ICONOS

Instituto de Investigación en Comunicación y Cultura

EL ANONIMATO COMO DEFENSA DE LA PRIVACIDAD DIGITAL

TESIS

QUE PARA OBTENER EL TÍTULO DE LICENCIATURA EN COMUNICACIÓN DIGITAL

PRESENTA:
JOSÉ LUIS FLORES GONZÁLEZ

ASESOR:
ROSELENA VARGAS VELASCO

Ciudad de México Mayo, 2018

RECONOCIMIENTO DE VALIDEZ OFICIAL DE ESTUDIOS DE LA SECRETARÍA DE EDUCACIÓN PÚBLICA SEGÚN ACUERDO NO. 20090956, CON FECHA DEL 16 DE OCTUBRE DE 2009. CLAVE 2008

Contenido

Índice de tablas

Índice de imágenes

Introducción

> Todo aquel que no quiera que las cosas que dice estén conectadas a su identidad permanente tiene interés en el anonimato. Puede que estén preocupados por retribuciones políticas o económicas, acoso, o incluso amenazas a sus vidas, o pueden usar el anonimato como parte de su expresión o desarrollo personal…
>
> Katitza Rodríguez
> Electronic Frontier Foundation

El uso de Internet en México ha aumentado considerablemente en los últimos años. Las personas que dentro de él navegan, comparten allí información de carácter privado todos los días de manera consciente o inconsciente, lo que puede poner en riesgo su libertad, prestigio, patrimonio, seguridad e integridad física y moral, como consecuencia del uso que terceros puedan hacer de ella.

Por esta razón, se planteó como objetivo principal de la investigación aquí vertida, **identificar los elementos que vulneran la privacidad de las personas en Internet y analizar la pertinencia del anonimato como medio para preservarla.**

Todo en aras del uso seguro de Internet; no sólo por periodistas, activistas o defensores de derechos humanos, sino por los usuarios en general, que pudieran llegar a ver también comprometida su privacidad, y en consecuencia, exponerse a los riesgos mencionados, o ser influenciados en sus decisiones y elecciones sin percatarse de ello, ante el desconocimiento de cómo funciona Internet.

A razón de lo anterior se eligieron las siguientes preguntas de investigación: **¿qué elementos vulneran la privacidad de las personas en Internet?,** y **¿qué medidas a considerar por el usuario pueden garantizar su**

privacidad digital en Internet? Que permitieron descubrir que usuarios y empresas en Internet, desconocen sus derechos y obligaciones respecto del cuidado de los datos personales, pese a lo que, los primeros comparten información con los segundos. Que existen riesgos comprobables en territorio nacional para los internautas como consecuencia de su interacción en la red, que abarcan; por mencionar algunos, la vigilancia, espionaje, extorsión, fraude, robo e interferencia en las decisiones; aunque también, existen distintas herramientas capaces de contribuir a la privacidad y al anonimato digital, entre las que se encuentran**:** buscadores, complementos para navegadores, redes sociales digitales y sistemas operativos, entre otros.

Para despejar ambas incógnitas se definió que es la intimidad y el derecho a la intimidad, asociados con los conceptos de zona y esfera reservada, lo secreto y lo oculto; los límites a terceros, depositarios de esa información, y se ubicó que son los datos personales, y qué involucra su protección, esto, a través de la información disponible en el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI), así como de los conceptos jurídicos adoptados en el mismo sentido, dentro del territorio nacional.

Sin dejar de lado la distinción entre intimidad y privacidad, sus similitudes, diferencias y el porqué de su uso, se abordó la reconfiguración de la segunda en el ámbito digital.

Definido lo anterior, se obtuvo certidumbre sobre la información de valor comprendida dentro de la privacidad, cómo se entiende ésta y su importancia en el mundo digital. Gracias a ello fue posible conocer qué de esta información se comparte en la red por parte de los usuarios y si se hace de manera consciente o inconsciente. Para dicho fin se retomaron algunos

trabajos de investigación realizados previamente, como el de la Asociación Mexicana de Internet (AMIPCI), que interrogó a usuarios y empresas del país para abundar en su conocimiento del tema, además de sus prácticas.

Se señalaron y ejemplificaron las formas en que el usuario puede perder el control de su información, al transmitirla en la red, sin dejar de considerar los peligros latentes que esto conlleva, para lo cual se tomaron en cuenta publicaciones de sitios informativos como WikiLeaks, investigaciones de empresas como Microsoft o Symantec, asociaciones no gubernamentales como ASI-México y pronunciamientos de activistas latinoamericanos preocupados por los derechos digitales, como Jesús Robles Maloof.

A fin de poder despejar la primera incógnita, previamente expuesta, se desarrolló la siguiente hipótesis: **ingresar y divulgar información personal en sitios y redes sociales digitales, por parte de los usuarios en Internet, supone la pérdida del control sobre ella, volviéndola accesible a terceros, posibilitando prácticas fraudulentas, intrusivas, acosadoras y de espionaje, además de limitar su libertad de expresión, en detrimento de su privacidad digital.**

Esto, tras inferir, que es el usuario la primer y principal figura de control de su información en lo físico y en lo digital, lo que le faculta para prevenir el daño en lugar de actuar en consecuencia, en la medida que esto sea posible.

Como resultado de los hallazgos vertidos en esta primera fase de la investigación y después de conocer claramente los conceptos, usos y riesgos para el usuario relacionados con su privacidad digital, la segunda parte de la investigación se centró en las medidas que posibilitan la salvaguarda de la misma. Lo que dio origen a la siguiente hipótesis, que dice: **bajo la figura del anonimato digital puede evitarse que empresas, gobiernos y**

terceros en México hagan mal uso de los datos personales de los usuarios, previniendo la pérdida de su privacidad digital.

Mediante el eje conductor de esta segunda hipótesis, se definió qué es el anonimato, para después hacer la distinción con el anonimato digital y en ese afán se retomaron los pronunciamientos de Katitza Rodríguez, máximo representante de la Electronic Frontier Foundation, asociación pro derechos digitales y pro anonimato digital; además de otras asociaciones y organizaciones.

Posteriormente se describieron las distintas formas del anonimato, comprendidas en el débil y el fuerte, además que se enunciaron sus posibilidades y desventajas.

El último apartado de esta investigación fue consecuencia de las respuestas adquiridas gracias a la primera y segunda pregunta.

Como consecuencia de los conocimientos adquiridos se enunciaron en la última parte de este documento, recomendaciones puntuales al usuario sobre si el anonimato es posible en aras de la defensa de la privacidad digital, así como los hallazgos que arrojó la propia investigación y que buscaron clarificar al usuario final las prácticas que pueden ponerle en riesgo, en mayor o menor medida, en todo lo que comprende el quehacer en Internet.

No está demás decir que la finalidad principal de este trabajo; además de verificar la viabilidad del anonimato digital, es divulgar los hallazgos, para que el usuario común, pueda obtener de manera sencilla y clara, conocimiento sobre las implicaciones de compartir información en la red; de la forma en que operan industrias, gobiernos y crimen imbuidos en el mundo digital; de los riesgos mayores y menores que sus prácticas implican; y de

las consideraciones necesarias que cada individuo debe hacer al momento de navegar en la Web, si es su deseo resguardar su privacidad. Lo anterior concebido bajo el objetivo de: **facilitar al usuario la proyección de su anonimato digital con un producto audiovisual que contribuya al conocimiento de estas posibilidades para su ejecución por parte de los usuarios interesados.**

Capítulo I. Privacidad digital y sus riesgos en México

El individuo contemporáneo, basa su vida social en gran medida en Internet, en específico en sitios web y redes sociales digitales, por este medio se informa y socializa. Es en este contexto que caben las preguntas: **¿se comparten datos personales al socializar en sitios web y redes sociales digitales?, ¿la privacidad es contemplada en sitios web y redes sociales digitales de Internet?, ¿en sitios web y redes sociales digitales de Internet se vulnera el derecho a la privacidad?**

Para poder explicar de qué formas puede ser vulnerada la privacidad digital de los usuarios en Internet, primero debe comprenderse qué es, por lo cual han de definirse la intimidad, el derecho a la intimidad, y su relación con los conceptos: dato personal y dato personal sensible, que tienen vigencia en el ámbito jurídico mexicano y que, a su vez, son vinculables con la idea de privacidad y privacidad digital. Dichas definiciones serán también abordadas con la profundidad necesaria, bajo el propósito de comprender su procedencia y particularidades, para finalmente determinar el porqué de su necesidad e importancia como garantía individual. Aproximaciones vertidas con el simple afán de que el lector reconozca la privacidad como su derecho, dentro y fuera de Internet. En dicho apartado ha de retomarse el pronunciamiento realizado por la Organización de las Naciones Unidas a ese respecto.

Enseguida se realizará una distinción y clasificación del tipo de información que los usuarios comparten y la recurrencia con la que lo hacen, así como los medios en que estás prácticas se llevan a cabo. Para ello, se expondrá el trabajo de investigación de la Asociación Mexicana de Internet (AMIPCI), que involucra a individuos y sus hábitos en Internet.

Estableciéndose las prácticas recurrentes e información compartida por los individuos, será oportuno enumerar y ponderar los diferentes riesgos que distintas organizaciones como Derechos Digitales, disponible en https://www.derechosdigitales.org/; y defensores de los derechos humanos como Jesús Robles Maloof, han denunciado y que se relacionan directamente con el tipo de datos personales y datos personales sensibles que el usuario comunica en Internet.

Como consecuencia de lo anteriormente expuesto se proyecta demostrar o invalidar la hipótesis objeto de este capítulo, que señala:

Ingresar y divulgar datos personales en sitios y redes sociales digitales, por parte de los usuarios en Internet, supone la pérdida de derechos sobre ellos, volviéndolos accesibles a terceros, posibilitando prácticas fraudulentas, intrusivas, acosadoras y de espionaje; y al no garantizarse su libertad de expresión, las personas son susceptibles de sufrir persecución por la información vertida, en detrimento de su privacidad digital.

I.I. Intimidad y derecho a la intimidad

Para que sea posible acceder al concepto de privacidad, sobre todo en la era digital, es necesario conocer sus aproximaciones y fronteras con otros términos. Es el caso del concepto de intimidad, que guarda una estrecha relación con la denominada privacidad, y del cual se desprenden otras nociones, como la protección de datos personales. Ideas vitales que es necesario comprender en su relevancia e importancia, a fin de garantizar el correcto resguardo de la información personal de los individuos.

La raíz etimológica de intimidad es el adverbio del latín *intus*, que significa *dentro de*. Por otra parte, la Real Academia de la Lengua Española (RAE) define a la intimidad como:

> 1. f. Amistad íntima.
>
> 2. f. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia. (Real Academia Española, Intimidad párrs.1–2)

A través del origen etimológico y de la segunda acepción que la RAE le otorga a la palabra, puede decirse que la intimidad es el grado superlativo de lo personal y que involucra el interior de los individuos, emocional e intelectualmente.

Según las consideraciones de Aristeo García González, especialista en transparencia, protección de datos personales, nuevas tecnologías, informática y derecho, dicho concepto tomó valía en la época burguesa del siglo XVIII, para limitar la injerencia de los poderes públicos en la esfera privada de las personas. (García 748)

El mismo autor, quién retoma a Georgina Battle, en su texto *El derecho a la intimidad privada y su regulación*, señala:

> La intimidad, marcada por un matiz individualista, era la facultad destinada a salvaguardar un determinado espacio con carácter exclusivo, y que consistía en un derecho del individuo a la soledad y "a tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella". (García 748)

Posteriormente, los movimientos sociales surgidos en el siglo XIX; que lograrían avances respecto de los derechos económicos, sociales y culturales, contribuirían a que finalmente, inmersos en la modernidad, la

intimidad fuera considerada un derecho, toda vez, que mediante ella debía garantizarse la libertad individual de las personas (García 746–748): *El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano - entendiéndose por propio y oculto la información que mantiene para sí mismo.* (García 748)

Bajo esta lógica debiera entenderse entonces a la intimidad como todo aquello del individuo que no es conocido o conocible por los demás, y que puede comprender pensamientos o acciones propias de su personalidad.

Por otra parte, Isabel Victoria Lucena Cid, profesora y doctora de Filosofía del Derecho y Política de la Universidad Pablo de Olavide de Sevilla, en su trabajo *La protección de la intimidad en la era tecnológica: hacia una reconceptualización,* señala*: Tradicionalmente se ha formulado la intimidad en términos de autonomía, secreto, libertad, desarrollo de la personalidad, sustrato inviolable de la dignidad personal, etc.* (Lucena 129)

Ambas posturas tienen en común el abundar en la individualidad, pero también, en la noción de ocultamiento o secrecía. Hablan de una concepción de la intimidad como un aspecto personalísimo, que debe estar exento de la intromisión de los demás.

Para poder proteger estos aspectos debieron imponerse por largo tiempo restricciones y límites, sin embargo, poco a poco comenzó a replantearse la noción, al considerar la información personal habida por otros.

Distintos pronunciamientos se hicieron escuchar, es uno de los más importantes, desde el punto de vista jurídico, el nacido de la letra de Samuel

Warren y Louis Brandeis en el artículo, *The right of privacy*[1], escrito en 1890 y en el que se tratan aspectos como la divulgación indebida de información personal por terceros y de las facultades de las que debieran gozar las personas para decidir hasta qué grado sus pensamientos, sentimientos y emociones, pueden ser comunicados (Warren; Brandeis 25–34):

> Bajo nuestro sistema político, nunca se puede forzar a alguien a expresarlos (salvo cuando se comparece como testigo); e incluso, cuando ha elegido expresarlos, retiene, por regla general, el poder de fijar los límites de la publicidad que se les podrá dar. (Warren; Brandeis 31)

Bajo esta nueva concepción el derecho a la intimidad comenzó a vislumbrar sus posibilidades de transformación y adecuación, abandonándose, por un lado, la mera noción de la limitación para dar cabida al control, mediante la decisión de qué se quiere compartir y qué no. (García 751)

Con la llegada de la informática y la elaboración cada vez mayor de bases de datos (que ya existían de manera análoga desde el medioevo), la manipulación extensa de información personal a través de computadoras, y por último, la llegada de Internet y los múltiples actores que en él participan (usuarios, gobiernos y empresas), estas adecuaciones han cobrado más vigencia que nunca.

Antonio Enrique Pérez Luño, filósofo y jurista del derecho español, citado por García González, puntualiza en ese sentido:

---

[1] En este apartado se entiende *privacy* como intimidad. Ambos conceptos han de esclarecerse en el numeral I.III.

> …la propia noción de intimidad o privacidad[2] es una categoría cultural, social e histórica. Por lo que ahora este concepto ha pasado de una concepción cerrada y estática de la intimidad a otra abierta y dinámica. Puesto que ahora se contempla la posibilidad de conocer, acceder y controlar las informaciones concernientes a cada persona. (García 751)

Lucena Cid, en un plano más acorde al presente y en similar tono, comenta respecto a la intimidad:

> … en la actualidad se reivindica como derecho del control de la información personal. Se demanda la protección de la información personal frente al potencial invasivo de las nuevas tecnologías, su almacenamiento, procesamiento, difusión y utilización en el ámbito telemático. (Lucena 129)

Finalmente, basado en Pérez Luño, en *Derechos humanos, Estado de derecho y Constitución*, García González acota:

> Consecuentemente, frente a una actual sociedad de la información, resulta insuficiente hoy concebir a la intimidad como un derecho garantista (estatus negativo) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla al mismo tiempo, como un derecho activo de control (estatus positivo) sobre el flujo de informaciones que afectan a cada sujeto. (García 751)

---

[2] Nótese que en este apartado se usan indistintamente las palabras intimidad y privacidad, su diferenciación se realizará en el numeral I.III..

Entendiéndose, en este caso, por estatus negativo, la simple capacidad de oponerse a la invasión de la privacidad; y derecho activo de control, a la posibilidad de tomar decisiones respecto de la información personal cuando se comparte con terceros o deposita en otros.

A fin de contribuir a la claridad del concepto en sus distintos matices y formas y sus modificaciones a lo largo del tiempo, se ha desarrollado la siguiente tabla:

Intimidad	**Características**	**Palabras clave**	**Aplicación**
RAE	Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.	Zona reservada Persona	General
Georgina Battle	La intimidad, marcada por un matiz individualista, era la facultad destinada a salvaguardar un determinado espacio con carácter exclusivo, y que consistía en un derecho del individuo a la soledad y "a tener una esfera reservada en el cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella".	Esfera reservada Individuo	Derecho - antecedentes

Isabel Victoria Lucena Cid	Tradicionalmente se ha formulado la intimidad en términos de autonomía, secreto, libertad, desarrollo de la personalidad, sustrato inviolable de la dignidad personal, etc.	Autonomía Secreto	Derecho - antecedentes
Antonio Enrique Pérez Luño	La propia noción de intimidad o privacidad es una categoría cultural, social e histórica. Por lo que ahora este concepto ha pasado de una concepción cerrada y estática de la intimidad a otra abierta y dinámica. Puesto que ahora se contempla la posibilidad de conocer, acceder y controlar las informaciones concernientes a cada persona.	Conocer Acceder Controlar Informaciones Persona	Derecho - presente

Tabla 1. Comparativa del concepto de intimidad y concepto derecho a la intimidad, por autor. Elaboración propia.

En el desglose anterior se aprecia de manera clara la asociación del concepto con zona y esfera reservada, con lo secreto y lo oculto, ya sea de personas, seres humanos o individuos; todos señalan la pertinencia de un límite ante la información personal que cada individuo debiera poseer. Noción que después se modifica para centrarse en el control. La intimidad

en el pasado comprendía entonces un espacio reservado para el individuo, donde podía desenvolverse y mantener ocultos aspectos de su vida. En el presente la intimidad es el poder de decisión que el individuo tiene al considerar qué, cómo, cuándo y a quién comunicar información personal e incluso el uso que se haga de ella. Como por ejemplo: cuando un individuo comparte con un banco información financiera, bajo ciertos límites de uso, para solicitar un servicio, sin que esta se vuelva necesariamente de carácter público.

En resumen, el concepto de intimidad y derecho a la intimidad ha debido modificarse, desprendiéndose de lo personalísimo e individual para aumentar su grado de incidencia. Sin embargo, como podrá observarse a continuación, parece haber engendrado otros como el de la protección de datos personales, mediante el cual se faculta al individuo a tomar el control sobre su información personal a través de distintos mecanismos.

I.II. Del derecho a la intimidad a la protección de datos personales

Tras ser ya reconocido el derecho a la intimidad; inicialmente cercano al límite y después al control, fue necesario ubicar qué medidas habrían de posibilitarlo de cara a los avances tecnológicos, que contribuyeron a mejorar la obtención de información de los ciudadanos y a incrementarla en cantidad, principalmente por los distintos Estados. En el tenor de esa meta debieron articularse otras ideas que en forma completa abarcarán aquello que debían poder resguardar las personas sobre sí mismas. Es allí donde cobra vigencia el término: protección de datos personales.

Si bien la información es diversa y amplia en todo lo que tiene que ver con la evolución de los conceptos de intimidad y protección de datos personales, es el afán de este apartado el describir solamente aquellos momentos de

importancia tanto, en el espectro mundial como en algunos países, para abonar a la claridad del concepto, e ilustrar de manera breve, las circunstancias en que estos cambios se han dado. Se nombran particularmente ejemplos de Alemania y España por su relación directa con el término pretexto de estas líneas, pero más por su irradiación hacia el resto del mundo.

Trabajos previos como *The right to be let alone* de Thomas Cooley en 1988 y el artículo *the right to privacy,* escrito en 1890 por los ya citados Warren y Brandeis; son considerados antecedentes serios para lo que en la década de los sesentas sería gestado como: protección de datos personales*.* En palabras de José Luis Piñar, Catedrático de Derecho Administrativo de la Universidad CEU San Pablo y exdirector de la Agencia Española de Protección de Datos, además de Presidente-Fundador de la Red Iberoamericana de Protección de Datos: *…el derecho a la vida ha pasado a significar derecho a disfrutar de la vida, que incluye el derecho a que te dejen estar solo…* (Murillo y Piñar 82–83), lo que podría traducirse como derecho a no ser observado.

El primer acercamiento a la clarificación de este derecho se dio en el continente europeo, específicamente en la resolución 509 de 1968 sobre *Los derechos humanos y los nuevos logros científicos y técnicos*, como resultado del trabajo de una comisión consultiva establecida previamente por el Consejo de Europa, que debía estudiar el potencial agresivo de las nuevas tecnologías de la información sobre los derechos de las personas.

Dicha resolución sería después conocida como *protección de datos*. Es considerado este, según Piñar, el origen del movimiento legislativo, que a partir de ese momento recorrió Europa. (García 754; Murillo y Piñar 85)

Poco tiempo después, la protección de datos personales comenzó a ser adoptada por distintos Estados y el primer ejemplo es Portugal, que dentro de su Constitución de 1976 incluyó el siguiente texto, en el artículo 35, apartado uno:

> Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. (García 755)

Queda de manifiesto en la cita anterior, que, a partir de ese momento en Portugal, se investía al usuario del poder de conocer qué información personal suya poseían otros y actuar según sus necesidades. Además, en un segundo apartado se clarificaría que datos debieran protegerse:

> No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe, religiosas o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. (García 755)

Aquí ya se distinguía qué tipo de información podría vulnerar a las personas. La informática señalada en este punto, es previa a la llegada de Internet, sin embargo, en ese momento ya se creaban bases de datos con la información de los ciudadanos y salían al mercado las primeras micro computadoras.

En el caso de la República Federal Alemana, caracterizada por su reconocimiento y protección de la dignidad humana, plasmada tiempo atrás en la Ley Fundamental Bonn; su constitución no reconocía en ese momento,

como tal, la protección de datos personales, pero subrayaba que el individuo debía poder elegir sobre su información:

> El hombre es una "personalidad capaz de organizar su vida con responsabilidad propia", es decir, el individuo tiene que tener la posibilidad de influir sobre su ambiente social, decidiendo él mismo dónde, cuándo, cómo y en qué contexto quiere presentarse ante su ambiente social. (García González 748–49)

Finalmente, fue en la Alemania de la década de los ochentas que se reconoció la importancia de la protección de los datos personales (Ana Cristina González Rincón cita a Guillermo Tenorio Cueto, Licenciado y Doctor en Derecho por la Universidad Panamericana):

> … gracias a dos derechos en pugna, dignidad humana y libertad general, surge la sentencia del Tribunal Constitucional Federal Alemán, en que se habla del surgimiento de un nuevo derecho, lo que más tarde se conocerá por "Protección de Datos Personales". Esta sentencia constituye en realidad lo que algunos autores han denominado "El sermón de la montaña de la protección de datos". (González y Tenorio 391–92)

Un tercer caso es el de España, que en la constitución de 1978, respecto del tratamiento de información por medios tecnológicos (se reitera que todavía no figuraba Internet), ya pronunciaba en su artículo 18.4: La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. (García González 748–49)

Cabe acotar que este último caso resulta trascendente para América Latina y México en particular, ya que sus conceptos han sido tomados en cuenta por legislaciones en este lado del globo.

Pero es en tiempos más recientes (2000), que, para Pablo Lucas Murillo, Catedrático de Derecho Constitucional de la Universidad de Córdoba; el reconocimiento a la protección de datos más solemne, se vertió en el artículo 8 de la carta de derechos fundamentales de la Unión Europea y en el tratado en el que se establece una Constitución para Europa. Momento mismo en el que en España fue finalmente comprendido, como derecho fundamental y aún más importante, como derecho autónomo e independiente del Derecho a la Intimidad; el Derecho a la Protección de los Datos Personales. (Murillo y Piñar 93)

Se retoman los conceptos anteriores a manera de recuento, para reconocer los alcances que han tenido las iniciativas europeas en las legislaciones latinoamericanas, con particular énfasis en México. Sin este breve análisis sería fácil extraviarse al considerar el porqué y el cómo de su existencia. En pocas palabras, se trata de un viaje a través del tiempo que permite inferir las causas de su adopción en territorio nacional.

Gracias a ello, es posible sabernos protegidos por este derecho, y como los principales actores en el control de nuestros datos personales, aunque falta determinar hasta este momento si en la realidad se aplican y ejecutan estas facultades. Aunque esto pudiera entenderse de manera simple en lo físico, también tiene que observarse en lo digital. La interrogante expuesta en este párrafo buscará ser respondida más adelante.

