Apache estadounidense disparando a un reportero y civiles iraquíes.
Octubre de 2010	Publicación acerca de la guerra de Afganistán con Iraq. Revelando el número de civiles iraquíes asesinados; el abuso de poder por parte de militares y policías y la tortura a prisioneros de guerra.
Diciembre de 2011	Publicación sobre SpyFiles, referente a empresas que venden a gobiernos software de espionaje masivo. Continuación en el 2013 y 2014
Febrero de 2016	Información referente a los líderes de países claves y organizaciones para intereses geopolíticos de Estados Unidos
Octubre de 2016	Publicación acerca de los acuerdos comerciales confidenciales entre EEUU y otros países.
Julio de 2016	Filtraciones sobre el Partido Demócrata de Estados Unidos, mostrando 1000 de mails y archivos adjuntos de políticos con más poder

Fuente: (CNNEspañol, 2016)

Elaborado por: Antonela Suárez

Fig. 17 revelaciones más importantes que han dado a conocer a WikiLeaks

Julian Assange mantiene una filosofía basada en el ciberpunk, término que define a una persona que usa encriptación cuando accede a redes computacionales con finalidad de asegurar su privacidad, especialmente de gobiernos autoritarios. El Cypherpunk nació a finales de la década de los setenta como una unión entre la actitud punk y la alta tecnología. “El objetivo de este movimiento ciberpunk es desmantelar el secreto como mecanismo de gobierno de los Estados-nación y corporaciones. Pero este objetivo no debe entrar en conflicto con el derecho a la privacidad del individuo.” (Quian, 2013). Assange reconoce el secreto como herramienta de la censura, y la búsqueda de información como camino hacia un estado de conocimiento y de justicia mejorada entre estructuras tradicionales de poder y los disidentes:

Assange persiste en denotar el valor de la información como vía al conocimiento, a la autonomía y libertad del individuo: “Puedes estar informado y ser tu propio gobernante, o bien puedes vivir en la ignorancia y dejar que otras personas, bien informadas, te gobiernen” (Quian, 2013)

2.2.1.1. Situación del uso del internet por parte de los gobiernos.

No hay nada que infunda más presión sobre los Estados-nación que una serie de disidentes ejerciendo influencia sobre el pueblo para informarlo e influenciarlo en la idea del cambio ante una ley, política, o accionar de los gobernantes que pueden llevar a todos a una vida en opresión e injusticias. Julian Assange, mediante su página de WikiLeaks, promueve una ética y valores vinculados a la verdad, la libertad, la transparencia y el acceso libre y universal a la información y el conocimiento haciendo un llamado a la prensa sobre su presentación al mundo de información vana y según la conveniencia de los poderosos, del estado, para mantener la “paz, confianza y tranquilidad” entre los ciudadanos.

Las revelaciones realizadas por WikiLeaks han despertado una necesidad de verdad entre varios individuos a nivel mundial; ha llegado a sembrar el cuestionamiento del accionar de los gobernantes donde el único motivo para guardar secretos es porque se trata de un régimen corrupto. Sin embargo, en los diferentes países del mundo el presentar estos contenidos representan grandes peligros de desestabilización de los regímenes; por lo que la libertad de expresión es aplastada y altamente controlada en todos los medios de comunicación, incluyendo el internet. Existen países donde el uso de internet se encuentra totalmente restringido, así como el acceso a la información independiente y donde la presa es silenciada con cárcel día a día.

Elaborado por: Antonela Suárez

Fig. 18 Diez países donde existe censura penetrante

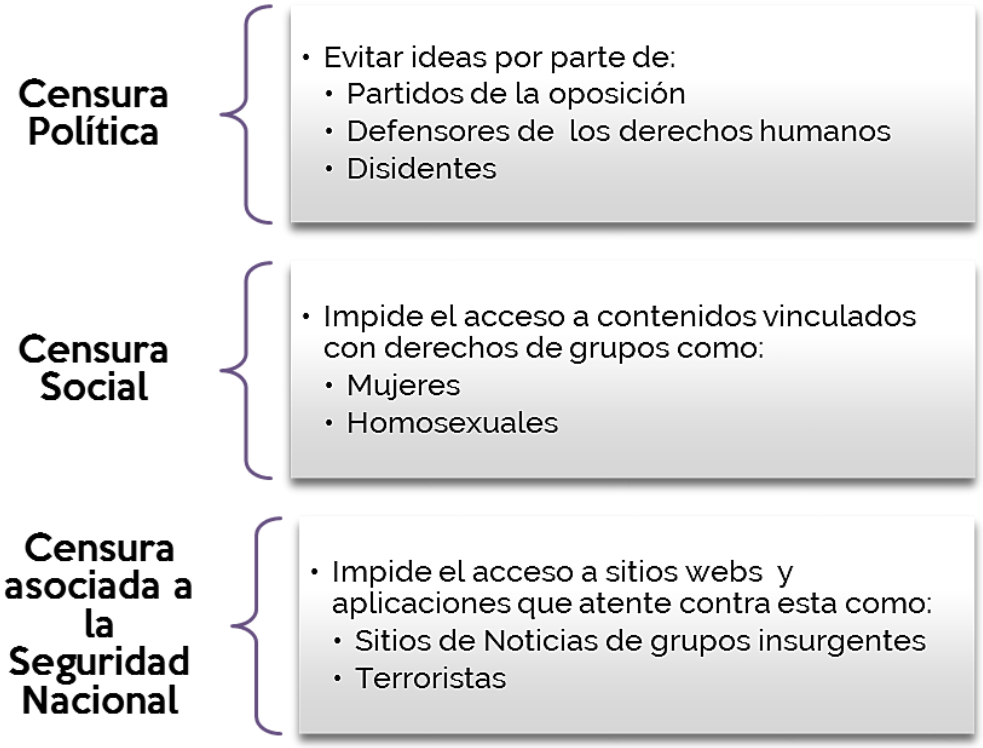
La Figura 18. Muestra los países donde la vigilancia y control sobre la información que es compartida sea de carácter político, social o cualquier otro tipo es estrictamente analizada y restringida si amerita el caso, además de amedrentar con represalias a quien publique contenido indebido o intente acceder a sitios prohibidos; incluyendo entre sus medidas el encarcelamiento o algún otro tipo de sanción. El acceso a internet se encuentra restringido en países con regímenes comunistas como China, Cuba, Corea del Norte y Vietnam.

La situación de restricción del internet es diferente para cada país, en Cuba por ejemplo el internet se encuentra disponible solo para una pequeña parte de la población; los ciudadanos deben usar puntos de acceso monitoreados por el gobierno, donde la actividad está controlada y puede ser bloqueada la dirección IP, además cuentan con filtros de palabras claves y la revisión del historial de navegación. El gobierno cubano continúa encarcelando periodistas que presenten reportes mediante la red en sitios ajenos a los del país y defiende su accionar argumentando que existe poco acceso al internet por las pocas o casi nulas relaciones con Estados Unidos. En China mientras tanto, mantiene la

Gran Muralla de Fuego, que consiste en una serie de censores humanos y herramientas tecnológicas para bloquear los sitios web considerados por parte del gobierno como “sensibles” y ayuda al control de medios sociables, es aplicado a todo el contenido que viaja en el internet por lo que incluye herramientas para el filtrado de términos clave, bloqueo de direcciones IP y no permite al acceso a sitios extranjeros como Facebook, Twitter y YouTube. En otras palabras “los ciudadanos viven en una realidad paralela, con fuentes de información, servicios e informaciones muy diferentes a las europeas y americanas” (Rivera, Usando internet en China durante una semana: una pradera repleta de vallas, 2017). China mantiene alrededor de 44 periodistas presos, de los cuales 32 son periodistas digitales y con sus últimas reformas de ley pretenden “controlar también las opiniones críticas y las posibles revueltas sociales que podrían organizarse mediante servicios de mensajería, chats y redes sociales.” (SANTOS, 2016)

Por otro lado, en Irán se encuentran restricciones similares con respecto a las redes sociales, sitios como Facebook, Twitter y aplicaciones como WhatsApp no existe acceso, pero el presidente del país cuenta con una cuenta oficial en Twitter donde va publicando un informe de lo que realiza, pero ningún ciudadano puede saber de esto a menos que utilice un servicio de VPN externa. Negando completamente el derecho a la información para sus ciudadanos.

La censura en la red no es realizada de la misma manera, ni en la misma medida en todos los países. Por ejemplo, en Corea del Sur, toda la información que se encuentre relacionada con Corea del Norte es restringida. Hay quienes prefieren restringir el acceso de forma temporal, este fue el caso de Turquía que aplicó censura puntual, en un video de YouTube al ser considerado ofensivo para la memoria del primer presidente turco. Se puede decir que la censura puede ser aplicada en tres ámbitos diferentes presentados a continuación:



Fuente: (Fernández De Lis, 2007)

Elaborado por: Antonela Suárez

Fig. 19 Ámbitos de aplicación de la censura

Existen países donde sus gobernantes han establecido leyes que restringen el uso de VPN o de herramientas que permitan usar direcciones IP fraudulentas o enmascaradas con el propósito de acceder a contenido online bloqueado geográficamente. Esto es considerado un delito, así como su prevención de descubrimiento del acto será sancionado con cárcel además de una multa que puede llegar a costar medio millón de dólares. Este es el caso de Emiratos Árabes Unidos que además de promulgar esta ley ha bloqueado los servicios de voz mediante IP presentes en aplicaciones como WhatsApp o Skype.

Finalmente, puede decirse que asuntos como la privacidad de las personas en internet se ha vuelto completamente inexiste sin importar el país de procedencia

del usuario que accede a este medio, dado que existe una monitorización “sin tregua y los datos están disponible en la red para las agencias de inteligencia (como posibles terroristas o enemigos del estado), como también para las firmas comerciales, que ven en los usuarios de internet un público objetivo” (Romero, 2013). Julian Assange señala “el Internet, que es nuestro mayor instrumento de emancipación, ha sido transformado en la mayor herramienta de totalitarismo que hayamos visto”. (Assange, 2013, págs. 121-126). Las medidas radicales de censura en diferentes países del mundo son la mejor evidencia de lo que sucedería si se deja herramientas tan poderosas como es el internet en manos de las elites, estas serán transformadas en grandes aparatos de control y vigilancia que permiten a los poderosos seguir abusando de su poder, bajo el lema de que luchas por el bien común de todos. Gobiernos que esconden y presentan solo la información de su conveniencia para mantener la tranquilidad de sus ciudadanos, son lugares en donde la transparencia está quedando completamente perdida.

2.2.1.2. Criptografía para la privacidad y Transparencia.

> “Si tenemos el derecho de que empresas y gobiernos no entren a nuestras casas a grabar lo que hacemos, tenemos el derecho de que nuestras actividades que ocurran en el ciberespacio no sean vigiladas.”
>
> *Lucas Teixeira, activista Oficina Anti vigilancia*

Uno de los problemas de la información que viaja mediante la red, es que ésta no se encuentra cifrada, es como si años atrás se enviara una carta por correo sin sellar el sobre, exponiendo a que en todos los lugares que ésta recorre hasta su destinario pueda ser leída. Una situación similar ocurre con los datos que van pasando a través de la red, cualquier persona que use una herramienta especializada para captar paquetes puede obtenerlos, leerlos y usarlos según su conveniencia. Según las revelaciones de WikiLeaks, hoy en día cualquier dispositivo móvil puede ser usado para vigilancia y como tal puede ser manipulado para retransmitir los datos (llamadas, fotografías, mensajes, etc.), sin el consentimiento del dueño del dispositivo y de la información que ha compartido con otra persona.

Es por eso que una de las armas para luchar en favor de la privacidad es la criptografía. Esta es una forma de acción directa y que no produce violencia, ni daños ante nadie como lo haría cualquier tipo de arma, pues al ser creado en base a operaciones matemáticas su presentación ante los demás va a llegar a ser un “simple” problema matemático a resolver.

Fuente: (Real Academia Española, 2001)

Elaborado por: Antonela Suárez

Fig. 20 Definición Criptografía

La criptografía no es más que un conjunto de reglas y combinaciones matemáticas relativas a la seguridad de los datos solo quien tenga la llave con el que algoritmo fue desarrollado será quien podrá descifrar y obtener el contenido; su uso trae consigue diferentes beneficios como son:

Fuente: (Rozas, 2013)

Elaborado por: Antonela Suárez

Fig. 21 Beneficios del uso de la criptografía

La lucha de la privacidad mediante la criptografía permite en cierto modo responder ante la vigilancia estatales y privadas y de las grandes organizaciones de espionaje gracias a que, si la información es cifrada desde los propios terminales, será casi imposible que una persona externa pueda descifrarlo y esto permitirá que los datos enviados mediante la red sean conocidos exclusivamente por el destinatario final y no por los proveedores de Internet o a su vez las diferentes compañías que se encargan de analizar los datos para realizar comercio a fin. Una de las preocupaciones al usar herramientas criptográficas provistas por compañías es que ellas al contar con las claves de encriptación puedan descifrar los mensajes fácilmente, es por eso que “la criptografía por si sola no es suficiente. Lo que se necesitan son herramientas de criptografía que sean Software Libre. Caso contrario existe la posibilidad de que las herramientas cerradas de criptografía tengan puertas traseras y podemos ser espiados cuando pensamos que tenemos privacidad.” (Bonifaz, 2013).

Cabe recalcar que la criptografía también debe ser usada por parte de los gobiernos, que mantienen altos índices de datos abiertos este es el caso de Taiwan, Dinamarca, Colombia entre otros. Con la finalidad de asegurar que la información que forma parte de los informes que presentan se encuentre seguro ante otros países y sobre todo ante las agencias de inteligencia.

3.1.11. Punto de vista de Snowden

> “Estoy dispuesto a sacrificar todo porque no puedo en buena conciencia permitir que el gobierno de Estados Unidos destruya la privacidad, la libertad de internet y las libertades básicas de la gente alrededor del mundo con esa masiva máquina de vigilancia que secretamente construyeron”
>
> *Edward Snowden*

Edward Snowden es un informático estadounidense autodidacta cuyas revelaciones se han convertido en uno de los casos más controversiales en los últimos años y han servido para la concientización sobre el estado actual de la privacidad en el internet. Sus trabajos como vigilante comenzaron en el 2006, luego de ser contratado por la CIA, adquiriendo acceso a la información confidencial categorizada como de alto secreto. Durante el 2007 y el 2009, Snowden fue enviado a Suiza como experto en ciberseguridad por parte de la CIA. Durante este tiempo, empezó a sentirse desilusionado al ver la forma de actuar de su gobierno con respecto a la información del resto del mundo. Años posteriores Snowden abandona su trabajo en la CIA y comienza a trabajar para la NSA en Hawaii, lugar donde su pensar rechaza totalmente las actividades que se están realizando sobre los cientos de datos que se encuentra en la red; la vigilancia masiva queda completamente apartada de sus principios y decide mostrar esta información al mundo. A partir de diciembre del 2012 a enero 2013, Snowden contacta con el diario The Guardian contando a breves rasgos sobre la información que conocía; durante este año Snowden comienza a enviar documento a los periodistas de The Guardian y del Washington Post, conjuntamente con ellos mantiene reuniones en Hong Kong, lugar donde se preserva varias políticas sobre la libertad de expresión, y empiezan a armar la historia sobre lo que ha encontrado Snowden durante su tiempo de trabajo en las agencias de seguridad nacional.

A continuación, algunos datos relevantes sobre el caso de Edward Snowden:

5 de junio de 2013	Los documentos proporcionados son publicados en el diario The Guardian. Especificando el titulo como: "NSA recolecta registros de llamadas telefónicas de millones de consumidores de Verizon".
6 de Junio de 2013	Ambos periódicos publican un artículo sobre PRISM. Programa que obliga a las grandes corporaciones a ceder los datos de usuarios a las autoridades.
11 de junio de 2013	The Guardian publica diapositivas que muestran el nivel de recolección de datos de la NSA. Además revela a Edward Snowden como el filtrador de todas las informaciones publicadas.
13 de Junio de 2013	Snowden confirma espionaje a sistemas chinos y rusos.
14 de Junio de 2013	Snowden recibe cargos por transmitir comunicaciones e informaciones de carácter confidencial asociados a los servicios de inteligencia de los Estados Unidos.
23 de Junio de 2013	Snowden es retenido en el aeropuerto de Rusia, durante su viaje a Ecuador
Enero de 2014	Continúan las revelaciones sobre las actividades de espionaje la NCA. Confirmando el desarrollo de software capaz de monitorizar YouTube.

Febrero de 2014	Servicios de inteligencia británicos interceptaron Y recolectaron imágenes procedentes de *webcams*.
	Revelación sobre el uso de técnicas ilegales como espionaje, virus informáticos, recolección de información contra otras naciones, terroristas, periodistas Y diplomáticos.
Octubre de 2015	El Parlamento Europeo celebra una votación en la que absuelven Edward Snowden de todos los cargos en los diferentes países de la Unión Europea. Snowden lo califica como un paso hacia delante.
Marzo de 2016	Emite una entrevista sobre su visión sobre el futuro de la privacidad para la cadena televisiva La Sexta.

Fuente: (Rivera, 2016)

Elaborado por: Antonela Suárez

Fig. 22 datos relevantes sobre el caso de Edward Snowden

Snowden ha sido catalogado como traidor a su patria, pero es considerado como héroe para muchos, tras dejar todas las oportunidades y altas remuneraciones que ofrecía su trabajo para abrir los ojos al mundo y hablar sobre la privacidad. Desde entonces lucha por su libertad y trabaja por la defensa de la privacidad, es considerado como la imagen de la libertad en internet.

2.2.1.3. Situación del uso del internet a nivel mundial

En el 2013, Edward Snowden filtró miles de documentos clasificados de la Agencia de Seguridad Nacional de Estados Unidos acerca de la vigilancia masiva de los usuarios y la colaboración de grandes compañías como Google, Facebook, Yahoo!, Verizon para la provisión de datos que permiten el espionaje y monitoreo no solo de los usuarios de Estados Unidos, sino de los diferentes países alrededor del mundo; lo que provocó una conversación global sobre los derechos de los ciudadanos a la privacidad, libertad en Internet y cuestionó por primera vez el rol de Estados Unidos en el control del Internet (Zuazo, 2015, pág. 135).

El uso del internet por parte de los países comenzó a dar un giro gracias a estas revelaciones y a las aportadas por Julian Assange años atrás. La presidente de Brasil Dilma Rousseff, la canciller de Alemania Ángela Merkel fueran las primeras en pronunciar su inconformidad y tacharon de inadmisible el espionaje realizado por Estados Unidos a través de la NSA. Así mismo, se generó el dilema sobre el manejo de la información en los medios digitales, la seguridad de los datos de los ciudadanos en internet y cómo manejar el abuso contra los usuarios de la red generado por las agencias de seguridad nacional y empresas. A su vez mientras los gobiernos debatían a nivel macro, cientos de usuarios se han convertido en activistas de los derechos digitales y buscan llegar a más usuarios a que se unan y luchen por un internet libre para las generaciones futuras, donde se mantengan sus ideales iniciales y no sea convertido en un arma contra las personas.

“Permitir a la vigilancia prevalecer en internet significaría transformar a la red en una herramienta de represión, en un sistema de vigilancia que amenaza en convertirse en el arma más extrema y opresora de la intrusión estatal

sometiendo a todas las formas de interacción humana, planificación y pensamiento a su control exhaustivo” (Greenwald, 2014).

Frente a estos acontecimientos, surge una tendencia hacia el nacionalismo digital es decir la creación de redes propias de los países, almacenamiento en servidores locales y la protección con estándares locales de la información y sistemas de protección de datos, de los provistos por sus ciudadanos, donde las empresas y el estado tengan regulaciones a nivel de la red. Uno de los principales países en acudir a estas medidas fue Brasil, el gobierno brasileño presentó una legislación para la protección de la privacidad de los usuarios brasileños además que asegura el acceso igualitario a internet respetando los principios de la neutralidad de la red. Una de las reformas realizadas para su aprobación fue impuesta a los proveedores de Internet, quienes deben guardar la información de los usuarios en Data Centers dentro del país. Por otro lado, empresas como Google o Facebook deben responder ante las cortes brasileñas en casos donde intervenga la información de los usuarios de este país, sin importar que los datos estén resguardados en servidores extranjeros. Balancear los derechos y responsabilidades los usuarios, gobiernos y compañías, a la par de asegurar que el internet continúe siendo una red abierta y descentralizada ha generado el descontento de las empresas de telecomunicaciones al no poder cobrar de formas diferentes los servicios presentes en internet como Netflix, Skype, Instagram etc. (Zamorano, 2014).

Si bien el uso del internet no se ha disminuido, las revelaciones realizadas tanto por Assange como por Snowden han evidenciado desde diferentes puntos de vista la militarización del internet y la gran ignorancia que mantienen los usuarios sobre cómo la tecnología ha enmarañado cada proceso de sus vidas. Con esto se puede decir que existen nuevas guerras que están surgiendo dentro la red que involucran los derechos humanos, empezando por la

privacidad y la libertad en una época donde se ve una gran movilización política y las denuncias sobre la opresión; siendo éste el primer paso para la lucha de lo que será el internet del futuro.

2.2.1.4. Visión hacia el futuro en la privacidad del internet.

En la era de la sociedad de la información para “existir en línea” es necesario que se publique contenido para compartir es decir imágenes, videos, audio, texto etc. en espacios abiertos y públicos como las redes sociales. Caso contrario, las personas no podrán enriquecer su círculo de amistades, encontrar o conformar comunidades, aprender cosas nuevas y actuar como agentes económicos en línea. Los datos son la materia prima de la economía del conocimiento, por lo que la captura de estos está en el centro de los modelos de negocios de las empresas tecnológicas más exitosas y permiten abordar todo tipos de campos para alcanzar mercado partiendo desde ámbitos como: la atención de la salud, el entretenimiento, los medios de comunicación, las finanzas, los seguros hasta las suposiciones de la relación que existe entre los ciudadanos y el estado.

En los próximos años, el Internet seguirá un indiscutible camino hasta llegar a ser un foro público en donde todos los usuarios usen su identidad real y cuenten con un perfil digital asociado, sujeto a modificaciones, pero ningún tipo de eliminación. Los términos de ciudadanía y la manera en que la vida social se desarrollará, seguirán cambiando de forma apresurada con el auge de nuevos componentes tecnológicos como los dispositivos con múltiples sensores, el establecimiento del internet de las cosas y las ciudades inteligentes tendrán grandes impactos en la manera que los datos serán transmitidos mediante la red. Solo para el 2025, se espera que se genere 2.5 quintillones de bytes de

datos nuevos cada día; de los cuales puedan analizarse y proveer a las aplicaciones personales de información necesaria para servir de soporte para la toma de decisiones, asistencia para conducir o para aplicar realidad aumentada. La idea es que una persona pueda contar con la información actualizada en tiempo real y localizada a través de aparatos como Google Glasses (Schunter, 2013). Del mismo modo, las empresas también se beneficiarán de esta información en todos los sentidos partiendo desde el aspecto comercial. Las herramientas para la protección de datos es un aspecto que no ha sido valorado y que se irá perdiendo poco a poco frente a la versatilidad de los nuevos dispositivos que aparecerán en unos años.

Según estudios, se cree que la privacidad no será más que un tema tabú, y que ya no será posible de alcanzar dado que es todo un reto integrar la privacidad y los controles de confidencialidad en un escenario donde los sensores serán el componente principal de los terminales. Sumado a la capacidad para detectar y recopilar datos lo que permitirá el monitoreo y registro permanente de un ambiente expuesto. Estos sensores y nuevos terminales aprenderán sobre la localización, podrán identificar a las personas y los objetos además de grabar su comportamiento sin ningún tipo de restricciones. Sin las medidas necesarias acerca de la privacidad todos los comportamientos específicos de los individuos quedarían almacenados en los servidores extranjeros a disposición de los poderosos, sean gobiernos, agencias de seguridad nacional y sus redes con empresas tecnológicas fuertes añadiendo los intereses económicos de estas compañías que continuarán bloqueando cualquier trabajo efectivo sobre políticas públicas para garantizar la seguridad, libertad y privacidad en línea. (Rainie & Anderson, 2014)

Otros enfoques dentro de las predicciones del futuro de la privacidad en línea creen que para el año 2025 existirá un consenso internacional entre

organizaciones de internet sobre las maneras de equilibrar la privacidad y la seguridad personal con los contenidos y servicios populares. Se creería que para este año el enfoque de las protecciones nacionales de la privacidad se armonizará globalmente y la primacía de las preocupaciones de seguridad será más equilibrada por un consenso internacional.