En ese tenor, no está de más puntualizar, que en México, hasta el 27 de abril de 2010, se publica la Ley Federal de Protección de Datos Personales, y que

en julio de ese mismo año se difunde la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), y el 21 de diciembre de 2011, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, siendo la autoridad en la materia, el en ese entonces llamado Instituto Federal de Acceso a la Información Pública (IFAI).

En este sentido, el marco jurídico protege los datos personales, con la finalidad de garantizar la privacidad y el derecho a la autodeterminación de las personas, así se indica en el artículo 1 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, como a continuación se indica:

> Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. (Diario Oficial de la Federación, LFPDPPP 1)

Es en este breve e ilustrativo resumen que se da luz sobre cómo las propias necesidades de la sociedad han provocado la transformación de los derechos y sus inherentes ampliaciones. Es en virtud de las circunstancias en que la interacción humana se da que los conflictos se originan, igual que las leyes que procuran resolverlos. Probablemente lo aquí expuesto hubiera resultado exagerado o inconcebible en otros tiempos, pero hoy ante las enormes cantidades de información que se transmiten por Internet, se demuestra su pertinencia. Igualmente, necesario es recapitular cómo el concepto de intimidad, gestó a su vez el de protección de datos personales.

Por último, destacar aspectos importantes en este apartado, el primero, que se reconoce la capacidad del individuo para decidir sobre su información y el segundo que establece la obligatoriedad de proteger ese derecho por parte de los Estados, por último, el tercero, que limita el grado de injerencia de otros sobre la información personal.

Anotación al margen importante, es que un reclamo general entre los activistas en pro de los derechos humanos digitales, es la falta de inclusión de expertos en la toma de estas decisiones (computólogos o tecnólogos, por ejemplo), lo que se traduce, desde su óptica, en imprecisiones y lagunas legales.

I.II. I. Definición de dato

Para poder comprender que es la protección de datos personales, hay que saber primero que es un dato personal y para ello acercarnos en primera instancia a lo que es un dato.

Según la definición de Julio Téllez Valdés, investigador jurídico de la Universidad Nacional Autónoma de México; citado por Sandra Cárdenas Sánchez, *un dato es la representación de información bajo una forma convencional destinada a facilitar su tratamiento.* (Cárdenas 60) En el caso de la Real Academia de la Lengua (RAE) existen dos consideraciones a destacar:

> 1. m. Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. *A este problema le faltan datos numéricos.*

> 3. m. Inform. Información dispuesta de manera adecuada para su tratamiento por una computadora. (Real Academia Española, párrs.1–3)

La primera definición abarca de un modo general el concepto, aunque lo establece como información y no como representación de información, como en la definición de Téllez. En el caso de la tercera definición dada por la RAE encontramos concordancias, las dos consideran el tratamiento, es decir el uso que se le da a la información.

Aun cuando el dato según Téllez es representación de información, debiera asumirse que esa representación, sobre cierta lógica, produce conocimiento y por tal motivo debe ser considerada al fin información. Por ejemplo, una lista de nombres puede verse a primera vista como datos, hasta el momento que hay un interés por conocer cuántos nombres empiezan con la letra J, a partir de lo cual se obtiene información, que genera conocimiento.

En lo digital un dato es también una representación de información, pero almacenada en código binario (unos y ceros,) dentro de unidades de información llamadas bits. Esta puede ser interpretada por sistemas, y por decirlo de algún modo, traducida al humano, para de la misma forma producir conocimiento. (Tecnología & Informática, párrs.1–2)

Gracias a ello puede decirse que un dato es información dispuesta y destinada a cumplir con un objetivo.

I.II. II. Definición de datos personales

Si el dato es información, la definición textual de dato personal podría ser *información de la persona*, pero es necesario profundizar más.

Desde la perspectiva legal, de conformidad con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), expedida por el Diario Oficial de la federación en 2010, los datos personales son: *Cualquier información concerniente a una persona física identificada o identificable.* (Diario Oficial de la Federación, LFPDPPP 1)

De acuerdo a lo mencionado por Javier Corral Jurado, Presidente de la Comisión de Gobernación de la H. Cámara de Diputados, al momento de la publicación; en la introducción del *Compendio de lecturas sobre la protección de datos personales*, publicado por el Instituto Federal de Acceso a la Información Pública (IFAI), en el mismo año, señala:

> Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros. (IFAI 9)

Una breve definición más es la de Tenorio Cueto, que considera que los datos personales suponen *cualquier información concerniente a una persona determinada.* (Tenorio y Rivero 55)

Algunas definiciones más, mencionadas por Sandra Cárdenas, creadora de la tesis *Necesidad de crear una regulación específica en México sobre protección de datos personales en el sector Privado*, refieren a lo dispuesto por las leyes de Austria, Noruega y Dinamarca que puntualizan *es toda*

información susceptible de ser relacionada con personas determinables o determinadas. La autora destaca también que en los primeros dos casos el término incluye a personas físicas y morales, pero no así en el país danés. (Cárdenas 60)

Datos personales	Características	Palabras clave	Aplicación
Ley de Protección de Datos Personales en Posesión de los Particulares	Cualquier información concerniente a una persona física identificada o identificable.	Información Persona física identificada Identificable	Derecho
Javier Corral Jurado	Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional.	Información Identifica Individuo Identificable Identidad Origen Edad Residencia Trayectoria	Derecho
Tenorio Cueto	Cualquier información concerniente a una persona determinada.	Información Persona	Derecho
Austria, Noruega y Dinamarca	Es toda información susceptible de ser relacionada con personas determinables o determinadas.	Información relacionada Personas determinables Determinadas	Derecho

Tabla 2. Comparativa del concepto de datos personales, por autor. Elaboración propia.

Luego entonces, es posible confirmar que los datos personales son aquellos que proporcionan información sobre las personas, lo que permite identificar o vincular información con las ya identificadas.

I.II. III. Definición de datos personales sensibles

No puede dejarse de lado qué información personal requiere de mayor protección y en este rubro toma relevancia el término *sensible*, pronunciado y 4esbozado líneas atrás.

Francia, Suecia y el Reino Unido, por ejemplo, distinguen los datos personales de los datos personales sensibles, que, según su lógica son: *Información cuyo contenido se refiere a cuestiones privadas y cuyo conocimiento general puede ser generador de perjuicio o discriminación.* (Cárdenas 60)

Una segunda aproximación al concepto corre a cargo de Sandra Cárdenas, para quien los datos personales sensibles son:

> … los que refieren a caracteres personalísimos y a la intimidad de un individuo; motivos por los cuales no deben ser objeto de registro por bancos de datos, salvo consentimiento previo y expreso del sujeto de datos por ser posibles motivadores de situaciones discriminatorias. (Cárdenas 87)

Una tercera definición es la contenida en la *Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal*, mencionada por Artemi Rallo Lombarte, quién al momento de redactarse el documento, fungía como Director de la Agencia Española de Protección de Datos [sic]:

> 1. Serán considerados sensibles aquellos datos de carácter personal:
>
> a. Que afecten a la esfera más íntima del interesado; o

b. Cuya utilización indebida pueda:

i. Dar origen a una discriminación ilegal o arbitraria, o

ii. Conllevar un riesgo grave para el interesado. (IFAI 218)

En el mismo sentido, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de México, diferencia los datos personales sensibles, bajo la siguiente lógica: *Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.* (Diario Oficial de la Federación, LFPDPPP 1)

Salta a la vista, que en el grueso de las definiciones analizadas una constante es la susceptibilidad a la discriminación y en tres de las cuatro enunciaciones también es ponderada la posibilidad del riesgo y el daño.

Lo siguiente ahora es saber qué datos pueden ser considerados sensibles, y a ese respecto Cárdenas enfatiza: *abarcan la vida sexual, las ideas políticas, creencias religiosas, historial clínico, etcétera.* (Cárdenas 87)

Por otro lado, la LFPDPPP también apunta con claridad:

> En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual. (Diario Oficial de la Federación, LFPDPPP 1)

Después de las enumeraciones anteriores y a manera de clarificar los conceptos para hallar de manera sencilla afinidades y discrepancias, se desarrolló la siguiente tabla.

Datos personales sensibles	Características	Palabras clave	Aplicación
Francia, Suecia y el Reino Unido	Información cuyo contenido se refiere a cuestiones privadas y cuyo conocimiento general puede ser generador de perjuicio o discriminación	Privadas Perjuicio Discriminación	Derecho
Sandra Cárdenas	…los que refieren a caracteres personalísimos y a la intimidad de un individuo; motivos por los cuales no deben ser objeto de registro por bancos de datos, salvo consentimiento previo y expreso del sujeto de datos por ser posibles motivadores de situaciones discriminatorias. abarcan la vida sexual, las ideas políticas, creencias religiosas, historial clínico, etcétera.	Caracteres personalísimos Intimidad Situaciones discriminatorias Vida sexual Ideas políticas Creencias religiosas Historial clínico	Derecho
Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con	1. Serán considerados sensibles aquellos datos de carácter personal: a. Que afecten a la esfera más íntima del interesado; o b. Cuya utilización indebida pueda:	Carácter personal Esfera íntima Discriminación ilegal o arbitraria Riesgo grave	Derecho

el tratamiento de datos de carácter personal	i. Dar origen a una discriminación ilegal o arbitraria, o ii. Conllevar un riesgo grave para el interesado		
LFPDPPP	Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.	Esfera íntima Discriminación Riesgo grave	Derecho
LFPDPPP	En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.	Origen racial Salud Genética Creencias religiosas Filosóficas Morales Afiliación Opiniones políticas Preferencia sexual	Derecho

Tabla 3. Comparativa del concepto de datos personales sensibles, por autor. Elaboración propia.

Una consideración importante es que la *Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal* y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*,* manejan conceptos muy similares, con la salvedad de que la última libera a la palabra discriminación de lo arbitrario e ilegal, algo que se presume correcto, dado que todo acto discriminatorio, en el sentido expuesto, debiera ser considerado nocivo.

A manera de resumen puede decirse entonces que los datos personales sensibles son aquellos que forman parte de la esfera íntima o privada y que de conocerse pueden poner en riesgo grave al individuo o hacerlo susceptible de discriminación. También, que los datos personales sensibles comprenden las ideas, creencias, opiniones, afiliaciones, salud, genética y preferencias sexuales de la persona.

Independientemente de las consideraciones aquí vertidas, se determinó señalar características y distinciones de los conceptos de datos personales y datos personales sensibles, toda vez que, como se ha visto, existen en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de México; territorio al que se encaminan los esfuerzos de este trabajo, aun cuando puedan hallarse conceptos que engloben en uno solo ambas definiciones.

Una última precisión de este apartado es que datos personales o datos personales sensibles son igual de importantes, puesto que, eventualmente, pueden generar información, conocimiento y ser utilizados indebidamente en nuestro perjuicio. Algo de lo que se hablará con más detalle en el apartado de riesgos en México.

I.II. IV. Definición de protección de datos personales

De manera breve, ha sido posible observar el recorrido que el concepto de intimidad ha realizado para llegar a la noción de protección de datos personales, un derecho considerado de tercera o cuarta generación[3]. Lo

[3] Los derechos de tercera generación, se relacionan con el acceso de todos los pueblos a la paz, la calidad de vida, etc. Los derechos de cuarta generación son aquellos relacionados con la tecnología y el individuo. (Encuentro jurídico y Ambar, párrs.7–14)

siguiente es ahora definir qué es el derecho a la protección de datos personales.

De acuerdo con Isabel Davara Fernández de Marcos, Doctora en Derecho, por la Universidad Pontificia Comillas en Madrid, España, citada en *Protección de Datos Personales, compendio de lecturas y legislación*, libro publicado por el IFAI en 2010; y quién se ha especializado en Derecho de las Tecnologías de la Información y las comunicaciones, la protección de datos personales es:

> El amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad. (IFAI 81)

Citado en el mismo libro, Hondius, F. W., autor de la publicación *A decade of international data protection, "Netherlands of International Law Review"*, define a la protección de datos personales como: *Aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos.* (IFAI 81)

Una tercera definición es la vertida por Pérez Luño, referenciada en el mismo espacio que las dos anteriores y en la que se dice que:

> La protección de datos personales tendría por objeto prioritario asegurar el equilibrio de poderes sobre y la participación democrática en los procesos de la información y la comunicación

a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos. (IFAI 81)

De la primera podemos decir que es una forma de dar facultad al ciudadano, titular de sus datos, de decidir cómo se utilizan, para evitar afectaciones profesionales, personales, sociales o en su intimidad. La segunda en sentido similar, describe la libertad del individuo sobre su intimidad y el procesamiento de sus datos, algo que redunda en la facultad que debe tener cada persona para decidir sobre su información. La tercera, por su parte, se centra en la disciplina que debe existir en la obtención, almacenamiento y transmisión de datos. Aquí no sólo el titular de la información es responsable de su protección, pues lo es también quién se haga de ella.

Protección de datos personales	Características	Palabras clave	Aplicación
Isabel Davara Fernández de Marcos	El amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad.	Amparo Utilización No autorizada Datos personales Afecte Entorno Personal Social Profesional Intimidad	Derecho
Hondius, F. W.	Aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos.	Derecho fundamental Libertad Intimidad Procesamiento Manual Automático Datos	Derecho

Pérez Luño	La protección de datos personales tendría por objeto prioritario asegurar el equilibrio de poderes sobre y la participación democrática en los procesos de la información y la comunicación a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos.	Protección Datos personales Equilibrio Participación democrática Procesos Información Sistemas Obtención Almacenamiento Transmisión	Derecho

Tabla 4. Comparativa del concepto de protección de datos personales, por autor. Elaboración propia.

En conclusión, la protección de datos personales es aquella parte de la legislación que protege la libertad de decisión del individuo sobre sus datos personales, lo que evita afectaciones en las fronteras de su intimidad, a través de medidas para el manejo de esa información.

Por último, es necesario decir que, las personas (no sólo en Internet) dan su consentimiento para que sus datos sean utilizados mediante un aviso de privacidad. Sin embargo, esta autorización es parcial, tiene límites y se hace bajo la promesa de que su información será bien utilizada y respetada, por lo que habrá que ver si a quiénes les son compartidos estos datos, tienen facultades, recursos e interés por obedecer la normatividad o no.

I.II. V. Qué comprende la protección de datos personales

Un derecho que garantiza otros derechos, es la protección de datos personales, de acuerdo a lo expuesto por Sandra Cárdenas en la *Necesidad de crear una regulación específica en México sobre Protección de Datos Personales en el sector privado* y que obedece a un recorrido detallado del desarrollo de este concepto. Entre esos derechos estaría el de la dignidad,

libertad, igualdad, derecho de propiedad, debido proceso, además del derecho a la intimidad y a la privacidad. (Cárdenas 65)

A propósito de, el Tribunal Constitucional español, particulariza a este derecho considerado fundamental respecto del derecho a la intimidad y su artículo 18.1 CE, apunta:

> … el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros *deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad*, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. (Murillo y Piñar 93)

Aquí se detalla a la perfección la definición lograda líneas atrás, o sea, el derecho del ciudadano sobre su información y la obligación de terceros a protegerla. En el apartado siguiente también se determina qué medidas han de posibilitar a los individuos su ejercicio de decisión:

> Se trata del derecho del afectado a que *se solicite su previo consentimiento para recoger y usar sus datos personales, del derecho a saber y ser informado sobre el destino y uso de esos datos y de los derechos a acceder, rectificar y cancelar dichos datos*. Es decir, de los instrumentos que hacen posible su poder de disposición sobre sus datos personales. (Murillo y Piñar 93)

Es oportuno decir también que todos los derechos mencionados son consecuencia de una serie de principios reguladores obedecidos en el

ejemplo siguiente, por la normatividad europea y que según el Dr. Oscar Raúl Puccinelli Parucci, docente e investigador citado por Cárdenas, son:

El de justificación social
El de limitación de la recolección
El de fidelidad de la información
El de especificación del propósito
El de confidencialidad
El de salvaguardia de la seguridad
El de política de apertura
El de limitación en el tiempo
El de control público
El de participación individual. (Cárdenas 65)

Es decir, que la obtención de información debe ser justificada, que esta debe ser real, que debe establecerse el fin por el cual se solicita, que no debe hacerse pública, que debe protegerse, que la autorización de uso tendrá cierta vigencia, que debe ser controlada y que el individuo debe poder participar en las decisiones relacionadas con su uso. Enunciados cercanos a los del Doctor en Derecho Aponte Núñez, quién enumera y describe se debe considerar el:

a) Consentimiento del titular de los datos
b) Calidad de los datos
c) Información en la recolección de los datos
d) Cesión o comunicación de datos
e) Principio de no discriminación (Aponte Núñez 113–14)

El primero habla del poder de decisión del individuo sobre su información. El segundo, de que sean pertinentes, adecuados y no excesivos esos datos,

en relación con el fin para que se obtienen. El tercero, de la obligatoriedad del responsable de esa información, de comunicar al usuario que tratamiento se dará a sus datos y para qué se han de recabar. El cuarto, busca garantizar que la sesión de esos datos se haya dado con previo consentimiento del titular y sólo para el fin que fueron otorgados. El último, de la prohibición de recolección de información que pueda originar discriminación (raza, color, vida sexual, religión, afiliación política y creencias). (Aponte Núñez 113–15)

En México, por supuesto, estos principios son observados en el Capítulo II de la Ley Federal de Protección de Datos Personales en Posesión de particulares, que a la letra dice:

> Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley. (Diario Oficial de la Federación, LFPDPPP 1)

Principios que describe en los artículos subsecuentes y en los que se entiende por:

> …licitud que los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable. Por consentimiento, el que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley. Por calidad que el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales

> fueron recabados. Por finalidad, que el tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. (Diario Oficial de la Federación, LFPDPPP 1)

Los siguientes principios no son mencionados específicamente en dichos artículos, pero pueden ser inferidos: *lealtad* se relaciona con la obligación de informar que datos se obtienen y que estos sean efectivamente utilizados únicamente para lo que se comunicó. Por *proporcionalidad* el que sólo se obtenga la información necesaria para concretar el fin y por *responsabilidad*, se han de entender las obligaciones que contrae el receptor de esa información sobre la protección de la misma. (Diario Oficial de la Federación, LFPDPPP 1)

A manera de reafirmar, a continuación, se parafrasea la descripción que Guillermo A. Tenorio Cueto y María Rivero del Paso, han vertido en su trabajo: *Análisis crítico de la protección de datos en México,* sobre los mismos principios rectores de la protección de datos personales: por *licitud* entienden que el depositante de esos datos debe tener completa certeza de que el depositario hará uso legítimo de esos datos (que se usen para lo que se otorgaron). Por *consentimiento*, que hay voluntad en dar esa información ya sea expresa o tácitamente. Por consentimiento expreso, se entiende que es aquél que, *mediante una expresión verbal, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos, proporcione al responsable la aceptación del manejo de los datos personales*. También el que el responsable debe eliminarlos después de utilizarlos. La *proporcionalidad* supone que *la recaudación de los datos deberá estar limitada por los fines para los cuales son recabados los mismos*, por lo que la información personal debe ser adecuada, pertinente

y no excesiva. Por último, la *responsabilidad* comprende el debido manejo de los datos proporcionados a través de medidas que garanticen el que esta información no se vea comprometida. (Tenorio y Rivero 56-58)

Qué comprende la protección de datos personales	Características	Palabras clave	Aplicación
Puccinelli Parucci	El de justificación social. El de limitación de la recolección. El de fidelidad de la información. El de especificación del propósito. El de confidencialidad. El de salvaguardia de la seguridad. El de política de apertura. El de limitación en el tiempo. El de control público. El de participación individual.	Justificación Limitación Fidelidad Especificación Confidencialidad Salvaguardia Apertura Tiempo Control público Participación individual	Derecho
Aponte Núñez	Consentimiento del titular de los datos. Calidad de los datos. Información en la recolección de los datos. Cesión o comunicación de datos. Principio de no discriminación.	Consentimiento Calidad Información Cesión Comunicación No discriminación	Derecho
Ley de Protección de Datos Personales	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad,	Licitud Consentimiento Información Calidad Finalidad Lealtad Proporcionalidad	Derecho

	proporcionalidad y responsabilidad, previstos en la Ley.	Responsabilidad	

Tabla 5. Qué comprende la protección de datos personales, por autor. Elaboración propia.

A golpe de vista, e incluso en una segunda y tercera aproximación al texto, puede inferirse que lo que ambos autores describen en sus trabajos de investigación, aunado a lo descrito en la LFPDPPP y la normatividad europea; es en extremo similar por no decir casi idéntico, por ello ahora se sabe que el usuario debe autorizar el uso de sus datos, que el responsable debe informar para qué son recabados y darles sólo ese uso para después eliminarlos o en su defecto informar al individuo de que tratamiento distinto podría dárseles para que el titular elija si los comparte o no. El que debe siempre tenerse sólo la información necesaria para el fin que ha de cumplimentarse y que no debe solicitarse información de más, sino es útil para el desarrollo de la empresa encomendada o por encomendar. Además, que la información siempre deberá estar actualizada y ser veraz.

Por último, hay que destacar que la mención a la discriminación hecha por Aponte bien puede estar comprendida en lo posteriormente expuesto (LFPDPPP y Tenorio Cueto), pero de una manera más general, porque los datos se protegen de toda intromisión para evitar cualquier afectación y en esos posibles daños, sin duda alguna, tiene espacio la discriminación. También resulta necesario destacar que no basta que el individuo pueda decidir sobre su información, sino que los responsables también deben proveer medidas para resguardarla.

I.II.VI. Derecho a la protección de datos personales y autodeterminación informativa

Como se ha externado en varias ocasiones a lo largo de este documento, para que sea posible resguardar la intimidad y privacidad de las personas,

son necesarios derechos que permitan a los ciudadanos conocer y decidir sobre el tratamiento de sus datos personales. Estos sí existen y son consecuencia de los principios previamente expuestos. Todos serán descritos en las líneas siguientes, con particular atención al escenario mexicano.

Emercio José Aponte Núñez, Doctor en Derecho venezolano, en su trabajo *La importancia de la protección de datos de carácter personal en las relaciones comerciales,* menciona son: el de acceso, el de rectificación y de cancelación. El primero supone:

> …la facultad que tiene el titular de los datos de dirigir al responsable del tratamiento una solicitud de información en relación con esa actividad. El segundo: consiste en la posibilidad que tiene el titular de los datos de exigir al responsable del tratamiento que cumpla con el principio de calidad, corrigiendo los errores o subsanando las informaciones incompletas, y permitiendo que el tratamiento sea reflejo cierto y fidedigno de la realidad. Y el finalmente el tercero: es la facultad o potestad que tiene el titular de los datos a que los mismos se excluyan del tratamiento, ya sea porque son errados, o por no tener interés en que sean tratados. (Aponte Núñez 113–15)

Sobre la Autodeterminación Informativa, él mismo apunta:

> Es indudable que el titular de los datos tiene el derecho de conocer todo lo relacionado con el tratamiento de sus datos personales, que es lo que la doctrina ha denominado el derecho a la autodeterminación informativa. (Aponte Núñez 113–15)

Si bien Aponte menciona tres derechos, en otras latitudes se señalan cuatro. Es el caso de México, que en el capítulo III de su LFPDPPP, reconoce:

> Artículo 22.- Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos. (Diario Oficial de la Federación, LFPDPPP 1)

A propósito de ello, Tenorio Cueto y Rivero describen:

> … cuando nos referimos a la protección de datos el derecho a la información obliga al responsable a informar sobre los datos que obran en su poder, pero de igual manera otorgan al titular de dichos datos a determinar que manejo quiere que se haga con ellos. Esto es conocido como la autodeterminación informativa. (Tenorio y Rivero 61)

Como acotación y bajo el pretexto de establecer brevemente foco en la autodeterminación informativa, se considera a Lucas Murillo, quién también se pronuncia al respecto en el libro titulado *El derecho a la autodeterminación informativa,* donde aclara porque prefiere este término sobre el de *Derecho a la Protección de Datos de Carácter Personal*:

> Me parece necesario advertir que he preferido utilizar la expresión "derecho a la autodeterminación informativa" en el título de mi intervención porque siempre me ha parecido más expresiva que otras adoptadas por los legisladores y por la doctrina para

> denominarlo…he seguido utilizándola, aun siendo consciente, de que ciertamente, el derecho positivo no la recoge… nada más lejos de mi intención que entablar una disputa sobre los nombres cuando está claro que cualquiera de los dos mencionados identifica esta figura y es igualmente evidente que lo importante es el contenido que encierra. (Murillo y Piñar 93)

Tras la pequeña digresión, se continúa con la inspección a los denominados Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), transcritos textualmente de la LFPDPPP para su mejor comprensión:

> Artículo 23.- Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento.
>
> Artículo 24.- El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos.
>
> Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.
>
> Artículo 26.- El responsable no estará obligado a cancelar los datos personales cuando:
>
> I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
>
> II. Deban ser tratados por disposición legal;

III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;

IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;

V. Sean necesarios para realizar una acción en función del interés público;

VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y

VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Artículo 27.- El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular. (Diario Oficial de la Federación, LFPDPPP 1)

De acuerdo a Tenorio Cueto y Rivero, la legislación describe que cualquier particular tiene derecho a acceder a sus datos personales cuando estén en poder de un responsable y que en el caso de que este acceso sea negado puedan accionarse mecanismos legales que lo posibiliten. El punto de partida es una solicitud ante la institución correspondiente. (Tenorio y Rivero 62)

Del derecho a la rectificación, los autores señalan su concomitancia con el acceso, pues queda claro que no puede realizarse lo segundo, lo tercero o lo cuarto sin lo primero. Por supuesto tiene consecuencias jurídicas diversas y como tal, implica la modificación de informaciones personales que sean equivocadas o estén incompletas. En este caso el titular tiene el derecho a obligar al responsable a rectificar el dato, que puede ser de acuerdo a Raúl Bertelsen, ex Ministro del Tribunal Constitucional de Chile (citado por ellos):

> a) erróneo o inexacto, es decir aquel dato que, pretendiendo asumir alguna referencia informativa por su inexactitud no completa adecuadamente la información; b) equívoco, cuando la información referida proveniente del dato conduce a diversas interpretaciones poco claras o; c) incompleto, es decir una información parcialmente cierta. (Tenorio y Rivero 62-63)

Dentro de la legislación mexicana el derecho de rectificación implica un período de bloqueo que permite al responsable conservar los datos, para efectos de cumplir con las *responsabilidades nacidas del tratamiento*, sin embargo, la cancelación de este derecho se agotará cuando venza el tiempo de bloqueo establecido por la ley. (Tenorio y Rivero 63)

El derecho a la cancelación supone también un período de bloqueo en la ley mexicana, por lo que su aplicación no es inmediata. Esto a los ojos de Tenorio y Rivero es un error, pues debiera diferenciarse la cancelación del bloqueo, pues lo primero refiere a la eliminación de esa información de manera permanente y lo segundo comprende solo su suspensión de manera temporal. (Tenorio y Rivero 63-64)

Por último, el derecho de oposición implica una acción de negación por parte del titular, de cómo son manejados sus datos y que pueden ser utilizados

con fines publicitarios, de investigación, encuestas, etc. La diferencia sustancial y el porqué de su existencia radica en que mientras la cancelación busca la eliminación, la oposición si acuerda su utilización, pero la limita a los fines para que fueron facilitados los datos. (Tenorio y Rivero 64)

Derechos ARCO	
Acceso	Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento.
Rectificación	El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos.
Cancelación	El titular tendrá en todo momento el derecho a cancelar sus datos personales.
Oposición	El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular.

Tabla 6. Derechos ARCO. Elaboración propia. (Diario Oficial de la Federación, LFPDPPP 1)

Estos derechos en México han cobrado vigencia a partir de julio de 2010, con el decreto publicado por el Diario Oficial de la Federación, por el que se expidió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reformaron los artículos 3, fracciones II, VII y 33, además de la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Pese a ello Tenorio y Rivero critican:

> Esta incorporación supone un cambio paradigmático en el tratamiento de los datos, incorporando a nuestro sistema jurídico la protección de los mismos a través del reconocimiento de los denominados derechos ARCO […] y que desafortunadamente no

establece procesos judiciales acordes con la reforma constitucional, dejando meros y simples procedimientos que no pueden alcanzar el ámbito jurisdiccional y que sólo se limitan a un ámbito de la justicia administrativa. (Tenorio y Rivero 68)

Momentos de ejercicio del derecho a la protección de datos personales			
	Momento 1	**Momento 2**	**Momento 3**
Solicitud de información del usuario por terceros	Aceptación del Aviso de Privacidad (Límites)	Solicitud de acceso a la información por el usuario (conocer qué información poseen y con qué fines)	Solicitud de rectificación de la información por el usuario (inexactos, equívocos, o incompletos) Solicitud de cancelación de la información por el usuario (eliminación) Oposición al manejo de la información por el usuario (la exigencia de obedecer los límites establecidos)

Tabla 7. Momentos para ejercer la protección de los datos personales. Elaboración propia.

Tras dejar la última consideración para profundizar en ella en numerales posteriores; se hace ya reconocible y entendible que es el derecho a la autodeterminación informativa y de él debiera decirse es la facultad que debe otorgarse al particular de conocer cómo y para qué se utilizan o utilizarán sus datos personales, permitiéndole actuar en consecuencia. Por otra parte, el derecho a la protección de datos personales, retoma la

importancia de conocer qué información se tiene del individuo y con qué fin, pero además provee mecanismos como: el derecho de acceso, rectificación, cancelación y oposición.

Aunque ambos conceptos resultan similares y para ciertos autores, como Lucas Murillo, prácticamente lo mismo, en este trabajo se considera el Derecho a la Protección de Datos personales por estar descrito así en México, por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, antes IFAI).

A continuación, con base en lo anterior, se hace inferencia en la tenue distinción entre ambos conceptos, desde el punto de vista del usuario común, aunque se sabe que esto por sí solo sería pretexto de múltiples debates y pronunciamientos en el ámbito jurídico.

Derecho a la autodeterminación informativa	**Derecho a la protección de datos personales**
Facultad que debe otorgarse al particular de conocer cómo y para qué se utilizan o utilizarán sus datos personales permitiéndole actuar en consecuencia.	Provee mecanismos para conocer qué información poseen terceros y con qué fin, así como los derechos de acceso, rectificación, cancelación y oposición.

Tabla 8. Derecho a la autodeterminación informativa y derecho a la protección de datos personales. Elaboración propia.

Se dirá entonces que el derecho a la protección de datos personales, posibilita al titular conocer qué información poseen o poseerán los particulares y para qué fines, a partir de ello podrá solicitar su rectificación, si considera que son inexactos, equívocos, o están incompletos; además, de inconformarse por el uso que se haga de ellos, tendrá la posibilidad de solicitar su cancelación, es decir su eliminación por parte del responsable.

Por último, el Derecho a la Oposición involucra la aceptación del titular sobre el uso de sus datos, pero los limita a los fines acordados implícita o explícitamente. Es necesario recordar que el responsable está obligado a informar en todo momento al particular, sobre los cambios en sus políticas de privacidad y otros posibles tratamientos que pudieran hacerse a los mismos, sobre todo cuando se trate de transferir la información a otros, para que el ciudadano siempre pueda actuar con conocimiento.

I.III. Privacidad

A lo largo de estas páginas se han utilizado en diversas ocasiones las palabras intimidad y privacidad, incluso juntas, esto no ha sido bajo el pretexto de enumerar sinónimos para aumentar el posible impacto de lo aquí expuesto, sino porque cada una tiene un peso específico.

El viaje realizado aquí y que ha iniciado con el concepto de intimidad, fue diseñado así para poder tener una idea global de como se ha avanzado en la protección de la misma, sin embargo, lo íntimo no es lo único que debe protegerse de las tecnologías del presente y futuro, lo privado también lo es y esto hace necesario identificar las diferencias entre conceptos.

Intimidad y privacidad se usan regularmente de manera indistinta, muchas veces incluso al mencionar la una por la otra y viceversa. Dicha práctica no ha escapado del entorno legal, donde su uso indiscriminado resta claridad a las diferencias que entre ellas debe hacerse.

José Antonio Díaz Rojo, Doctor en Filología e investigador, en su trabajo *Privacidad: ¿neologismo o barbarismo?* Se da a la tarea de determinar la pertinencia de utilizar esta palabra y tras un análisis exhaustivo concluye:

1. Morfológicamente, privacidad es un calco del inglés *privacy* y del francés *privacité*. Es posible que el término en español no sea

un ejemplo de «pureza» morfológica, pero se encuentra dentro de los límites del sistema de la lengua, es decir, dentro de las posibilidades expresivas que ofrece el sistema...

2. Semánticamente, el concepto de privacidad no es sinónimo de intimidad y confidencialidad. La confidencialidad implica el hecho de no dar publicidad o transmitir a terceros datos e informaciones reservadas; la intimidad es lo más interno del sujeto, sus sentimientos y pensamientos profundos; la privacidad está constituida por las facetas que forman nuestra vida personal, frente a nuestra dimensión pública o profesional. Los asuntos íntimos son privados, pero no todos los aspectos privados son íntimos…

3. El término privacidad puede ser sustituido directamente por vida privada en muchos casos, y, en otros en que no es tan factible este cambio, sería necesaria una modificación de la construcción para evitar el uso del galoanglicismo […] en algunos contextos privacidad se emplea con el matiz de 'propiedad' más que de 'ámbito o esfera de la vida', lo que hace que resulte forzada su sustitución por vida privada.

4. Por todo ello, no creemos que privacidad sea estrictamente un barbarismo, sino más bien un neologismo tolerable, que está disponible para los hablantes que deseen emplearlo, y que puede ser evitado y sustituido por otras opciones por quienes lo rechazan. (Díaz Rojo, párrs.101–104)

De lo anterior debe destacarse el punto número dos, donde el autor señala que, si bien todo lo íntimo es privado, no todo lo privado es necesariamente

íntimo. Es decir, que lo íntimo es lo más personal y lo privado aquello que comprende una esfera reservada, un círculo social pequeño.

Una segunda valoración de intimidad y privacidad es la de Ernesto Garzón Valdés, filósofo del derecho, filósofo moral y filósofo político, quien propone:

> Intimidad: "el ámbito de los pensamientos de cada quien… lo aún no expresado y que probablemente nunca lo será…". Privacidad: "la esfera personal reconocida… el ámbito reservado para las relaciones interpersonales donde la selección de los participantes depende de la libre decisión de cada individuo. Lo público: "la esfera de libre accesibilidad de los comportamientos y decisiones de las personas en sociedad, las cosas que pueden y deben ser vistas por cualquiera". (Garzón Valdés 6)

Bajo esta lógica, la intimidad es aquello que cada persona guarda para sí, la privacidad, por otra parte, involucra un espacio limitado donde tienen cabida muy pocos. Lo público ha de ser desmenuzado tras una aproximación más a lo íntimo y lo privado.

Fernando Escalante Gonzalbo, Doctor en Sociología e investigador del Centro de Estudios Internacionales del Colegio de México, también se pronuncia en ese sentido (lo relativo a la privacidad y no a lo privativo):

> No hay nada en las conductas o los lugares que los haga ser intrínsecamente privados; no se trata de una propiedad objetiva, no es un rasgo que corresponda a la naturaleza de las cosas, sino una definición jurídica. La legislación traza una frontera y caracteriza lo público y lo privado. No se limita a constatar un hecho. Por un motivo u otro, las leyes separan un extenso conjunto de espacios, hechos y decisiones que se designan como privados,

> lo cual quiere decir que están protegidos contra la intervención de la autoridad, son materias en que se puede decidir con libertad y sin dar cuentas a nadie. (Escalante Gonzalbo 6–7)

Escalante también refiere, que, si bien hay límites a la observación y que lo privado permite la libertad de ser y hacer, este derecho habría de ser perdido cuando las sospechas de actos nocivos para la sociedad se den, el único cuestionamiento en ese sentido es de qué grado debe ser la sospecha para que está libertad sea desechada.

Respecto de lo privado y lo íntimo, el autor continúa:

> ... podríamos decir que la definición de lo privado es objetiva, mientras que la definición de lo íntimo es relativa, se refiere al círculo de gente que de manera natural pueden saber de nuestra vida privada, en cualquier aspecto. (Escalante Gonzalbo 15)

Luego entonces, lo privado (privacidad) comprendería aquello que está lejos de la mirada de otros (incluida la autoridad) es decir, al primer círculo social de gente que puede saber sobre nuestra vida personal.

Un apartado pendiente es el de lo público, que solo consideramos aquí a fin de realizar una distinción respecto de lo íntimo y privado. Podemos decir de él que es aquello de conocimiento general. En ese sentido, toda persona pública, por las propias implicaciones de su quehacer tiene menos espacio para la privacidad, pero siempre debiera tenerlo para la intimidad. El propio desempeño de sus funciones implica el conocer si su conducta es adecuada y reflejada en ciertos aspectos privados, pese a ello, una figura no pública debiera poder tener a mayor resguardo los aspectos de su vida privada.

Lo íntimo, lo privado y lo público	Intimidad	Privacidad	Lo público
Doctor en Filología. José Antonio Díaz Rojo	La intimidad es lo más interno del sujeto, sus sentimientos y pensamientos profundos.	La privacidad está constituida por las facetas que forman nuestra vida personal, frente a nuestra dimensión pública o profesional. Los asuntos íntimos son privados, pero no todos los aspectos privados son íntimos.	
Filósofo en Derecho. Ernesto Garzón Valdés	El ámbito de los pensamientos de cada quien… lo aún no expresado y que probablemente nunca lo será…	La esfera personal reconocida… el ámbito reservado para las relaciones interpersonales donde la selección de los participantes depende de la libre decisión de cada individuo.	...la esfera de libre accesibilidad de los comportamientos y decisiones de las personas en sociedad, las cosas que pueden y deben ser vistas por cualquiera.
Doctor en Sociología. Fernando Escalante Gonzalbo	podríamos decir que la definición de lo privado es objetiva, mientras que la definición de lo íntimo es relativa, se refiere al círculo de gente que de	No hay nada en las conductas o los lugares que los haga ser intrínsecamente privados; no se trata de una propiedad objetiva, no es un rasgo que	

	manera natural pueden saber de nuestra vida privada, en cualquier aspecto	corresponda a la naturaleza de las cosas, sino una definición jurídica.	

Tabla 9. Lo íntimo, lo público y lo privado. Elaboración propia.

La privacidad entonces debe entenderse como la esfera reservada y determinada por cada individuo, donde sólo tienen cabida ciertas personas. Esta debe estar lejos de la mirada de aquellos no contemplados en dicha esfera, lo que incluye a la autoridad. Luego entonces, la intimidad, privacidad y lo público pueden ser entendidos así:

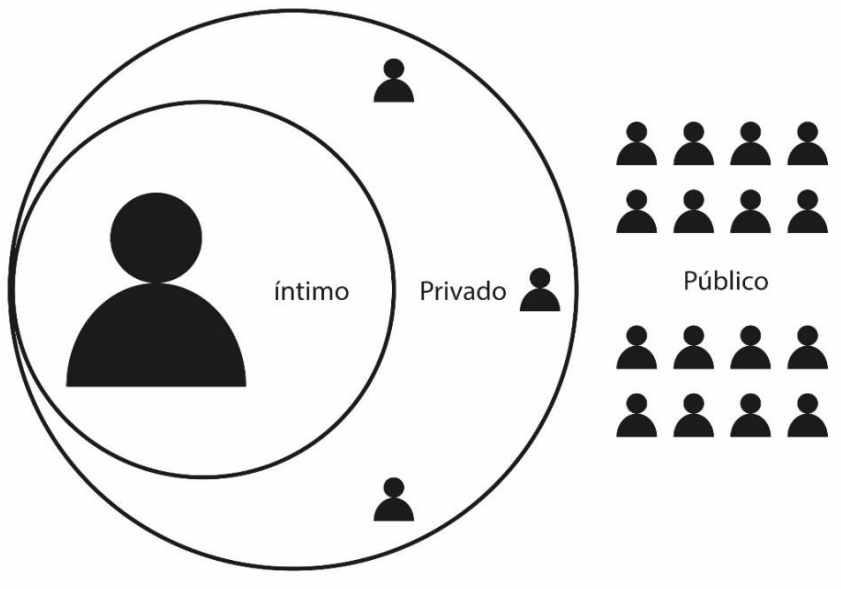

Imagen 1. La intimidad, la privacidad y lo público. Elaboración propia.

A manera de conclusión, debe decirse que se considera de mayor valor en este trabajo el concepto de privacidad, porque dentro de este se engloba el de intimidad y porque este último solo contempla aspectos personales y no otras interacciones que involucran mayores círculos sociales, sin que se pierdan ciertos límites que los hagan ser considerados públicos. No hay que

olvidar que la protección de datos personales de igual forma involucra ambos, aunque uno este inmerso en el otro.

I.III. I. La privacidad en lo digital

Como se ha observado, la privacidad es un espacio de reserva que debe ser definido por el individuo y protegido por la ley y era factible dentro de las prácticas cotidianas cuando no involucraban el uso de las tecnologías del presente (celular, computadora, tabletas, relojes inteligentes, cámaras de video vigilancia u otros dispositivos conectados a Internet). En la actualidad, por ejemplo, servicios web, redes sociales digitales y programas informáticos pueden dar una aparente sensación de intimidad o privacidad, pero recopilar, almacenar e interpretar información de los usuarios para sus propios fines.

Antes era posible adquirir productos y/o servicios físicamente y estar exento de precisar datos personales en la mayoría de las ocasiones, siempre que el desembolso se realizara en efectivo. Por igual, la convivencia y sus niveles de intimación eran consecuencia de una decisión con origen en la mirada e interpretación de las circunstancias de cada persona y efecto de sus valoraciones respecto de los individuos y lugares, pero, con el *boom* del Internet, que sucedió a partir de la década de los noventas y donde salas de conversación (chats) y foros se volvieron populares; las relaciones sociales migraron paulatinamente a sitios web y redes sociales digitales donde se observa la apariencia, pero no lo interno; la superficie, pero no las entrañas, la fachada, pero no la infraestructura; la interfaz del usuario, pero no el código que le hace funcionar, lo que suma a la opacidad.

Por si fuera poco, cada operación en Internet, en lo aparente, exige datos, por ejemplo: sitios acreditados, seguidores de la ley, solicitan llenar

formularios y aceptar acuerdos de privacidad o utilización de *cookies*[4], pero esto no es una práctica adoptada por todos, lo que abona a la incertidumbre respecto de qué información se recaba y para qué fines, sin olvidar los sitios fraudulentos que pueden hacerse de nuestra información mediante engaños sin que el usuario pueda saberlo.

Los buscadores de Internet indexan[5] (enlazan y ordenan nuestros datos para posibilitar su consulta) y ponen a disposición de los usuarios nuestra información (al menos la pública mediante resultados de búsqueda), lo que hace posible en ocasiones la triangulación para obtener mayor conocimiento de nosotros, con ignorancia propia de por medio. Los dispositivos nos acompañan diariamente casi en todos los momentos de la vida, nuestras experiencias y vivencias son almacenadas en ellos, aparatos con micrófono, cámara y localizador GPS, vulnerables a ataques y a la intromisión, no sólo de piratas informáticos, sino también desarrolladores de *apps* (aplicaciones), creadas con el fin de recabar información y a las que otorgamos el permiso de operar en nuestros aparatos para distintos fines.

---

[4] Una *cookie* es una pequeña cantidad de datos que almacena información específica sobre el usuario. (Vitaliev 42) Más información en el apartado Cómo opera Internet.

[5] *En terminología de internet, indexar hace referencia a la acción de agregar una o más páginas web a las bases de datos de los buscadores de internet, para que estas aparezcan en los resultados de búsquedas de los mismos.* (Alegsa, "Definición de indexar" párr.1)

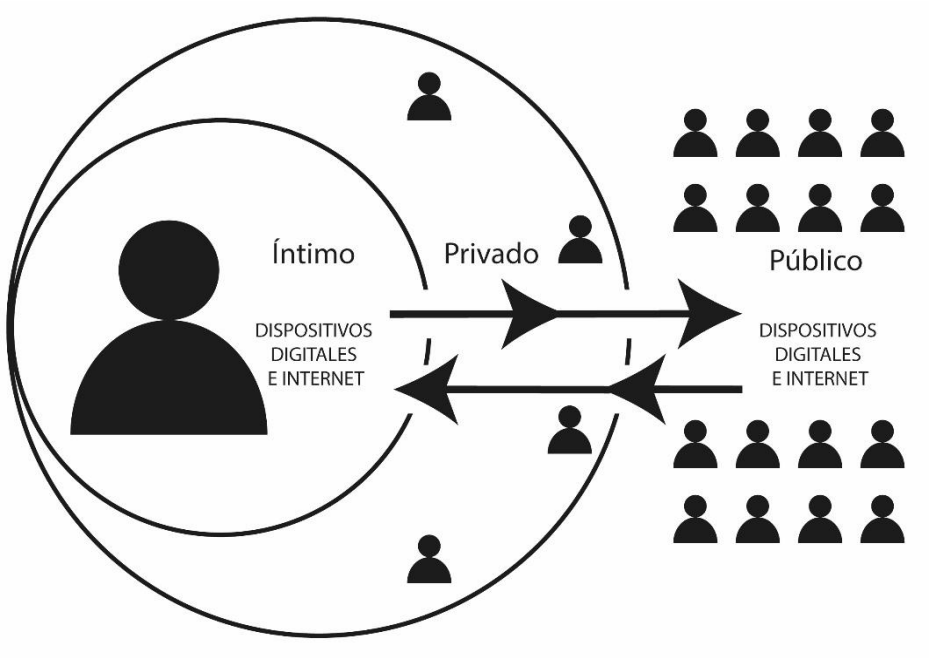

Imagen 2. La intimidad, la privacidad y lo público en Internet. Elaboración propia.

Ya la Organización de las Naciones Unidas, en su Asamblea General llevada a cabo en junio de 2014 y que se centró precisamente en el derecho a la privacidad en la era digital, externó su preocupación en el informe (Punto 2 de la introducción), y precisó cómo en *la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos.* Sin dejar de considerar los efectos de la injerencia a la privacidad (Naciones Unidas 3):

> … toda captura de datos de las comunicaciones es potencialmente una injerencia en la vida privada y, además, la recopilación y conservación de datos de las comunicaciones equivale a una injerencia en la vida privada, independientemente de si posteriormente se consultan o utilizan esos datos. Incluso la mera posibilidad de que pueda captarse información de las comunicaciones crea una injerencia en la vida privada y puede

> tener un efecto negativo en derechos como los relativos a la libertad de expresión y de asociación. (Naciones Unidas 7)

Los tiempos han cambiado y, en consecuencia, las formas de ejercer nuestro derecho a la privacidad también. Antes el ejercicio recaía de una manera más directa en cada persona, sin que, por supuesto, fuera infalible, pero si más confiable. Hoy la privacidad digital es compartida, de alguna u otra forma, ha sido extendida y aun cuando existen mecanismos para hacerla valer (numeral anterior donde se menciona el derecho a la protección de datos personales), no puede existir certeza completa de que seguros están, al residir en las manos de terceros, cuando incluso estos obligan a los usuarios a ingresar o compartir información para utilizar sus servicios sin que exista claridad en la práctica, sobre cómo se almacena y qué se hace con esa información. Algo que sucede incluso con programas informáticos de pago (ahora descargables y actualizables desde Internet), que son utilizados como única herramienta a ciertas necesidades (a consecuencia del sistema educativo que sólo pondera estas opciones), olvidándose de alternativas como el *software* libre o de código abierto, que pueden ser vigilados y corregidos por una comunidad, para que no se haga mal uso de ellos.

I.IV. Usuarios e Internet

Al entender la privacidad desde lo digital, junto con los peligros que involucran su perdida en la actualidad, es pertinente descubrir qué datos comparten los usuarios en su quehacer cotidiano en Internet, independientemente del dispositivo que media esa comunicación, así como las acciones que llevan a cabo las empresas para garantizar su protección.