Varios aspectos sobre el futuro del internet dependen mucho de las acciones que se ejecuten hoy en día. Mark Zuckerberg dijo que “la privacidad es un bien del pasado y que, tecnológicamente hablando, el mundo actual es un lugar en el que no tiene cabida. Creo que son visiones profundamente erradas, pues la privacidad es un asunto fundamental para la libertad de las personas, y también estoy convencido de que se pueden construir herramientas tecnológicas con un mejor tratamiento para la privacidad de los usuarios” (Rotta, 2915). Si hoy en día se continua con la lucha por alcanzar la privacidad para los usuarios el futuro de esta será más prometedor que los estudios y predicciones realizadas.

Desde hace unos años, las revelaciones de WikiLeaks y de Edward Snowden que evidenciaron con hechos y documentos oficiales que el Internet puede ser usado con la intención de espiar a ciudadanos locales y extranjeros, para perseguir disidentes y esconder secretos de Estados, han generado iniciativas para la concientización de usuarios a través de la red. Por otro lado, las empresas implicadas en las revelaciones emitieron comunicados explicando sus puntos y han tomado medidas y reformas en sus políticas de privacidad. Gracias a esto temas como la criptografía, la encriptación punto a punto y anonimato han emergido y generado preocupación en algunas empresas como por ejemplo Telegram, quien ha incorporado el cifrado de conversaciones y ha recibido múltiples usuarios tras la compra de WhatsApp por parte de Facebook que han preferido evitar el uso de ciertas aplicaciones dado el material presentado por Snowden.

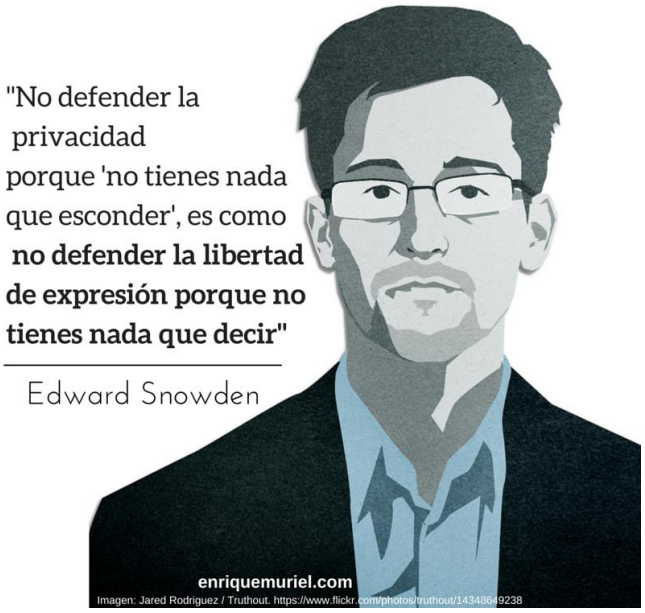
La construcción de reglamentación en favor de la privacidad debe empezar por los usuarios, quienes deben exigir regulaciones a sus gobiernos y empresas nacionales e internacionales que se encuentran colaborando con el espionaje, así como empezar con el uso de herramientas que encripten información y se regule el contenido publicado en redes sociales.

“Las Naciones Unidas están trabajando en una resolución para que la Asamblea General haga un llamamiento a los Estados para que se respete y proteja el derecho global a la privacidad.” Países como Brasil y Alemania han arremetido sus fuerzas en presentar un proyecto ante la ONU con la finalidad de restringir el espionaje y considerar la privacidad como un derecho de las personas, tanto en el “mundo real” como en Internet.

Al hablar sobre privacidad en Internet se encuentran puntos de vista diversos, uno de los más frecuentes es en los que los usuarios dicen: “No tengo nada que esconder”, “No van a revisar mis conversaciones, soy una persona común y corriente no significa nada la información que comparto” “¿qué más me da que el Gobierno lea mis mensajes? Total, es por mi seguridad ¿no?”. Es decir, una resignación por parte de los usuarios ante la vigilancia, justifican el espionaje.

Al menospreciar la privacidad cayendo en la falacia de “no tener nada que esconder”, se está quitando el derecho a mantener un espacio integral para el autoconocimiento, para el desarrollo de la personalidad, ideales y decisiones; sino se mantiene un espacio afín para cada uno, el comportamiento sería diferente y bajo vigilancia constate afectaría el bienestar común. “No se trata de si somos inocentes o culpables de algo. Se trata de que la privacidad importa porque es un derecho de ciudadanos que vivimos en democracia” (TEDIC, 2016) y es un pre-requisito para poder gozar de otras libertades tal como la libertad de expresión u opinión.

“No se trata de defender paranoicamente la privacidad como una esfera de privilegio individual, sino de destacar que sin ella no hay posibilidad de ejercer otros derechos humanos ni de vivir en democracia.” (Fundación Via Libre Argentina, 2015)



Fuente: (Rodriguez, 2015)

Elaborado por: Jared Rodríguez

Fig. 23 Opinión de Edward Snowden acerca de la defensa de la privacidad

3.1.12. El Internet Profundo

> “En la Deep Web no hay sólo delitos, también existe la mayor red de seguridad y privacidad que navega sobre internet y permite que activistas, periodistas, empresas y hasta fuerzas de seguridad compartan trabajen de forma segura”
>
> (Gonzalo, 2015)

La internet se caracteriza por un sin número de páginas en las cuales el usuario, realiza búsquedas de información; el principal motor para llevar a cabo la ejecución de búsqueda de cualquier índole es Google en la actualidad, pero en realidad dicho motor tiene parametrizaciones de seguridad en la información que es reflejada hacia el usuario. Por lo tanto, existe mucha más información de la creemos. El Internet profundo es un medio, el cual el usuario común lo desconoce, ya que los navegadores con sus motores de búsqueda, establecen restricciones para el reporte de la información que se llevará en ejecución como resultado de la misma.

Pero cuál es la razón, para que el internet sea limitado hacia el usuario. Nacen diferentes paradigmas como la seguridad y la veracidad de la información a ser mostrada, por lo tanto según el esquema actual que maneja el internet, no serían libres de navegar en la misma, tienen restricciones de navegabilidad, pero la gran pregunta es ¿por qué?, pues la verdad, actualmente el internet no solo se caracteriza como el medio de búsqueda de información, llegó a ser una herramienta o un puente entre la realidad de la ética y el engaño, ya que al navegar en este espacio del internet en los últimos años se han presentado denuncias de robo y estafa de información a los usuarios de la misma, en dicho lugar ya no solo se encuentra información sobre documentos a los que se desea ingresar para realizar alguna actividad o aclarar alguna duda, pues hoy en día, se encuentra información sobre venta de armas ilegales, drogas, pornografía

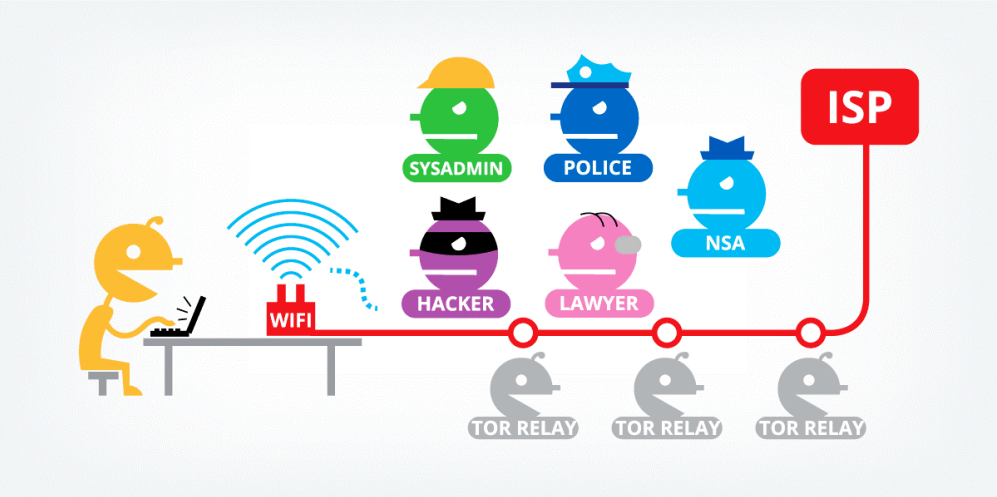
infantil, imágenes e información que pueden no ser aptas para varias personas. Este medio perdió la lógica de su creación, se contaminó y se volvió inseguro en la consulta de sus datos.

Queda una gran duda sobre si es bueno o malo que los motores de búsqueda pongan restricciones para el resultado de la información y en realidad si es que lo hacen por seguridad o por convenios con otras entidades para no hallar documentos o información que cambien la ideología, política, social, y religiosa de las personas.

Aunque la creencia de que el internet profundo es un lugar de actividades ilícitas, existe varios usuarios y colectivos que prefieren el uso de este espacio ya que están en contra del rastreo de información que sucede en la web superficial. Además de preferir herramientas que encriptan completamente los mensajes. (Camacho, 2016)

2.2.1.5. Navegador Tor

Tor, está constituida por una red de túneles virtuales dentro del internet que permite a las personas y organizaciones salvaguardar su seguridad y privacidad, además permite a los desarrolladores de software crear herramientas para la comunicación que cuenten con opciones de privacidad. Luego de las revelaciones realizadas por Snowden, la vulnerabilidad de los canales comunes de internet, abrieron paso a que herramientas como Tor tengan su espacio, alcanzando once millones de usuarios de internet y 750 000 que lo ocupan a diario como una medida contra la NSA.



Fuente: (Alarcon, 2013)

Elaborado por: Steph Alarcon

Fig. 24 Modo de Trabajo de TOR

Tor es una herramienta construida con software libre y oculta tanto el origen como el destino del tráfico de datos circulantes en la red haciendo un cifrado de datos que circulan en múltiples capas como si fuera una cebolla. Por lo que la identidad de la persona y los registros de navegación no son fáciles de

determinar, también oculta el destino de los datos, lo cual permite sobrepasar ciertas formas de censura que están expuestas en ciertos países del mundo.

Aunque Tor es una herramienta que permite navegar a través del internet profundo y la internet oscura no significa que todos la usan de forma ilícita; por ejemplo dentro de esta se encuentran periodistas que protegen la seguridad de sus fuentes, aquellas empresas que mantienen sus documentos a salvo de escuchas y creen en el análisis de la competencias, grupos de apoyo para personas con enfermedades o víctimas de abuso que utilizan foros para motivarse entre ellos y también se encuentran activistas por los derechos civiles. El uso de Tor para ellos ha significado que sus datos mantienen la confidencialidad al igual que sus comunicaciones y evita el análisis de la información y la vigilancia de la red. (Gonzalo, 2015)

2.2.1.6. Creación de transparencia

En la sociedad actual, las herramientas que se crean tienen dos funcionalidades, buenas y malas. Las buenas, son aquellas a las que se da un correcto uso y manejo de la misma; en el caso de este navegador, su uso ético como una herramienta que protege a quien lucha por los derechos civiles en regímenes totalitarios, ya sean periodistas, informadores o disidentes políticos e incluso en la búsqueda de información requerida para un manejo correcto de la misma, pero el funcionamiento erróneo que se puede lograr al estar en la oscuridad y no ser visto ni hallado por otros medios, implica acciones como la distribución de contenidos ilegales, el comercio ilegal, el espionaje y la comunicación entre grupos criminales. Estos dos factores permiten llegar a un paradigma de si debería existir o no, por un lado ayuda enormemente a los usuarios en acciones legales y en el otro ayuda a cometer crímenes, es algo

que debería entrar en consulta, pero es muy difícil aceptar la realidad, por la sociedad actual, ya que si se busca restringir información, este navegador ya no brindaría las acciones para las que fue creado, pero si sigue funcionando, el espacio y las personas que lo utilizan de una manera muy errónea podrán hacer más daño a la sociedad que en realidad no se encuentra en su lado.

3.1.13. Normas Internacionales

En la actualidad el control de la privacidad y la protección de datos personales se encuentran regido por diferentes legislaciones de carácter internacional. Estas leyes tienen como finalidad garantizar la protección de datos personales, libertades públicas y derechos fundamentales de las personas físicas, salvaguardando así su intimidad personal y familiar. (Sánchez Pérez & Rojas González, 2016)

En 1948 la Asamblea General de las Naciones Unidas proclama la Declaración Universal de los Derechos Humanos, documento en el que representantes de todas las regiones del mundo establecen como finalidad común los derechos humanos fundamentales que deben protegerse en el mundo entero.

En el artículo 12 este documento señala lo siguiente:

> ***"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia; ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."*** (Nila, 2013)

La información receptada a la población puede clasificarse dentro de dos grandes grupos: datos personales o datos biométricos.

Un dato personal se define como la información asociada a una persona o individuo, la cual permite que sea identificado del resto de personas o en un

grupo determinado de individuos. Entre estos datos se incluyen: nombre, domicilio, teléfono, fotografía, huellas dactilares, sexo, nacionalidad, edad, lugar de nacimiento, raza, filiación, preferencias políticas, fecha de nacimiento, imagen del iris del ojo, patrón de la voz, etc. (Sánchez Pérez & Rojas González, 2016)

Entre estos es posible encontrar también, datos personales sensibles. Estos se refieren a aquellos datos que se relacionan íntimamente con su titular y cuya divulgación significa un riesgo para el mismo. Entre ellos están características específicas de los individuos tales como origen étnico o racial, estado de salud, creencias religiosas, opiniones políticas, preferencia sexual, pertenencia a sindicatos, creencias filosóficas y morales, entre otras.

Por otro lado, los datos biométricos son aquellos que cumplen tanto los rasgos físicos como los rasgos biológicos o patrones de comportamiento de una persona. Estos rasgos lo hacen único dentro del resto de la población. Entre los principales datos biométricos se encuentran huellas dactilares, geometría de la mano, análisis del iris, análisis de retina, venas del dorso de la mano, rasgos faciales, patrón de voz, firma manuscrita, dinámica de tecleo, cadencia del paso al caminar, análisis gestual, análisis del ADN, entre otros. (Martinez, 2016)

Actualmente, una gran cantidad de datos personales y biométricos son almacenados en sistemas computacionales, por lo que son susceptibles a sufrir ataques informáticos. Por esta razón a nivel mundial varios países han unido esfuerzos para crear legislaciones internacionales que regulen el manejo de datos y contenidos.

2.2.1.7. Protección de datos en Europa

Europa es el continente en el que la protección de datos ha alcanzado un nivel elevado. Este tema formó parte fundamental de la agenda normativa de la Unión Europea desde comienzos de los años setenta. Así en el año 1970 se aprobó la primera legislación en este tema denominada la Datenschutz, ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania. Con la creación de esta ley se buscaba brindar protección a personas naturales con respecto a los datos informatizados que se encontraban en poder de las entidades públicas del Estado.

Posteriormente, en 1977, el Parlamento Federal Alemán aprueba la Ley Federal de Protección de Datos Bundesdatenschutzgesetz. Estas leyes impiden la transmisión de cualquier dato personal sin que exista la autorización de la persona interesada y la misma era aplicable tanto para el sector público como para el privado.

Por otro lado, en el año 1973 en Suecia se publica una de las primeras leyes de protección de datos en el mundo. Esta ley impone un sistema de control previa autorización para realizar un registro abierto de bancos de datos personales de personas físicas. Para velar el respeto de esta ley, se asocia la misma a la Datainspektionen, una autoridad de control con facultades para requerir la aplicación judicial de sanciones en caso del irrespeto de la norma.

En Francia de igual manera se adopta en el año de 1978 la Loi nº 78-17 du janvier, relative à l'informatique, aux fichiers et aux libertés, que reglamenta la automatización de datos personales de personas físicas realizado por personas naturales o jurídicas tanto del sector público como del sector privado.

Debido a la creación de numerosas leyes sobre protección de datos, el Parlamento Europeo analiza la necesidad de promulgar la creación de una normativa comunitaria en esta materia. Al emerger tal variedad de legislaciones sobre protección de datos, la necesidad de disponer de una normativa comunitaria en la materia. Por esta razón en el año de 1974 elabora un estudio para elaborar una directiva que rija la protección de datos dando como lugar el Convenio 108, adoptado por la Comunidad Económica Europea en 1981.

Este convenio se establece como el primer instrumento internacional creado para regular el manejo de datos de personas naturales.

El convenio garantiza el respeto de los derechos y libertades fundamentales de sus ciudadanos en cada estado, entre los que se incluye el tratamiento correcto de los datos de carácter personal de cada uno de ellos. El ámbito de aplicación de este convenio incluía todo el proceso de manejo de estos datos, desde su almacenamiento hasta su borrado e incluía la verificación de la utilización de métodos automatizados para esta tarea tanto en el sector público como en el privado.

Para realizar esta tarea, el convenio recogía los siguientes principios básicos para la protección de datos:

- Principio de lealtad
- Principio de exactitud
- Principio finalista
- Principio de pertinencia

- Principio de utilización no abusiva
- Principio del derecho al olvido
- Principio de publicidad
- Principio de acceso individual
- Principio de seguridad
- Principio de prohibición de tratamiento automático de datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas o de otro tipo, o datos relativos a la salud o vida sexual, a menos que el derecho interno prevea garantías adecuadas. (AGPD, 2013)

Incluye además normativas de control de flujo internacional de datos de carácter personal para normar a los participantes de esta transferencia. También contempla el flujo internacional de información existente y por tanto establece una cláusula de auxilio mutuo entre los Estados firmantes para controlarlo. Finalmente se estipula que todo país que acepte este convenio debe establecer medidas internas que den efecto a los principios del convenio con respecto a la protección de datos.

Producto de la creación del convenio se crean en Europa otras legislaciones tales como la Data Protection Act de 1984 adoptada por Reino Unido, la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD), adoptada por España en 1992, o la Ley de Datos de la República Federal Alemana de 1990.

En la actualidad, Europa busca dar respuesta a los retos propuestos por la tecnología debido al incremento de herramientas sistematizadas para recolección e intercambio de datos, que se enlazan en línea y que constituyen

un factor indispensable para el desarrollo económico del mundo globalizado de hoy.

Por esa razón en el 2012 se aprueba el Reglamento General de Protección de Datos, que constituye un marco jurídico sólido en este ámbito para la Unión Europea pues establece una política de protección de datos común para los países miembros. (AGPD, 2013)

2.2.1.8. Protección de datos en Estados Unidos

En el año de 1798 Estados Unidos reconoce el derecho de sus habitantes a la inviolabilidad del domicilio en la cuarta enmienda de su Constitución sin embargo el concepto de privacidad como tal se establece en el siglo XIX a partir del cuestionamiento de la sociedad sobre la necesidad de regular la vida privada.

A finales de este siglo se produce la publicación de un artículo en la revista de la Universidad de Harvard con el título The Right to Privacy, realizado por los juristas Samuel Warren y Lous Brandeis, introduciendo por primera vez a la privacidad como acción civil y promoviendo la creación de un nuevo derecho de amparo de la información personal a público no autorizado. (Martinez, 2016)

A partir de este punto la protección de la privacidad en Estados Unidos se considera dentro de cuatro ámbitos fundamentales: la esfera privada, la apropiación del nombre, la distorsión de la imagen y la difusión pública de hechos privados. Estos conceptos se consolidan dentro de nuevas normas a partir del año de 1974 de la siguiente manera:

Privacy Act	Ley de protección de la Intimidad de 1974. Objetivo: la protección de la intimidad de personas cuyos datos se encuentren en bancos de datos del gobierno.
Freedom of Information Act	Ley de Libertad de la Información, FOIA. Objetivo: Protección a bases de datos del Gobierno Federal con limitaciones como son archivos de servicios de inteligencia, inmigración y lucha contra el narcotráfico.
Fair Credit Reporting Act	Ley de Equidad Financiera de 1978. Objetivo: regulación de tratamiento de datos por parte de entidades financieras. Exige garantías de confidencialidad a estas entidades.

Fuente: (Martinez, 2016)

Elaborado por: Antonela Suárez

Fig. 25 nuevas normas de protección de la privacidad en Estados Unidos, 1994

Adicionalmente a estas leyes generales existen legislaciones específicas para cada estado. Estas normas se orientan a la protección de la información previo a la recolección de datos, sobre todo cuando sean datos considerados sensibles (salud, información financiera, información de menores de edad) y su uso para finalidades lícitas. Con respecto a las obligaciones establecidas, las leyes estatales y federales exigen garantías a la confidencialidad de la información, así como comunicar la existencia de brechas de seguridad que puedan darse en materia de protección de datos. (Martinez, 2016)

2.2.1.9. Protección de datos en EE.UU. y Unión Europea

A pesar de que existen puntos de convergencia entre las normativas de Estados Unidos y la Unión Europa, los principios evolucionaron de manera diferente Mientras que en Estados Unidos su legislación se dirige a la autorregulación, en la Unión Europa se considera fundamental el poseer una normativa vinculante entre sus estados miembros.

Entre las principales diferencias y convergencias que existen se encuentran:

CRITERIO	UNIÓN EUROPEA	ESTADOS UNIDOS
DIFERENCIAS	Concepción del derecho a la vida privada de carácter amplio reconociendo a todos los individuos amparados bajo la norma según artículo 7 de la carta de la Unión Europea.	Concepción del derecho a la vida privada de carácter limitado según cuarta enmienda de su Constitución
	La normativa abarca toda la información de datos personales e identifica o hace identificable a una persona.	La normativa se centra más en los datos específicos que identifican y no en aquellos que hacen posible la identificación de la persona.
	Sus normas no se centran en resarcir daños por cuanto las organizaciones y empresas de la Unión Europea están sometidas a muchas más restricciones.	Sus normas se centran en reparar el daño causado al consumidor y en alcanzar el equilibrio entre privacidad y las necesidades de información de las transacciones comerciales.
CONVERGENCIAS	La Unión Europea y Estados Unidos son líderes mundiales en temas de protección de libertades individuales de sus ciudadanos en temas de privacidad. Ambos fomentan la innovación y el comercio en un marco de cooperación transatlántica sólida en el ámbito de protección de datos, a fin de mejorar la confianza del consumidor y promover el crecimiento de la economía mundial y del mercado común. Promueven el desarrollo del concepto de puerto seguro a fin de facilitar la exportación de datos entre ambas partes.	

Fuente: (Martinez, 2016)

Elaborado por: Antonela Suárez

Tabla 1. Diferencias y convergencias entre protección de datos EE UU. Y Unión Europea

Por encima de estos particulares, ambas partes son conscientes de la importancia de suavizar las barreras orientando iniciativas con el objeto de restablecer la confianza entre las partes y trabajar en favor de la correcta gestión de información entre ellos.

2.2.1.10. Acuerdo Privacy Shield

El Privacy Shield es el nuevo Acuerdo alcanzado por la Unión Europea y Estados Unidos el 12 de julio de 2016 para transferencia de datos entre los mismos. El acuerdo indica que no será necesario contar con autorización previa para la transferencia de datos entre la Unión Europea y Estados Unidos, siempre y cuando la empresa receptora de la información se encuentre adherida al acuerdo y haya realizado la firma del contrato para el caso. (IABSPAIN, 2016, págs. 1-2)

Este nuevo instrumento de protección de datos aplica solamente para aquellas empresas estadounidenses que se adhieran a él. Esta adhesión implica aceptar sus condiciones y colaborar con las autoridades de control según lo dispuesto en sus cláusulas, además de cumplir con los principios de tratamiento de datos de la Unión Europea en él estipulados.

2.2.1.11. Reglamento General de Protección de Datos

El Parlamento Europeo y el Consejo han aprobado el Reglamento General de Protección de Datos (RGPD), que entró en vigor el 25 de mayo de 2016 y su cumplimiento es obligatorio transcurridos dos años desde esta fecha. Este consiste en un nuevo conjunto de normas establecidas por la Comisión Europea para normar la privacidad y seguridad de datos personales. (ESET, 2017)
Se trata de un nuevo conjunto de normas establecidas por la Comisión Europea que rigen la privacidad y la seguridad de los datos personales, devolviéndoles a los ciudadanos de los países miembros el control sobre los mismos.

De acuerdo con esta nueva legislación las personas naturales tienen derecho a solicitar a las empresas la eliminación total de su información cuando ya no sea necesario que la posean. Además, la ley incluye disposiciones que permiten que las personas transfieran sus datos de un servicio a otro más fácilmente, lo que facilitará a los consumidores el cambio de proveedor de servicios cuando así lo requieran,

El acuerdo contempla como sanciones, multas a aquellas compañías que no cumplan con la normativa, las mismas que alcanzarán hasta el 4% de su facturación global. También posee implicaciones para las empresas de países externos a la Unión Europea pues independientemente de que se encuentre establecido en el extranjero, si posee datos de ciudadanos europeos, es responsable y se rige bajo esta ley. (ESET, 2017)

Nuevas obligaciones para empresas

- Será obligatorio asignar a un Delegado de Protección de Datos (DPO), interno o externo, que asista a las organizaciones en el proceso de cumplimiento normativo.