De acuerdo al *Primer Estudio sobre Protección de Datos Personales entre Usuarios y Empresas en México*, realizado en 2012 por la Asociación Mexicana de Internet (AMIPCI) y que comprende un diseño muestral probabilístico que incluyó 187 empresas y 734 usuarios (de representatividad nacional y nivel de confianza del 95% con base en su información) (AMIPCI 4):

- 11% de los encuestados no supo que el Derecho a la Privacidad es un Derecho Constitucional.
- 31% de los internautas no pudieron definir lo que es un dato personal. (AMIPCI 21–22)

Pese a ello, 77% reconoció haber dejado información personal en redes sociales digitales, 64% mencionó haberlo hecho en la banca en línea y el 62% señaló que lo hizo en compras en línea. (AMIPCI 23)

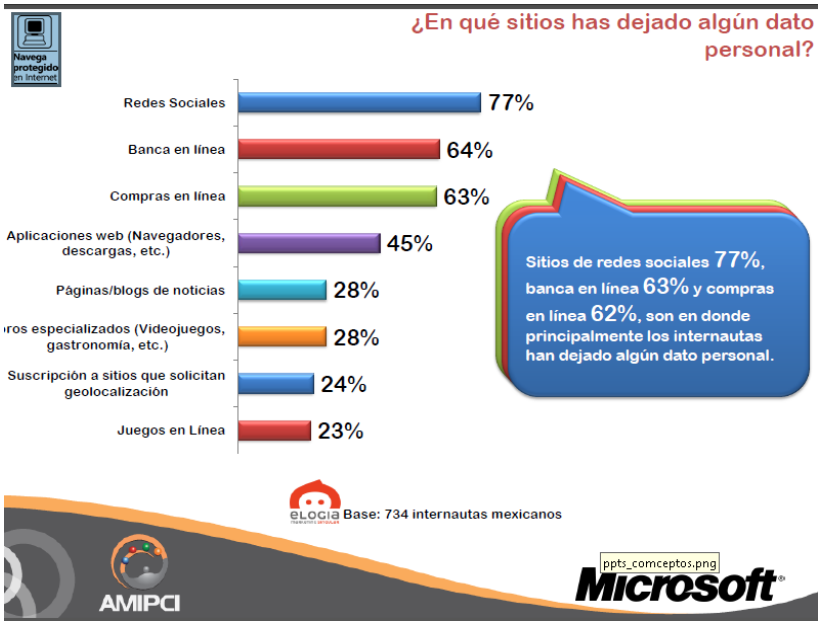

Imagen 3. Sitios en los que se dejan datos personales. AMIPCI.

En cuanto al tipo de datos personales que los usuarios han compartido en Internet se señalan los de identificación 90%, sensibles 39%, patrimoniales 25%, de salud 17% y biométricos 4%. (AMIPCI 24)

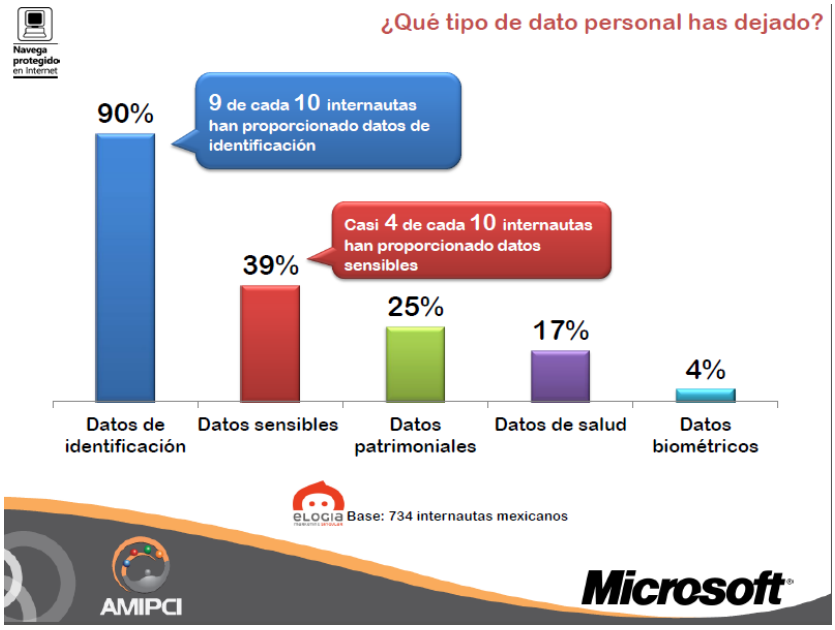

Imagen 4. Tipos de datos personales proporcionados por usuario. AMIPCI.

34% manifestó no considerar necesario que las organizaciones les informen sobre el tratamiento de datos personales y sólo el 24% dijo revisar siempre o casi siempre los avisos de privacidad. 26% consideró nada y poco probable ejercer sus derechos ARCO (Acceso, rectificación, Cancelación y Oposición). (AMIPCI 25)

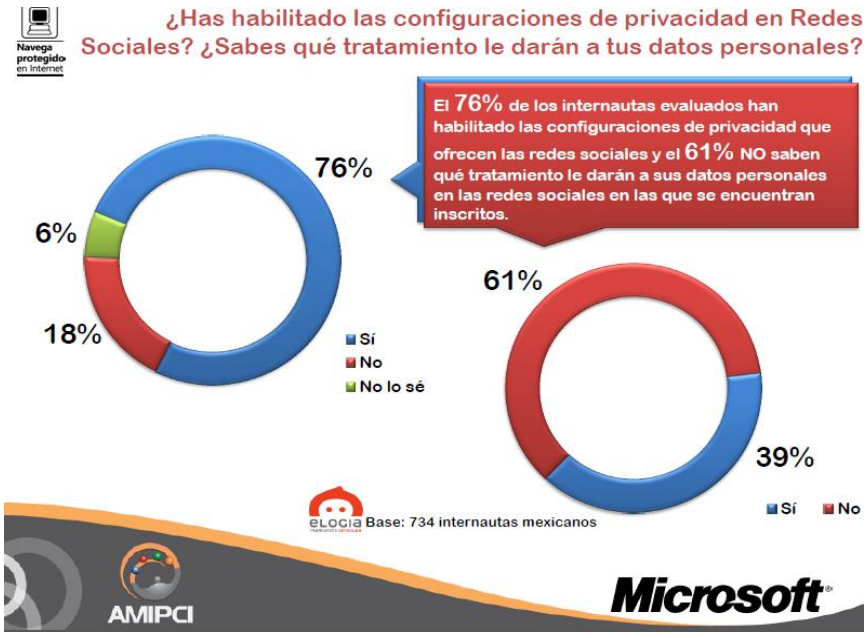

Imagen 5. Conocimiento sobre el tratamiento de los datos personales y configuración de privacidad de redes sociales digitales. AMIPCI.

Aun cuando el 76% de los evaluados habilitaron sus configuraciones de privacidad, el 61% no sabe cómo se tratarán sus datos personales. (AMIPCI 31)

El 21% y 11%, en desacuerdo y completamente en desacuerdo, respectivamente, suman un 32% sobre la percepción de control respecto a sus datos personales. (AMIPCI 32)

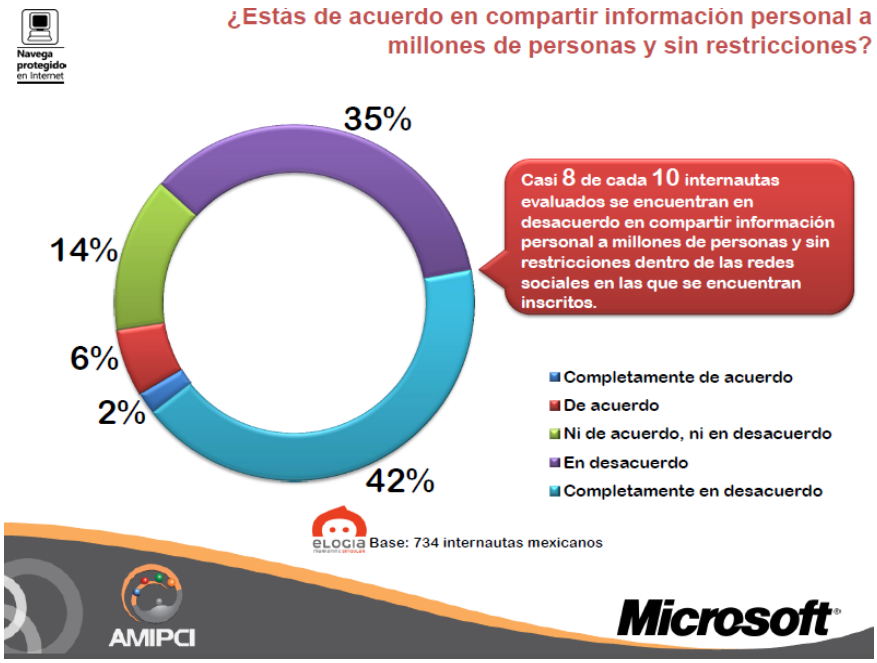

Imagen 6. Opinión de usuarios sobre compartir información sin restricciones. AMIPCI.

Finalmente, un 63% considera que es una responsabilidad compartida entre usuario y responsables del tratamiento, el correcto uso de los datos personales. (AMIPCI 36)

En este acercamiento es constatable que, en cuanto a percepción, las personas manifiestan duda sobre cómo se trata su información por empresas y personas, pero es más relevante saber que pese a ello comparten información en sitios y redes sociales digitales, además que un amplio porcentaje no da la importancia debida a la lectura de los avisos de privacidad de los sitios y redes sociales digitales que utiliza, de tal suerte que aun cuando hay preocupación y duda sobre el manejo que se hace de su información, no se vislumbra un correcto conocimiento sobre cómo operan los responsables del tratamiento de ella, lo que los imposibilita de ejercer control sobre los mismos y actuar en consecuencia.

I.V. Empresas e Internet

Tras conocer los hábitos de los usuarios en Internet; además de su noción, percepción y conocimiento del concepto de datos personales y derechos relacionados a su protección, ha de darse cuenta ahora del interés y acciones que las empresas ejecutan para el correcto resguardo y tratamiento de los datos personales en su haber, bajo el pretexto de bien saber si son confiables y seguras para tal propósito.

Para cumplir con dicho objetivo se ha retomado el ya citado *Primer Estudio sobre Protección de Datos Personales entre Usuarios y Empresas en México*, realizado en 2012 por la Asociación Mexicana de Internet (AMIPCI), y el cual contempló 187 casos de empresas con representatividad en 32 Estados, en la República Mexicana.

En lo que atañe al concepto de Dato personal, el 28% de las empresas evaluadas no pudo definirlo (AMIPCI 7):

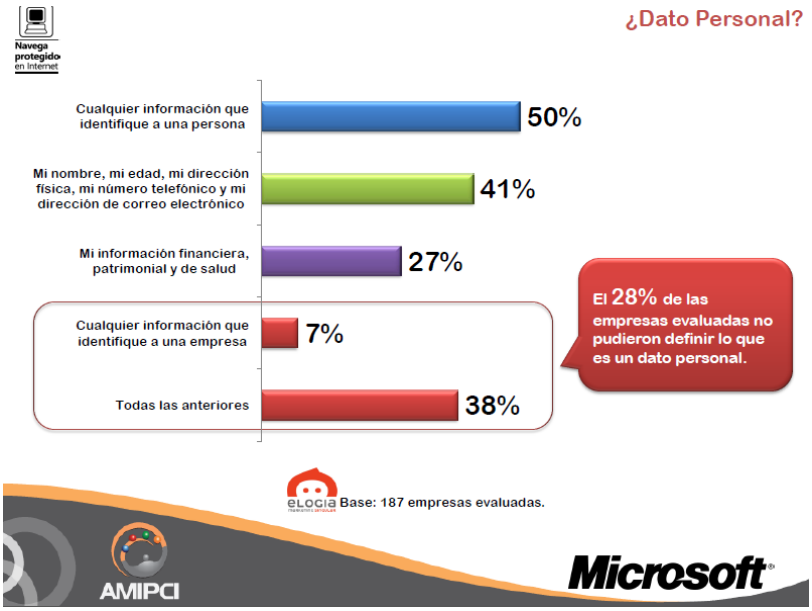

Imagen 7. Qué es un dato personal. AMIPCI.

En los datos personales que las empresas almacenan, predominan los de identificación, seguidos de los datos patrimoniales y en tercer lugar los de salud.

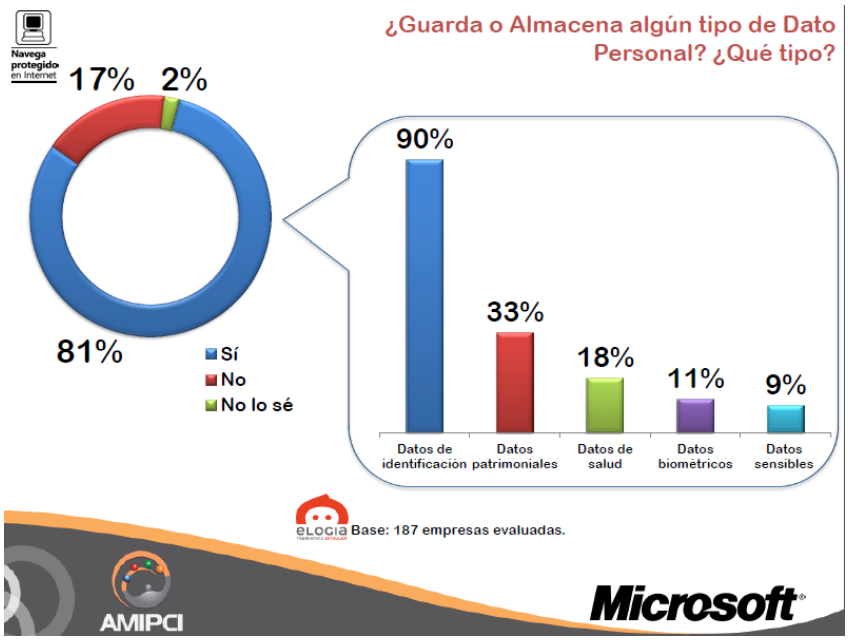

Imagen 8. Datos personales almacenados. AMIPCI.

Un dato positivo es, que de dichas empresas, 95% consideran las políticas de privacidad y seguridad de la información que ofrecen los desarrolladores de *software* y servicios de almacenamiento en la nube, pese a ello el 44% de las empresas evaluadas no manifestó el conocimiento necesario sobre la LFPDPPP. (AMIPCI 10–11)

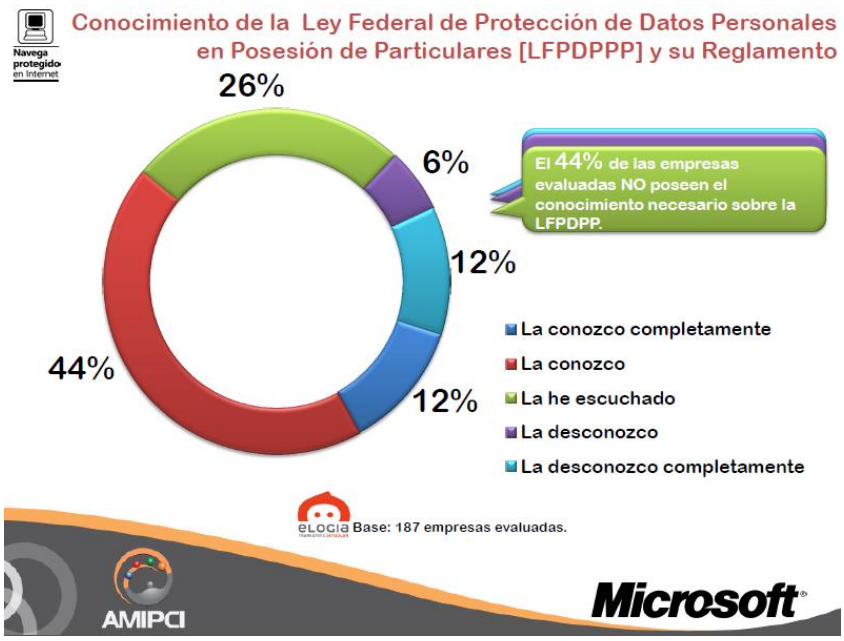

Imagen 9. Conocimiento de la LFPDPPP. AMIPCI.

Las respuestas: la he escuchado con 26%, la desconozco con 6% y la desconozco completamente con 12%, arrojan el 44% señalado. Así se observa que poco más de la mitad conoce de que trata la LFPDPPP. De ser esto replicable, de acuerdo al grado de confianza de la muestra, puede decirse, que casi la mitad de las empresas tiene un conocimiento deficiente de dicha ley, lo que suma a la incertidumbre sobre el cuidado de la información de cada usuario.

Respecto a las acciones a realizar para cumplir con la LFPDPPP, las empresas prefieren capacitar a alguien dentro de su organización para que desempeñe esa función (48%), sin embargo, un 32% no sabe qué acciones llevar a cabo para ese fin. (AMIPCI 12)

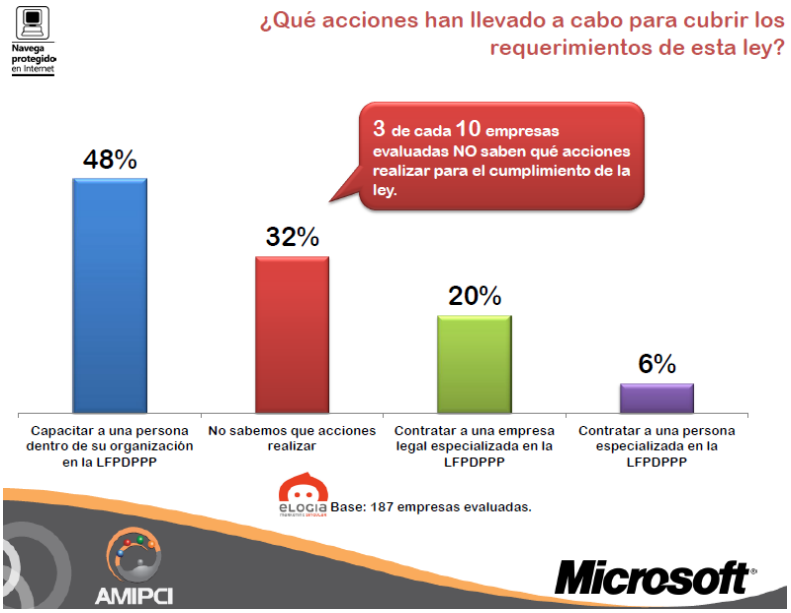

Imagen 10. Acciones a implementar por la LFPDPPP. AMIPCI.

Aun así, 63% de las empresas consideró que el principal obstáculo para cubrir los requerimientos de ley son el desconocimiento parcial o total de la LFPDPPP. (AMIPCI 13)

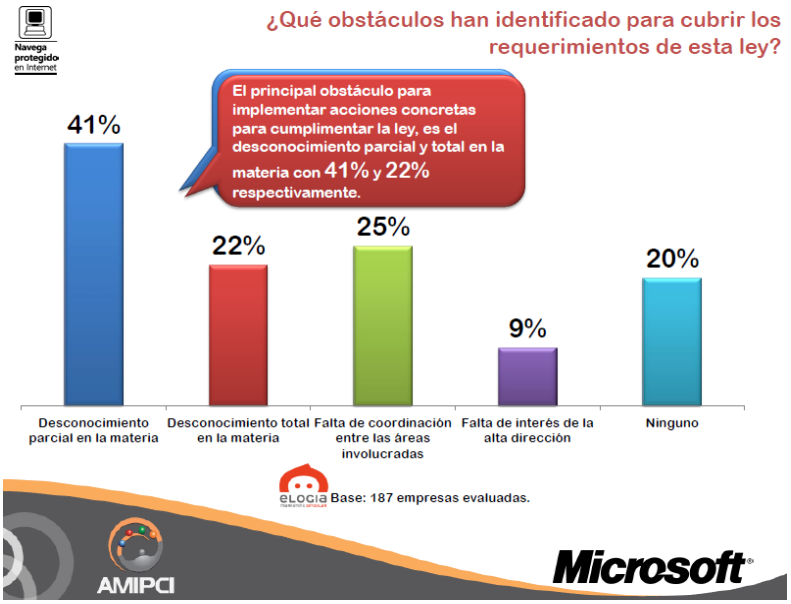

Imagen 11 Obstáculos para hacer cumplir la LFPDPPP. AMIPCI.

En contraste, 64% dijo ya haber establecido políticas de privacidad y 62% haber elaborado un aviso de privacidad. (AMIPCI 13)

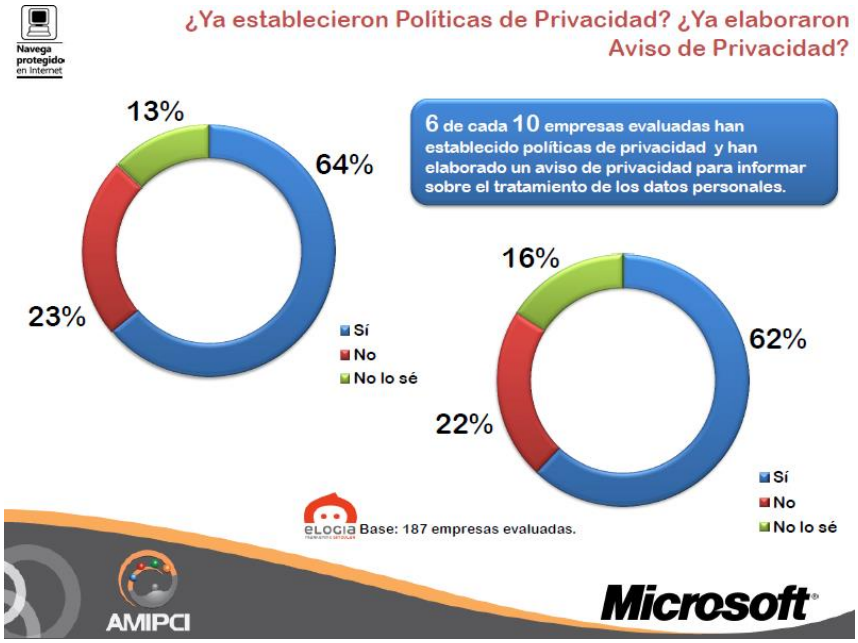

Imagen 12. Políticas y aviso de privacidad. AMIPCI.

Para ser claros, debe describirse al aviso de privacidad como el documento que informa al usuario, quién recaba información y para qué fin, así como los medios para ejercer sus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y este debe mostrarse siempre que se recaba algún dato salvo que se haya facilitado previamente. (Diario Oficial de la Federación, LFPDPPP 5–7)

En ese sentido, si bien es posible ver el vaso un poco más que medio lleno, puede decirse, que existe un 32% y 36%, que aún no cumple con esta. Pero donde el vaso se ve un poco vacío, es en lo referente a los derechos ARCO, donde un 58% apenas lo ha escuchado o lo desconoce completamente. (AMIPCI 16)

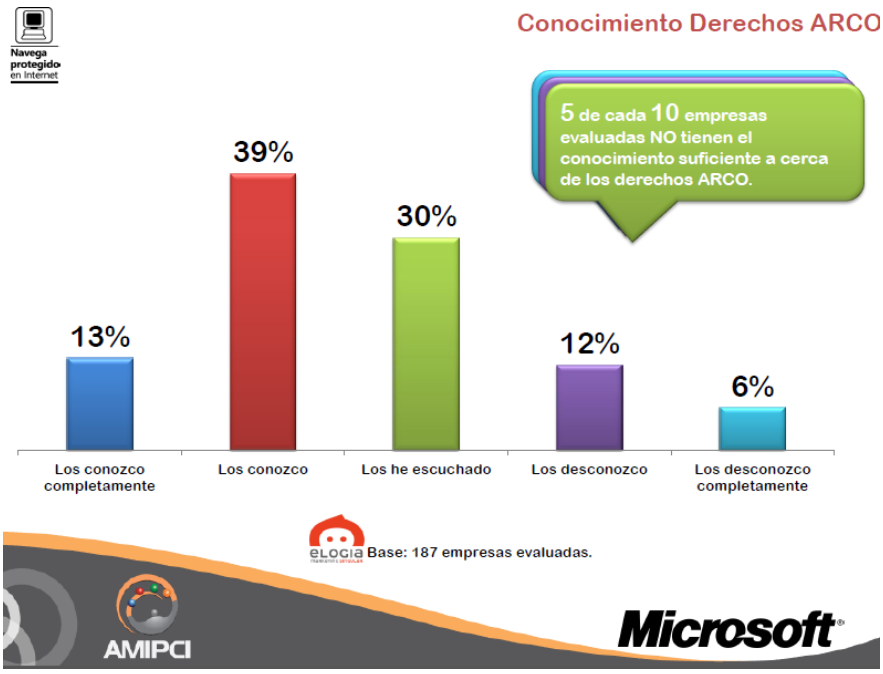

Imagen 13. Conocimiento sobre los derechos ARCO. AMIPCI.

Imagen 14. Delimitación del proceso para ejercicio de los derechos ARCO. AMIPCI.

Finalmente, sólo el 34% de las empresas encuestadas delimitó un proceso para las solicitudes de ejercicio de derechos ARCO, contra un 68% que no lo hizo o lo ignora. (AMIPCI 17)

A manera de resumen debe decirse, que al menos en 2012, el conocimiento y aplicación por parte de las empresas no fue total ni mayor, en la mayoría de los casos, al 50% y si no se cumple con la LFPDPPP y no se ejecutan mecanismos para el ejercicio del usuario de sus derechos ARCO, de poco sirve el aviso de privacidad, que hay que recalcar, tampoco en todos los casos existe.

Por otra parte, la asociación civil en pro de la privacidad digital, SonTusDatos, disponible en https://sontusdatos.org, mediante encuesta realizada a 49 empresas mexicanas, entre 2016 y 2017 (siete empresas representativas de siete sectores de la economía) descubrió que:

- El total de las empresas encuestadas (49 empresas) cuentan con avisos de privacidad, pero ninguno de ellos menciona el procedimiento de notificación de vulneraciones de datos personales a las y los titulares.
- 24 declaran tener un departamento de protección de datos personales, pero en los hechos son mucho menos las empresas que cuentan con el personal adecuado en la materia.
- En general, ninguna de las empresas encuestadas conoce su obligación de cumplir con la obligación de notificar vulneraciones de seguridad de los datos personales que manejan, o por lo menos demuestra haber empezado a implementarla. (SonTusDatos, párr.13)

Con lo que se esboza el incumplimiento de las obligaciones de estas empresas, respecto del cuidado de los datos personales, en un contexto más cercano al presente.

En conclusión, muchos usuarios podrían haber accedido y seguir haciéndolo, a sitios web y redes sociales digitales, ingresar información personal e ignorar si la empresa gestora protege (y si lo hace adecuadamente) sus datos personales, o sí hay alguien capacitado que se encargue de ese rubro en la organización, bajo qué límites se trata su información (si existen) y si esta se comparte con terceros. Es decir, se trata de un territorio incierto, aguas peligrosas en las que es aventurado navegar.

I.VI. Riesgos y pérdida del control de la información personal en Internet

En un breve resumen, se puede decir, que la privacidad en lo digital es un derecho y que la información que la involucra puede autorizarse para ciertos fines y con ciertos límites. Las empresas o personas que acceden a dicha información deben poseer facultades para revisar que en todo momento se cumpla con los criterios establecidos, pero hay falta de claridad, como se ha observado, en los conceptos y acciones que usuarios-empresas deben vigilar.

Lo anterior supone riesgos, mismos que es necesario esquematizar para, que una vez se haya definido un eje, sea posible valorarlo por sus partes y así conocer todo aquello que puede comprometer la privacidad de las personas en Internet.

Daniel Solove, experto en derecho de privacidad y profesor de leyes de la Facultad de Derecho de la Universidad George Washington; preocupado por la noción de privacidad dentro de las nuevas tecnologías de comunicación e

información, en su artículo *A Taxonomy of Privacy* y en su obra *Understanding Privacy,* describe que la privacidad puede ser entendida de modos diferentes de acuerdo al entorno. En ese afán enumera cuatro grupos básicos, dentro de los cuales pudiera menoscabarse la privacidad. Ellos son el de recopilación de información, procesamiento de información, diseminación de información y el de invasión. Dicha taxonomía busca hallar de forma más estructurada los peligros y sus soluciones. (Lucena Cid 137–38)

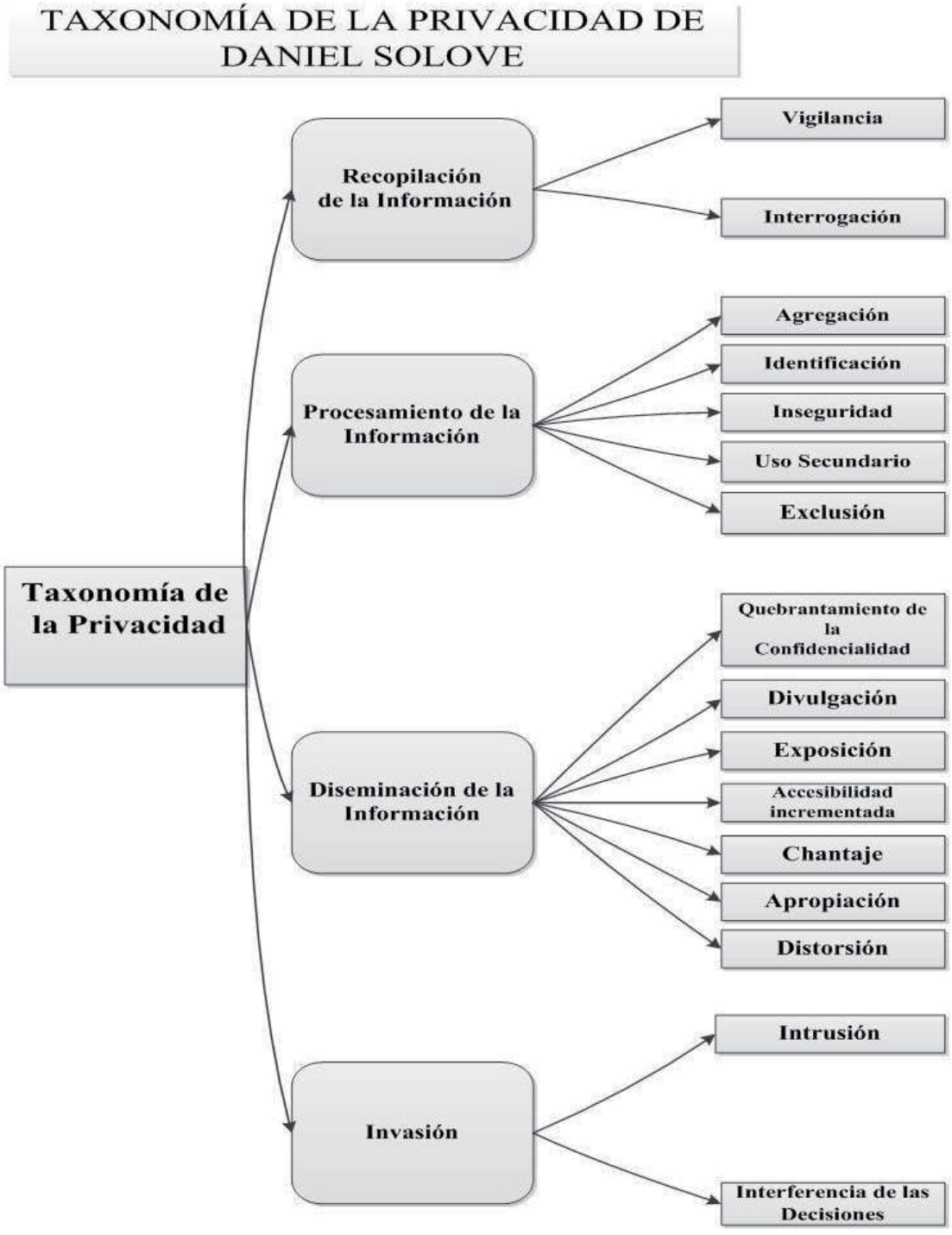

Imagen 15. Taxonomía de Solove. (Lucena Cid 141)

I.VI.I Recopilación de información

A propósito de la recopilación de información de datos se distinguen dos rubros, el que nace con el propósito de la vigilancia y que el surge de la interrogación.

La vigilancia como tal existe desde hace tiempo y de algún modo, estamos acostumbrados a ella, pero su existencia, sobre todo en grados fuera de los acostumbrados, modifica el comportamiento de las personas e inhibe ciertas conductas, a la vez que puede falsear otras. (Lucena Cid 138) En el presente no sólo es posible analizar información de personas específicas, puede hacerse también en masa.

Una consideración importante al respecto, expresada en palabras de Isabel Victoria Lucena Cid, profesora titular del Área de Filosofía del Derecho y Política, licenciada en Filosofía por la Universidad de Sevilla y doctora con mención europea y Premio de Doctorado en 2008, habla de las posibilidades coercitivas como medio para hacer valer ciertas normas, pero sus consecuencias también son en contra de la libertad, individualidad y espontaneidad que cada sujeto podría poseer.

Procesamiento de la información

Posterior a la recolección de datos se da el procesamiento de la información, momento, en el que Solove encuentra cinco problemáticas latentes: *agregación, identificación, inseguridad, uso secundario y exclusión.* (Lucena Cid 139)

En el apartado de *agregación*, Solove se refiere a la posibilidad de desarrollar el perfil de una persona a partir de la triangulación y posterior organización de sus datos, para generar a través de ellos nueva información. Sobre este nuevo contexto, el usuario puede no tener conocimiento y por ende, el

control. Solove en voz de Lucena expresa: *la agregación puede ser una amenaza a la intimidad porque altera las expectativas de las personas.* (Lucena Cid 139)

Identificación, de acuerdo con el autor, es asociar datos distintos de una persona para cerciorarse de su identidad. Aunque es positivo; según se considera en el texto fuente, cuando se trata de asegurarse de la fiabilidad de los individuos, se vuelve negativo si el anonimato les es arrebatado a las personas. (Lucena Cid 139)

La *inseguridad* tiene que ver con los llamados delitos cibernéticos. Todos aquellos que son susceptibles de ser, a partir del mal manejo de los datos de los usuarios. (Lucena Cid 139)

Como su nombre lo indica, el *uso secundario*, refiere a una segunda utilización de la información de las personas, para fines no mencionados y lejanos a la justificación original. Aquí se defrauda la confianza de las personas, dejándoles en un estado de duda y vulnerabilidad. (Lucena 139)

Por *exclusión* debe entenderse el impedimento al usuario de participar en el mantenimiento y utilización de su información personal. Su problemática radica de acuerdo a Solove y Lucena, en que cada vez en mayor grado se toman decisiones sobre las personas a partir de sus datos personales sin que ellos puedan intervenir previamente la información que de ellos existe digitalmente. (Lucena Cid 139)

I.VI.III. Diseminación de la información

En este rubro se tratan de igual forma los conflictos derivados de la revelación de la información personal, además de la amenaza de difundirla. Aquí se enumeran los de *quebrantamiento de la promesa de confidencialidad*, el de *divulgación*, el de *exposición*, el de *accesibilidad*

incrementada, el de *chantaje*, el de *apropiación* y el de *distorsión.* (Lucena Cid 140)

El *quebrantamiento de la promesa de confidencialidad* comprende divulgar la información personal que poseen profesionales o compañías. Esta sólo se rompe si el bien común lo requiere. Por otra parte, la *divulgación* supone una amenaza a la seguridad de las personas, pues les hace susceptibles de recibir daño físico, financiero, moral, etc. Un contrasentido es el que hace suponer que limitar la divulgación atenta contra la libertad de expresión, pero ambas promueven la libertad individual. Aquí se habla de información sobre la salud y cuerpos de las personas. (Lucena Cid 140)

La información personal de un ciudadano común sólo debería ser divulgada con autorización, un caso distinto de los servidores públicos, que están obligados parcialmente a transparentar su quehacer cotidiano, en aras de la certidumbre sobre su proceder.

La *exposición* está íntimamente ligada con la *divulgación* y se entiende como la exhibición a terceros de aspectos físicos, psíquicos y emocionales de las personas. Aquí se abarca un rango mayor de datos alusivos a la reputación de los individuos. (Lucena Cid 140)

La *accesibilidad incrementada* se da para que las personas encuentren la información necesitada con mayor facilidad. Los riesgos de esta es que posibilita la explotación para propósitos distintos a los originalmente pensados. Aquí Lucena Cid, menciona como ejemplos las bases de datos que las compañías crean con los registros públicos con fines comerciales o de análisis. (Lucena Cid 140)

La exigencia de dinero u otro tipo de favores con la amenaza de divulgar información que pudiera causar perjuicio a una persona es el *chantaje*. A través de ellas se pueden someter sus decisiones. (Lucena Cid 140)

En otro apartado, Solove habla de *apropiación*, pero precisa, un término más cercano es el de *explotación*, sin embargo, se decanta por utilizar el primero. Este refiere al uso indebido de la identidad de una persona para perseguir los fines u objetivos de otra. Un ejemplo es cuando se asocia a cierto individuo con un producto. Se le considera un uso nocivo por atentar contra la libertad y desarrollo personal. En palabras de Lucena (Lucena Cid 140):*Utilizar la imagen de una persona sin su consentimiento para promover un producto se asemeja mucho a obligarla a representar y respaldar ciertos puntos de vista.* (Lucena Cid 140)

Finalmente, la distorsión es la divulgación y exposición de información, incompleta o falsa, en la que se pretende hacer que una cosa pueda parecer otra. (Lucena Cid 140)

Es en este punto donde se pueden apreciar la mayor cantidad de riesgos posibles para la persona y su privacidad, ahí la importancia de mantener estos conceptos presentes para su posterior análisis en el contexto nacional.

I.VI. IV. Invasión

Los conflictos de la *invasión* para Solove, son divididos en dos, por una parte, la *intrusión* y por otro la *interferencia en las decisiones*.

La *intrusión* es la afectación de la intimidad del individuo a causa de la presencia o actividad de otra. (Lucena Cid 141)

A ese respecto Solove puntualiza:

> La intrusión es cualquier acto que atenta contra el derecho que tienen todas las personas a ser dejadas en paz. La intrusión no necesariamente involucra incursiones espaciales; el *spam*, el correo basura, no por ser aparentemente un mal menor en el uso de las tecnologías de la información, es menos molesto e incluso nocivo. (Lucena Cid 141)

Por último, *la interferencia en las decisiones*, consiste en la intromisión del Estado en las determinaciones que el individuo debiera poder tomar en lo que concierne a su vida. Solove la relaciona con la autonomía (Lucena Cid 141):

> Algunos ejemplos de intromisión del Estado en decisiones privadas de cada individuo serían la prohibición de usar anticonceptivos, la prohibición de mantener relaciones sexuales entre personas del mismo género, etc. (Lucena Cid 142)

Es con estos puntos que el autor simplemente busca delimitar las problemáticas posibles para su correcta interpretación y medición. Solove toma en cuenta todos los contextos posibles, aunque reconoce no deben verse como rubros inamovibles o únicos, aun así, son un punto de partida para su estudio.

Son puestos aquí porque se ven cercanos y análogos a la protección de datos personales y porque engloban los distintos niveles en que la intimidad y privacidad de los individuos puede ser atacada o verse en peligro.

Lo que se puede deducir de lo anterior, es que evitar la recopilación de información imposibilita el procesamiento y diseminación indebida de la misma, así como la invasión; los otros tres puntos planteados por Solove.

También podría ayudar compartir o ingresar información, únicamente, en sitios y plataformas que sepamos seguras.

I.VII. Riesgos en México

Con base en la taxonomía de Solove, el paso siguiente es ubicar si estos riesgos se traducen en realidades para los usuarios de Internet en México.

Para tal meta, se han buscado datos que den evidencia de los principales riesgos dentro de los límites geográficos establecidos. Si bien, en algunos casos, no se hallaron datos contundentes que reflejen su realidad en territorio nacional, se sabe hay información a nivel continental o mundial que puede dar certidumbre de su existencia y de la posibilidad de su presencia en México. En los casos que se consideren necesarios, se describirá aquello que se crea de valor para este trabajo para no dejar de lado su consideración.

A fin de cumplir el objetivo se ha intentado echar mano de aquella información disponible, que comprende a organismos no gubernamentales, oficiales, artículos periodísticos, académicos e investigaciones; útiles para ilustrar el panorama.

I. VII.I. Recopilación de información: interrogación y vigilancia

Luis Fernando García y Jesús Robles Maloof, ambos abogados especializados en derechos humanos y digitales, exponen en el libro *Internet en México, Derechos Humanos en el Entorno Digital*, publicado por Derechos Digitales; Organización, enfocada en derechos humanos y tecnología de américa latina, la realidad que descubren tras su investigación respecto de la privacidad en Internet, dentro de México y sus principales retos. Así pues, se habla de ambigüedad sobre qué autoridades y bajo qué circunstancias están facultadas para vigilar (Derechos Digitales et al. 168):

> La legislación no señala con precisión la identidad de las autoridades facultadas para llevar a cabo medidas de vigilancia. En particular, la Ley Federal de Telecomunicaciones y Radiodifusión no es clara respecto a qué autoridades pueden implementar medidas como la localización geográfica en tiempo real de dispositivos de comunicación o el acceso a metadatos de comunicaciones conservados por las empresas de telecomunicaciones. (Derechos Digitales et al. 181)

Además, pese a existir certidumbre de ciertas autoridades facultadas para vigilar, la instrucción de cuándo, cómo y porqué deben hacerlo todavía no es clara. Es el caso de los Ministerios Públicos Federales y Locales, el Centro de Investigación y Seguridad Nacional (CISEN) o la Policía Federal. En ese sentido, *amenaza a la seguridad nacional* que sería la premisa para dar cabida a la vigilancia, es susceptible de ser interpretada de muchas maneras. (Derechos Digitales et al. 182)

Lo anterior se traduce en poca claridad en cuanto a los métodos de colaboración que existen entre autoridades y empresas para llevar a cabo medidas de vigilancia.

> Es el caso del artículo 189 de la LFTR o el artículo 301 del CNPP, los cuales hacen exigencias genéricas, incluso de carácter técnico, para facilitar la vigilancia de comunicaciones. (Derechos Digitales et al. 183)

Para mayor claridad, a continuación, se muestran los artículos 189 y 190 de La Ley Federal de Telecomunicaciones y Radiodifusión (LFTR):

> Artículo 189. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y

contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.

Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación. (Diario Oficial de la Federación, LFTR 56)

El artículo 190 a continuación:

Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.

Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable.

El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna;

II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud. (Diario Oficial de la Federación, LFTR 56)

En ambos artículos puede observarse la obligatoriedad de las empresas de compartir información cuando les sea solicitada por las autoridades; que esta comprende toda clase de datos personales que pueden ser o no sensibles; que mediante la triangulación puede construirse el perfil completo de una persona. Incluso se señala la obligación de proveer mecanismos para acceder a esa información (datos y metadatos[6] de todas las comunicaciones), por 12 meses y almacenarla 12 meses más (24 meses totales).

---

[6] Metadatos: consisten en información que caracteriza datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos. (Secretaría del Gobierno Digital, párr.1)

Luego entonces, ante la ambigüedad sobre qué autoridades pueden vigilar y solicitar información; la poca certidumbre sobre los protocolos autoridad – empresa y opacidad sobre la correcta invocación de estas prácticas; además, del prolongado tiempo que nuestros datos deben estar almacenados por las empresas, se puede inferir, hay pocas garantías de que nuestra privacidad esté bien resguarda y que sea respetada, más si vivimos en un país con altos índices de corrupción.

Dos precisiones son prudentes, la primera, estas obligaciones son para empresas que proveen tanto servicios de comunicación, como comunicación móvil (Telmex, Axtel, Telcel, AT&T, Movistar, entre otros); la segunda, estos artículos ya fueron ratificados por la Suprema Corte de Justicia de la Nación, al considerar que no transgreden los derechos humanos a la intimidad, así como a las comunicaciones privadas toda vez que el campo de acción está limitado a temas de prevención, investigación y persecución del delito. (El economista, párrs.1–7)

De acuerdo con información periodística del diario Animal Político, en México, desde la administración pasada de Felipe Calderón Hinojosa, se contrataron los servicios de Hacking Team. (Animal Político 1)

Dicha empresa, dentro de su sitio http://www.hackingteam.it/, se auto define como la suite de hackeo[7] para la intervención gubernamental: *the*

[7] Se asocia regularmente, de manera errónea, la palabra *hacker* con pirata informático, cuando en realidad suelen ser investigadores, con amplios conocimientos informáticos, capaces de introducirse en sistemas, no necesariamente para fines ilícitos y en muchas ocasiones sí para lograr mayor seguridad. Cuando de actos delictivos se trata, algunos se decantan por utilizar el término *cracker*. Por ello no hay que criminalizar el concepto en lo general, pese a la connotación que en algunos casos (como este), adquiere. (Fundéu BBVA, “hacker y cracker, diferencias de significado”, párrs.1–6)

hacking suite for governmental interception y dice ofrecer soluciones de ciberseguridad ofensivas y defensivas. (Hacking Team, párrs.1–3)

Con base en la información investigada y dada a conocer por Reporteros Sin Fronteras y la mencionada publicación, (consecuencia de 400 Gb de información sustraída de la firma), el 5 de junio de 2015; son 16 los clientes mexicanos que han adquirido los servicios de la empresa italiana. Los montos de estos contratos suman poco menos de 100 millones de pesos. (Animal Político, "México, el principal cliente ", párrs.2–18)

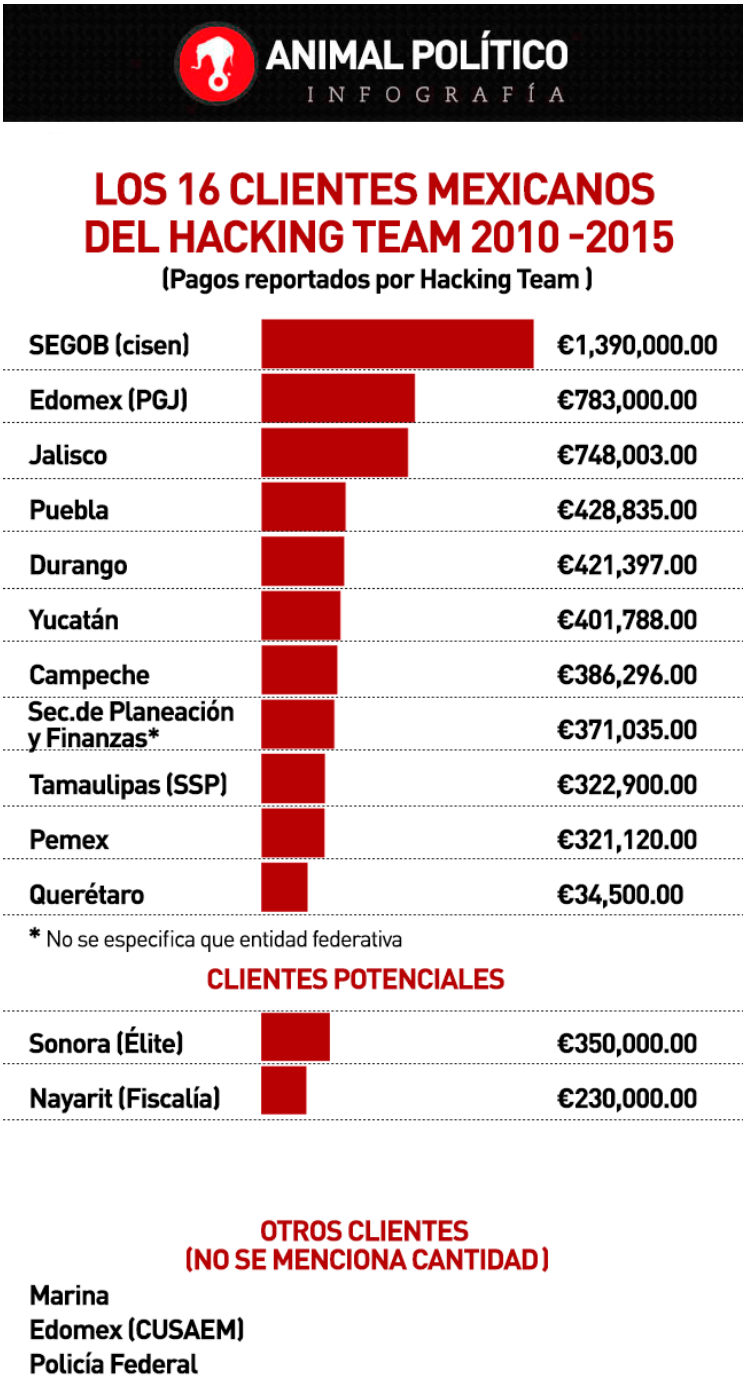

Imagen 16. Lista de adquisiciones por dependencia y / o Estado de los servicios de Hacking Team. Animal Político. (Animal Político, "México, el principal cliente ", párrs.2–18)

Imagen 17. Ubicación de los lugares donde Hacking Team tiene contratos. (Animal Político, "Gobierno de Puebla" párr.11)

Un dato importante a señalar es que entre los elementos listados en la infografía anterior (Gráfico 16); y que obedecen a documentos filtrados de Hacking Team, entre las dependencias señaladas, hay varias que no tendrían la facultad legal para realizar prácticas de vigilancia e intervención, tal es el caso de la Secretaria de Planeación y Finanzas o Petróleos Mexicanos (Pemex).