- Se deberán realizar Evaluaciones de impacto sobre la privacidad, con el fin de determinar los riesgos específicos que implica tratar ciertos datos de carácter personal y adoptar medidas para evitar o eliminar estos riesgos.

- Se creará una Ventanilla Única, es decir una sola autoridad de control nacional que actúe como interlocutora de las empresas multinacionales.

- Las brechas de seguridad deberán ser comunicadas a las autoridades de control y, en casos graves, a los afectados, tan pronto sean conocidas en un plazo máximo de 72 horas.

- Se amplían los datos sensibles especialmente protegidos, incluyendo ahora los datos genéticos y biométricos. Se incluyen en esta categoría las infracciones y condenas penales, aunque no las administrativas.

- El proceso de selección de un encargado del tratamiento de datos será más estricto pues se elegirá una persona que aporte suficientes garantías de cumplimiento normativo.

- Establecimiento de garantías más estrictas y mecanismos de seguimiento en relación con las transferencias internacionales de datos fuera de la Unión Europea.

- Se crearán sellos y certificaciones de cumplimiento que permitan realizar la acreditación por parte de las organizaciones.

- Desaparecerá la obligatoriedad de inscribir ficheros y en su lugar se colocarán controles internos, así como un inventario de las operaciones de tratamiento de datos que se realicen.

(RGPD, s.f.)

Nuevos derechos para los ciudadanos

- Transparencia e información: Las empresas responsables de tratar los datos personales deben proporcionar mayor información al ciudadano de modo completo y sencillo a fin de facilitar la toma de decisiones.

- Consentimiento: El consentimiento para poder tratar datos de carácter personal ha de ser inequívoco, libre y revocable y deberá darse mediante un acto afirmativo claro. No se admite consentimiento tácito.

- Derecho al olvido: Se podrá revocar el consentimiento prestado para el tratamiento de datos personales en cualquier momento, pudiendo exigir la supresión y eliminación de los datos en redes sociales o buscadores de internet.

- Derecho a la limitación del tratamiento: El ciudadano puede solicitar el bloqueo temporal del tratamiento de sus datos cuando existan controversias sobre su licitud.

- Portabilidad de los datos: El ciudadano podrá solicitar la transferencia de los datos personales de un proveedor de servicios en Internet a otro.

- Denuncias: Se podrán presentar denuncias a través de asociaciones de usuarios.

- Indemnizaciones: Se reconoce la posibilidad de exigir indemnización de daños y perjuicios derivados del tratamiento ilícito de los datos personales.

(RGPD, s.f.)

2.3. Situación de la Privacidad en el País

3.1.14. Situación en Ecuador

Ecuador ha pasado por una revolución en el manejo de la información desde la incorporación de nuevas tecnologías como el internet, combinado con el paso de los procesos cotidianos al mundo globalizado de la Red. La incorporación de estas herramientas ha traído múltiples ventajas para desarrollar proyectos en búsqueda de adecuar y mantener un gobierno en línea, iniciativas que han sido posibles de realizar gracias a la masificación del acceso a los datos, así como la virtualización de las relaciones de los ciudadanos, consumidores, autoridades, proveedores y usuarios que han marcado una tendencia en constante crecimiento surgidas a partir de las infraestructuras que ofrece el internet. Las implementaciones de estas iniciativas han generado un enfoque a la transparencia de la gestión pública que ha permitido proveer el acceso a información pública de los ciudadanos y a la realización electrónica de trámites de diferentes instituciones del estado. (Estrada, Estrada, Rodríguez, & Tipantuña, 2015)

Sin embargo, las presencias de grandes cantidades de datos accesibles por internet representan riesgos para la seguridad de la información dado que no todos los datos presentados son necesariamente privados, sino que incluye datos personales que si se combinan entre diferentes instituciones del estado contribuirían a inferir información sobre la identidad de un individuo determinado y vulnerarían la privacidad del mismo, a pesar de que estas medidas sean un paso para la creación de transparencia en el gobierno.

La penetración del internet en los últimos años ha crecido de forma exponencial hasta llegar al 83%, gracias a la reducción de los costos de acceso a Internet y a la publicidad sobre el uso de canales electrónicos para la interacción con la empresa pública y privada. A comparación de otros países, la expansión de los servicios de internet ha sido tardía.

Ecuador se encuentra entre los países con mayor incremento de la conectividad en la región en los últimos años. Este cuenta con más de 60,000 km de fibra óptica en la mayoría de cantones del país.

Fuente: (WeAreSocial, DIGITAL IN 2016, 2016)

Elaborado por: WeAreSocial

Fig. 26 Uso del Internet en Ecuador en el 2016

Temas sobre la privacidad en el internet no ha sido puesto en discusión con profundidad en el país y a comparación de otros países de la región como Brasil, Argentina, Colombia y Paraguay que han expedido normativas para la protección de datos ante las revelaciones realizadas sobre el espionaje Ecuador ha dejado de lado este tema y ha hecho muy poco por realizar una legislación que proteja a los ciudadanos y sus datos personales.

Históricamente, en las primeras constituciones políticas existía una pequeña referencia al derecho a la intimidad y el secreto de la correspondencia (1998). Luego en el 2002, con la emisión de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el artículo 9 se encuentre dedicado a la protección de datos concentrada solamente en determinar que los datos personales “podrán ser usados o transferidos únicamente con autorización del titular o la orden de autoridad competente”. (Estrada, Estrada, Rodríguez, & Tipantuña, 2015)

Para el 2008 con la aprobación de la Constitución vigente, se determina a acción jurisdiccional del *habeas data*, en el artículo 92. Con el cual establece que el derecho de permitir a una persona o institución a: conocer, autorizar y rectificar la información que sobre ella se almacene en bases de datos públicas o privadas. No obstante, el habeas data sólo permite reparar un daño ya realizado y no sitúa la existencia de una autoridad de protección de datos que pueda actuar de oficio. (Birnbaum, 2004). Finalmente, en el año 2010, se consignó la Ley del Sistema Nacional de Registro de Datos Públicos (LSNRDP), la cual regula la manera en la se registra y se accede a los datos públicos con la finalidad de asegurar la transparencia y organizar el acceso a la información de las diferentes instituciones públicas y privadas que almacenan información sobre un individuo. Si bien esta ley define los datos considerados de carácter confidenciales y disponen que el acceso a ellos podrá ser autorizado por el

titular o por el mandato de ley (Estrada, Estrada, Rodríguez, & Tipantuña, 2015). Esta legislación no promueve ningún tipo de mecanismos que asegure la protección de datos personales dentro del país. A nivel jurídico han sido repetidas las ocasiones en que se ha propuesto el desarrollo de una normativa para la privacidad y protección de datos (Ciespal, 2014), estos temas no has sido de relevancia y no se han desarrollado hasta el año pasado que se presentó un proyecto de ley para la protección de datos el cual no ha sido evaluado por la Asamblea.

En el actual Código Integral Penal (COIP) del Ecuador se establece en su artículo 229 como delito la divulgación de información de archivos obtenidos de un medio electrónico o de telecomunicaciones, materializando la violación del secreto, intimidad y privacidad de las personas.

3.1.15. Leyes a Nivel Interno

2.3.1.1. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Protección de Datos	Artículo 9 de la ley de comercio electrónico, firmar electrónicas y mensajes de datos.	
	Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de datos, es necesario el consentimiento expreso del titular; quien decidirá qué información se compartirá con terceros	La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizada por la constitución de la república. Los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de una autoridad competente

Fuente: (Jaramillo, 2014)

Elaborado por: Antonela Suárez

Fig. 27 Acerca de la protección de datos en la ley de comercio electrónico

2.3.1.1. Ley del Sistema Nacional de Registro de Datos Públicos

SINARDAP	Publicada el 31 de marzo de 2010 en el registro oficial
	Consolida, administrar y estandarizar los datos públicos de los ciudadanos
	Su creación tiene por finalidad la protección de los derechos constituidos en normas de registros con el objeto de coordinar el intercambio de información de los registros de datos públicos
	Entidades privadas que posean información de carácter público, serán incorporadas a este sistema.

Fuente: (Jaramillo, 2014)

Elaborado por: Antonela Suárez

Fig. 28 Qué es el SINARDAP

2.3.1.2. Proyecto de ley para Protección de datos

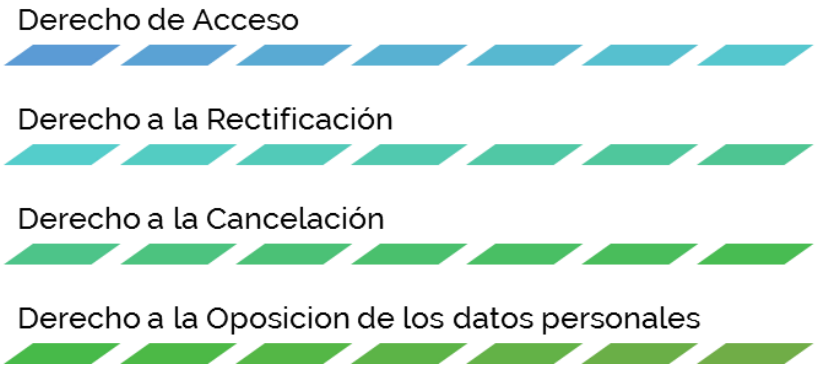
Las normas sobre protección de datos mantienen un rol de vital importancia puesto que plantean un gran desafío al encontrar el equilibrio y balance entre la protección de los derechos de intimidad y privacidad de las personas y el principio de libre circulación de información en internet.

Este proyecto de ley abarca dos objetivos fundamentales los cuales son:

- Conferir y reconocer las facultades que tiene los titulares sobre los datos de personales frente a terceros que gestionan la información personal, en virtud de la "tutela jurídica de la intimidad y privacidad del ser humano, que ha despertado gran interés en el ordenamiento jurídico moderno" (Cuadros, 2016)

- Regular la recopilación, modificación, eliminación o cualquier tipo de manejo sobre los datos personales almacenado en archivos, ficheros, bancos, registros etc.

Entre sus principios cabe destacar la implementación de los derechos ARCO, los cuales se encuentran ampliamente reconocidos adecuando "por el titular en cualquier escenario de presunta vulneración de la privacidad o intimidad." (Cuadros, 2016)



Fuente: (Cuadros, 2016)

Elaborado por: Antonela Suárez

Fig. 29 Derechos ARCO

Entre las definiciones legales del proyecto se encuentra la diferenciación entre datos personales y datos íntimos o datos sensibles, se incluye en su artículo 5 prohibición total del tratamiento y análisis de los datos sensibles y determina como excepciones, en el numeral 1 que se requiere autorización del titular y que se encuentre expresado por escrito. El manejo de datos sensibles está sujeto a exigencias de acuerdo al entorno digital actual. (Colamarco, 2016)

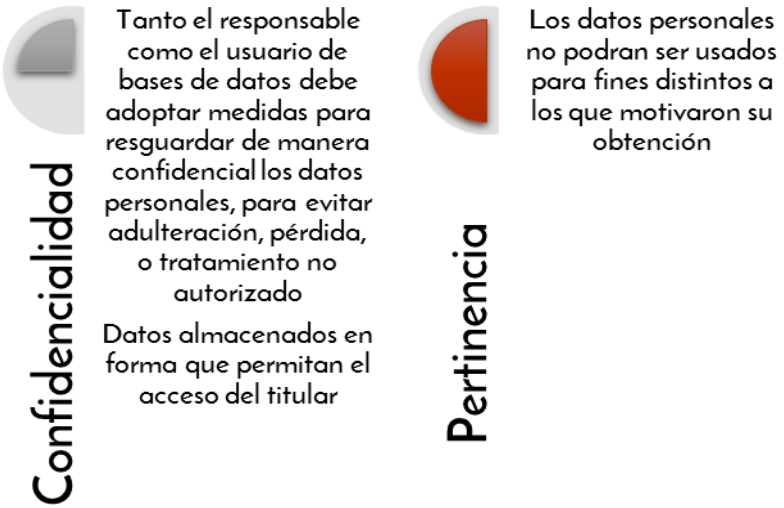
Acerca de los principios que están obligados a observar los involucrados en la formación y manejo de bases de datos están enfocados en tres puntos fundamentales según el tercer artículo del proyecto, los cuales se presentan a continuación:

Fuente: (ASAMBLEA NACIONAL, 2016, pág. 6)

Elaborado por: Antonela Suárez

Fig. 30 Puntos fundamentales en el manejo de bases de datos

Manteniendo los principios de:



Fuente: (ASAMBLEA NACIONAL, 2016, pág. 6)

Elaborado por: Antonela Suárez

Fig. 31 Principios en el manejo de bases de datos

Es importante destacar lo expuesto en el artículo 7 respecto a los niños, niñas y adolescentes cuya información personal no puede ser tratada; esta acción queda completamente prohibida a menos de que se trate de datos que sean datos de naturaleza pública (ASAMBLEA NACIONAL, 2016).

Al hablar sobre los encargados del tratamiento de la información se detalla dos categorías enmarcadas en el artículo 4:

- **“Responsable del Tratamiento de la Información**: persona natural o jurídica, pública o privada que administra el sistema de tratamiento de datos, por cuenta del responsable del archivo.
- **Responsable del Archivo:** persona natural o jurídica, pública o privada, titular del archivo, custodio u operador de la información.”

(ASAMBLEA NACIONAL, 2016)

Autoridad Nacional de Protección de Datos Personales

El artículo 11 del proyecto de ley establece que la Dirección Nacional de Registro de Datos Públicos, adscrita al Ministerio de Telecomunicaciones y de la Sociedad de la Información, será la Autoridad Nacional de Protección de Datos Personales.

Resumen

Hoy por hoy el mundo está frente a una de las guerras más importantes dentro de Internet: la guerra de los datos. La lucha por la búsqueda de la privacidad de los datos y la concientización del manejo inadecuado de estos por partes de gobiernos poderosos y grandes compañías; cuyos percusores han sido Julian Assange fundador de WikiLeaks y Edward Snowden considerado como traidor a la patria por presentar el espionaje que realizaba estados unidos a sus ciudadanos y a ciudadanos de todo el mundo. Gracias a sus revelaciones ha comenzado una motivación por la protección los datos y el qué hacer frente a las amenazas futuras.

Julian Assange mantiene una filosofía basada en el ciberpunk término que define a una persona que usa encriptación cuando accede a redes computacionales con finalidad de asegurar su privacidad, especialmente de gobiernos autoritarios. El objetivo de este movimiento es desmantelar el secreto como mecanismo de gobierno de los Estados-nación y corporaciones.

Assange persiste en denotar el valor de la información como vía al conocimiento, a la autonomía y libertad del individuo: “Puedes estar informado y ser tu propio gobernante, o bien puedes vivir en la ignorancia y dejar que otras personas, bien informadas, te gobiernen” (Quian, 2013)

Uno de los problemas de la información que viaja mediante la red, es que esta no se encuentra cifrada, es como si años atrás se enviara una carta por correo sin sellar el sobre, exponiendo a que en todos los lugares que recorre hasta su destinario pueda ser leída. Una situación similar ocurre con los datos que van pasando a través de la red, cualquier persona que use una herramienta especializada para captar paquetes puede obtenerlos, leerlos y usarlos según su conveniencia.

Es por eso que una de las armas para luchar en favor de la privacidad es la criptografía; la cual, es una forma de acción directa y que no produce violencia, ni daños ante nadie

como lo haría cualquier tipo de arma, pues al ser creado en base a operaciones matemáticas su presentación ante los demás va a llegar a ser un “simple” problema matemático a resolver.

La criptografía no es más que un conjunto de reglas y combinaciones matemáticas relativas a la seguridad de los datos solo quien tenga la llave con el que algoritmo fue desarrollado será quien podrá descifrar y obtener el contenido; su uso trae consigo diferentes beneficios.

Edward Snowden, informático estadounidense autodidacta cuyas revelaciones se han convertido en uno de los casos más controversiales en los últimos años y han servido para la concientización sobre el estado actual de la privacidad en el internet.

Snowden ha sido catalogado como traidor a su patria, pero es considerado como héroe para muchos, tras dejar todas las oportunidades y altas remuneraciones que ofrecía su trabajo para abrir los ojos al mundo y hablar sobre la privacidad. Desde entonces lucha por su libertad y trabaja por la defensa de la privacidad, es considerado como la imagen de la libertad en internet.

Si bien el uso del internet no se ha disminuido, los develamientos realizados tanto por Assange como por Snowden han evidenciado desde diferentes puntos de vista la militarización del internet y la gran ignorancia que mantienen los usuarios sobre como la tecnología ha enmarañado cada proceso de sus vidas.

Desde hace unos años, WikiLeaks y Edward Snowden evidenciaron con hechos y documentos oficiales que el Internet puede ser usado con la intención de espiar a ciudadanos locales y extranjeros, para perseguir disidentes y esconder secretos de Estados, generando iniciativas para la concientización de usuarios a través de la red.

En la actualidad el control de la privacidad y la protección de datos personales se encuentran regidos por diferentes legislaciones de carácter internacional. Estas leyes tienen como finalidad garantizar la protección de datos personales, libertades públicas

y derechos fundamentales de las personas físicas, salvaguardando así su intimidad personal y familiar.

Europa es el continente en el que la protección de datos ha alcanzado un nivel elevado en las prácticas de protección de datos. Este tema formó parte fundamental de la agenda normativa de la Unión Europea desde comienzos de los años setenta. En la actualidad, buscan dar respuesta a los retos propuestos por la tecnología debido al incremento de herramientas sistematizadas para recolección e intercambio de datos, que se enlazan en línea y que constituyen un factor indispensable para el desarrollo económico del mundo globalizado de hoy.

Ecuador ha pasado por una revolución en el manejo de la información desde la incorporación de nuevas tecnologías como el internet, combinado con el paso de los procesos cotidianos al mundo globalizado de la Red. La incorporación de estas herramientas ha traído múltiples ventajas para desarrollar proyectos en búsqueda de adecuar y mantener un gobierno en línea, iniciativas que han sido posibles de realizar gracias a la masificación del acceso a los datos, así como la virtualización de las relaciones de los ciudadanos, consumidores, autoridades, proveedores y usuarios que han marcado una tendencia en constante crecimiento surgidas a partir de las infraestructuras que ofrece el internet.

Para el 2008 con la aprobación de la Constitución vigente, se determina a acción jurisdiccional del habeas data, en el artículo 92. Con el cual establece que el derecho de permitir a una persona o institución a: conocer, autorizar y rectificar la información que sobre ella se almacene en bases de datos públicas o privadas. No obstante, el habeas data sólo permite reparar un daño ya realizado y no sitúa la existencia de una autoridad de protección de datos que pueda actuar de oficio. Finalmente, en el año 2010, se consignó la Ley del Sistema Nacional de Registro de Datos Públicos (LSNRDP), la cual regula la manera en la se registra y se accede a los datos públicos con la finalidad de asegurar la transparencia y organizar el acceso a la información de

las diferentes instituciones públicas y privadas que almacenan información sobre un individuo.

Las normas sobre protección de datos mantienen un rol de vital importancia puesto que plantean un gran desafío al encontrar el equilibrio y balance entre la protección de los derechos de intimidad y privacidad de las personas y el principio de libre circulación de información en internet.

CAPÍTULO 3

El presente capítulo tiene como objetivo conocer la noción de los estudiantes de la Pontificia Universidad Católica del Ecuador con respecto a la privacidad y la transparencia en Internet. Por lo cual se presentará un análisis de los resultados encontrados tras realizar encuestas y la evidencia de casos encontrados que atentan contra la privacidad y censura del internet en Ecuador.

Privacidad y Transparencia en el Ecuador

3.2. Privacidad

3.2.1. Conocimiento de las personas sobre privacidad en Internet

Al hablar sobre la situación de Ecuador frente a la privacidad es importante denotar que muchos usuarios de internet tienen un conocimiento efímero de lo que implica el manejo de datos y proveen sin precaución alguna sus datos personales (nombres completos, ubicación geográfica, números de tarde crédito, teléfonos, etc.) a cambio de obtener distintos servicios en línea sin pensar qué es lo que pasará a futuro con ellos.

Ecuador es considerado un país totalmente colectivista, lo que supone que sus habitantes tienen un mayor grado de confianza en otras personas comparado con los habitantes de otros países como Estados Unidos, España, México o Argentina cuya cultura es más individualista. (Goldfarb, y otros, 2015). Si bien estos estudios permiten conocer la actitud y los valores culturales que mantienen los grupos frente a la privacidad y la seguridad en Internet, es curioso notar que países con menor grado de confianza son aquellos que han establecido legislaciones para la protección de datos desde hace algunos años. Si bien este tema es de vital importancia tanto para autoridades como ciudadanos es importante conocer cuál es la noción

que mantienen los ecuatorianos hoy en día frente a lo que pasa en Internet, con su privacidad, por lo que se ha realizado un pequeño estudio preliminar para determinar la percepción de la privacidad, así como de la transparencia. Para ello se realizó 330 encuestas a estudiantes de diversas carreras de la Pontificia Universidad Católica del Ecuador considerando carreras afines al manejo de tecnología (Ingeniería en Sistemas), como para el desarrollo integral de la persona (Psicología y Sociología).

Aunque las conclusiones que a obtenerse de las preguntas no son de ninguna forma transmisibles a toda la población, se puede evidenciar que son un interesante punto de partida para conocer algo sobre los grupos con un mínimo conocimiento técnico sobre los cuales se aplicó la muestra. (Estrada, Estrada, Rodríguez, & Tipantuña, 2015).

3.2.2. Tabulación de encuesta y Presentación de resultados

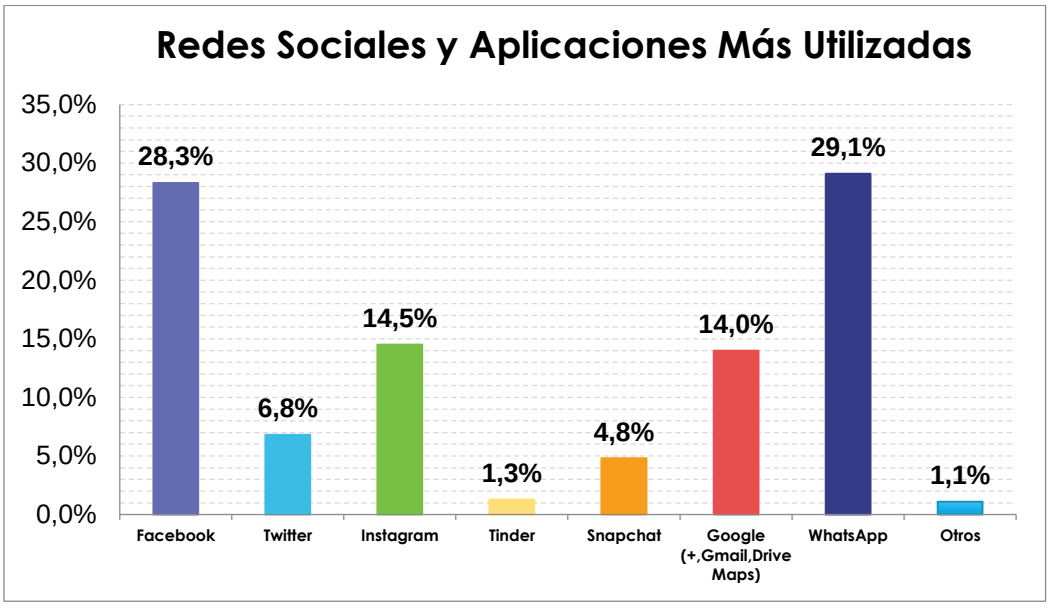
Pregunta N°1: ¿Cuáles son las redes sociales y aplicaciones que más utiliza?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Facebook	93	28,3%
●	Twitter	22	6,8%
●	Instagram	48	14,5%
●	Tinder	4	1,3%
●	Snapchat	16	4,8%
●	Google (+,Gmail,Drive Maps)	46	14,0%
●	WhatsApp	96	29,1%
●	Otros	4	1,1%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 2. Redes Sociales y Aplicaciones con mayor uso



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 32 Redes sociales y aplicaciones con mayor uso

De las 330 personas encuestadas como usuarios de estos servicios provistos mediante Internet, se encuentra que el 29.1% de ellos utilizan con mayor frecuencia WhatsApp para comunicarse, seguidos por la red social Facebook con el 28.3% e Instagram con el 14.5%. Sin embargo, las herramientas provistas por Google como Drive, Maps, Gmail entre otros obtienen un impacto del 14% entre los encuestados. Se puede observar que aplicaciones como Twitter (6.8%), SnapChat (4.8%), Tinder (1.3%) y Otras aplicaciones (1.1%) no son determinantes para la muestra aplicada.

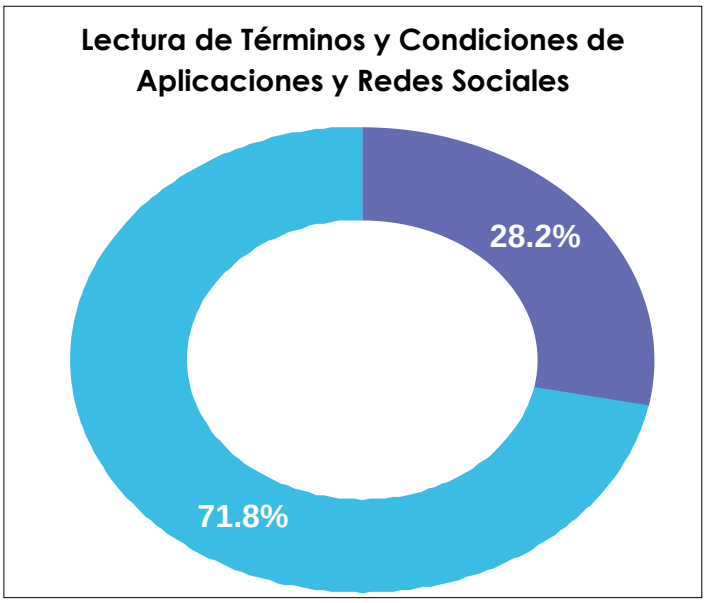
Pregunta N°2: ¿Ha leído los términos y condiciones expuestos antes de ingresar a una red social o al instalar una aplicación?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	93	28,2%
●	No	237	71,8%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 3. Lectura de Términos y Condiciones de Aplicaciones y Redes Sociales



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 33 Lectura de Términos y Condiciones de Aplicaciones y Redes Sociales

De acuerdo a los resultados, un elevado porcentaje representado en un 71.8% de los encuestados no han leído los términos y condiciones de las aplicaciones y redes sociales a las que acceden. Mientras tanto, se encontró que un 28.2% sí lo hace lo que quiere decir que estos usuarios conocen perfectamente que datos van a interferir al usarlas.

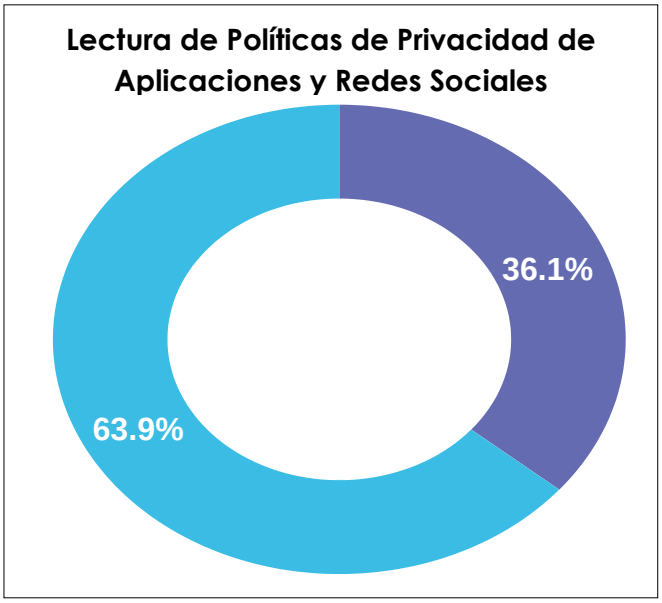
Pregunta N°3: ¿Ha leído las políticas de privacidad de estas redes sociales o aplicaciones?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	119	36,1%
●	No	211	63,9%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 4 Lectura de Políticas de Privacidad de Aplicaciones y Redes Sociales



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 34 Lectura de Políticas de Privacidad de Aplicaciones y Redes Sociales

La lectura de las políticas de privacidad es un tema de vital importancia dado que aquí se determina de qué manera serán manejados los datos personales que toman las aplicaciones y redes sociales; sin embargo, al evidenciar los resultados se observa que el 63.9% no realiza una lectura de estos y que solo el 36.1% da lugar a la lectura y se preocupa por saber acerca de la información que comparte.

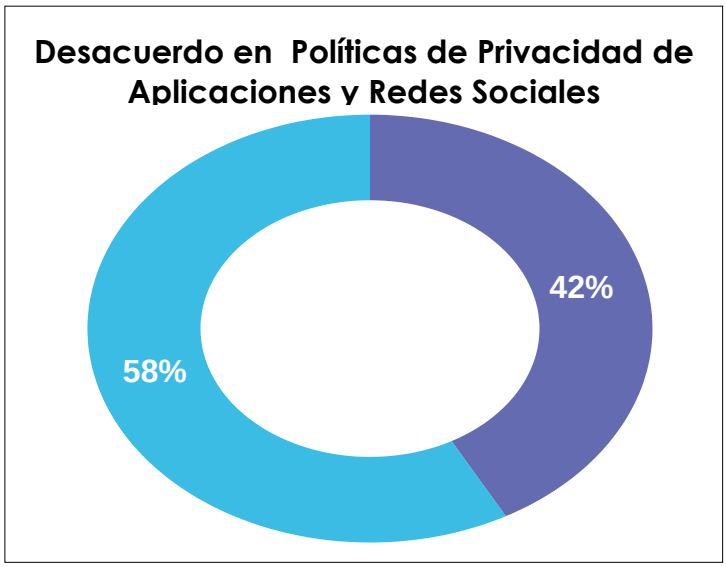
Pregunta N°4: Si su respuesta anterior fue "si". ¿Ha estado en desacuerdo con alguna de estas políticas?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	50	42%
●	No	69	58%
TOTAL		**119**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 5 Desacuerdo en Políticas de Privacidad de Aplicaciones y Redes Sociales



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 35 Desacuerdo en Políticas de Privacidad de Aplicaciones y Redes Sociales

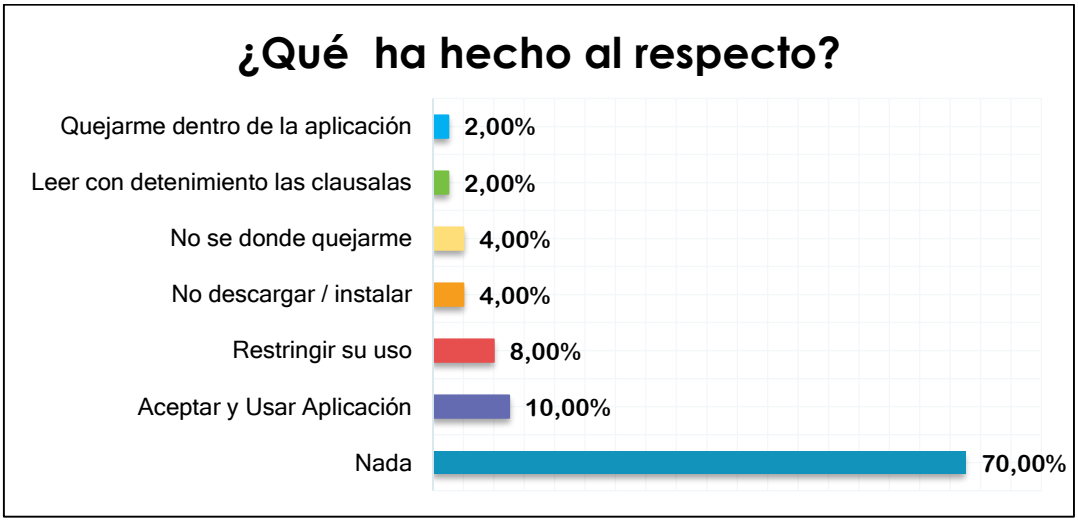
Según los resultados obtenidos el 42% de los encuestados han tenido desacuerdos con las políticas de privacidad, pero no han evidenciado la realización de alguna acción para expresar su inconformidad como se puede véase *Tabla 6* presentada a continuación. Mientras que el 58% no han encontrado fallos en estas políticas de privacidad.

OPCIÓN		FRECUENCIA	PORCENTAJE
	Nada	35	70.00%
	Aceptar y Usar Aplicación	5	10.00%
	Restringir su uso	4	8.00%
	No descargar / instalar	2	4.00%
	No sé dónde quejarme	2	4.00%
	Leer con detenimiento las cláusulas	1	2.00%
	Quejarme dentro de la aplicación	1	2.00%
TOTAL		**50**	**100.00%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 6 Acciones frente a desacuerdo con políticas de privacidad.



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 36: Acciones frente a desacuerdo con políticas de privacidad

Según las opiniones provistas por los participantes, es evidente que, aunque no estén de acuerdo con las políticas de privacidad de una red social o aplicación, optan por dejarlo pasar y no realizar nada.

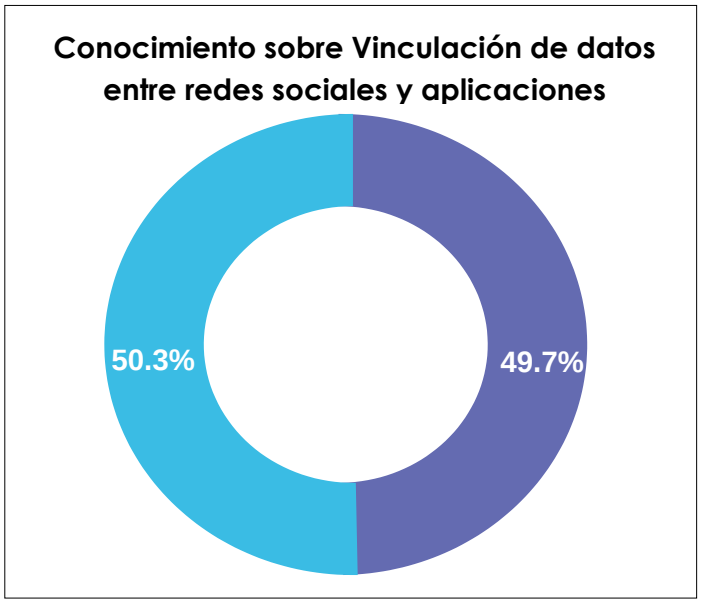
Pregunta N°5: ¿Tiene conocimiento sobre la vinculación de los datos entre aplicaciones y redes sociales que acceden a internet?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	164	49,7%
●	No	166	50,3%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 7 Conocimiento sobre Vinculación de datos entre redes sociales y aplicaciones



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 37 Conocimiento sobre Vinculación de datos entre redes sociales y aplicaciones.

El conocimiento de la vinculación de datos entre aplicaciones y redes sociales difere con su desconocimiento en un 0.6% según los resultados obtenidos en la encuesta. Esto implica que no todos los usuarios son concientes de que sus datos son compartidos entre grandes compañías tecnológicas.

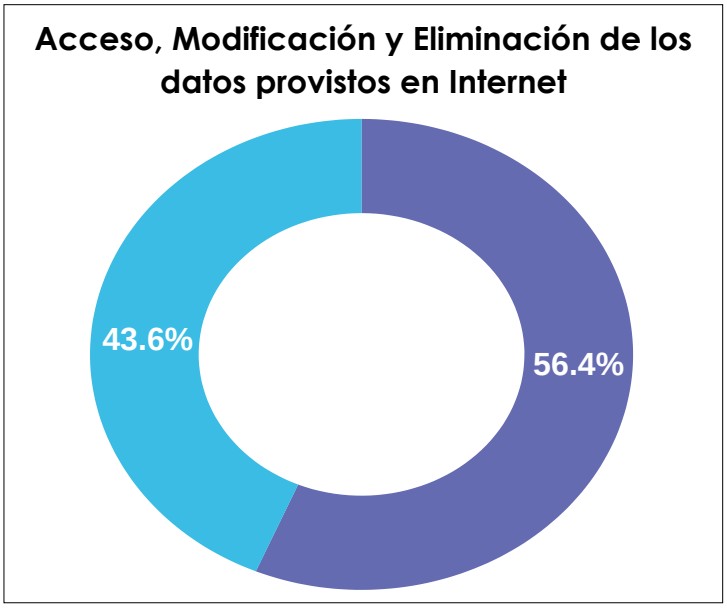
Pregunta N°6: Alguna vez, ¿Ha querido acceder a los datos almacenados en internet? ¿Ha querido modificarlos o eliminarlos?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	186	56,4%
●	No	144	43,6%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 8 Acceso, Modificación y Eliminación de los datos provistos en Internet



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 38 Acceso, Modificación y Eliminación de los datos provistos en Internet

Se observa que un 56,4% de los usuarios de aplicaciones mediante internet han querido acceder a los datos dejados mediante la red, mientras que el 43.6% de los mismos manifiestan que no han querido acceder, modificar o eliminar estos datos. Por lo tanto, los usuarios no conocen la problemática existente en el manejo de datos personales.

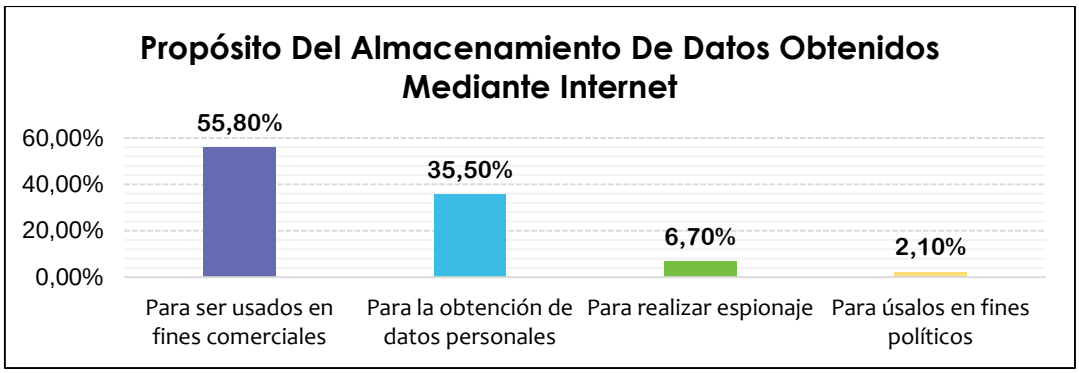
Pregunta N°7: ¿Cuál cree que es el propósito del almacenamiento de datos obtenidos mediante Internet?

OPCIÓN	FRECUENCIA	PORCENTAJE
Para ser usados en fines comerciales	184	55,8%
Para la obtención de datos personales	117	35,5%
Para realizar espionaje	22	6,7%
Para úsalos en fines políticos	7	2,1%
TOTAL	**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 9 Propósito Del Almacenamiento De Datos Obtenidos Mediante Internet



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 39 Propósito Del Almacenamiento De Datos Obtenidos Mediante Internet

Según lo observado, el 55.8% de los encuestados considera que el almacenamiento de datos se lo realiza para utilizarlos en fines comerciales realidad visualizada en redes sociales como Facebook, Instagram y en sitios como Amazon, YouTube, etc. Por otro lado, el 35.5 % considera que esta recopilación es exclusiva para obtención de datos personales. El 6.7% considera que los datos son recolectados para realizar espionaje directamente; lo que evidencia el bajo conocimiento acerca del espionaje masivo por parte de las agencias de seguridad nacional. Por último, el 2.1% cree que los datos son usados para fines políticos.

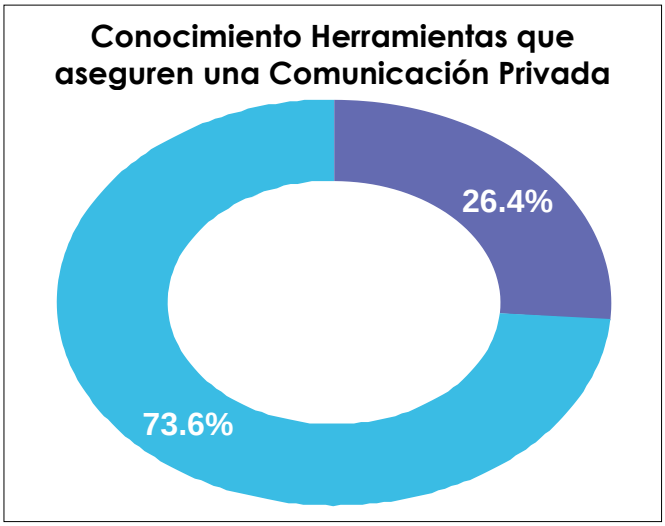
Pregunta N°8: ¿Conoce de herramientas que aseguren una comunicación privada?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	87	26,4%
●	No	243	73,6%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 10 Conocimiento de herramientas que aseguren una comunicación privada



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 40 Conocimiento de herramientas que aseguren una comunicación privada

Al aplicar la encuesta, se obtiene que el 73.6% de los encuestados no tiene conocimiento sobre herramientas que aseguran una comunicación privada. El 26.4% manifestó que si conoce sobre ellas.

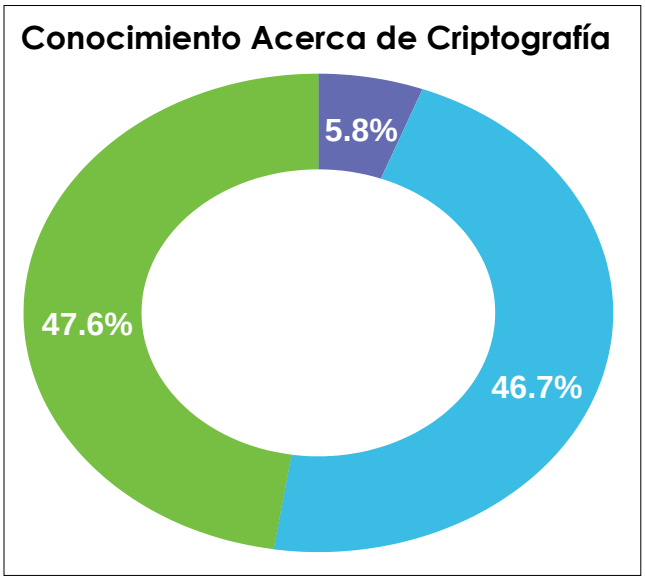
Pregunta N°9: ¿Cuánto sabe acerca de Criptografía?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Mucho, busco aplicaciones y sitios web que cuenten con ello	**19**	**5.8%**
●	Un poco, he leído respecto a eso	**154**	**46.7%**
●	Nada en absoluto	**157**	**47.6%**
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 11 Conocimiento acerca de criptografía



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 41 Conocimiento acerca de criptografía

Con respecto a la criptografía, el 47.6% de los participantes no tiene conocimiento acerca de esta, y solo existe una diferencia de 0.9% con los que tienen una ligera noción de lo que se trata la criptografía. Pero apenas el 5.8% buscan aplicaciones y sitios web que tengan esta herramienta.

3.2.3. Casos relevantes en Ecuador

Al igual que otros países de la región, en Ecuador se han presentado varios casos que atentan contra la privacidad de los ciudadanos en plataformas digitales. Algunos de estos son el reflejo de ataques cibernéticos provenientes del exterior pero otros en cambio son ocasionados por parte de los propios gobernantes de turno.

A continuación se presentará algunos casos relevantes suscitados en contra de la privacidad de las personas ocurridas en medios digitales asociados con Internet.

- ***Entidades gubernamentales en razón de la privacidad***

Uno de los deberes primordiales del estado es el proveer a sus ciudadanos de garantías para el cumplimiento de sus derechos. Al hablar del derecho a la privacidad se puede decir que el estado ecuatoriano centró su atención en el manejo adecuado de la información por lo que destinó una entidad especializada en la inteligencia nacional; la Secretaría Nacional de Inteligencia de Ecuador (SENAIN) establecida en el 2009, que tiene por objetivo garantizar la libertad y seguridad ciudadana a través del buen manejo de la información.

No obstante se ha encontrado envuelta en denuncias de espionaje y persecución hacia los periodistas y grupos opositores al régimen durante su ejercicio en el paso de los años.

Encontrándose los siguientes hechos:

FECHA	HECHO
4 DE AGOSTO DE 2015	el Portal Ecuador Transparente publicó 31 documentos distintos de información provenientes de la SENAIN , que documentan el espionaje sistemático a políticos de oposición y activistas por parte del gobierno entre 2012 y 2014
	Entre los documentos publicados se encuentran peticiones de información de 16 ciudadanos, solicitados a la plataforma "datoseguro.ec"; cuyas peticiones no se encuentran fundamentadas en investigaciones judiciales
SEPTIEMBRE 2017	Presencia de cámara de video en el despacho presidencial cuestiona el accionar de la SENAIN. (La Hora, 2017)

Fuente: (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 5)

Elaborado por: Antonela Suárez

Tabla 12. Hechos relevantes sobre la privacidad en entidades establecidas para el manejo de datos

Las actividades realizadas por la SENAIN se encuentran vinculadas al DINARDAP (Dirección Nacional de Registro de Datos Públicos) creada en el 2010 con la finalidad de consolidar, administrar y estandarizar los datos públicos de los ciudadanos. Reúne los datos del registro civil, movimientos migratorios, seguridad social, los registros de la propiedad, societario, mercantil y civil de todos los ecuatorianos en el portal datoseguro.gob.ec. A través de la información provista por el SRI se puede conocer detalles de consumo de cada uno de los habitantes visualizando hasta sus facturas. (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 5)

El acceso a la información de un usuario se realiza mediante una clave única entregada al mismo que le dota de acceso a esta, pero a que su vez puede ser manejada por el administrador del sistema.

Fuente: (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 6)

Elaborado por: Antonela Suárez

Fig. 42 Acceso a la información del portal datoseguro.gob.ec.

El portal de datoseguro.gob.ec al igual que otros sitios de internet que manejan datos ha sufrido de vulnerabilidades:

FECHA	HECHO	AFECTADO	TIPO DE DELITO
26 NOVIEMBRE 2012	Paúl Moreno alertó la vulnerabilidad del portal Dato Seguro tras crear una cuenta que obtenía la información del ex presidente Rafael Correa, aseverando la grave falla que tenía el sistema al momento de autenticar datos. (El Universo;, 2012)	Paúl Moreno	Acceso fraudulento a sistemas informáticos y bases de datos

Fuente: (El Universo;, 2012)

Elaborado por: Antonela Suárez

Tabla 13. Vulnerabilidad portal datoseguro.gob.ec

Según un estudio realizado por la Fundación Mil Hojas con colaboración de Usuarios Digitales, la información almacenada en estos registros de ciudadanos considerados opositores al gobierno, ha sido expuesta públicamente por funcionarios públicos y utilizada como medios de agravio.

FECHA	HECHO	AFECTADO	TIPO DE DELITO
AGOSTO 2015	Esperanza Martínez denunció ante la Fiscalía General del Estado el hackeo de su correo electrónico y envío de varios correos electrónicos que suplantaba su identidad mientras realizaba la recolección de firmas para la consulta popular. Hecho denunciado por el Colectivo Yasunidos dentro de la investigación previa No.-170101815085018 (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 11)	Esperanza Martínez, Colectivo Yasunidos	Violación a la intimidad por presuntos funcionarios públicos del estado ecuatoriano que accedieron a correos electrónicos personales.
AGOSTO 2016	Presentación de facturas cifras reales provistas por el SRI correspondiente Enrique Ayala Mora en Enlace Ciudadano. (Ecuadorenvivo, 2016)	Enrique Ayala Mora	Divulgación de Información, según el código tributario la información debe ser manejado únicamente por la administración fiscal y el contribuyente (art. 99)
JUNIO 2017	Exposición de datos personales (servicio de rentas internas) mediante Twitter por parte del ex presidente correa en respuesta a comentario expresado por periodista (Fundamedios, 2017)	Jean Paul Canon Medina	Divulgación de datos personales: privacidad

Fuente: (Usuarios Digitales & Fundación 1000 Hojas, 2016)

Elaborado por: Antonela Suárez

Tabla 14. Divulgación de datos personales por parte de funcionarios públicos

- ***Violación a la privacidad, ataques a la honra y/o reputación***

Hoy por hoy, el material circulante en redes sociales se encuentra predominado por fotografías, videos de múltiples tópicos. Sin embargo, la información que es considerada de carácter "viral" se comparte miles de veces en un minuto y puede llegar a millones de personas en todo el mundo, que a su vez estas emiten sus comentarios lo que llevará a afectar a los participantes del video, foto u opinión originalmente publicada.