Otro caso significativo es el de la Secretaria de la Defensa Nacional (Sedena), que en el mismo 2015, pese a no estar facultada para intervenir comunicaciones privadas, negoció un contrato por 66 millones de pesos con Hacking Team, para adquirir *software* de espionaje con la capacidad de

intervenir y extraer información de hasta 600 blancos u objetivos. Esto según los documentos filtrados y anteriormente mencionados. (Animal Político, "Sedena negoció", párrs.1–15)

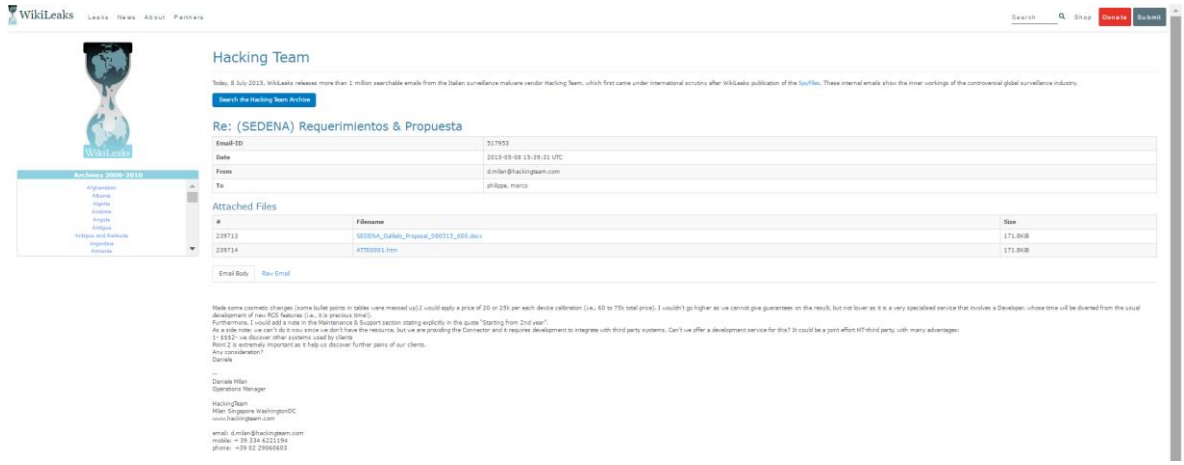

Imagen 18. Correo de la propuesta de Hacking Team a Sedena. (WikiLeaks, párrs.1–5)

Entre las precisiones requeridas por la Sedena se encuentran:

> * Sistema de Monitoreo Remoto (Galileo)*600 licencias para instalar agentes de monitoreo (espionaje) en computadoras y smartphones*21 estaciones de trabajo (computadoras nuevas y de fábrica) para operar sistemas*Capacidad para intervenir sistemas operativos Android, iOS, BlackBerry, Windows, Mac OSX, Linux Kernel*Capacidad para intervenir objetivos en redes Wi-Fi y de empresas Telcel, Movistar, Iusacell, Unefon y Nextel*Infección de smartphones vía SMS, WhatsApp, Facebook, Messenger, Skype, Line, etc.*Infección mediante envío de imágenes en general.
>
> *Infección a través de códigos QR.
>
> *Infección capaz de activar micrófonos, cámara de fotos, cámara de video.

*Infección en computadora capaz de extraer toda la información además de registrar pulsos en el teclado.

*Mantenimiento correctivo y preventivo de todo el equipo. (Animal Político, "Sedena negoció", párrs.24–27)

Precisamente, de los servicios contratados por las distintas entidades destaca *Da Vinci* o *Galileo*, *Remote Control System*, programa malicioso que se instala en *smartphones* y ordenadores, que posibilita extraer información además de registrar que botones son oprimidos en el teclado. (Animal Político"México, el principal cliente", párr.5)

De acuerdo con Luis Fernando García, director de la Red en Defensa de los Derechos Digitales (R3D), organización no gubernamental, dicho programa *tiene la capacidad de espiar conversaciones vía Skype o WhatsApp, saquear toda la información de un disco duro y convertir en auténticos micrófonos espía teléfonos o equipos de cómputo*. Lo que coincide con las necesidades precisadas por la Sedena. (Animal Político, "Sedena negoció", párrs.21–24)

Un ejemplo de utilización no ética de este *software,* es el del gobernador de Puebla Rafael Moreno Valle, que, según investigación de Animal político, intervino computadoras de sus adversarios para hacerse de información valiosa (Animal Político,"Gobierno de Puebla", párrs.1–8):

Entre mayo de 2013 y junio de 2015 el gobierno de Puebla solicitó a Hacking Team, bajo el usuario "UIAPUEBLA", la creación de al menos 47 archivos *exploit* camuflados como archivos de Word o presentaciones de PowerPoint para infectar equipos de cómputo y comunicación. (Animal Político, "Gobierno de Puebla" párr.32)

En el artículo citado y consultable aún en su página web, se describe como con estos *exploits* (archivos que posibilitan la instalación de *software*

malicioso para la extracción de información), y mediante la suplantación de identidad en correos electrónicos, se intervinieron equipos computacionales, lo que facilitó la adquisición de información, en un presumible atentado a la privacidad de las personas. Estos ataques fueron dirigidos, no a probables delincuentes, sino a actores políticos.

Tras lo anterior, se constata que este tipo de *software* tiene cabida en el gobierno mexicano y no necesariamente para fines legítimos, ¿bajo qué lógica Petróleos Mexicanos o la Secretaria de Planeación de Finanzas requiere o debe intervenir y espiar la comunicación de las personas? ¿Qué medidas precautorias existen que validen que este tipo de aplicaciones no sean utilizadas fuera de sus límites como en el caso de los intereses políticos brevemente ejemplificados?

Si bien no somos todos actores políticos o empresariales, periodistas, activistas, etc., en algún momento de la vida podríamos ser intervenidos (o ya serlo), sin que exista legislación que valide este tipo de prácticas.

Por otra parte, esa vigilancia, aun de suponerse que existieran fines válidos, permite el conocimiento de aspectos de la vida privada de los individuos fuera de la motivación inicial y como se ha dicho en el apartado anterior, no hay certidumbre o rendición de cuentas que de fe de a quién o quiénes se ha vigilado y por qué circunstancias, lo que deja un camino abierto a toda clase de intenciones en la utilización de este tipo de programas.

Finalmente, es oportuno destacar los medios por los cuales pueden ser intervenidos los dispositivos (imágenes, códigos QR y *exploits*). Y que estas intromisiones se dan incluso en nuestras redes sociales digitales (WhatsApp, Facebook, Messenger, Skype, Line, etc.), que esto puede darse sin distingo de compañías de telefonía móvil o sistema operativo. En pocas

palabras, en apariencia, no habría modos simples de defenderse de este tipo de ataques. Algo a analizar y desarrollar en el siguiente capítulo.

Dentro de este apartado se entremezclan y observan la vigilancia a la población en general y la interrogación, que, si bien en este caso no es apreciable totalmente en el usuario final, se da a los prestadores de servicio, que se ven obligados a tomar acciones ante la posibilidad de ser interrogados. Por otra parte, es difícil saber cuánta gente en México modifica su comportamiento en Internet por sentirse vulnerable u observada, aunque también ya se ha visto, como un porcentaje alto de personas teme por su información y patrimonio al interactuar en las redes sociales digitales y ese temor, hay que decir, no obedece únicamente a las instituciones, también provoca miedo el ser víctima de la ciberdelincuencia. Una apreciación final de este numeral, es que, por las características propias de operación de los *softwares* y protocolos mencionados, aquí tiene cabida la intrusión, un concepto manejado por Solove en lo referente a la Invasión.

I.VII. II. Procesamiento de la información: agregación, identificación e inseguridad

La posibilidad de ser perfilado a través del rastro y triangulación de nuestro quehacer cotidiano en Internet, ya sea dentro o fuera del territorio nacional, es una realidad, incluso hay sitios en Internet que, mediante el cobro de cierta cantidad de dinero, mejoran las posibilidades de búsqueda de personas por su correo electrónico, nombre, ubicación o lugar de nacimiento, entre esos servicios se encuentran 123people.es, Pipl.com, Peekyou y Whozat.

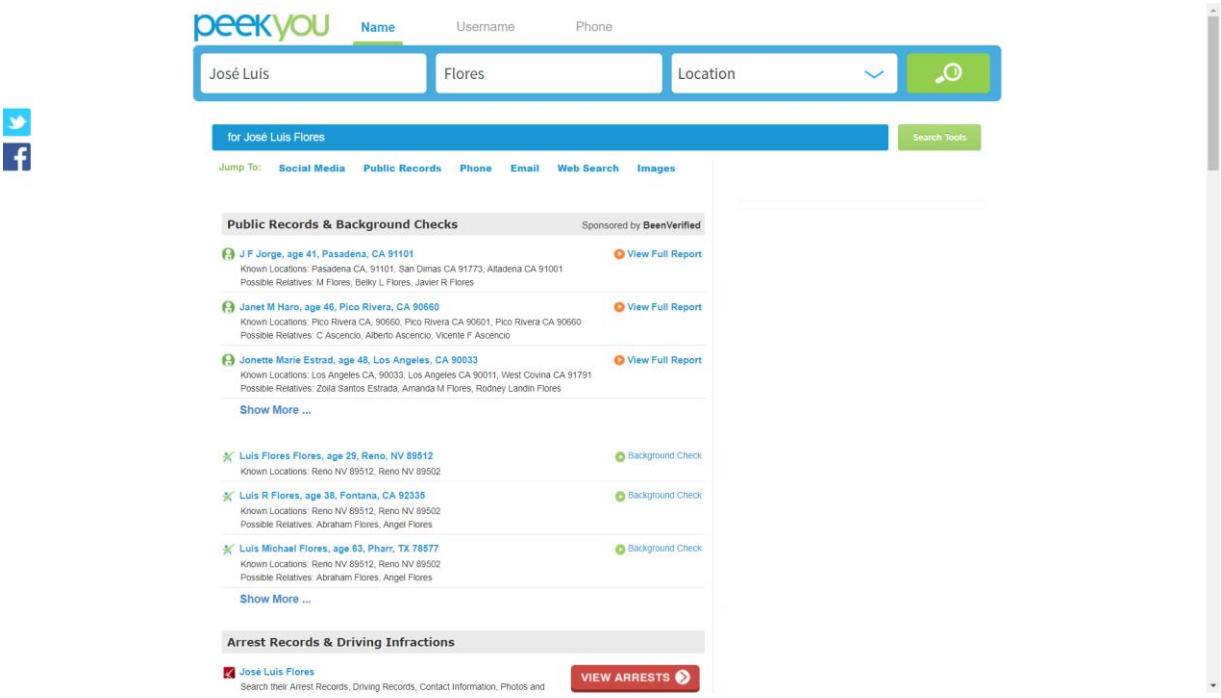

Imagen 19. Agregación en Peekyou.com. Captura de pantalla.

En el gráfico anterior, por ejemplo, puede observarse como a través del nombre, apellido y lugar de residencia, es posible conseguir más información, entre ella, las redes sociales digitales, publicaciones, imágenes, número telefónico si está disponible o hasta litigios en curso, de la persona de interés.

Sin embargo, en muchas ocasiones, ni siquiera ello es necesario, porque con una simple búsqueda en las redes sociales digitales de preferencia (Facebook, Twitter, etc.), o en el buscador de Google, se puede obtener información de la persona deseada, si esta es pública en dichos lugares.

Por ejemplo, si conocemos el nombre de una persona y/o su cuenta de correo electrónico y esta cuenta se encuentra vinculada a todos sus servicios de redes sociales digitales, aplicaciones y además participa activamente en Internet, seguramente podrá conocerse alguna red social a la que esté suscrita, si esa cuenta tiene carácter parcial o completamente

público, habrá información sobre sus intereses y lugares frecuentados, amistades y parentescos, sin olvidar que ciertas empresas e instituciones manejan directorios públicos en sus sitios web, lo que facilita el trabajo; dicha información con cierta pericia puede brindar un perfil completo de la persona.

Ejemplo de agregación

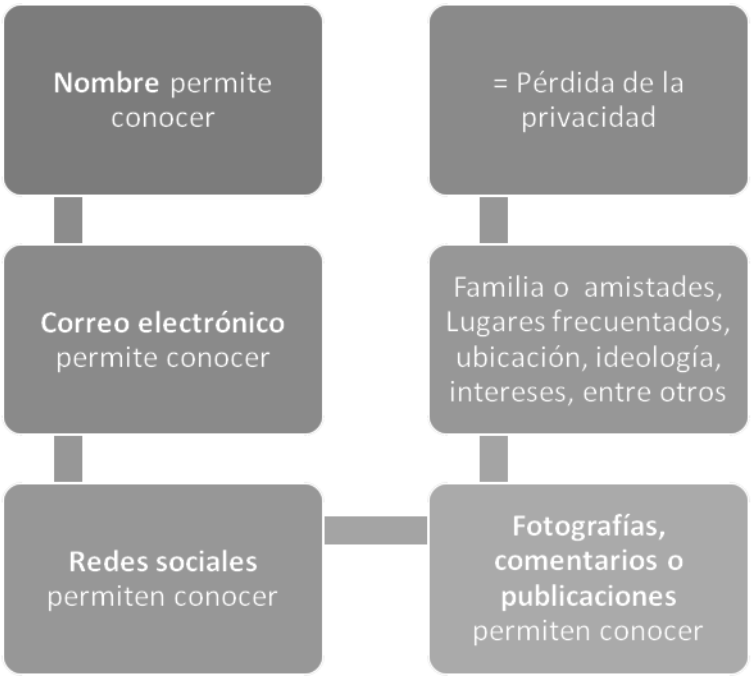

Imagen 20. Ejemplo de agregación. Elaboración propia.

Si bien, la privacidad de la red social digital o aplicación que se quiera utilizar muchas veces es configurable, la atención que como usuario se le da puede no ser la debida. Aquí se hace una atenta invitación al lector a que ejecute la búsqueda mencionada para reconocer que información sobre su persona existe en Internet y como podría ser triangulada. Intente identificarse. Para esto pruebe con sus distintos nombres de usuario, nombre real o correo electrónico.

Lo anterior supone un riesgo real casi para la mayoría de personas que utilicen internet y podría pensarse que con ciertas precauciones es posible solventarlo parcialmente; no es el caso de ataques de mayor envergadura que involucran a gente especializada, que puede acceder a la información de forma más sofisticada, como es el caso del *phishing*; obtención de información confidencial, obtenida, mediante la suplantación de identidades morales o físicas con fines fraudulentos (regularmente una cuenta de correo apócrifa dirige a un sitio que aparenta ser conocido y de confianza, por lo que el usuario ingresa su nombre y contraseña u otra información, con desconocimiento de las intenciones reales). (Panda Security, Phishing párrs.1–3)

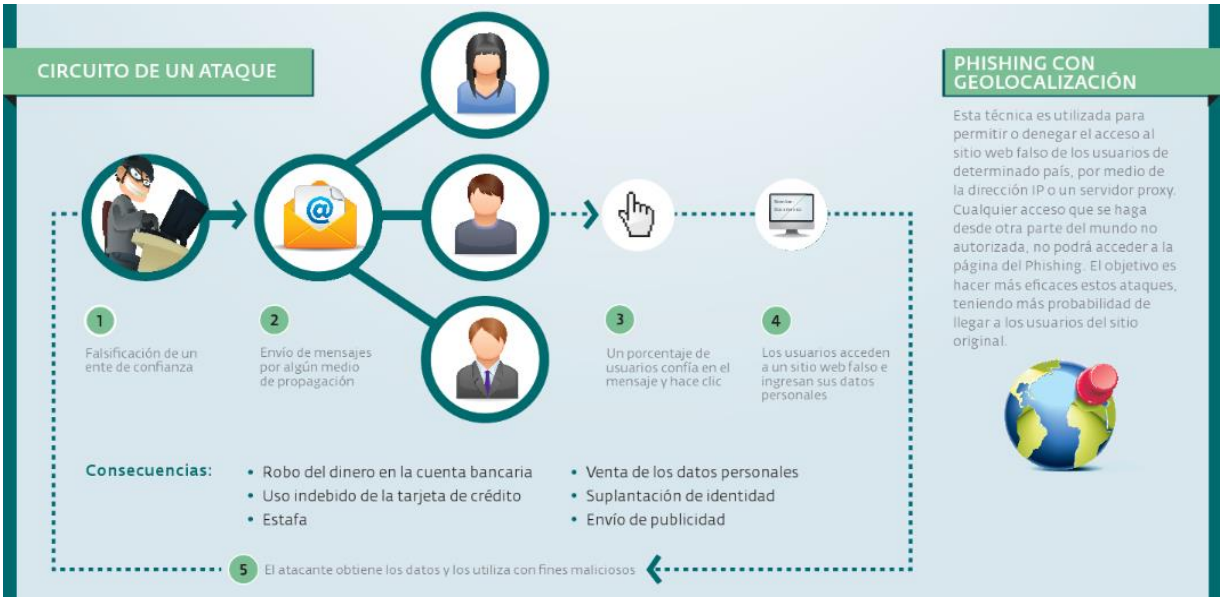

Imagen 21. *Phishing*. (InfoSpyware, ¿Qué es el Phishing?, párr.4)

Tras acceder a la información, el usurpador la utiliza para realizar pagos y/o contratar servicios, que incluyen la adquisición de tarjetas de crédito, seguros médicos y hasta pagos inmobiliarios. Según el Banco de México, este país es el octavo a nivel mundial en lo que a robo de identidad se refiere. (Condusef, "Protege tu identidad", párr.5)

Otra práctica conocida y recurrente es la del secuestro de datos, mejor conocido como *ransomware* que de acuerdo a Panda Security:

> … es un *software* malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear el PC desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. Para desbloquearlo el virus lanza una ventana emergente en la que nos pide el pago de un rescate. (Panda Security, "¿Qué es un Ransomware?" párr.1)

Una consideración al margen es si estos delincuentes trabajan sobre el azar o de qué manera saben con qué servicios cuentan las posibles víctimas.

De acuerdo al reporte del antivirus Norton by Symantec, publicado en 2013, los ciberdelitos en México dejaron pérdidas por 39,000 Millones de pesos con un costo promedio por víctima de 4,381 pesos. La misma empresa calculó un total de 10 millones de víctimas en 12 meses, lo que representa 27,397 víctimas por día y 19 víctimas por minuto. Con base en la misma información, la firma mencionada determinó que un 54% de los adultos han sido víctimas de algún ciberdelito. Como acotación también es prudente señalar que estos están vinculados al uso de dispositivos móviles sin protección adecuada, así como a la utilización de los mismos tanto para cuestiones laborales como personales. (Norton by Symantec, "Reporte Norton 2013", 5–19)

Imagen 22. Porcentaje de uso para trabajar y jugar en dispositivos móviles. (Norton by Symantec 5–19)

Otro dato no menos importante, es sobre la afectación a las empresas, que según Telefónica y Data Warden, genera en México, pérdidas por 3,000 millones de dólares anuales (Telefónica, párr.1):

> … las empresas son una de las principales víctimas de estos delitos y tardan en promedio 6 meses en reestructurar su información. Tan sólo en el rubro de Pymes, una de cada cinco empresas sufre algún tipo de ciberataque al año, de las cuales más de la mitad se va a quiebra después de 6 meses del ilícito. (Telefónica, párr.5)

Para ambas firmas, enfocadas conjuntamente en ofrecer servicios de seguridad en estos entornos, el país es el segundo lugar en ataques

cibernéticos con 22 millones de víctimas hasta enero de 2017. (Telefónica, párr.2)

Otros delitos cibernéticos no menos graves y punibles cuando se utilizan computadoras o sistemas como medios para, son:

- Exhibición, publicación, difusión, intercambio y comercialización de pornografía infantil.
- Extorsiones, fraudes electrónicos y amenazas.
- Falsificación de documentos vía computarizada.
- Negociaciones de secuestros.
- Lectura, sustracción o copiado de información confidencial.
- Aprovechamiento indebido o violación de código para ingresar a sistemas.
- Variación del destino de sumas de dinero a otras cuentas (transferencias electrónicas) (ASI-México, "Internet S.O.S", 4)

Por otro lado, cuando el acto va en agravio de sistemas, computadoras o dispositivos, puede categorizarse de la siguiente manera:

- Manipulación en los datos e información contenida en archivos o soportes físicos informáticos ajenos.
- Acceso a los datos y utilización de los mismos por quien no está autorizado para ello.
- Utilización del equipo y/o programas de otras personas, sin autorización, con el fin de obtener beneficios en perjuicio de otro.
- Introducción de rutinas o programas para destruir datos, información o programas.
- Utilización de la computadora con fines fraudulentos, con o sin conexión a Internet. (ASI-México, "Internet S.O.S", 4)

Se mencionan todos ellos con la intención de poder conocerlos y reconocerlos. Algunos de ellos, como la extorsión y amenazas han de ser recapitulados más adelante. Si bien, lamentablemente no de todos ellos hay datos concretos, es sabido que existen y en mayor o menor medida somos susceptibles de padecerlos.

Como ha podido observarse, cada uno de los rubros, pretextos del subtítulo de este apartado, están vinculados, lo que hace difícil su mención sin relacionarlos, por ello se dispuso explicarlo del modo que se hizo. Pese a ello ha de intentarse realizar un breve resumen.

En primera instancia la agregación de nuestra información posibilita la creación de un perfil, de igual forma estos datos, permiten la identificación de nuestra persona, cuentas o información personal, lo que puede comprometer nuestra privacidad e intimidad; en muchos casos, hace peligrar nuestro patrimonio y/o bienestar e integridad y el de las personas a nuestro alrededor. Por si fuera poco, este problema no debe observarse solo como personal, porque también afecta a las empresas (aquí se alude a aquellas que ofrecen toda clase de productos y servicios, no necesariamente relacionados con Internet), pues como pudo verse, la puerta de entrada siempre es el ámbito personal, por lo que se sabe, no solo el patrimonio individual está en juego. Todo esto entraría en el rango de la inseguridad.

I.VII.III. Procesamiento de la información: uso secundario y exclusión

En el caso de usos indebidos de datos personales, no contemplados al ser recabados por las empresas y por ende no mencionados. Se sabe que de 2012 a 2016, 113 empresas que hicieron mal uso de ellos han sido sancionadas, esto de acuerdo al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), lo que derivó en

multas por 275 millones 533 mil pesos. (Animal Político, “113 empresas”, párrs.1–6)

Las instituciones financieras, serían las que desobedecen en mayor medida la ley, aunque también se encontró que escuelas, hoteles, hospitales y tiendas departamentales, también lo hicieron. (Animal Político, “113 empresas”, párr.4)

Es necesario señalar que algunas de estas empresas no pueden ser mencionadas según el INAI, por encontrarse en proceso de impugnación, pero de acuerdo a una solicitud de información hecha por sontusdatos.org, hoy se sabe que entre las empresas que han impugnado y nulificado el pago de dichas multas se encuentran:

- Tarjetas Banamex, S.A. de C.V.
- Operadora Oceánica Internacional, S.A. de C.V.
- Señalética y Publicidad S.A. de C.V.
- Afore XXI Banorte S.A. de C.V.
- BBVA Bancomer S.A. Institución de Banca Múltiple, Grupo Financiero BBVA Bancomer.
- Banco Nacional de México, S.A., integrante del Grupo Financiero Banamex.
- Pharma Plus S.A. de C.V. (San Pablo Farmacia). (SonTusDatos.org, párrs.8–9)

La transferencia de base de datos o reutilización con fines distintos para lo que los datos personales fueron dados, son una constante. Lo que se traduce en recepción de llamadas o correos electrónicos para ofrecer productos o servicios. Hay que recordar que el agravio no es sólo la utilización indebida, también lo es no informar al usuario de la transferencia de su información o uso secundario.