En la siguiente tabla se presenta algunos casos de violación a la privacidad que han repercutido gravemente en la honra y buen nombre de una persona:

FECHA	HECHO	AFECTADO	TIPO DE DELITO
11 ENERO 2014	El periódico gubernamental "El Telégrafo" publicó correos obtenidos por hackeo sobre un posible financiamiento entre La NED y la Sra. Roldós, originando en los meses siguientes, una campaña de desprestigio hacia ella, en medios públicos. Llegando a ser exhibidos durante el Enlace Ciudadano #356. (El Telégrafo;, 2014)	Martha Roldós	- Violación a la intimidad a través de medios electrónicos - Violación al derecho a la honra.
01 SEPTIEMBRE 2015	Difusión video de concejal Antonio Ricaurte expresándose de forma inadecuada de Carla Cevallos, tras una intromisión en las comunicaciones , el video es expuesto mediante redes sociales (Barreto, 2015)	Antonio Ricaurte Carla Cevallos	- Violación a la intimidad - Intromisión de las comunicaciones - Afectación a la honra

24 JUNIO 2015	El canal público EcuadorTV en una edición especial de su programa "Desenmascarando", exhibió un vídeo llamado "La rebeldía de los 'Pelagatos'", conocido como Pelucoleaks. En el video se exhibían las conversaciones (chats) privadas mantenidas por decenas de personas en las plataformas Telegram y WhatsApp. La transmisión los acusaba de estar detrás de las marchas en contra del régimen (Desenmascarando PelucoLeaks, 2015)	- Bernardo Abad - Janneth Hinostroza - Andrés Páez, - Juan Carlos Solines, entre otros.	Exhibición de comunicaciones privadas
17 NOVIEMBRE 2016	Ex Jueza Lorena Collantes : divulgación de video en estado etílico de la jueza afectando directamente a su honra (Reyes, 2016)	Lorena Collantes	- Violación a la intimidad - afectación a la honra
8 MARZO 2017	"Lady Tantra": esposa infiel, marido divulga información personal. (El Universo, 2017)	María Gabriela Torres	- Violación a la intimida - afectación a la honra
06 AGOSTO 2017	El Capitán Edwin Ortega tras publicar un mensaje en redes sociales en contra del presidente Rafael Correa recibe múltiples amenazas, además de la divulgación de sus datos personales incluyendo fotografías de su domicilio y teléfonos de contacto. Seguido de estas acciones su cuenta fue hackeada y múltiples mensajes fueron enviados en su nombre. (FUNDAMEDIOS, 2017)	Edwin Ortega	Divulgación de datos personales, suplantación de identidad

Fuente: (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 10)

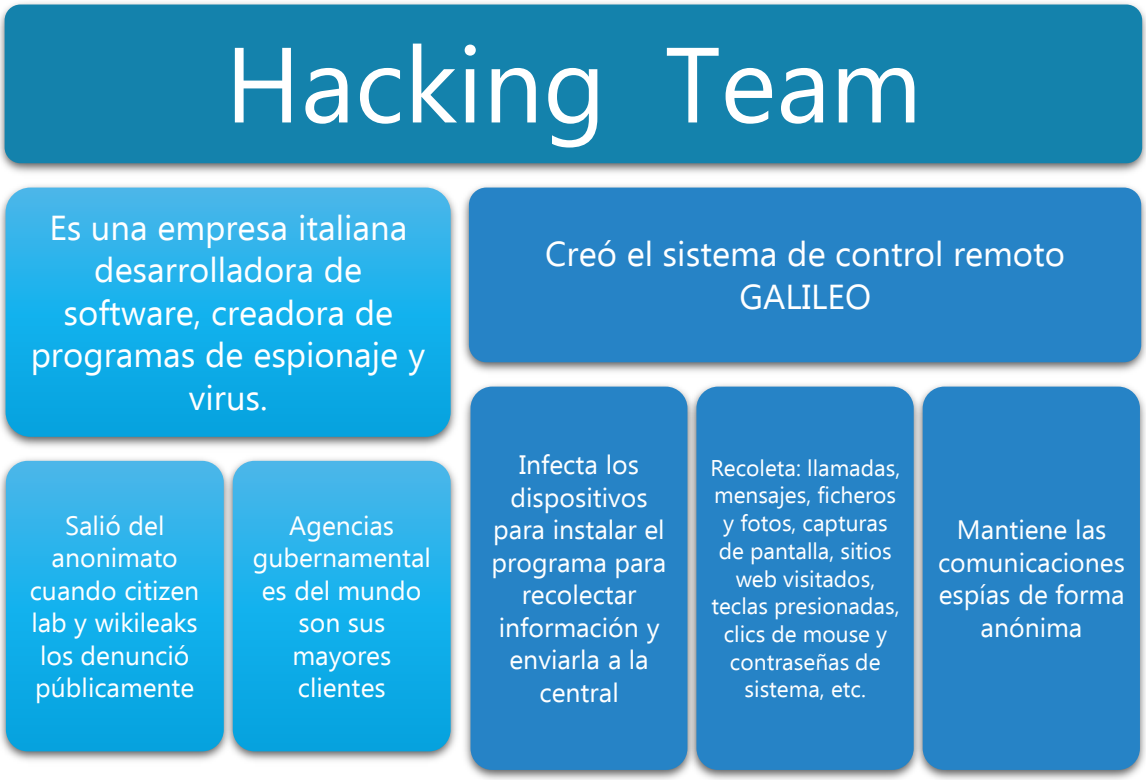
Elaborado por: Antonela Suárez

Tabla 15 Violaciones a la privacidad con afectación a la reputación de una persona en Ecuador

En el ámbito de las comunicaciones, la privacidad, seguridad y anonimato son factores decisivos para poder gozar plenamente del derecho a la privacidad. Sin embargo, hoy por hoy el hecho de llevar una identidad anónima en las comunicaciones, produce un efecto intimidatorio.

- ***Seguridad Informática y vigilancia estatal***

En julio de 2015 WikiLeaks difundió un informe sobre la afectación de la vigilancia estatal. En el cual describe una campaña de malware, phishing y desinformación activa en varios países latinoamericanos, incluyendo al Ecuador en el informe.



Fuente: (Fundación Mil Hojas;, 2015)

Elaborado por: Antonela Suárez

Fig. 43 ¿Qué es Hacking Team?

Transparency Toolkit y posteriormente WikiLeaks difundieron información que fue filtrada de dicha empresa; allí se encuentra la lista de gobiernos, agencias de inteligencia y policía que compraron RCS(Remote Control System) y realizaron pagos para su mantenimiento, entre ellos Ecuador a partir de la secretaría de Inteligencia (SENAIN) posiblemente adquirida en 2013.

Otro caso sobre la violación a la seguridad se registra en Diciembre de 2015 mediante operación PackRat (Remote Access Trojans) descubierta por Citizen Lab con la finalidad de infectar computadoras y teléfonos inteligentes, cuyos objetivos incluyen periodistas y políticos de oposición. (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 14)

Fuente: (John Scott-Railton, 2015)

Elaborado por Morgan Marquis-Boire

Fig. 44 Ataque mediante PACKRAT América del Sur

3.3. Transparencia

3.3.1. Conocimiento actual sobre transparencia en Ecuador.

La iniciativa de datos abiertos (open data) ha sido una de las herramientas para medir el nivel de transparencia que manejan los países alrededor del mundo. En donde se evalúa que la información entregada a los ciudadanos cumpla con el principio del "conocimiento abierto" el cual estable que cualquier contenido, información o datos puede ser usado, reutilizado, redistribuido libremente por las personas sin ninguna restricción legal, tecnológica o social; considerando los siguientes criterios:

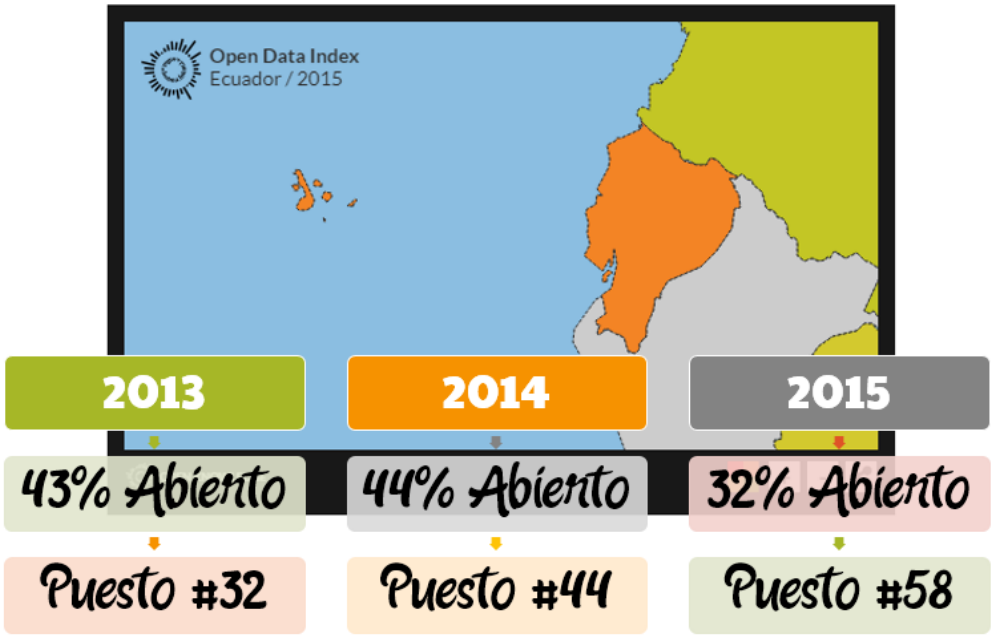
	Cuenta con una licencia que permita que los datos sean libremente utilizados, reutilizados y redistribuidos.
	Se encuentran los datos en forma gratuita
	Todos los archivos se encuentran en digital y pueden ser procesados o analizados fácilmente por cualquier computadora.
	Los datos se encuentran disponibles a granel y es sencillo de descargar. Se considera limitado si los ciudadanos pueden obtener partes del conjunto de datos a través de una interfaz
	Los datos se encuentran actualizados conforme al año de censo realizado, proveen información sobre cuándo fue la última vez que actualizaron y con qué frecuencia realizaron esta actualización
	Los datos se encuentran públicamente disponibles, Se puede acceder en línea sin la necesidad de una contraseña o permisos. Si los datos están en papel, pueden ser accedidos por el público, y no hay restricciones en el número de fotocopias que se pueden hacer.
	Los datos se encuentran en forma digital pero no son accesibles online
	Los datos están en Línea y son accesibles mediante internet.
	Los datos deben provenir de un recurso oficial emitido directamente por el gobierno o por un tercero que representa oficialmente al gobierno. Los datos ofrecidos por empresas, iniciativas ciudadanas o cualquier organización no gubernamental no cuentan para el Índice.

Fuente: (Open Knowledge, 2015)

Elaborado por: Antonela Suárez

Fig. 45 Criterios para evaluación de datos abiertos

Según los parámetros evaluados por “Open Knowledge” en el año 2013, el Ecuador se encontraba en lugar 32 del ranking de datos abiertos a nivel mundial; para el siguiente año, descendió un puesto en el estudio. Sin embargo, para el 2015, Ecuador se encontraba en el puesto #58 a nivel mundial; según estos estudios se deduce que la transparencia ha ido decayendo con el paso de los años.



Fuente: Global Open Data Index

Elaborado por: Antonela Suárez

Fig. 46 Ranking Ecuador del 2013 al 2015

A continuación, se muestran los puntos con mayor restricción de acceso a la información y como variables fundamentales que indican el manejo primordial por parte del gobierno pasaron de ser algo accesibles y reveladoras de información a no presentar ningún tipo de acceso:

Rank	Dataset	Breakdown	Location (URL)	Format	Info	Prev.	Score
14	National Map		http://inec.gob.ec/estadistica...	n/a	n/a	n/a	70%
16	National Statistics		http://inec.gob.ec/estadistica...	n/a	n/a	n/a	70%
16	Company Register		http://www.supercias.gob.ec/po...	n/a	n/a	n/a	45%
20	Government Spending		n/a	n/a		n/a	10%
21	Location datasets		http://www.codigopostal.gob.ec...	n/a	n/a	n/a	45%
35	Government Budget		http://www.finanzas.gob.ec/el-...	n/a	n/a	n/a	50%
35	Election Results		http://resultados.cne.gob.ec/R...	n/a	n/a	n/a	45%
35	Pollutant Emissions		http://suia.ambiente.gob.ec/am...	n/a	n/a	n/a	35%
48	Transport Timetables		n/a	n/a		n/a	25%
60	Legislation		http://www.registroficial.gob....	n/a		n/a	30%

Fuente: Global Open Data Index

Elaborado por: (KNOWLEDGE, 2013)

Fig. 47 Análisis Datos Abiertos, Ecuador 2013

La Figura 45 muestra la situación en el año 2013, donde el indicador con respecto a las legislaciones era el tópico con mayor restricción, en el cual se debía realizar un pago para poder obtener información acerca de leyes y sus enmiendas además de que no todos se los encuentra en forma digital. Cabe recalcar que la información liberada por distintas instituciones gubernamentales no maneja ningún tipo de licenciamiento que sea conveniente para sus ciudadanos.

Rank	Dataset	Breakdown	Location (URL)	Format	Info	Prev. (2014)	Score
6	Government Spending		http://www.finanzas.gob.ec/eje...	n/a		#11 45%	45%
14	Company Register		http://appscvs.supercias.gob.e...	HTML, ...		#14 60%	60%
20	Water Quality		http://www.agua.gob.ec/bibliot...	n/a		n/a	35%
26	Procurement tenders		https://www.compraspublicas.go...	Proprie ...		n/a	60%
36	Land Ownership		n/a	n/a		n/a	20%
40	Location datasets		n/a	n/a		#18 45%	20%
45	Government Budget		http://www.finanzas.gob.ec/inf...	HTML, ...		#22 70%	60%
45	Election Results		http://resultados.cne.gob.ec/	n/a		#51 45%	45%
45	National Map		http://app.sni.gob.ec/visorseg...	n/a		#25 60%	35%
65	Pollutant Emissions		n/a	n/a		#51 35%	10%
80	Weather forecast		n/a	n/a	n/a	n/a	0%
106	National Statistics		http://inec.gob.ec/estadistica...	n/a		#66 45%	0%
107	Legislation		http://www.registroficial.gob....	n/a		#85 30%	30%

Fuente: Global Open Data Index

Elaborado por:(Open Knowledge,2015)

Fig. 48 Análisis Datos Abiertos, Ecuador 2015

A diferencia de la Figura 45, en el 2015 (véase Figura 46) se puede observar un gran decaimiento en la liberación de datos. Indicadores como las estadísticas nacionales han sido completamente restringidas durante este año de análisis en comparación del 2013 que tenían el 70% de libertad y se podía acceder mediante internet para conocer sobre indicadores demográficos y económicos como el PIB, la tasa de desempleo, la población, etc. Estos datos para el último año de análisis no se los encontraba actualizados.

Por otro lado, WikiLeaks se ha encargado de revelar la realidad de las actividades gubernamentales de una de las potencias más grandes del mundo, así como ha expuesto el accionar de ciertos gobiernos obligando a una transparencia total forzada. Con respecto a Ecuador, existen algunos documentos que tratan acerca de casos de intromisión ilegal de Estados Unidos que revelan conversaciones entre este país y aliados en sectores políticos, sociales o empresariales, lo cual solo una pequeña fracción ha salido a la luz.

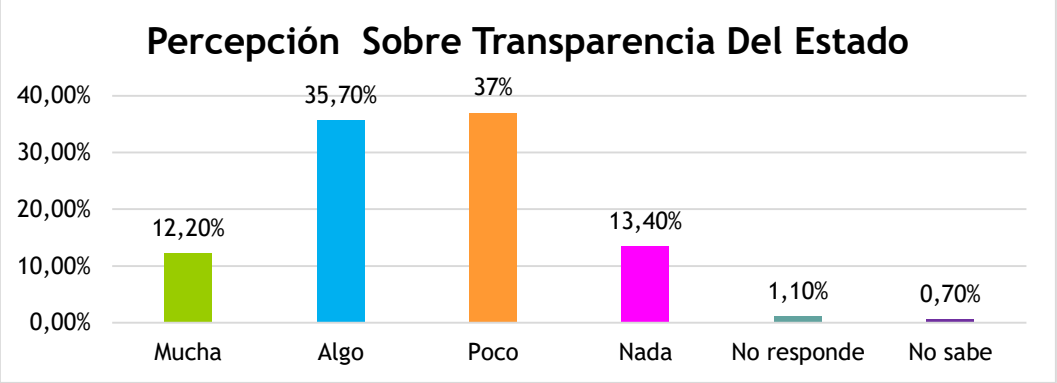
Durante el 2015, se realizó un estudio por parte de Latinobarómetro para conocer la noción sobre la transparencia del estado en el país. Los resultados fueron los siguientes luego de realizar 1200 encuestas:

Resultados ponderados	Nº de casos	Total
Mucha	146	12.2%
Algo	428	35.7%
Poco	444	37%
Nada	161	13.4%
No responde	13	1.1%
No sabe	8	0.7%
Total	**1200**	**100%**

Fuente: (Latinobarómetro, 2015)

Elaborado por: Latinobarómetro

Tabla 16 Percepción sobre transparencia del Estado



Fuente: (Latinobarómetro, 2015)

Elaborado por: Latinobarómetro

Fig. 49 Percepción sobre transparencia del Estado

Al conocer sobre estos estudios, se puede decir que Ecuador es un país que se encuentra tratando de implementar indicadores que ayuden a establecer la transparencia, pero aún mantienen un largo camino por delante y se espera que con el nuevo gobierno mayores reformas sean aplicadas y exista mayores aperturas para el dialogo que es fundamental para fomentar este aspecto.

3.3.2. Tabulación de encuesta y Presentación de resultados

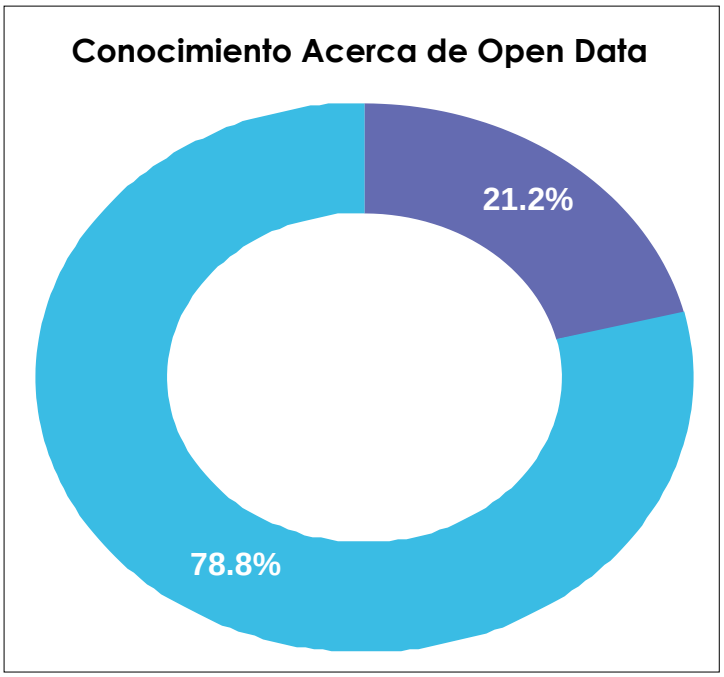
Pregunta N°10: ¿Conoce acerca de Open Data?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	70	21,2%
●	No	260	78,8%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 17 Conocimiento sobre Open Data



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 50 Conocimiento sobre Open Data

El presente gráfico denota que la mayor parte de los participantes no conoce acerca de Open Data y tal solo el 21.2% conoce acerca de ellos.

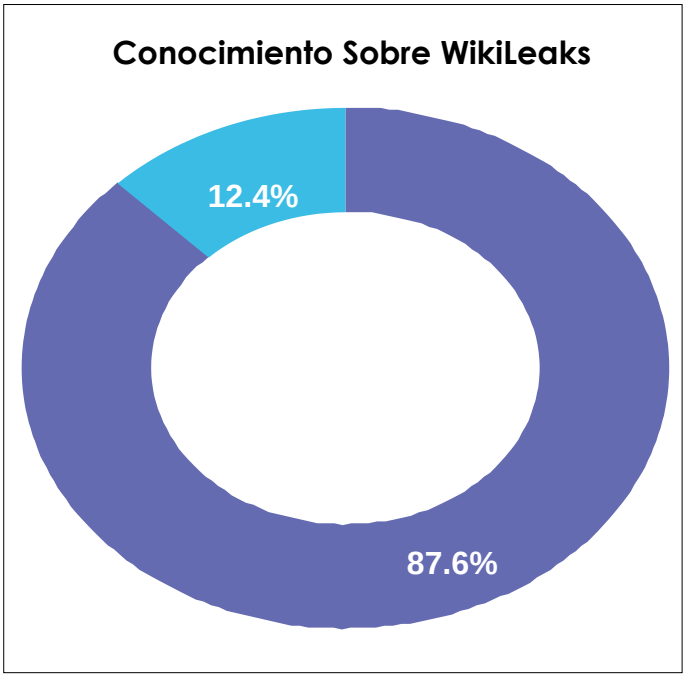
Pregunta N°11: ¿Ha escuchado hablar sobre WikiLeaks?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	289	12,4%
●	No	41	87,6%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 18 Conocimiento sobre WikiLeaks



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 51 Conocimiento sobre WikiLeaks

En su mayoría (87.6%) existe un conocimiento acerca de WikiLeaks. Mientras que el 12.4 % dicen no conocerlo.

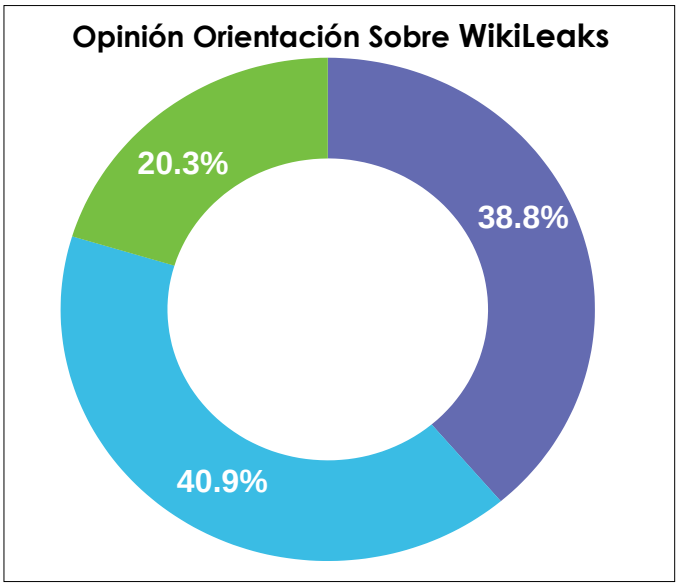
Pregunta N° 12: Considera que es un sitio orientado hacia:

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Los Hackers	128	38.8%
●	El aseguramiento de la transparencia en la red	135	40.9%
●	La Prensa	67	20.3%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 19 Opinión orientación sobre WikiLeaks



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 52 Opinión orientación sobre WikiLeaks

Para el 40.9% de los encuestados WikiLeaks es un sitio en internet que permite asegurar la transparencia en la red, dado los múltiples documentos presentados en su blog. El 38.8% en cambio considera que es un sitio orientado hacia los hackers y los actos indebidos y solo un 20.3% considera que es un sitio orientado hacia la prensa.

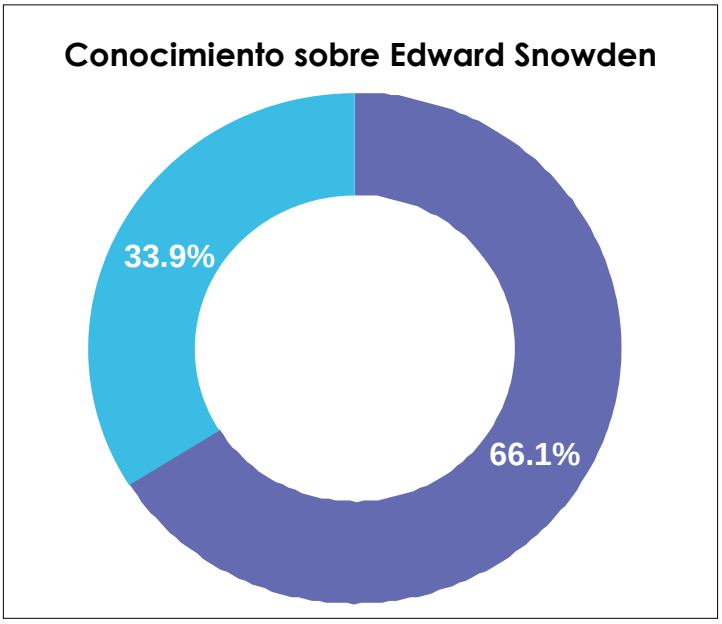
Pregunta N° 13: Conoce usted ¿quién es Edward Snowden?