El caso específico de la exclusión es ambiguo, pero pudiera ser entendido si ubicamos a cualquier persona que sea impedida de acceder a un sitio, foro, servicio, entre otros, por su credo, ideología, género, etc., lo que no corresponde necesariamente a un delito, pero es algo que ocurre en el plano físico y puede suceder también en el digital. Otra forma de verlo sería el acceso desigual a Internet que priva en México como consecuencia de las políticas públicas locales y nacionales, pero esto escapa del objeto de estudio pretexto de esta tesis.

Luego entonces, el uso secundario ya fue descrito en el panorama mexicano para su contextualización, basta decir, que se ha comprobado su existencia, y puntualizar que es de igual forma, una invasión a la esfera privada de las personas, toda vez que implica abusar de su confianza y extralimitarse en los permisos que conceden. Si hiciéramos una analogía con el mundo físico, equivaldría a que alguien vendiera nuestra dirección, nombre y hasta intereses a otro para que ofrezca algo presentándose en nuestra casa sin invitación.

I.VII. IV. Diseminación de la información: quebrantamiento de la confidencialidad, divulgación y exposición

Si bien, en el caso específico del quebrantamiento de la confidencialidad, no ha sido posible precisar información de carácter cuantitativo que refleje la realidad en el contexto mexicano, puede establecerse, que esta también se da al compartir información privilegiada a personas o empresas fuera del círculo de autorización del usuario, lo que permite identificarlo. Como pudo observarse en apartados previos, esto constituye una falta a los derechos ARCO.

Luego entonces, el quebrantamiento de la confidencialidad puede dar paso a la divulgación, en círculos fuera de los previstos en el acuerdo de privacidad, hasta llegar a lo público.

Tal es el caso de la empresa Banamex sancionada en 2012, por el entonces llamado IFAI, Instituto Federal de Acceso a la Información Pública, por la cantidad de 9 millones, 848 mil 140 pesos, luego de que un particular se quejará de que sus datos se entregaran a un despacho de cobranza, lo que incluía su teléfono, por lo que recibía llamadas para reclamarle por adeudos ajenos a su persona. Dicho individuo recibió en un par de ocasiones del mismo banco respuesta por escrito sobre el cese de dichas acciones, sin que se tradujera en una realidad. Ante solicitud del IFAI de un pronunciamiento por parte de Banamex al respecto y caso omiso de la misma, se determinó finalmente la multa. (Animal Político, "IFAI multa", párrs.1–6)

Lo anterior se expone a fin de ejemplificar lo que puede y debe entenderse en nuestro contexto por quebrantamiento de la confidencialidad y divulgación. Aunque esto último no haya sucedido necesariamente en Internet, esboza la idea de cómo estas prácticas pudieran darse en el entorno digital.

Finalmente, la exposición, re explicada llanamente, es la divulgación con afán de establecer cierta reputación de las personas. Aquí las redes sociales digitales juegan un papel importante. En muchas ocasiones información vertida allí es retomada por otros con la intención de mostrar ilícitos o actos que creemos contravienen nuestra moral, pero también con el fin de entretener, muchas veces a expensas de otros, sin considerar el daño que se puede provocar a ciertas personas. En estos casos se vinculan imágenes, videos, documentos, información de números telefónicos y correos

electrónicos en un claro atentado contra nuestra privacidad, que, en muchas ocasiones, pone en peligro a las personas del círculo inmediato del afectado.

El origen de este problema radica en el usuario, que comparte información sin precisar las posibles consecuencias o alcances para otros, lo que hace necesario cierta sensibilización al respecto.

Como consecuencias de la divulgación, exposición e incluso la distorsión de información personal, ya fuera de control del usuario, se encuentran las amenazas, el llamado troleo[8], el ciberacoso, e incluso el denominado stalkeo[9], posible al conocer las cuentas públicas o semi públicas de la posible víctima, más vulnerable si comparte información sensible. Esto se visualiza en mayor medida en las redes sociales digitales.

Con lo anterior no se pretende culpar al usuario, pues se entiende que es un problema de índole social, no exclusivo de Internet, pero se pondera, que ciertas precauciones o acciones contribuirían a evitarlo, aunque no sea, bajo ninguna circunstancia, la única la solución de este problema.

Con base en un trabajo de investigación realizado por Microsoft titulado *Índice de Civismo Digital* y de alcance nacional e internacional, los usuarios manifestaron haber sufrido como consecuencia de su interacción en Internet: contacto no deseado, maltrato, provocación, mensajes de sexo no deseados y acoso en línea. 76% de los mexicanos reportó en ese sentido que el contacto no deseado es el mayor riesgo. Esto último también podría

---

[8] Troleo: intervenir con ánimo de hacer fracasar algo, molestar, cansar o enfadar. (Fundéu BBVA, *Troleo*, párrs.4–5)

[9] Stalkear: Acechar, espiar, husmear o incluso acosar, según el contexto, son alternativas en español preferibles a stalkear, término que se asocia con *seguir a alguien en las redes sociales para obtener información y observar sus movimientos.* (Fundéu BBVA, *Stalkear*, párr.1)

acotarse en el apartado de intrusión, una invasión clara del aspecto privado, que equivaldría a la irrupción de personas no deseadas en nuestros espacios de convivencia. (News Center LATAM, párrs.7–9)

I.VII. V. Diseminación de la información: accesibilidad incrementada

Una labor importante es la llamada minería de datos, que (de acuerdo con la doctora por el Departamento de Ingeniería de la Universidad de la Rioja, Ana González Marcos), se entiende es el: *proceso de extraer conocimiento útil y comprensible, previamente desconocido, a partir de grandes volúmenes de datos*. (González Marcos 7)

En el caso de algunos sitios web y redes sociales digitales como Facebook, se desarrollan procesos de análisis de información que permiten hacer lecturas de lo que se hace dentro o fuera de la red social, como en el caso específico de compras e intereses, contactos afines, etc., lo que permite realizar una perfilación precisa, que más tarde dará pie a mecanismos de publicidad hechos a la medida, así como a incidir en los individuos para que elijan aquello que más convenga a los intereses de estas empresas y sus clientes. Esto eventualmente abonará a la interferencia en las decisiones del usuario, que quedará expuesto a información "a modo" sin conocer otras posibilidades dentro del espacio que navega.

En el caso concreto de Facebook, parte de las condiciones de servicio sobre la recopilación de información (documentos digitales extensos que demandan demasiado tiempo de lectura de los usuarios), hasta el 26 de mayo del 2017, que se hizo esta revisión, fueron:

> Tus acciones y la información que proporcionas.

Recopilamos el contenido y otros datos que proporcionas cuando usas nuestros Servicios, por ejemplo, al abrir una cuenta, al crear o compartir contenido, y al enviar mensajes o al comunicarte con otras personas. La información puede corresponder a datos incluidos en el contenido que proporcionas o relacionados con este, como el lugar donde se tomó una foto o la fecha de creación de un archivo. También recopilamos información sobre el modo en que usas los Servicios, por ejemplo, el tipo de contenido que ves o con el que interactúas, o la frecuencia y la duración de tus actividades.

Las acciones de otras personas y la información que proporcionan.

También recopilamos el contenido y la información que otras personas proporcionan cuando usan nuestros Servicios y que puede incluir datos sobre ti, por ejemplo, cuando alguien comparte una foto en la que apareces, te envía un mensaje o sube, sincroniza o importa tu información de contacto.

Tus redes y conexiones.

Recopilamos información sobre las personas y los grupos con los que estás conectado y sobre el modo en que interactúas con ellos, por ejemplo, las personas con las que más te comunicas o los grupos con los que te gusta compartir contenido. También recopilamos la información de contacto que proporcionas si subes, sincronizas o importas estos datos (por ejemplo, una libreta de direcciones) desde un dispositivo. (Facebook, "Política de datos", párrs.4–6)

Según Emilio Godoy, periodista y colaborador de la revista Proceso, quién escribe sobre derechos humanos, desarrollo sustentable y ambiente:

> La red social Facebook diseñó un algoritmo para llevar a cabo publicidad personalizada para las mayores tiendas departamentales o *retailers* mexicanas. El pasado 25 de marzo en un hotel de Polanco, esa red social presentó el proyecto que ha aplicado en diversas variantes en Estados Unidos y otros países. La empresa anunciará publicidad de los almacenes, para que el usuario haga click [sic] sobre el banner e ingrese en la web de la tienda. (Proceso, "El Data mining", párr.21)

De acuerdo al artículo publicado en 2015, la red social digital en cuestión almacena información de navegación del internauta y los productos que adquiere, para cotejarla con la información de otros usuarios y así añadir publicidad personalizada, extendida a usuarios de intereses similares. (Proceso, "El Data mining", párr.21) E incluso a no usuarios de la red social digital que ingresen a perfiles o sitios en donde Facebook haga rastreo de información.

Actualmente Facebook tiene por socios a empresas como Acxiom, Epsilon y Datalogix, especializadas en el análisis y lectura de datos. (Proceso, "El Data mining", párr.21)

Otro caso anecdótico se da en Twitter (revisado en la misma fecha) donde dentro de las condiciones de servicio, en lo que comprende la privacidad, se establece:

> Twitter disemina amplia e instantáneamente su información pública a una amplia gama de usuarios, clientes y servicios, incluyendo motores de búsqueda, desarrolladores y editores que

> integran contenido de Twitter en sus servicios y organizaciones, tales como universidades, agencias de salud pública y empresas de investigación de mercado que analizan la información en busque [sic] de tendencias y conocimiento. Cuando comparta información o contenidos como fotografías, videos y enlaces a través de los Servicios, debería reflexionar cuidadosamente sobre aquello que está publicando. Podemos utilizar esta información para hacer deducciones, por ejemplo, sobre los temas que le pueden interesar. Por defecto, casi siempre publicamos la información que usted nos facilita a través de los Servicios de Twitter hasta el momento en que usted la elimine, pero generalmente ponemos a su disposición configuraciones o características, como Tweets protegidos, para hacer que la información sea más privada si usted quiere… (Twitter, "Política de privacidad", párr.10)

Si bien se asume, que, en los contratos de aceptación de servicios de sitios y redes sociales digitales, la gente da su consentimiento para la recolección de ciertos datos, también se sabe por información anteriormente vertida, que la mayoría de la gente no toma siquiera el tiempo requerido para leer un aviso de privacidad, o desconoce parcialmente cómo será utilizada su información.

Aun cuando pueda considerarse no se trata de un uso alevoso de nuestra información; de asumirse de buena fe la ética de su funcionamiento, supone un riesgo para nuestra privacidad.

I.VII.VI. Diseminación de la información: chantaje

En lo general, dentro del territorio nacional, de acuerdo a la división de Prevención de Delitos Cibernéticos de la Policía Federal, en 2012, se

registraron tres mil denuncias relacionadas con algún tipo de extorsión. (Dinero en Imagen, párr.11) Una variante de ella es la sextorsión, que se da a través de imágenes y videos de contenido sexual, lo que de acuerdo a Kapersky Lab es:

> … la amenaza de revelar información íntima sobre una víctima a no ser que esta pague al extorsionista. En esta era digital conectada, dicha información podría incluir mensajes de texto sexuales (en inglés conocidos como sexts), fotos íntimas e, incluso, vídeos. Los delincuentes suelen pedir dinero, pero a veces buscan material más comprometedor (envía más o divulgaremos tus secretos). (Kaspersky Lab, párr.2)

Es difícil conocer con absoluta certeza la cantidad de víctimas de chantaje, por el temor de las personas a que se conozcan estos aspectos de su vida íntima, sin embargo, es una problemática que ya está en el foco de medios de comunicación, organizaciones e instituciones, dentro y fuera del país.

Ejemplo de ello es el documento *La violencia en línea contra las mujeres en México*, *realizado* por la colectiva feminista Luchadoras, que, si bien no menciona directamente el chantaje, da certidumbre sobre la violencia que sufren las mujeres del mundo en lo digital y que bien puede estar relacionada con el tema de este apartado:

> — Las mujeres jóvenes, de entre 18 y 30 años, son los más vulnerables en los espacios digitales.
>
> — El 40% de las agresiones son cometidas por personas conocidas por las sobrevivientes y el 30% por desconocidos.
>
> — Hay tres perfiles principales de mujeres que viven esta forma de violencia: mujeres que viven en una relación íntima de

> violencia, mujeres profesionales con perfil público que participan en espacios de comunicación (periodistas, investigadoras, activistas y artistas), y mujeres sobrevivientes de violencia física o sexual. (Luchadoras et al. 16)

Dentro del mismo documento se comenta el caso de Ana, quién fue extorsionada por su exnovio, por videos y fotografías íntimos, a través de la red social digital Facebook e Instragram. (Luchadoras et al. 16)

Como se ha observado, la identidad y generación de contenido vinculante a ella, son determinantes en la comisión de este tipo de delitos. Aquí radica la importancia de la protección de la privacidad y perfil de las personas.

I. VII.VII. Diseminación de la información: apropiación

La descripción de Solove, en este sentido, refiere a la utilización de la identidad de una persona para explotarla para sus propios fines, como las imágenes de una celebridad para anunciar algo que desconoce, aprovechándose de sus imágenes. Aquí se propone considerar aquella información personal propia que publicamos y que es retomada para fines distintos y que desconocemos, acercándonos incluso a la figura de la propiedad intelectual (nuestras fotografías, videos, pensamientos, etc.), por lo que se reitera la necesidad de leer y conocer las condiciones de los servicios que se adquieren para tener certeza sobre si lo nuestro puede ser expuesto y reutilizado por terceros.

Facebook, al respecto, en sus condiciones de servicio establece:

> En el caso de contenido protegido por derechos de propiedad intelectual, como fotos y videos ("contenido de PI"), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de la privacidad y de las aplicaciones: nos concedes

> una licencia no exclusiva, transferible, con derechos de sublicencia, libre de regalías y aplicable en todo el mundo para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook ("Licencia de PI") Esta Licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se compartió con terceros y estos no lo eliminaron.
>
> Cuando eliminas contenido de PI, este se borra de forma similar a cuando vacías la papelera de reciclaje de tu computadora. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros). (Facebook, "Declaración de derechos", párrs.6–8)

El texto anterior (*Eres el propietario de todo el contenido y la información que publicas en Facebook y puedes controlar cómo se comparte a través de la configuración de la privacidad y de las aplicaciones),* deja ver, que se considera a cada usuario como dueño y responsable de la información que comparte. Sin embargo, se concede una licencia de uso sin pago de regalías para utilizar todo lo que se comparta públicamente en Facebook o en conexión con él.

Twitter, en similar tono determina:

> Usted conserva sus derechos sobre cualquier Contenido que envíe, publique o muestre a través de nuestros Servicios. Lo que es suyo, es suyo: usted es el dueño de su Contenido (y de las fotos y vídeos que formen parte del Contenido).
>
> Al enviar, publicar o mostrar Contenido a través de los Servicios, nos otorga una licencia mundial, no exclusiva, libre del pago de

> derechos (con derecho a sublicencia) para usar, copiar, reproducir, procesar, adaptar. modificar, publicar, transmitir, mostrar y distribuir dicho Contenido en todos y cada uno de los medios de comunicación o métodos de distribución posibles (conocidos ahora o desarrollados con posterioridad). Esta licencia nos autoriza a poner su Contenido a disposición del resto del mundo y a permitir que otros hagan lo mismo. Usted acepta que esta licencia incluye el derecho de Twitter a proporcionar, promover y mejorar los Servicios y a poner el contenido enviado a o a través de los Servicios a disposición de otras empresas, organizaciones o personas para la sindicación, emisión, distribución, promoción o publicación de dicho contenido en otros medios y servicios, sujeto a nuestros términos y condiciones para el uso de dicho Contenido. Dichos usos adicionales por parte de Twitter u otras empresas, organizaciones o personas pueden realizarse sin abonarle a usted una compensación con respecto al Contenido que haya enviado, publicado, transmitido o puesto a disposición pública de cualquier otra forma a través de los Servicios. (Twitter, "Términos del servicio", párrs.9–10)

Hay que decir, que, aunque no toda información compromete la privacidad de las personas, sí pudiera dar pie a explotación fuera de nuestros intereses, en contra de nuestro poder de decisión y libertad de elección, por lo que hay que ser conscientes de lo que se comparte en Internet.

En este sentido la responsabilidad de cada usuario es mayor, si su afán es preservar su privacidad, porque como se ha visto, aun cuando no se pierda propiedad se acepta que otros utilicen nuestros contenidos de acuerdo a sus intereses y para ejemplo no hay más que mirar dichas redes sociales

digitales, donde imágenes, videos, audios y textos son reutilizados en muchas ocasiones fuera de los fines pensados originalmente y si en ellos se exponen aspectos de nuestra identidad o privacidad, la pondremos en riesgo.

Se han observado aquí las redes sociales digitales Facebook y Twitter, tras considerar a la primera, la de mayor uso en el país. La segunda por su incorporación a los medios de comunicación tradicionales y porque también forma parte de las redes sociales digitales más utilizadas, (Según estudio de la consultora The Competitive Intelligence Unit (CIU), en 2016, 98% de los internautas mexicanos utilizaba Facebook, 23% Instagram y 21% Twitter). (Garrido, párr.4) Sin embargo, lo descrito aquí puede resultar similar en otros servicios vinculados a Internet, por lo que se recomienda leer sus términos y condiciones antes de acceder a ellos.

I.VII. VIII. Invasión: intrusión

La intrusión en si misma ya ha sido comentada relacionalmente con otros puntos, como cuando a partir de *software* malicioso, delincuencia y gobierno intervienen nuestras comunicaciones en Internet, muchas veces sin rendir cuentas claramente de su proceder. Estos casos, aunque graves no deben hacer suponer, que son las únicas formas de intrusión.

El envío de *spam* o información no solicitada*,* también es intrusión, toda vez que no existe autorización previa para recibirla, sumado a que, la mayoría de las veces los motivos de este tipo de prácticas son fraudulentos.

Según la Alianza por la Seguridad en Internet, México (ASI México), los tipos de *spam,* practicados en el país y de los que tienen reporte son:

a) Correo electrónico

b) Mensajería instantánea (también llamado SPIM)

c) Foros

d) Blogs

e) Teléfonos móviles

f) Grupos de noticias. (ASI-México, "Radiografía del SPAM", párr.3)

Y entre los temas reportados se encuentran:

Cadenas:

Te piden que le avises a todos tus contactos sobre nuevos virus, oraciones por la paz, etc…

Fraude Nigeriano.

Te escribe un supuesto funcionario bancario corrupto de algún país lejano (normalmente africano o del este de Europa) que busca sacar grandes cantidades de dinero con tu ayuda ofreciéndote una jugosa comisión. Pueden hacerte creer que ganaste una lotería, eres el beneficiario de una herencia, etc… Este es uno de los temas de engaño con más reportes, sobre él te recomendamos mucho que revises nuestro artículo "El fraude nigeriano en internet".

Newsletter que no ofrecen mecanismos de desuscripción.

También llamado Opt-out, todo *newsletter* debe ofrecer al usuario un mecanismo para dejar de recibir los correos. Si no lo tiene, o bien, si pides la cancelación y no te hacen caso, debes reportarlo en Profeco.

Ofertas de Pornografía gratuita.

Ofertas de trabajo falsas.

Personas que enviaron sus datos completos y currículum en una solicitud de trabajo, pero son contactados por alguien externo quien les ofrece asignarle el puesto a cambio de dinero.

Phishing bancario.

El usuario recibe un mensaje supuestamente desde su banco en que se le informa que por diferentes razones es necesario que actualice sus datos completos, y ofrecen ligas que te llevan a portales igualmente falsos que intentan robar tu información confidencial.

Tarjetas Postales falsas.

Clásico mensaje que dice "un amigo te ha enviado una postal", ahora usan nombres comunes para tratar de engañarte, por ejemplo "Manuel te ha enviado una postal", buscando la posibilidad de que conozcas a alguien que se llame Manuel.

Recargas de tiempo aire.

Sin duda, el tema más frecuente con el que se busca engañar al usuario, ofreciendo el doble o triple de tiempo aire siguiendo ligas o instrucciones falsas. Sobre este tema te recomendamos mucho que revises nuestro artículo "Las imágenes del fraude".

Robo de contraseñas.

Muy difundido entre los jóvenes, son mensajes que te ofrecen darte a conocer quién te ha borrado de su mensajería instantánea,

> pero te piden tu nombre de usuario y contraseña y comúnmente la conservan para mandar mensajes en tu nombre a terceros.
>
> Diversos.
>
> Es la última vez que te molesto, ¿Ya te olvidaste de mí?, Mensajes que llegan como si vinieran de tu misma cuenta de correo, Piratería, Invitaciones a cursos, Servicios de asesorías, etc…(ASI-México, "Radiografía del SPAM en México", párrs.6–18)

El *Phishing* bancario, por ejemplo, ya también ha provocado la emisión de boletines que alertan a la ciudadanía, por parte de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (Condusef, "Fraude", 2017)

Finalmente, de acuerdo al sitio Security List, perteneciente a Kaspersky Lab, el porcentaje de envío de *spam* proveniente de México representa el 4.40% del total en el mundo. (Kaspersky Lab et al.,"El spam en 2016-2", párr.58)

I.VII. IX. Invasión: interferencia en las decisiones

Derivado de la propuesta de considerar previamente a la minería de datos como apropiación, hay que apuntar, esta condiciona la interferencia en las decisiones.

La lectura que se hace de nuestro proceder en sitios web y redes sociales digitales alimenta extensas bases de datos que se relacionan con nuestros enlaces y contactos, a fin de generar un perfil útil para la venta y fines propagandísticos.

Por ejemplo, en el contrato de aceptación de Facebook y Twitter, ya comentado en este trabajo, se sabe el usuario autoriza la lectura de su proceder para ofrecerle "información de acuerdo a sus intereses", pero no

se precisa la forma en que esta se hará llegar y regularmente es impresa en nuestra pantalla bajo leyendas discretas que dan certeza de que se trata de publicidad, pero son colocadas estratégicamente para que se confundan con el resto del contenido.

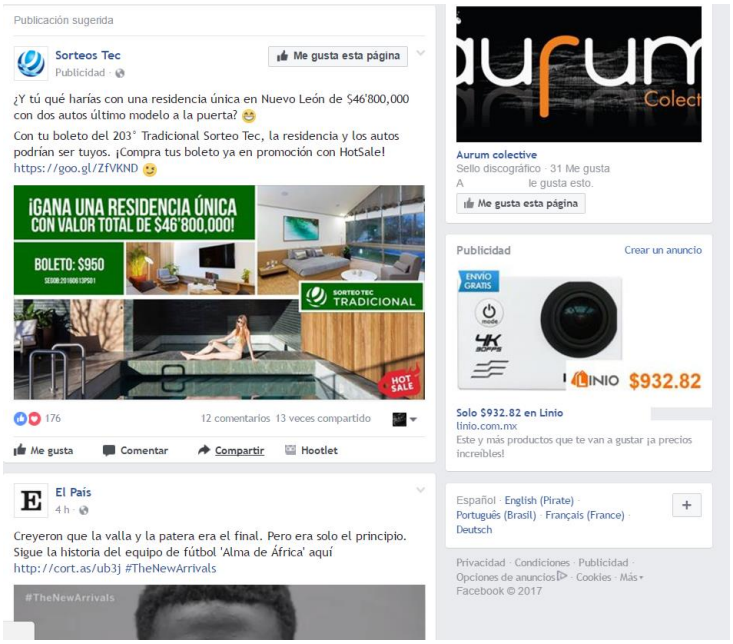

Imagen 23. Publicidad en muro de Facebook.com. Captura de pantalla.

En el caso de la navegación en sitios web que utilizan *cookies* (archivos para rastrear nuestro comportamiento e intereses), sucede algo similar. Tras acceder a un sitio web este determina la publicidad más cercana a nosotros en términos de empatía para persuadirnos de comprar (el término *cookie*, será retomado en el apartado Cómo opera internet).