OPCIÓN		FRECUENCIA	PORCENTAJE
●	Si	218	66,1%
●	No	112	33,9%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 20 Conocimiento sobre Edward Snowden



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 53 Conocimiento sobre Edward Snowden

Este gráfico demuestra que el 66.1% de los participantes tienen una noción básica de quién es Edward Snowden, pero existe un segmento del 33.9% que jamás ha escuchado sobre él y su lucha por la privacidad.

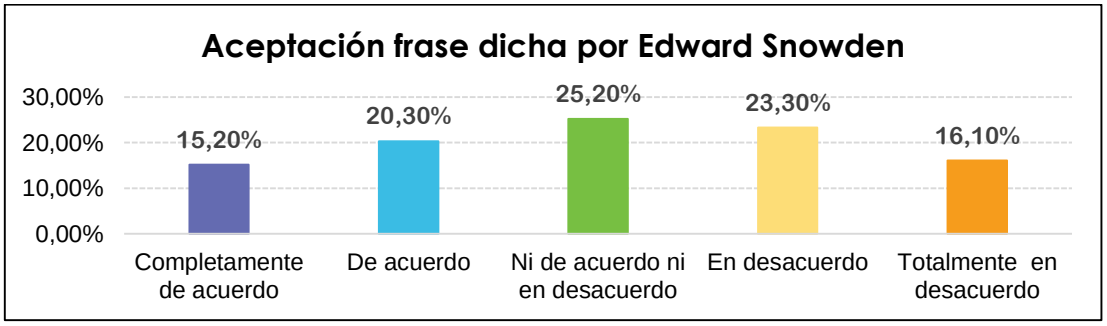
Pregunta N° 14: Está de acuerdo con la frase: "No quiero vivir en un mundo donde todo lo que digo, todo lo que hago, todo lo que hablo, toda expresión de creatividad o de amor o de amistad queda grabada"

OPCIÓN	FRECUENCIA	PORCENTAJE
Completamente de acuerdo	120	36.4%
De acuerdo	115	34.8%
Ni de acuerdo ni en desacuerdo	75	22.7%
En desacuerdo	12	3.6%
Totalmente en desacuerdo	8	2.4%
TOTAL	**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 21 Aceptación frase dicha por Edward Snowden



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 54 Aceptación frase dicha por Edward Snowden

El 71,2 % de los encuestados concuerda en que no desea vivir en un mundo donde la vigilancia continua sea parte del día a día, lo que refleja la importancia que mantienen sobre su privacidad y la noción que mantienen. Es interesante encontrar respuestas "neutras" ni de acuerdo, ni en desacuerdo tiene el siguiente porcentaje significativo 22,8% esto demuestra una perdida sobre la concepción de la privacidad y se lo podría asociar con frases como "no tengo nada que esconder" que son los puntos de partida ante el respeto de la privacidad. Finalmente el 3,6% y 2,4% no están de acuerdo con la frase dicha por Snowden.

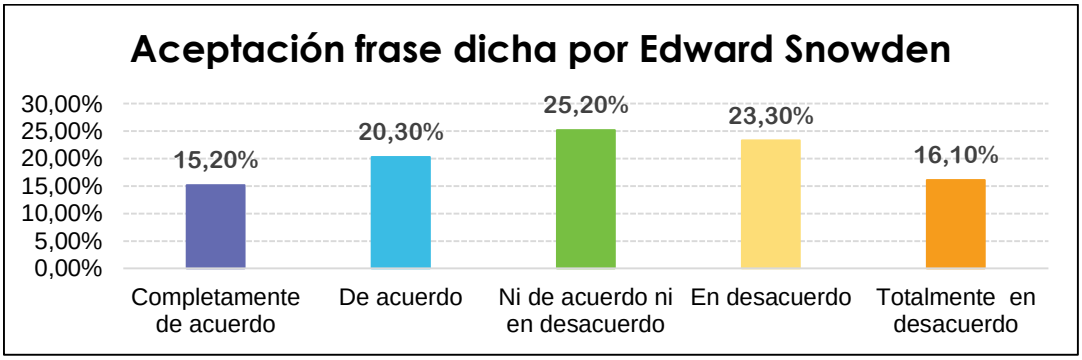
Pregunta N° 15: Está de acuerdo con la frase: "Privacidad para el débil, Transparencia para el poderoso". *Considerando como "Poderoso" a aquella persona que desempeña alguna función pública*.

OPCIÓN		FRECUENCIA	PORCENTAJE
	Completamente de acuerdo	50	15.20%
	De acuerdo	67	20.30%
	Ni de acuerdo ni en desacuerdo	83	25.20%
	En desacuerdo	77	23.3%
	Totalmente en desacuerdo	53	16.10%
TOTAL		**330**	**100%**

Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Tabla 22 Aceptación frase dicha por Julian Assange



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 55 Aceptación frase dicha por Julian Assange

Según los resultados la opinión "neutra" de estar ni de acuerdo o en desacuerdo encabeza la lista con el 25.2 % lo que refleja que la transparencia no es un tema conocido y primordial como ciudadanos de este país. El 23.3% se encuentra en desacuerdo, y el 16.1% en completo desacuerdo ante esta ideología y apenas un 25,5% se encuentra de acuerdo y completamente de acuerdo.

3.3.3. Casos de Censura del Internet en Ecuador

Tras un estudio realizado por Latinobarómetro en el 2016 el país con mayor percepción de censura y autocensura en la Latinoamérica es Ecuador. Dado que solo el 34% de los ecuatorianos dicen poder usar el internet con libertad.

Algunas evidencias de censura en el país son los siguientes:

FECHA	HECHO
MARZO 2014	El apagón digital de 2014, consistió en restringir el acceso a páginas como YouTube y Google entre las 19H20 a las 19h53, solicitada por el gobierno nacional a la AEPROVI. (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 17)
SEPTIEMBRE 2014	Facebook elimina la cuenta personal de un ciudadano ecuatoriano tras publicar videos e imágenes de abusos policiales cometidas durante las protestas. El video contenía imágenes y grabaciones de audio del ex presidente Correa donde felicitaba el accionar de la policía. (Bertoni, 2014)
DICIEMBRE 2015	Bloqueo del servidor de imágenes de Twitter durante la sesión de votación de las Enmiendas Constitucionales. (ElComercio.com, 2015)
AGOSTO 2017	Twitter suspende la cuenta oficial de CrudoEcuador sin razones justificables, en diciembre de 2016 la empresa exigió la eliminación un 'tuit', referente al caso del exdirector del diario estatal El Telégrafo, Orlando Pérez, quien fue denunciado por maltrato a su expareja. Sin embargo, tras eliminar dicho mensaje y recuperar su cuenta, el 28 de julio la red social suspendió la cuenta sin dar explicaciones del hecho. (Fundamedios, 2017)

Fuente: (Usuarios Digitales & Fundación 1000 Hojas, 2016)

Elaborado por: Antonela Suárez

Tabla 23. Casos de Censura en Ecuador

“El Estado ecuatoriano hace uso de la Ley de Derechos de Autor del Milenio Digital (DMCA) por la cual la Ley otorga a los titulares de derechos un sistema para la “notificación y eliminación del contenido” y solicitar a proveedores en red como buscadores o redes sociales en Internet, que eliminen contenidos o enlaces argumentando que violan derechos de propiedad intelectual sin necesidad de una orden o control judicial.” (Usuarios Digitales & Fundación 1000 Hojas, 2016, pág. 19)

- La creación de Trolls o bots por parte del gobierno anterior ha sido un medio para atacar e insultar a los críticos del oficialismo desde el anonimato.

3.3.4. La ley de la transparencia en Ecuador

En el 2004, en Ecuador se aprobó la ley Orgánica de Transparencia y Acceso a la información Pública, se la implemento con el fin de garantizar el acceso a la información pública del estado, a través del artículo 91 de constitución. Está ley se redacta de una forma muy general a la información pública que poseen las instituciones del estado, aunque mucha de esta información se puede considerar confidencial como es el caso de la intimidad personal; es decir, datos y registros confidenciales de las personas que se ampara en los derechos civiles de la constitución de 1998.

Esta ley implica que las instituciones públicas, publiquen en un periodo de tiempo cierta información de las entidades y de los funcionaros que trabajan para dichas instituciones de no ser así, los funcionarios responsables de dar dicha información pueden ser sancionados e incluso a la remoción del cargo que desempeñan.

La información que puede ser publicada y además que la ley dispone transparentar, es la remuneración mensual salarial de los funcionarios asociada al cargo que desempeñan en la institución, dicha información se la publica en la web, hay que considerar que la información financiera es muy sensible e incluso un atropello a la intimidad de las personas.

Resumen

Al hablar sobre la situación de Ecuador frente a la privacidad es importante denotar que muchos usuarios de internet tienen un conocimiento efímero de lo que implica el manejo de datos y proveen sin precaución sus datos personales (nombres completos, ubicación geográfica, números de tarde crédito, teléfonos, etc.) a cambio de obtener distintos servicios en línea sin pensar que es lo que pasará a futuro con ellos.

Ecuador es considerado un país totalmente colectivista lo que supone que sus habitantes tienen un mayor grado de confianza en otras personas. Por ello, es importante conocer cuál es la noción que mantienen los ecuatorianos hoy en día frente a lo que pasa en Internet, con su privacidad; por lo que se ha realizado un pequeño estudio preliminar para determinar la percepción de la privacidad, así como de la transparencia. Para ello se realizó 330 encuestas a estudiantes de diversas carreras de la Pontificia Universidad Católica del Ecuador.

Las conclusiones son un interesante punto de partida para conocer algo sobre los grupos con un mínimo conocimiento técnico sobre los cuales se aplicó la muestra.

El 29.1% utilizan con mayor frecuencia WhatsApp para comunicarse, seguidos por Facebook con el 28.3% e Instagram con el 14.5%. Un 71.8% de los encuestados no han leído los términos y condiciones de las aplicaciones y redes sociales a las que acceden. El 63.9% no realiza una lectura de las políticas de privacidad. El 42% han tenido desacuerdos con las políticas de privacidad. El conocimiento de la vinculación de datos entre aplicaciones y redes sociales difieren con su desconocimiento en un 0.6%. Un 56,4% de los usuarios de aplicaciones mediante internet han querido acceder a los datos dejados mediante la red. El 55.8% de los encuestados considera que el almacenamiento de datos se lo realiza para utilizarlos en fines comerciales. El 73.6% de encuestados no tiene conocimiento sobre herramientas que aseguran una comunicación privada. Apenas el 5.8% buscan aplicaciones y sitios web que tengan la herramienta de criptografía.

La iniciativa de datos abiertos (open data) ha sido una de las herramientas para medir el nivel de transparencia que manejan los países alrededor del mundo. En donde se evalúa que la información entregada a los ciudadanos cumpla con el principio del “conocimiento abierto”.

Según los parámetros evaluados por “Open Knowledge” la transparencia en el Ecuador ha ido decayendo con el paso de los años. En base a estos estudios, se puede decir que Ecuador es un país que se encuentra tratando de implementar indicadores que ayuden a establecer la transparencia, pero aún mantienen un largo camino por delante.

Solo el 21.2% del universo encuestado conoce sobre Open Data. El 87.6% denota un conocimiento acerca de WikiLeaks. Para el 40.9% de los encuestados WikiLeaks es un sitio en internet que permite asegurar la transparencia en la red; el 38.8% considera que es un sitio orientado hacia los hackers y los actos indebidos, y solo un 20.3% considera que es un sitio orientado hacia la prensa. El 66.1% de los participantes tienen una noción básica de quien es Edward Snowden. El 71,2 % de los encuestados concuerda en que no desea vivir en un mundo donde la vigilancia continua sea parte del día a día, lo que refleja la importancia que mantienen sobre su privacidad y la noción que mantienen. Según los resultados la opinión “neutra” de estar ni de acuerdo o en desacuerdo encabeza la lista con el 25.2 % lo que refleja que la transparencia no es un tema conocido y primordial como ciudadanos de este país.

En el 2004 en el Ecuador se aprobó la ley Orgánica de Transparencia y Acceso a la información Pública, se la implemento con el fin de garantizar el acceso a la información pública del estado, a través del artículo 91 de constitución. Está ley, que se la redacta de una forma muy general, implica que las instituciones públicas, publiquen en un periodo de tiempo cierta información de las entidades y de los funcionaros que trabajan para ellas; la información que puede ser publicada, es la remuneración mensual salarial de los funcionarios asociada al cargo que desempeñan en la institución.

CAPÍTULO 4

El presente capítulo tiene como objetivo presentar una serie de herramientas que ayuden a la protección de la privacidad enfocándolas al manejo del usuario común y las limitaciones que presenta al enfrentarse a la tecnología. Por lo cual se presentará un análisis de las herramientas y una guía de referencia de las mismas.

Herramientas Tecnológicas para obtener privacidad

El conocimiento del perfil digital construido a partir de las actividades realizadas en internet por parte de un usuario ha sido conocido gracias a las revelaciones presentadas por Assange y Snowden. La vigilancia continua así como la comercialización de los datos entre grandes compañías, siendo una de las revelaciones que mayor impacto ha generado y lo sigue haciendo entre las personas que utilizan Internet y diferentes tipos de aplicaciones que se conectan a la red; es por eso, que surge la necesidad de conocer acerca de herramientas que protejan la privacidad de las personas y que se encuentren al alcance y comprensión en el manejo por parte de todos los usuarios de la red, enfocándose en aquellos que no tienen tanta afinidad con la tecnología y que a su vez son migrantes digitales, para los cuales representa una trivialidad entender cómo manejar una herramienta compleja que requiere mayor conocimiento computacional. El conocimiento de herramientas y complementos para el aseguramiento de la privacidad es fundamental para asegurar el futuro de esta en internet y por lo cual depende de todos los usuarios de internet su protección y exigir que no sobrepasen sobre los derechos digitales.

4.1. Presentación de Herramientas para la Privacidad y Transparencia.

ALTERNATIVA	MOTIVO	HERRAMIENTA
Uso de Software Libre	Al momento de usar software libre, se puede conocer la manera en que fue construida una aplicación y permite detectar de “puertas traseras” es decir espacios por donde se puede ingresar a la aplicación, la haga vulnerable y permita realizar espionaje o, a su vez, actividades ilícitas.	Sistemas operativos GNU/Linux: - Tails - Qubes OS - Ipredia OS - Whonix
Análisis Políticas de Privacidad - Datos	Conocer el tratamiento sobre el manejo de datos que realiza una aplicación o sitio web al que accede un usuario es fundamental para conocer para qué necesitan la información, cómo es almacenada y manejada dentro del programa.	Acceso previo a las políticas de privacidad de aplicaciones, disponibles en Internet antes de acceder a ellas.
Anonimato en la navegación en la red	Ocultar la identidad del usuario frente a la red de terceros permite reducir los riesgos de espionaje y rastreo de la procedencia además de mejorar la comunicación mediante el uso de encriptación de datos	- Freenet Project - TOR - I2P
Encriptación	La codificación de cualquier tipo de información permite disfrazar el contenido	Mensajería: - Telegram

	para que no pueda ser conocido con facilidad. Este proceso se lo realiza mediante una clave que, en la mayoría de los casos, se encuentra en manos de quien provee el servicio lo que le confiere total acceso a los datos que se comparta; además de que los gobiernos pueden obligar a estas empresas a liberar el contenido.	- Imessage Correo Electrónico: - Lavit - Hushmail Voz: - Redphone
Cifrado Extremo a Extremo	El cifrado punto a punto realiza el mismo proceso de encriptación, pero la diferencia se encuentra en que la clave se queda con los usuarios permitiendo que la información se quede con los mismo y con quienes se comunican, excluyendo a los proveedores del servicio y permitiendo mayor privacidad	Mensajería: - TextSecure - meet.jit.si - hack.chat Correo Electrónico: - Mailvelope Voz: - meet.jit.si Almacenamiento en la nube: - SpiderOak

Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Tabla 24 Herramientas para mantener la privacidad en Internet

4.2. Guía de referencia para preservar la privacidad en internet

Esta guía tiene por finalidad presentar al usuario común una serie de herramientas sencillas que pueden ser utilizadas para proteger su privacidad en el mundo de la red considerando los últimos acontecimientos presentados en años anteriores donde instituciones gubernamentales como privadas y grandes corporaciones han hecho un mal uso de los datos de los ciudadanos.

Es importante informar a los usuarios sobre el panorama actual de la privacidad en internet por lo que se abordan los siguientes tópicos con la finalidad de crear una cultura acerca de esta y su protección:

- ✓ **¿Qué es la privacidad?**

  La privacidad es aquello que se realiza en un ámbito reservado y permite el desarrollo del ser humano. En Internet, Se entiende como el control que realizamos sobre nuestra información para limitar la cantidad de personas autorizadas a verla y se encuentra estrechamente ligada con la protección de datos.

Es necesario, recalcar que todo tipo de entidad sea privada, gubernamental o pública debe informar a los usuarios acerca del manejo y uso de los datos que proporcionan por lo que es fundamental hablar acerca de la transparencia

- ✓ **¿Qué es la transparencia?**

  La transparencia hace referencia a la comunicación total, a exponer qué es lo que sucede con la información y está estrechamente ligada con el derecho a la información. Todos los gobiernos, entidades, compañías desarrolladores de tecnología, de aplicaciones, etc. deben comunicar a los usuarios sobre la administración de sus datos.

En años atrás las primeras evidencias en contra de la privacidad fueron dadas por Edward Snowden señalando el trabajo que realizaba la Agencian de Seguridad Nacional de los Estados Unidos al vigilar a ciudadanos estadounidenses así como de otros países lo que alerto a el resto de naciones a preocuparse sobre la protección de los datos personales de un usuario. Al igual en Ecuador esta realidad no ha quedado muy lejano dado los hechos contra la privacidad presentados en el capítulo anterior.

Al conocer la noción con respecto a la privacidad y transparencia en Ecuador se evidenció que un porcentaje muy bajo tenia pleno conocimiento de esta situación por lo que los usuarios se les debe informar que es lo que está sucediendo actualmente para que toman conciencia de la importancia de sus datos y que exijan a sus gobernantes leyes concretas que los protejan.

- ✓ **Situación de la Privacidad en Internet**

  Durante los últimos años, las actividades realizadas en Internet se han incrementado radicalmente. Tan sólo en un minuto billones de datos son entregados a la red.

  Todas las transacciones que son realizadas mediante internet dejan huellas que construyen el perfil digital de quien lo usa y lo hace perfectamente identificable ante el mundo real.

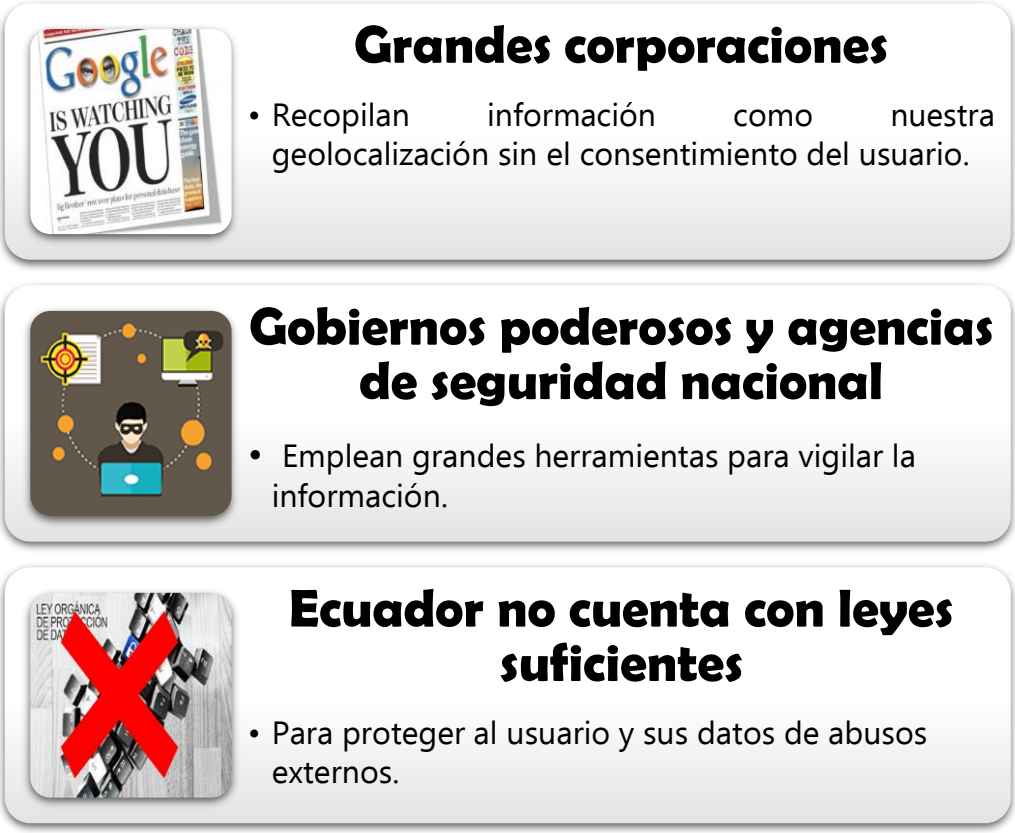
  Toda la información provista por aplicaciones y sitios de internet está sujeta a peligros si no son tratados de manera adecuada. Por ejemplo:

Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 56 Peligros que enfrentan los datos en internet

Desde hace algunos, años las revelaciones realizadas por Edward Snowden y WikiLeaks han dado a conocer el manejo inadecuados de los datos de los usuarios de aplicaciones y sitios web conectados a internet además de los distintos gobiernos que atentan contra la privacidad de sus propios ciudadanos como una forma de control hacia ellos.



Fuente: Antonela Suárez

Elaborado por: Antonela Suárez

Fig. 57 Motivos por lo que es importante la privacidad de los datos de los usuarios

El tráfico de datos de internet está compuesto por un sin número de datos compartidos de toda clase en internet. Pero si se sigue el rastro de un usuario y se reúne todo lo que ha dejado en internet y se analiza muchos de estos lo harán completamente identificable.

- **¿Qué datos que exponen los usuarios?**

Datos Personales

Información relacionada a una persona que permite identificarla y la caracteriza como individuo.

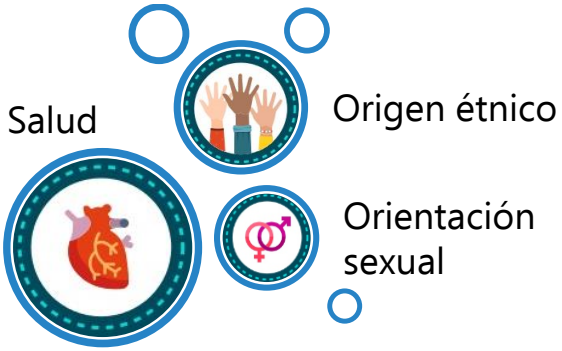
Fuente: (ESET, 2015)

Elaborado por: Antonela Suárez

Fig. 58 Datos personales

Datos Sensibles

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



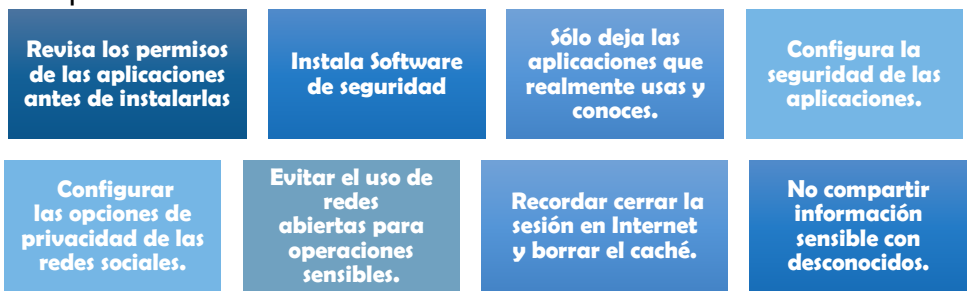
Fuente: (ESET, 2015)

Elaborado por: Antonela Suárez

Fig. 59 Datos Sensibles

L **Recomendaciones básicas para el manejo de privacidad**

Al momento que un usuario accede a un sitio en internet que solicita el ingreso de sus datos expone su identidad y lo hace vulnerable de sufrir de ciber crímenes, y otros abusos. Es necesario que los usuarios empiecen por ser conscientes de que existen estas amenazas y cómo funcionan, sin esto la tarea para los atacantes se hace más sencilla.



Fuente: (ESET, 2015)

Elaborado por: Antonela Suárez

Fig. 60 Recomendaciones básicas para el cuidado de la privacidad

Fuente: (ESET, 2015)

Elaborado por: Antonela Suárez

Fig. 61 Políticas de Privacidad

Conocer el tratamiento sobre el manejo de datos que realiza una aplicación o sitio web al que accede un usuario es fundamental para conocer para qué necesitan la información, cómo es almacenada y manejada dentro del programa.

- **Herramientas para proteger la privacidad contra el seguimiento global de los usuarios**

  Cuidar la privacidad de las personas en internet comprende una serie de cambios de los hábitos comunes de navegación hacia herramientas fáciles de usar y que a su vez tengan pre configuraciones que garanticen la seguridad. Por ejemplo:

- **Navegación anónima en la red**

Ocultar la identidad del usuario frente a la red de terceros permite reducir los riesgos de espionaje y rastreo de la procedencia además de mejorar la comunicación mediante el uso de encriptación de datos.

¿Por qué el anonimato en Internet?

Toda actividad en internet deja rastros partiendo desde la dirección IP hasta aspectos como:

- La geolocalización.
- Las búsquedas que realizas
- Denuncias que hayas hecho etc.

¿Qué se puede usar?

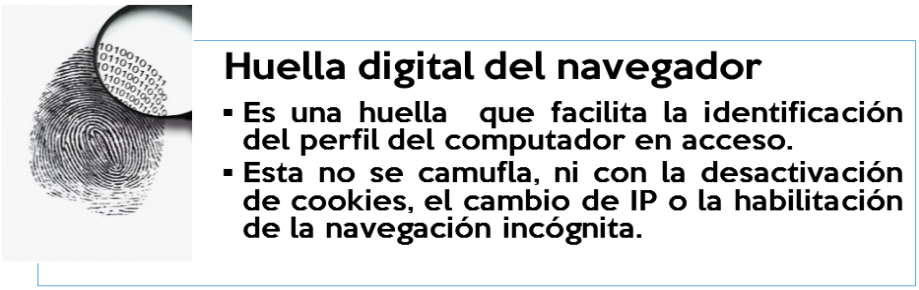
Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 62 Redes autónomas para navegación anómina en internet

- **Navegadores Web**

Los navegadores de internet comunes, mantienen huellas digitales que hacen a una persona identificable entre millones de usuarios. Estos programas que se conecta a la red envían de forma voluntaria información sobre el tipo de navegador, las fuentes tipográficas instaladas, el sistema operativo desde el que se está accediendo además de los pluggins y otros elementos que al compararse con las configuraciones de otros usuarios de Internet resulta en una marca relativamente única que permite rastrear actividad del usuario en la Web. Cada vez que un usuario visita una página web estos datos son enviados y quedan a la espera de conocer cuando el usuario accede nuevamente a esta página.



Fuente: (López Ponce, 2010)

Elaborado por: Antonela Suárez

Fig. 63 Huella digital en navegador y computador

La huella digital no es estable en el tiempo dado los cambios de configuración o actualización el software. Sin embargo es un elemento altamente rastreable que expone al usuario fuertemente.

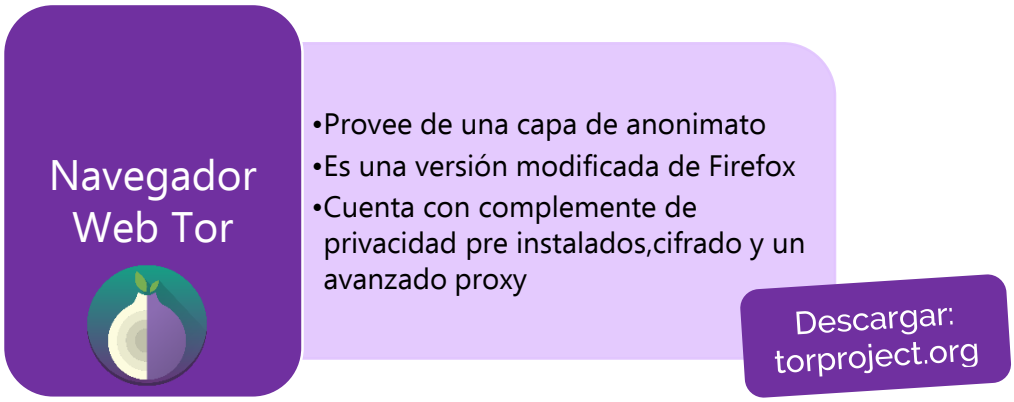
“La EFF ha puesto en marcha un sitio Web Panopticlick.org para que los usuarios puedan informarse sobre la huella digital de su propio equipo.” (López Ponce, 2010)

Fuente: (López Ponce, 2010)

Elaborado por: José López

Fig. 64 Comprobar si el navegador cuenta con una huella digital o de rastreo

Una manera de evitar que el usuario sea rastreado a traves de un navegador, es optar por cambiar los navegadores convencionales por unos amigables con la privacidad como por ejemplo:



Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 65 Navegador Tor

Para instalar este navedor solo hace falta ingresar a la pagina y oprimir en “descargar” se ejecutará la instalación como cualquier programa. Al finalizar la instalación se mostrará el siguiente ícono en la pantalla

Elaborado por: Antonela Suárez

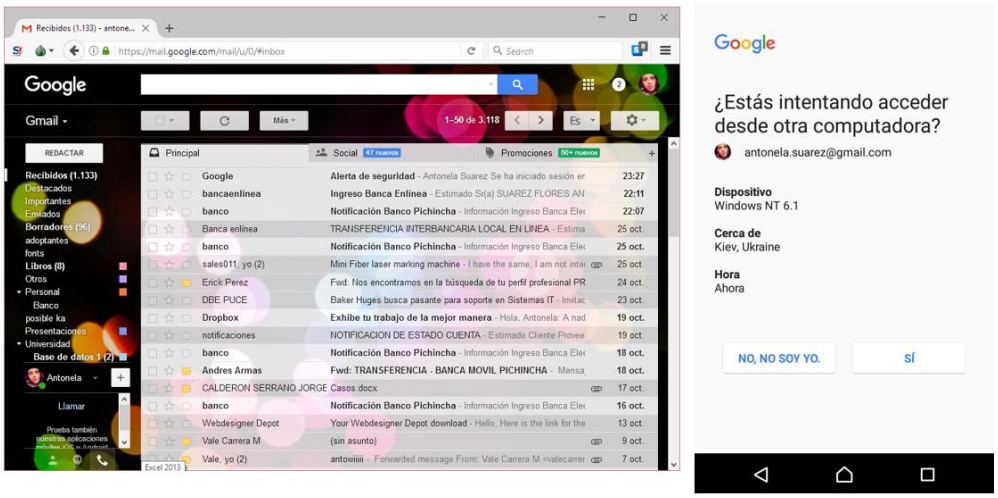
Fig. 66 Ejecución navegador Tor

La apariencia del navegador Tor es igual a le todos los navegadores, sin embargo cuenta con motores de búsquedas adecuados para preservar la provacidad, si se intenta acceder a “google.com” permite hacerlo. Sin embargo hacer busquedas mediante el es imposible por prohibiciones de google como se muestra a continuación

Elaborado por: Antonela Suárez

Fig. 67 Navegación con google mediante navegador Tor

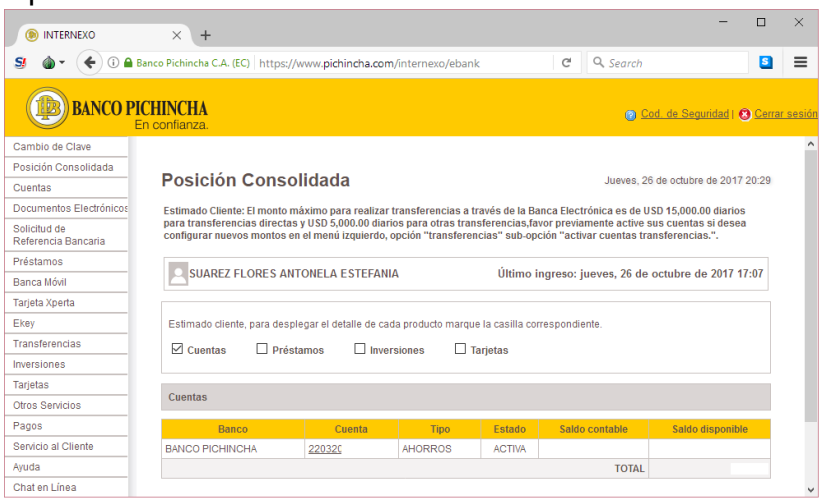
La filosofia de google sobre la identificación queda plasmada cuando se quiere utilizar Gmail. Ya que se puede acceder perfectamente a el desde Tor pero la validación de acceso es mucha mas estricta



Elaborado por: Antonela Suárez

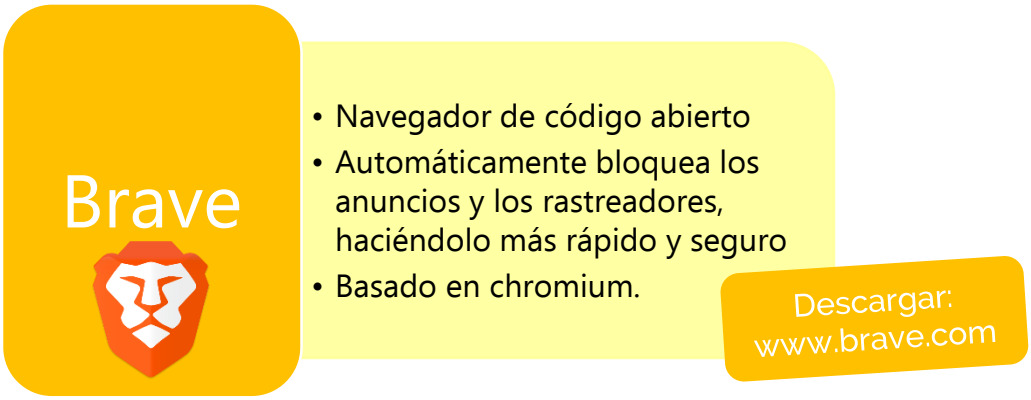
Fig. 68 Acceso a Gmail desde navegador Tor

El navegador Tor, permite el acceso a páginas de banca en línea sin ningún tipo de restricción



Elaborado por: Antonela Suárez

Fig. 69 Ingreso a portales de banca en línea mediante navegador Tor

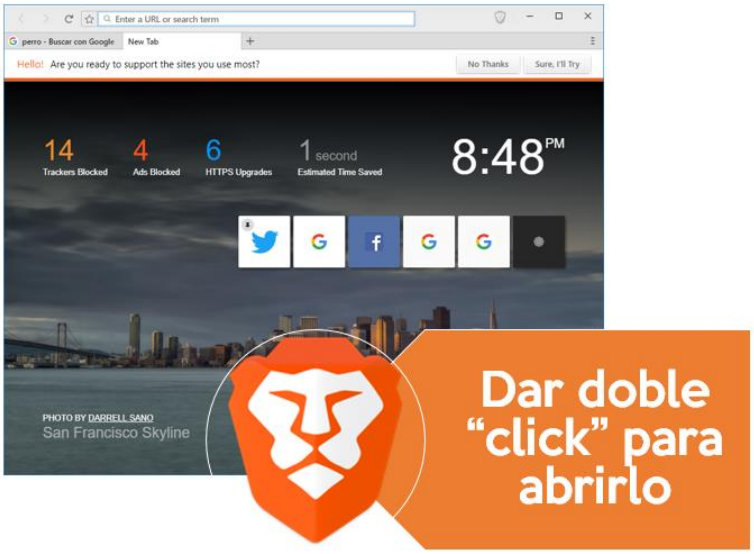


Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 70 Navegador Brave

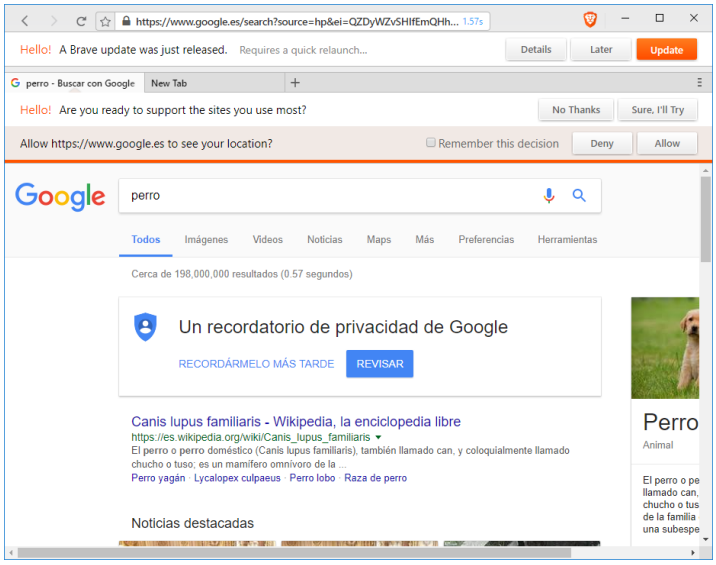
Para instalar este navedor solo hace falta ingresar a la pagina y oprimir en “descargar” se ejecutará la instalación como cualquier programa. Al finalizar la instalación se mostrará el siguiente ícono en la pantalla



Elaborado por: Antonela Suárez

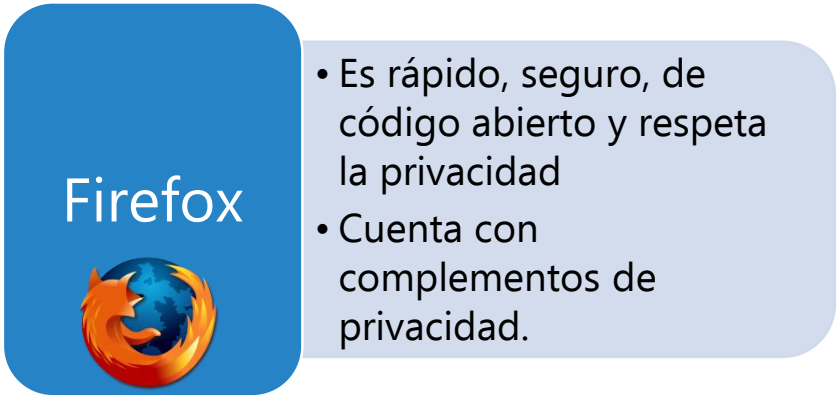
Fig. 71 Ejecución navegador Brave

Brave permite la navegación mediante Google, pero el buscador de google recalca el uso de la privacidad



Elaborado por: Antonela Suárez

Fig. 72 Búsquedas mediante buscador de Google en Brave



Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 73 Navegador Firefox

Si bien Firefox es una de las opciones mas sencilla de usar, es necesario implementar pluggins que ayuden a salvaguardar la privacidad.

Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 74 Complementos para incrementar la privcacidad de un navegador

Motores de Búsqueda

Los motores de búsqueda como Google o Bing, almacenan la información de la persona que está usándolo, así como el historial de cada página que visita así este utilizando el modo incognito provisto en distintos navegadores. A continuación se presentan motores de búsqueda que respetan la privacidad de los usuarios

DUCKDUCKGO

- Utiliza un rastreador propio que no guarda la información del usuario
- La publicidad que muestran no es personalizada y va a destinada a financiar el buscador.
- No almacena datos mediante ningún tipo de cookies, por lo que no tendrán información como la procedencia geográfica, idioma, hábitos o gustos
- Disponible en diferentes buscadores Firefox, Chrome, IE,

StarPage

- Google busca los resultados, con completa protección de la privacidad. Detrás de StartPage hay una compañía europea que está obsesionada con la privacidad desde 2006.

Fuente: (Victorhck, 2016)

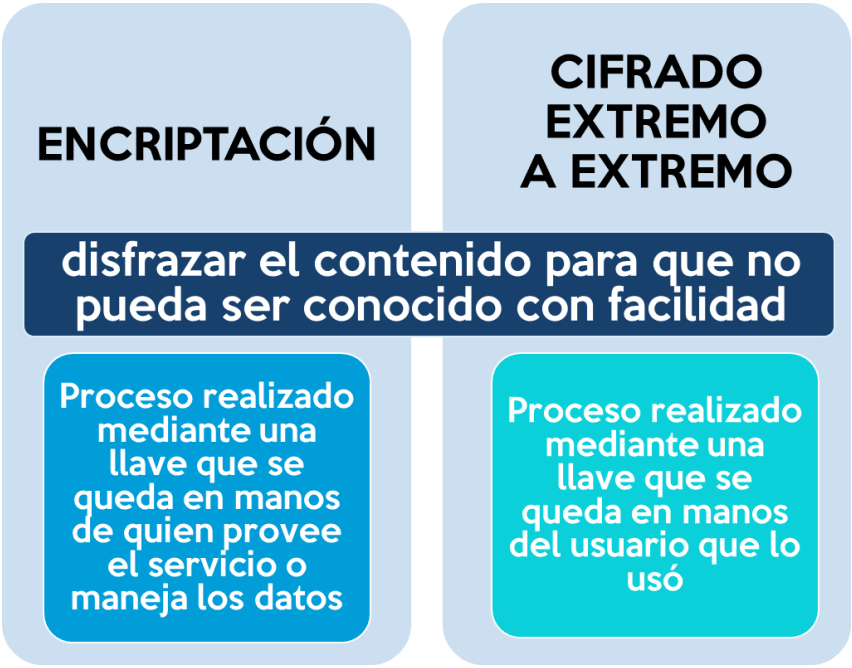
Elaborado por: Antonela Suárez

Fig. 75 Motores de búsqueda en favor de la privacidad

- **Mensajería instantánea cifrada**

  Optar por herramientas que oculten la información que enviada mediante la red, para evitar que otros puedan leer las conversaciones de los usuarios, revisar sus archivos etc.

  Se tiene:



Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 76 Tipos de Cifrado

- ***Chats Privado***

Aplicaciones que utilizan encriptación para el paso de mensajes, imágenes, etc. Sin embargo quien provee el servicio puede acceder a la información a su vez entregar a otras entidades completamente descifradas

Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 77 Aplicación mensajería encriptada

- ***Chat privado sin rastros***

Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 78 Aplicaciones mensajería instantanea cifradas punto a punto

Chats y video conferencias privadas

Existen sitios web que ofrecen servicios de mensajería con cifrado extremo a extremo

Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 79 Mensajería instantánea, video y voz cifrados punto a punto

- **Sistemas operativos**

TAILS

Es un sistema operativo que preserva tu privacidad y anonimato

Internet Anónimo	•Burlar la censura casi donde quiera, sin dejar pistas.
Aplicaciones pre configuradas	•Su configuración implica que las aplicaciones con salida al internet salgan a través de TOR
No requiere Instalación	•Puede ejecutarse desde un CD o Memoria Flash •Cambia su apariencia a un tema similar a Windows XP

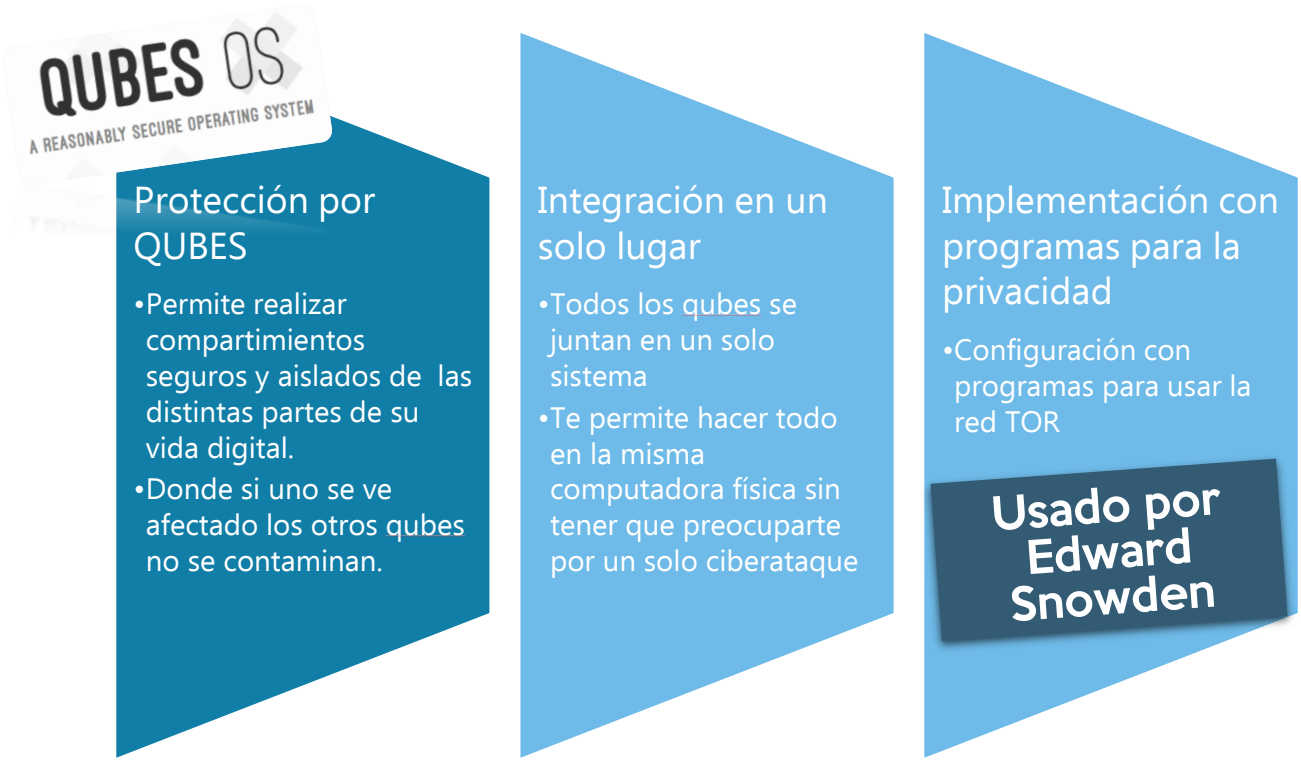
Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 80 ¿qué es Tails?

QUBES OS

Es un sistema operativo que permite resguardarte mediante espacios independientes.



Fuente: (Victorhck, 2016)

Elaborado por: Antonela Suárez

Fig. 81 ¿qué es QUBES OS?

CAPÍTULO 5

Conclusiones y Recomendaciones

5.1. Conclusiones

- Los conceptos sobre privacidad y transparencia requieren de un nuevo concepto que se ajuste al uso de medios digitales y más aun de internet.

- El internet ha sido uno de los componentes tecnológicos más penetrante en los últimos veinte años, su auge ha sido tal que más del 80% de los dispositivos cuentan con acceso a él. Internet ha permitido múltiples investigaciones sin embargo ha servido como instrumento para realizar vigilancia masiva y reprimir la libertad de expresión por parte de los gobiernos. La privacidad de las personas ha sido descuidada y las compañías no tienen respeto por la información de sus usuarios con tal de obtener productos con gran demanda.

- El Ecuador no se encuentra preparado en lo referente a la protección de datos, su único accionar frente a las revelaciones sobre el espionaje realizado por Estados Unidos y otros países poderosas ha sido presentar un proyecto de ley; el cual continua en revisiones por parte de la Asamblea Nacional y mientras tanto los datos y a su vez la información no cuentan con ningún tipo de respaldo, ni existe instituciones que protejan a los usuarios de Ecuador frente abusos por parte compañías extranjeras.

- A nivel de transparencia el país tiene un largo camino por recorrer, si bien, dio pequeños pasos en el año 2013 permitiendo que los datos se vuelvan abiertos y gratuitos en algunos aspectos con el paso de los años y la

administración del gobierno anterior se han ido cerrando y resguardando la información. Por otro lado, muchas compañías y universidades del país no contribuyen a la liberación de datos que sean útiles para investigaciones y desarrollo de productos futuros.

- Por otro lado, el conocimiento acerca temas de privacidad de datos continúa siendo muy poco al igual que en el año 2015 donde se realizó una investigación por parte de la Universidad Politécnica Nacional sobre la noción en temas de privacidad de datos. El desconocimiento sobre el tema se mantiene y el impacto sobre los individuos al hablar sobre lo que pasa en internet con la información genera temor.

- Dentro de internet se encuentran ahora múltiples comunidades que abordan estos temas y que quieren fomentar una cultura que exija a sus autoridades sobre la privacidad de la información y que aportan con herramientas y guías al usuario para el uso de estas en forma fácil y gratuita.

- Al momento de tabular los resultados de la encuesta se evidenció el conformismo de los usuarios frente a la vigilancia masiva además del desconocimiento sobre el contenido de las políticas de privacidad de datos presente en todas las aplicaciones y redes sociales más usadas hoy en día.

- Existen múltiples herramientas para asegurar la privacidad en línea, pero la mayoría de estas requieren de configuraciones de expertos y conocedores de tecnología por lo que los usuarios comunes encuentran trabas al intentar usarlas.

5.2. Recomendaciones

- Las universidades en sus carreras orientadas a la tecnología deberían implementar en su enseñanza la importancia de la protección de los datos y como deberían desarrollar software que mantengan la privacidad además de que se presenten al usuario de forma sencilla y entendible.

- Es importante fomentar y educar en temas de privacidad de datos dado que es la única manera de asegurar un futuro estable del internet.

- Difundir sobre los peligros que representa publicar datos personales es uno de las formas de crear conciencia en los jóvenes de hoy para que regulen la cantidad de material que publican y difunden en redes sociales y aplicaciones.

- La transparencia debe ser implementada en cada una de las instituciones privadas y gubernamentales para conocimiento de los usuarios. Es fundamental concientizar a los usuarios de las herramientas que tienen a mano frente a esta.

- Ecuador debe optar por la creación de una legislación adecuada para crear datos personales basada en la legislación de Uruguay pioneros en la protección de datos en Latinoamérica.

- Se recomienda continuar con el desarrollo de guías más amplias para el manejo de herramientas que ayuden a preservar la privacidad.

Bibliografía

López Ponce, J. (27 de Septiembre de 2010). *¿Sabías que tu ordenador tiene una huella digital?* Obtenido de Rizomática: http://www.rizomatica.net/sabias-que-tu-ordenador-tiene-una-huella-digital/

¿qué es y para que sirve la transparencia gubernamental? (2012). Obtenido de LauraRojasH-Senadora: http://www.laurarojash.net/que-es-y-para-que-sirve-la-transparencia-gubernamental/

¿qué son los datos sensibles? (s.f.). Obtenido de Centro de Protección de Datos Personales. Ciudad Autónoma de Buenos Aires.: http://www.cpdp.gob.ar/index.php?view=items&cid=1%3Afcat_cpdp&id=7%3Afac_Qu%C3%A9+son+los+datos+sensibles&option=com_quickfaq&Itemid=72

¿Qué sucede en internet cada minuto? . (23 de Marzo de 2017). Obtenido de El Economista: http://www.eleconomista.es/tecnologia/noticias/8236038/03/17/Que-sucede-en-internet-cada-minuto-De-900000-accesos-a-Facebook-a-35-millones-de-busquedas-de-Google.html

AGPD. (2013). *Protección datos en el mundo.* Obtenido de AGDP: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php

Alarcon, S. (28 de Enero de 2013). *Tor basics in plain English.* Obtenido de stephalarcon: http://www.stephalarcon.org/tag/tor/

Alorza. (28 de Marzo de 2013). *Tres tipos de transparencia*. Obtenido de Administraciones en Red: https://eadminblog.net/2012/03/28/tres-tipos-de-transparencia/

ANDES. (06 de Junio de 2016). *Investigación del canal regional TeleSur devela injerencismo de la CIA en Ecuador*. Obtenido de ANDES: http://www.andes.info.ec/es/noticias/investigacion-canal-regional-telesur-devela-injerencismo-cia-ecuador.html

ASAMBLEA NACIONAL. (2016). Análisis y Comentarios sobre el proyecto de Ley de Protección de Datos Personales en Ecuador. En A. NACIONAL, *Principios generales* (pág. 18). Quito.

Assange, J. (2013). Privacidad para el débil, transparencia para el poderoso. En J. Asange, *Criptopunks, La Libertad y el Futuro de Internet* (págs. 121- 126). Montevideo: Tilce.

Baraniuk, C. (15 de Octubre de 2014). *What will the internet look like in 2040*. Obtenido de bbc: http://www.bbc.com/future/story/20141015-will-we-fear-tomorrows-internet

Barreto, D. (01 de Septiembre de 2015). *Reacción de Antonio Ricaurte: 'Carla es una mujer inteligente, le pido disculpas por lo que está atravesando'*. Obtenido de El Comercio: http://www.elcomercio.com/actualidad/antonioricaurte-declaraciones-video-redessociales-carlacevallos.html

Bertoni, J. M. (15 de Diciembre de 2014). *La censura en Ecuador llegó a Internet*. Obtenido de JuicioCrudo: http://www.juiciocrudo.com/articulo/la-censura-en-ecuador-llego-a-internet/1373

Birnbaum, M. H. (2004). Human research and data collection via the Internet. *Annual review of psychology*, 33.

Bonifaz, R. (11 de Marzo de 2013). *Software Libre, Criptografía y Privacidad*. Obtenido de Rafael Bonifaz Software libre, criptografía, privacidad y algo más: https://rafael.bonifaz.ec/blog/2013/03/software-libre-criptografia-y-privacidad/

Breene, K. (17 de Enero de 2016). *What is the future of the internet?* Obtenido de World Economic Forum: https://www.weforum.org/agenda/2016/01/what-is-the-future-of-the-internet/

Camacho, V. E. (20 de Febrero de 2016). *Deep web, el otro lado del Internet.* Obtenido de El Telégrafo: http://www.eltelegrafo.com.ec/noticias/de7en7/35/deep-web-el-otro-lado-del-internet

Carpizo, J. (2000). Derecho a la información y derechos humanos. En J. y. Carpizo, *Derecho a la información y derechos humanos* (págs. 3-4). México: UNAM.

Caruso, D. (2005). *¿ QUÉ ES INTERNET?* Obtenido de Localizacion de informacion especifica en la web: https://books.google.com.ec/books?hl=es&lr=&id=9fsgpKPvKuwC&oi=fnd&pg=PA2&dq=que+es+internet&ots=vHYkMqbLgH&sig=c-owfdkMZUVCwBRNSspL2oOGyus&redir_esc=y#v=twopage&q&f=false

Castells, M. (2001). *INTERNET Y LA SOCIEDAD RED*. Obtenido de UOC: http://www.uoc.edu/web/cat/articles/castells/castellsmain10.html

CEPAL. (12 de Septiembre de 2016). *CEPAL: Aumenta fuertemente el uso y el acceso a Internet en América Latina y el Caribe*. Obtenido de Comisión Economica para América Latina y el Caribe: http://www.cepal.org/es/comunicados/cepal-aumenta-fuertemente-uso-acceso-internet-america-latina-caribe

Ciespal, J. (2014). Protección de datos y privacidad en procesos electorales, hacia la Declaración de Ecuador y unificación de criterios. Quito.

CNNEspañol. (04 de Octubre de 2016). *Las 10 filtraciones más importantes de WikiLeaks en sus 10 años.* Obtenido de CNN Español: http://cnnespanol.cnn.com/2016/10/04/las-10-filtraciones-mas-importantes-de-wikileaks-en-sus-10-anos/

Colamarco, J. (20 de Septiembre de 2016). *Análisis y Comentarios sobre el proyecto de Ley de Protección de Datos Personales en Ecuador*. Obtenido de Legaltech: http://legaltech.com.ec/analisis-y-comentarios-sobre-el-proyecto-de-ley-de-proteccion-de-datos-personales-en-ecuador/

Cuadros, X. (19 de Septiembre de 2016). *BREVE ANÁLISIS DEL PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR.* Obtenido de Blog Jurídico Digital: https://xaviercuadros.com/2016/09/19/breve-analisis-del-proyecto-de-ley-de-proteccion-de-datos-personales-en-el-ecuador/

Desenmascarando PelucoLeaks. (03 de Julio de 2015). Obtenido de YouTube: https://www.youtube.com/watch?v=25w-car-Qko

Ecuadorenvivo. (17 de Agosto de 2016). *Enrique Ayala Mora: "¿Quién entregó (mis facturas) a Correa, sus esbirros y hasta a los trolls?"*. Obtenido de Ecuadorenvivo: http://ecuadorenvivo.com/politica/83-videos/50517-enrique-ayala-mora-quien-entrego-mis-facturas-a-correa-sus-esbirros-y-hasta-a-los-trolls-exrector-de-la-universidad-andina-anuncia-acciones-legales-en-contra-del-sri-si-no-responden-su-cuestionamiento.html

El manual de Open Data. (2016). Obtenido de Open Knowledge International: http://opendatahandbook.org/guide/es/

El Telegrafo. (06 de Agosto de 2017). *La neutralidad de internet garantiza una navegación sin ninguna restricción.* Obtenido de El Telegrafo: http://www.eltelegrafo.com.ec/noticias/tecnologia/30/la-neutralidad-de-internet-garantiza-una-navegacion-sin-ninguna-restriccion

El Telégrafo;. (06 de Enero de 2014). *La NED de EE.UU. financiará proyecto mediático en Ecuador*. Obtenido de El Telégrafo: http://www.eltelegrafo.com.ec/noticias/politica/2/la-agencia-tamia-news-se-construiria-como-soporte-para-una-red-internacional-de-medios-de-oposicion

El Universo. (12 de Marzo de 2017). *Violación a la intimidad, entre delitos por difusión de videos en redes sociales*. Obtenido de El Universo: http://www.eluniverso.com/noticias/2017/03/12/nota/6084508/violacion-intimidad-delitos-difusion-videos

El Universo;. (30 de Noviembre de 2012). Bloguero detenido por usar datos del presidente Correa en sistema Dato Seguro. *El Universo*.

ElComercio.com. (03 de Diciembre de 2015). *Usuarios de Twitter denuncian que sus fotos no se visualizan en Ecuador*. Obtenido de El Comercio: http://www.elcomercio.com/actualidad/usuarios-twitter-denuncian-fotos-visualizacion.html

ESET. (15 de Octubre de 2015). *Guía de Privacidad en Internet.* Obtenido de WeLiveSecurity: https://www.welivesecurity.com/wp-content/uploads/2015/09/guia-privacidad-internet-eset.pdf

ESET. (24 de Marzo de 2017). *8 datos clave sobre el Reglamento General de Protección de Datos (GDPR)*. Obtenido de WeLiveSecurity: https://www.welivesecurity.com/la-es/2017/03/24/claves-reglamento-general-de-proteccion-de-datos/

Estrada, J. A., Estrada, J. C., Rodríguez, A., & Tipantuña, C. (2015). Ecuador y la Privacidad en Internet: Una Aproximación Inicial. *Revista Politécnica*, 9.

Falconí, J. C. (2008). Derechos Constitucionales a la intimidad, privacidad y la imagen. *Derecho Ecuador*, 20.

Fernández De Lis, P. (18 de Mayo de 2007). 25 países ejercen la censura en Internet. *El País*.

Florez, A. (s.f.). *MARCO MODELO DE NEUTRALIDAD DE LA RED.* Obtenido de Centro de Estudios en Libertad de Expresión y Acceso a la Información : http://www.palermo.edu/cele/pdf/MODEL-NEUTRALITY.pdf

Fundación Mil Hojas;. (14 de Julio de 2015). *Así funciona Hacking Team en Ecuador*. Obtenido de Fundación Mil Hojas: http://milhojas.is/612318-asi-funciona-hacking-team-en-ecuador.html

Fundación Via Libre Argentina. (9 de Noviembre de 2015). Obtenido de 1.3.Algunos malentendidos sobre la privacidad: “no tengo nada para ocultar”: https://canvas.instructure.com/courses/981219

FUNDAMEDIOS. (13 de Agosto de 2017). *Amenazas y suplantación de identidad tras publicar un mensaje al exPresidente*. Obtenido de FUNDAMEDIOS: http://www.fundamedios.org/alertas/amenazas-suplantacion-identidad-tras-publicar-mensaje-al-presidente/

Fundamedios. (06 de Junio de 2017). *ExPresidente expone datos personales de periodista, molesto por comentario en Twitter*. Obtenido de Fundamedios: http://www.fundamedios.org/alertas/expresidente-expone-datos-personales-de-periodista-molesto-por-comentario-en-twitter/

Fundamedios. (08 de Agosto de 2017). *Fundamedios condena censura de Twitter tras suspensión de cuenta de Crudo Ecuador*. Obtenido de Fundamedios: http://www.fundamedios.org/alertas/fundamedios-condena-censura-twitter-tras-suspension-cuenta-crudo-ecuador/

Goldfarb, R., Cole, D., Wasserman, E., Blanton, T., Carter, H., Mills, J., & Siegel, &. B. (2015). *After Snowden: Privacy, Secrecy, and Security in the Information Age. .* Nueva York: St. Martin´s Press.

Gonzáles, M. S. (17 de 09 de 2013). *Historia de Internet - Nacimiento y Evolución*. Obtenido de Redes Telemáticas: http://redestelematicas.com/historia-de-internet-nacimiento-y-evolucion/

González, E. G. (2016). *BIG DATA, PRIVACIDAD Y PROTECCIÓN DE DATOS.* Madrid: IMPRENTA NACIONAL DE LA AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO.

González, M. (11 de Noviembre de 2014). *Neutralidad de la red: qué es, cómo se vulnera y la situación en los principales países*. Obtenido de XATAKA: https://www.xataka.com/aplicaciones/neutralidad-de-la-red-que-es-como-se-vulnera-y-la-situacion-en-los-principales-paises

Gonzalo, M. (10 de Marzo de 2015). Proyecto Tor: cómo es la comunidad alrededor de la red que resiste a la NSA. *Diario Turing*.

Greenwald, G. (2014). *Snowden, Sin un lugar donde esconderse .* Buenos Aires: Ediciones B.

Gutiérrez, E. G. (2008). *La Transparencia.* México: Nostra Ediciones.

HOTT, F. V. (12 de Junio de 2014). *¿Por qué es importante defender la neutralidad de la red?* Obtenido de Derechos Digitales: https://www.derechosdigitales.org/7497/por-que-es-importante-defender-la-neutralidad-de-la-red/

IABSPAIN. (12 de Julio de 2016). *Preguntas frecuentes sobre el Marco de Protección de Datos entre Unión Europea- Estados Unidos (Privacy Shield).* Obtenido de IABSPAIN: http://www.iabspain.net/wp-content/uploads/downloads/2016/07/FAQS-Privacy-Shield-IAB.pdf

Jaramillo, F. (28 de Enero de 2014). *La protección de datos personales en Ecuador.* Obtenido de infodf:

http://www.infodf.org.mx/dp/doctos/14/presenta/dia28/ecuador_fabian_jaramillo.pdf

Jiménez Cano, R. (16 de Junio de 2011). *¿Cómo será Internet en el futuro?* Obtenido de ElPais: https://elpais.com/tecnologia/2011/06/16/actualidad/1308214870_850215.html

John Scott-Railton, M. M.-B. (Diciembre de 2015). *PACKRAT Seven Years of a South American Threat Actor*. Obtenido de Citizen Lab: https://citizenlab.ca/2015/12/packrat-report/

KNOWLEDGE, O. (2013). *Open Knowledge.* Obtenido de OPEN GLOBAL DATA INDEX: http://2015.index.okfn.org/place/ecuador/2013/

La Hora. (22 de Septiembre de 2017). La larga historia de una pieza política llamada Senain. *La Hora*.

Latinobarómetro. (2015). *Latinobarómetro*. Obtenido de Latinobarómetro: http://www.latinobarometro.org/latOnline.jsp

Lewis, L., & Callahan, C. (2 de Agosto de 2017). *What Happens in an Internet Minute in 2017?* Obtenido de visualcapitalist: http://www.visualcapitalist.com/happens-internet-minute-2017/

Ley Orgánica de Protección de Datos de Personales. (2007). *Ley Orgánica de Protección de Datos de Personales.* Obtenido de Ley Orgánica de Protección de Datos de Personales: https://alojamientos.uva.es/guia_docente/uploads/2013/458/42907/1/Documento7.pdf

Licklider, J. C. (2002). Historia de Internet., (pág. 14). Boston.

Lynch, A. B. (31 de Agosto de 2012). *El derecho a la privacidad.* Obtenido de CATO: https://www.elcato.org/el-derecho-la-privacidad

MARGETTS, H. (2011). The Internet and Transparency. *Political Quarterly,*, 82(4), 518-521.

Martinez, R. (Septiembre de 2016). Privacidad y Protección de Datos. La Rioja, España.

Mediano, S. (30 de Noviembre de 2016). *Guía sobre los procedimientos de anonimización de datos personales*. Obtenido de Santiago Mediano Abogados: http://www.santiagomediano.com/guia-sobre-procedimientos-anonimizacion-datos-personales/

Mendoza, M. Á. (2 de Marzo de 2017). *El Derecho a la Privacidad en la Era Digital*. Obtenido de Welivesecurity de ESET: https://www.welivesecurity.com/la-es/2017/03/02/derecho-a-la-privacidad-era-digital/

Nila, D. (04 de Agosto de 2013). *Leyes de protección de datos personales en el mundo y la protección de datos biométricos.* Obtenido de Portada Informática: https://darionila.wordpress.com/2013/08/04/leyes-de-proteccion-de-datos-personales-en-el-mundo-y-la-proteccion-de-datos-biometricos/

Open Knowledge. (2015). *Open Knowledge.* Obtenido de Global Open Data Index: http://2015.index.okfn.org/dataset/

Pastor, J. (10 de diciembre de 2015). *Cómo ha cambiado internet después de las filtraciones de Snowden*. Obtenido de xalaka: http://www.xataka.com/privacidad/como-ha-cambiado-internet-despues-de-las-filtraciones-de-snowden

Piscitelli, A. (2005). La dinámica de la web . En A. Piscitelli, *Internet, la imprenta del siglo XXI* (pág. 20). Barcelona: Editorial Gedisa.

Puron, D. (2017). *¿Eres consciente de la privacidad en internet?* Obtenido de ABC TECONOLOGÍA: http://www.abc.es/tecnologia/redes/20150128/abci-proteccion-datos-personas-wearables-201501271726.html

Quian, A. (2013). *El impacto mediático y político de WikiLeaks.* Barcelona: UOC.

Rainie, L., & Anderson, J. (18 de Diciembre de 2014). *The Future of privacy*. Obtenido de PEW RESEARCH CENTER Internet & Technology: http://www.pewinternet.org/2014/12/18/future-of-privacy/

Real Academia Española. (2001). *Diccionario de la lengua española (22.a ed.)*. Obtenido de Diccionario de la lengua española: http://dle.rae.es/?id=LvskgUG

REDACCIÓN PERU21. (01 de Octubre de 2015). *70% de las transacciones por Internet ya se hacen desde celulares y tablets*. Obtenido de Peru21: https://peru21.pe/mis-finanzas/70-transacciones-internet-celulares-tablets-198683

Reyes, S. (17 de Noviembre de 2016). *Exjueza Collantes no llamó a ningún poderoso tras denuncia, según Fiscal provincial del Guayas*. Obtenido de El Comercio: http://www.elcomercio.com/actualidad/exjueza-lorenacollantes-llamada-poderoso-guayaquil.html

RGPD. (s.f.). *Reglamento General de Protección de Datos Y listado de empresas de protección de datos* . Obtenido de Reglamento General de Protección de Datos : http://rgpd.es/

Rivera, N. (15 de Marzo de 2016). *Cronología del caso Edward Snowden, el hombre más buscado del mundo*. Obtenido de Hipertextual: https://hipertextual.com/2016/03/cronologia-edward-snowden

Rivera, N. (02 de Febrero de 2017). *Usando internet en China durante una semana: una pradera repleta de vallas*. Obtenido de Hipertextual: https://hipertextual.com/2017/02/internet-china

Rodriguez, J. (2015). *Flickr.* Obtenido de Flickr- Snowden: https://www.flickr.com/photos/truthout/14348649238

Romero, P. (2013). *Una visión de Criptopunks. La libertad y el futuro del Internet.* Santiago de Chile: LOM Ediciones.

Rotenberg, M. S. (2015). *Privacy in the Modern Age.* New York: The New Press.

Rotta, S. L. (q de Junio de 2915). *El mundo despúes de snowden*. Obtenido de El Espectador: http://www.elespectador.com/jscroll_view_entity/node/563960/full/x563960-559212-560363-p564120

Rozas, C. (2013). *Criptografía, que es uso y beneficios.* Obtenido de http://www.neuquen.gov.ar/seguridadinformatica/pdf/Criptografia,%20que%20es,%20usos%20y%20beneficios%20-%20Claudia%20Rozas.pdf

Sánchez Pérez, G., & Rojas González, I. (2016). Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I. *revista.seguridad.unam*, 3. Obtenido de https://revista.seguridad.unam.mx/node/2124

SANTOS, E. (10 de Noviembre de 2016). *Esto es lo que cuesta saltarse la censura en internet*. Obtenido de Genbeta: https://www.genbeta.com/a-fondo/esto-es-lo-que-cuesta-saltarse-la-censura-en-internet

Sarmiento, S. A. (05 de Febrero de 2017). *¿Cuál es el Futuro de Internet? 5 predicciones*. Obtenido de youngmarketing: http://www.youngmarketing.co/el-internet-que-tendremos-en-25-anos/

Schunter, M. (06 de Junio de 2013). *Data Security and Privacy in2025?* Obtenido de Schunter: https://www.schunter.org/blog/wp-content/uploads/2013/06/SecurityAndPrivacy2025-final-2013-06-06-1.pdf

Taiwán primer lugar en el mundo en acceso a datos abiertos del gobierno. (12 de Mayo de 2017). Obtenido de Taiwan Republic of China: http://www.roc-taiwan.org/mx_es/post/15552.html

TEDIC. (8 de Febrero de 2016). *Sin privacidad, no hay Internet segura*. Obtenido de TEDIC: https://www.tedic.org/sin-privacidad-no-hay-internet-seguro/

Ucha, F. (10 de Marzo de 2010). *Transparencia*. Obtenido de Definición ABC: https://www.definicionabc.com/general/transparencia.php

Usuarios Digitales, & Fundación 1000 Hojas. (11 de Octubre de 2016). *Informe sobre privacidad y acceso al internet.* Obtenido de fundamedios: http://www.fundamedios.org/wp-content/uploads/2016/10/11.-EPU-Informe-sobre-privacidad-i-acceso-al-internet-Mil-hojas-y-Derechos-Digitales.pdf

Véliz, C. (05 de Junio de 2014). *¿Por qué es importante la privacidad?* Obtenido de HuffingtonPost: http://www.huffingtonpost.es/carissa-veliz/por-que-es-importante-la-_b_5408354.html

Victorhck. (05 de Septiembre de 2016). *Herramientas y software para proteger la privacidad en la red.* Obtenido de Herramientas y software para proteger la privacidad en la red: https://victorhckinthefreeworld.com/2016/05/09/herramientas-y-software-para-proteger-la-privacidad-en-la-red/

Villaescusa, R. R. (Dieciembre de 2012). ¿Qué es transparencia? *Biolex. Revista del Departamento de Derecho de la Universidad de Sonora* , pág. 17. Obtenido de https://works.bepress.com/ramirezvillaescusa/3/

WeAreSocial. (Enero de 2012). *We Are Social's Guide to Social, Digital and Mobile Around the World* . Obtenido de WE ARE SOCIAL: https://www.slideshare.net/wearesocialsg/we-are-socials-guide-to-social-digital-and-mobile-around-the-world-jan-2012/2-JAN2012_WORLDWIDE_USER_NUMBERS_6809560473

WeAreSocial. (Enero de 2014). *SOCIAL, DIGITAL & MOBILE WORLDWIDE IN 2014*. Obtenido de WeAreSocial: https://wearesocial.com/uk/special-reports/social-digital-mobile-worldwide-2014

WeAreSocial. (27 de Enero de 2016). *DIGITAL IN 2016*. Obtenido de WeAreSocial: https://wearesocial.com/uk/special-reports/digital-in-2016

WeAreSocial. (24 de Enero de 2017). *WeAreSocial.* Obtenido de WeAreSocial: https://wearesocial.com/special-reports/digital-in-2017-global-overview

Zamorano, E. (23 de Abril de 2014). *Senado brasileño aprueba unánimemente "La Constitución de Internet"*. Obtenido de Fayerwayer: https://www.fayerwayer.com/2014/04/senado-brasileno-aprueba-unanimemente-la-constitucion-de-internet/

Zuazo, N. (2015). *Guerras de Internet.* Buenos Aires: Debate .