Imagen 24. Publicidad en sitio web (AristeguiNoticias.com) de AdWords. Captura de pantalla.

Un tercer ejemplo es la interacción a partir de navegadores que precisan estar registrado; en este caso, la información adquirida sirve para mostrarnos toda clase de anuncios encaminados en el mismo sentido, dentro de todos los sitios a los que accedamos. Es el caso de Google, que toma lectura de lo que hacemos con sus aplicaciones, principalmente el navegador, para después mostrarnos publicidad a modo, cuando los sitios en que navegamos insertan espacios de publicidad de AdWords, que anunciantes contratan directamente en esta plataforma. Otros casos de publicidad invasiva son Youtube y Spotify.

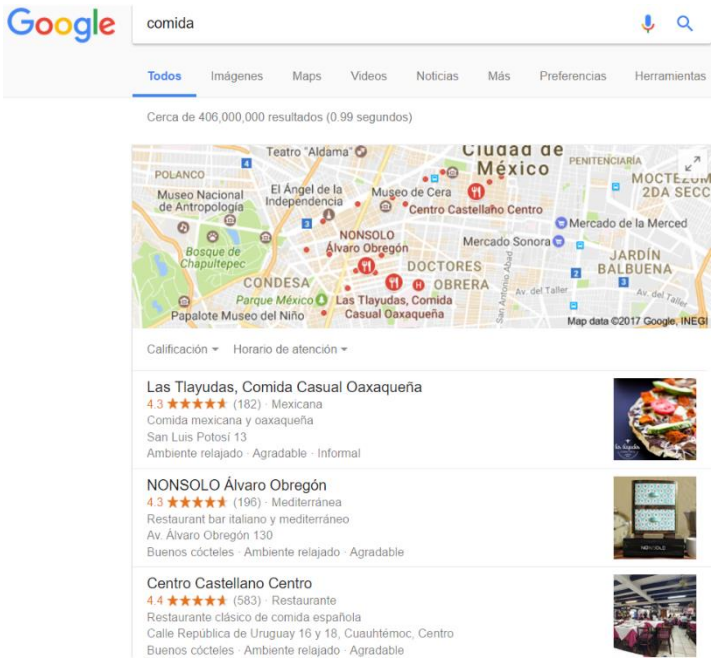

Imagen 25. Resultado de búsqueda por palabra en Google. Captura de pantalla.

Cabe decir que dicho rastreo no se da sólo en la búsqueda, sucede también después de esta, durante la navegación y uso de aplicaciones vinculadas a cuentas comunes. Así es posible conocer toda nuestra actividad en la red y ubicar las sombras que dejamos.

Lo anterior es considerado interferencia en las decisiones, porque impide el conocimiento de otras posibilidades, por lejanas o cercanas que puedan ser a nosotros.

Ejemplo de ello es el reciente caso de Cambridge Analytica, que, a partir de la delimitación de usuarios por ciertas características psicológicas, publicó información acorde a sus intereses y rasgos emocionales, para impulsar la candidatura de Donald Trump a la presidencia de Estados Unidos de Norte América. (Krogerus, párrs.1–9)

Mismo caso es la perfilación en navegadores, que nos mostrarán información en primer lugar de acuerdo a nuestra ubicación, intereses,

acciones y pago de los anunciantes. Para poder tomar decisiones acertadas es necesario un contexto global, al romperse esto somos privados de ello.

I. VII.X. Taxonomía de Solove y riesgos en México

A continuación, se describe una tabla que busca complementar la idea de los riesgos latentes y evidentes en Internet, redes sociales digitales y sus circunstancias en territorio nacional.

Momentos	Riesgos	Ejemplos
Recopilación de la información	Vigilancia	Vigilancia gubernamental ilegal y legal
	Interrogación	Almacenamiento de información por las empresas a solicitud del gobierno
Procesamiento de la información	Agregación	Extralimitación de empresas sobre el uso de datos personales
	Identificación	Identificación por triangulación de información
	Inseguridad	Fraude Reemplazo de la identidad Persecución Acoso
	Uso secundario	Uso de datos personales para fines no autorizados por empresas
	Exclusión	Discriminación en Internet
Diseminación de la información	Quebrantamiento de la confidencialidad	El nulo resguardo de la información y expansión arbitraria de los límites, por empresas
	Divulgación	Información

	Exposición	Información privada que se hace pública
	Accesibilidad incrementada	Minería de datos
	Chantaje	Extorsión y sextorsión
	Apropiación	Reutilización de contenidos, por las empresas
	Distorsión	Calumnia y desinformación sobre las personas en sitios y redes sociales digitales
Intrusión	Invasión	*Spam*
	Interferencia de decisiones	Publicidad invasiva

Tabla 10. Taxonomía de Solove y riesgos en México. Elaboración propia.

Todos y cada uno de los aspectos señalados han buscado generar cierta perspectiva de los peligros que la pérdida de nuestra privacidad conlleva relacionándolos con el territorio nacional, pero esto no quiere decir que se trate de problemas endémicos, porque como sabemos, en un mundo interconectado, estos son más bien globales.

La mayoría de ellos dan pie a los delitos cibernéticos ya expuestos, así que deben entenderse unos como consecuencia de otros, al estar casi siempre vinculados.

Los individuos bajo estas amenazas pueden ver comprometida su seguridad e integridad física y moral, además de ser influenciados con fines poco éticos, lo que puede convertirse en un instrumento de control de la sociedad, privilegiándose sólo a ciertos grupos de poder. Lo que sucede en Internet puede ser consecuencia o reflejo del mundo físico, por lo que es importante observar con la misma atención lo digital, para poder actuar en consecuencia.

Es tras lo anterior que se valida la existencia de riesgos reales y latentes para todos los que somos usuarios de Internet y que vivimos en México.

Preliminares

Después de este primer recorrido, en respuesta a la primera pregunta sobre si **se comparte información personal en Internet**, se sabe que es así. Los usuarios ingresan información personal en sitios web y redes sociales digitales que los hace identificables. Datos personales y datos personales sensibles, además de contenido que da cuenta de aficiones e intereses, quedan plasmados en las redes sociales digitales, igual que su interacción general en Internet es analizada por empresas a través de la lectura de metadatos.

¿Tiene cabida el concepto de privacidad en sitios web y redes sociales digitales? Sí, la privacidad es un derecho y este es extensible al ámbito digital, donde se puede ejercer positivamente, de acuerdo a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Los sitios y redes deben informar al usuario para qué se va a utilizar su información.

Sobre si Internet y redes sociales digitales vulneran el derecho a la privacidad, se sabe que sí. La omisión de los usuarios, por una parte, de informarse sobre las políticas de privacidad de sitios web y redes sociales digitales, además del desconocimiento y malas prácticas de las empresas sobre la información que recopilan, aunado a la ciberdelincuencia, que aprovecha ambas circunstancias; la vigilancia gubernamental y la minería de datos, afectan eventualmente la privacidad de los individuos.

Tras la resolución de estas tres interrogantes, pueden definirse los **elementos que vulneran la privacidad de las personas**, que es la pregunta principal de este primer capítulo.

Lo hacen los propios usuarios por desconocimiento o desinterés de aprender sobre las dinámicas propias de Internet y los acuerdos de privacidad que suscriben tácitamente o no. Lo hacen las empresas porque no resguardan ni utilizan adecuadamente la información, por desconocimiento o incapacidad, algunas otras más (el caso de las redes sociales digitales señaladas), porque no describen con claridad el uso que se dará a la información recabada. Las instituciones gubernamentales, porque vigilan e invaden la privacidad con cierta opacidad sobre el porqué de su proceder; sin lineamientos claros y muchas veces contra la ley. La delincuencia, porque aprovecha las carencias de usuarios y empresas para obtener recursos indebidamente; y finalmente, por otros usuarios, parte de círculos privados, que por ignorancia o insensibilidad comparten información sin considerar las consecuencias de sus actos.

El usuario, más vulnerable en esta ecuación, es privado de su libertad ante el desconocimiento de cuestiones relacionadas a la informática y al cómputo.

Por lo anterior se puede decir que la hipótesis queda verificada; luego entonces, ingresar y divulgar datos personales en sitios web y redes sociales digitales, por parte de los usuarios en Internet, sí supone la pérdida de derechos sobre ellos, volviéndolos accesibles a terceros, lo que posibilita prácticas fraudulentas, intrusivas, acosadoras y de espionaje; y al no garantizarse su libertad de expresión, las personas son susceptibles de sufrir persecución por la información vertida, en detrimento de su privacidad digital.

La intimidad y privacidad se consideran derechos positivos (que cada persona puede ejercer activamente), que esta privacidad tiene cabida en el mundo digital, razón por la que se le denomina privacidad digital.

Que hay desconocimiento por parte de usuarios y empresas sobre la forma de protegerla, así como sus derechos y obligaciones (Derechos Arco).

Que los riesgos son reales y están presentes tanto para usuarios como para empresas, aunque el interés de este documento es centrarse en los primeros. Los tres riesgos principales están relacionados con el gobierno, las empresas y la ciberdelincuencia, sin dejar de lado las omisiones de los usuarios.

Una aclaración pertinente antes de concluir este capítulo es, que, al dar el sí a un contrato para usar aplicaciones, redes sociales digitales u otros servicios en Internet, así como la aceptación tácita de *cookies* al navegar en los sitios web que las utilizan, se garantiza que no hay violación de la privacidad y en términos legales así es, pero ello no quiere decir que no la comprometa, porque aun cuando se aceptan ciertos términos y condiciones, se ignora el buen o mal ejercicio que se hace con nuestra información y si las medidas de seguridad que implementan son correctas, es decir, se pueden dar transgresiones que la comprometan.

En el mismo sentido, al compartir información en redes sociales digitales, éstas aparentemente respetan nuestras decisiones en cuánto a privacidad, pero se ignora si los contactos y usuarios, con cuenta o no, que acceden a esta información lo harán de igual forma. Por ejemplo, si se comparte una imagen en Facebook en un círculo al cual solo acceden amigos, no podrán estos compartirlo a sus círculos, pero si toman una captura de pantalla o descargan la imagen, sí.

Ante tal panorama hay que evaluar qué posibilidades se tienen para resguardar la privacidad, la que aquí se ha de estudiar, es la del anonimato digital, que se explicará más adelante.

Capítulo II. El anonimato como defensa de la privacidad digital

Luego de conocer que es la intimidad, privacidad, privacidad digital, datos personales, los derechos que sobre ellos tenemos y que posibilitan resguardar nuestra privacidad, además de los riesgos presentes y latentes en territorio nacional, se vuelve necesario conocer bajo que formas se puede proteger entonces la privacidad, con el fin de empoderar al usuario y hacerlo consciente de la implicación de nuestro accionar en Internet y redes sociales digitales.

En el caso específico de este documento se aborda la idea del anonimato digital, como una de las posibilidades de protección de la misma, es decir, el anonimato en Internet y no el del mundo físico, que probablemente también tendrá sus ventajas en lo que a la protección de los individuos se refiere.

La interpretación de anonimato digital, no versa aquí sobre lo que existe en el imaginario general, que sostiene sólo se utiliza para acciones nocivas en la red (robo de información, compra de productos en el mercado negro, acoso, chantaje, entre otros), pues de ser factible, también pudiera utilizarse positivamente como medida de protección del usuario.

Las preguntas a responder sobre esta base son: ¿qué es el anonimato digital?, ¿en qué consiste el anonimato digital?, ¿qué tipos de anonimato digital existen?, ¿el anonimato digital ayuda a proteger la privacidad digital? Todas nacidas de la pregunta principal: **¿qué medidas a considerar por el usuario pueden garantizar su privacidad digital en Internet?**

Todo lo anterior, sobre la hipótesis de que **bajo la figura del anonimato digital puede evitarse que empresas, gobiernos y terceros en México hagan mal uso de los datos personales de los usuarios, previniendo la pérdida de su privacidad digital.**

II.I. Anonimato

La palabra anonimato viene del griego ἀνώνυμος (anonymous) y está compuesta del prefijo de negación αν- (a = sin) y la palabra ὄνομα (onoma = nombre), y significa "sin nombre". (Etimologías, párr.1)

La Real Academia Española de la lengua define al anonimato como el Carácter o condición de anónimo y a este como (Real Academia Española, "anonimato", párr.1):

> 1. adj. Dicho de una obra o de un escrito: Que no lleva el nombre de su autor. U. t. c. s. m.
>
> 2. adj. Dicho de una persona, especialmente un autor: De nombre desconocido o que se oculta. U. t. c. s. m.
>
> 3. adj. Indiferenciado, que no destaca de la generalidad. Gente anónima.
>
> 4. m. Carta o papel sin firma en que, por lo común, se dice algo ofensivo o desagradable.
>
> 5. m. p. us. Situación de quien oculta su nombre. Vivir en el anónimo. (Real Academia Española, "Anónimo", párrs.1–6)

Por otra parte, para Diego Fernando Migliorisi, abogado especialista en derechos informáticos, el anonimato:

> ... no significa permanentemente una acción negativa o ilegal sino también una protección o un *modus operandi* para realizar acciones positivas pero en carácter secreto. (Migliorisi 10)

Como lo reflejan las distintas acepciones, el anonimato se asocia regularmente con la omisión de la identidad de un autor o persona y esta se da por desconocimiento u ocultamiento:

Dentro del documento enviado por la Electronic Frontier Foundation (organización con presencia en múltiples países y que tiene por causa salva guardar los derechos digitales), a la Relatoría Especial de la Comisión de Derechos Humanos sobre la promoción y protección del derecho a la libertad de opinión y de expresión, de la Organización de las Naciones Unidas, en 2015, se describe al anonimato como el:

> … actuar o comunicarse sin usar o presentar el nombre o identidad propios; o cómo actuar o comunicarse en una manera que protege la determinación del nombre o identidad propios, o usando un nombre asumido o inventado que no puede necesariamente asociarse con la identidad legal o habitual de uno. (Rodríguez 3)

Luego entonces, el anonimato se entiende, es la omisión de la identidad de un individuo y puede tener por fin el protegerse. A propósito, debe señalarse que el anonimato es considerado un derecho y a través de él es posible expresar nuestro sentir sobre cualquier tema sin temer a las probables represalias (Derechos Digitales et al. 21):

> La capacidad de "ser anónimo" como derecho es una consecuencia del desarrollo de la libertad de expresión; reside en la voluntad de la persona para revelar o no uno de sus atributos personalísimos, la identidad, para establecer contacto con el

> mundo y para expresar sus ideas o acceder a información. (Derechos Digitales et al. 26)

Tras lo anterior, un tercer aspecto a considerar es que cada persona puede elegir ser anónimo o no según las circunstancias y un cuarto, que nos acerca más a las dinámicas que se dan en Internet, que el anonimato no sólo tiene cabida para emisores sino también para receptores:

> El artículo 19 de la Declaración Universal de Derechos Humanos, que consagra el derecho a la libertad de opinión y de expresión, incluye el derecho a buscar, recibir e impartir información e ideas a través de cualquier medio. Esta inclusión es necesaria porque no puede haber una protección significativa de la libertad de expresión de los ciudadanos si los individuos carecen del derecho a leer y comunicarse anónimamente. (Rodríguez 7)

Un quinto punto es, que ese anonimato no es absoluto y que sus límites son impuestos por las leyes de los distintos países, sobre todo cuando sea el medio para cometer actos indebidos, tal como lo menciona Dawn Carla Nunziato, abogada experta en los temas de libertad de expresión e Internet, y reconocida internacionalmente:

> Las garantías de expresión anónima no son absolutas y pueden ser suspendidas, pero siempre en el marco de un procedimiento judicial que tenga en cuenta los intereses tanto del demandante que exige una reparación genuina, como de los demandados que pretenden continuar resguardando sus derechos de libertad de expresión en la mayor medida posible. (Bertoni 26)

Dentro de lo conocido como el mundo físico u *offline,* ese en el que no se tiene presencia en Internet, el anonimato existe al publicar una obra cuando

el autor no desea ser conocido, o cuando alguien denuncia ilícitos, pero teme a las posibles represalias, incluso en el periodismo se usa para poder obtener información sin tener que revelar la fuente y así llegar a la profundidad de ciertos hechos y hasta en la donación para hacer más transparentes los procesos con el fin de evitar malas prácticas.

Un sexto punto es el del anonimato como medio para metas poco éticas, como la difamación o la injuria, lo que permite en ese caso al emisor ser expuesto a denuncias o castigos. Esto ha provocado voces que pugnan por una identidad real obligada para interactuar. (Derechos Digitales et al. 29)

Por el momento, basta decir que ambas caras de la moneda, es decir, el anonimato como protección y el anonimato como calumniador, existen en lo físico y en lo digital pero no por ello debiéramos vivir en un estado permanente de vigilancia que afecte nuestro desenvolvimiento humano.

Anonimato	Características	Palabras clave	Aplicación
RAE	Dicho de una persona, especialmente un autor: De nombre desconocido o que se oculta. U. t. c. s. m.	Nombre desconocido Oculta	General
Diego Fernando Migliorisi	No significa permanentemente una acción negativa o ilegal sino también una protección o un *modus operandi* para realizar acciones positivas pero en carácter secreto.	Protección Acciones positivas Secreto	Derecho
Electronic Frontier Foundation	Actuar o comunicarse sin usar o presentar el nombre o identidad propios; o cómo actuar o comunicarse en una manera que protege la determinación del nombre o identidad propios, o usando	Sin usar Nombre Identidad Protege Nombre asumido o inventado	Derecho

	un nombre asumido o inventado que no puede necesariamente asociarse con la identidad legal o habitual de uno		
Declaración Universal de los Derechos Humanos	Esta inclusión es necesaria porque no puede haber una protección significativa de la libertad de expresión de los ciudadanos si los individuos carecen del derecho a leer y comunicarse anónimamente	Protección Libertad de expresión Ciudadanos Individuos	Derecho
Dawn Carla Nunziato	Las garantías de expresión anónima no son absolutas y pueden ser suspendidas, pero siempre en el marco de un procedimiento judicial que tenga en cuenta los intereses tanto del demandante que exige una reparación genuina, como de los demandados que pretenden continuar resguardando sus derechos de libertad de expresión en la mayor medida posible	No absolutas Suspendidas Procedimiento judicial	Derecho

Tabla 11. Concepto de anonimato. Elaboración propia.

El anonimato se entiende como el ocultamiento de la identidad o atributos de la misma, por decisión propia y que puede tener muchos orígenes, como el temor a represalias, la determinación de que las obras u opiniones tengan valor por sí mismas y no sean ponderadas o descalificadas por causa del autor, por ostracismo, mejor ejercicio de la libertad de expresión, etc., todos válidos siempre y cuando no atenten contra la ley y que este anonimato sirve para difundir y acceder a información. Este mismo nivel de protección puede desearse en Internet por lo que hay que saber si es posible y eficaz.

Pero ¿qué es el anonimato digital y para qué sirve?

II.II. Anonimato en Internet

Nuestra interacción en Internet y participación en redes sociales digitales, hace necesaria la protección de nuestra privacidad, igual que en el llamado mundo físico; de la misma forma, el anonimato, tiene cabida en ambos espacios, pero la noción de anonimato en línea, también llamado anonimato digital, se distingue porque:

> El anonimato involucra más que esconder el nombre de uno. Más bien, implica la capacidad de mantener la confidencialidad de una amplia variedad de actividades propias en línea, incluyendo la ubicación, la frecuencia de las comunicaciones, y tantos otros detalles. El anonimato en línea debe entenderse no sólo como el estado de no ser identificado por terceros, sino también como la cualidad de ser *incognoscible* para terceros. (Rodríguez 12)

Es decir, mantener todo nuestro quehacer, que incluye la obtención y difusión de información, desasociado de nuestra identidad, u oculto para evitar la mirada de otros, puede ser considerado anonimato en Internet.

La misma Electronic Frontier Foundation (EFF), señala que observar al anonimato, como la simple omisión del nombre, en los entornos digitales, es una visión incompleta. En ese sentido, la relatora de la Comisión Internacional de Derechos Humanos, de 2013, mencionó dos líneas específicas a considerar para garantizar la libertad de pensamiento y expresión: *… la protección del discurso anónimo y la protección de datos personales.* (Rodríguez 12)

Por otra parte, Nadia Kayyali quién también es activista, citada por Antonio Martínez Velázquez y José Flores Sosa, impulsores de los derechos de los usuarios de Internet, menciona que algunas ventajas del anonimato en Internet, son:

> … permite que las personas establezcan códigos de comunicación para expresarse libremente. Estos códigos rompen los obstáculos que agentes externos imponen a la libre transmisión de ideas y opiniones. El anonimato se ha vuelto una forma de protección frente a posibles abusos, mientras que las políticas de revelación de identidad en la red afectan particularmente a grupos vulnerables y comunidades marginadas, como el caso de la política de nombres reales de Facebook y las personas transgénero. (Derechos Digitales et al. 27)

En ese sentido, la navegación web anónima debiera entenderse como:

> … una suerte de elusión a los métodos informáticos de control de la navegación privada de las personas. Sería como el paradigma del "esta vez navego y espío las páginas públicas sin que me espíen". (Migliorisi 187)

El anonimato digital, pensado como medio para garantizar la libertad de pensamiento y expresión es adecuado, pero sus alcances pueden ser mayores, al evitar compartir información personal en Internet, que sea vinculada con nuestra identidad, nos protegemos de prácticas nocivas, de vigilancia, intrusión, invasión, suplantación y delitos cibernéticos, ya que todos estos puntos necesitan de una identidad a la cual asociar sus datos.

Ese anonimato debiera ser accesible por los usuarios y garantizado por los distintos proveedores de servicios, pero no ha podido constatarse que esto sea así, por lo que dentro de los términos legales debe ser conocido y ejecutado por el usuario, si lo desea, o considera necesario, siempre que se valide su utilidad.

Anonimato en lo digital	Características	Palabras clave	Aplicación
Electronic Frontier Foundation	El anonimato involucra más que esconder el nombre de uno. Más bien, implica la capacidad de mantener la confidencialidad de una amplia variedad de actividades propias en línea, incluyendo la ubicación, la frecuencia de las comunicaciones, y tantos otros detalles. El anonimato en línea debe entenderse no sólo como el estado de no ser identificado por terceros, sino también como la cualidad de ser incognoscible para terceros.	Confidencialidad Actividades Ubicación Frecuencia Comunicaciones No identificado Incognoscible	Derecho
Relatora de la Comisión Internacional de Derechos Humanos, de 2013	La protección del discurso anónimo y la protección de datos personales.	Protección Discurso Datos personales	Derecho
Nadia Kayyali	Permite que las personas establezcan códigos de comunicación para expresarse libremente. Estos códigos rompen los obstáculos que agentes externos imponen a la libre transmisión de ideas y opiniones. El anonimato se ha vuelto una forma de protección frente a posibles abusos, mientras que las políticas de revelación de identidad en	Códigos de comunicación Expresión libre Libre transmisión Ideas Opiniones Abusos Grupos vulnerables Comunidades marginadas Transgénero	Derecho

	la red afectan particularmente a grupos vulnerables y comunidades marginadas, como el caso de la política de nombres reales de Facebook y las personas transgénero.		
Diego Fernando Migliorisi	Una suerte de elución a los métodos informáticos de control de la navegación privada de las personas. Sería como el paradigma del "esta vez navego y espío las páginas públicas sin que me espíen.”	Elusión Navegar Espiar No espiado	Derecho

Tabla 12. Concepto de anonimato en lo digital. Elaboración propia.

El anonimato digital entonces va más allá del simple ocultamiento del nombre e identidad. Este permite evitar también la obtención de información por terceros de nuestra ubicación, comunicaciones y frecuencia de las mismas, en apoyo a nuestra libertad de expresión y protección de nuestros datos personales, en detrimento de los abusos, sobre todo a comunidades o personas marginadas o vulnerables. Aunque puede resultar valioso para cualquier individuo que quiera mantenerse seguro mientras interactúa en entornos digitales e Internet.

II.II.I. Anonimato débil y fuerte

El anonimato en línea, de acuerdo a The Electronic Frontier Foundation, tiene dos posibilidades, la primera es la del anonimato débil, en apariencia sencillo de conseguir y la segunda, el anonimato fuerte mucho más complicado de ejecutarse.

El primero, como desventaja tiene, que ofrece una frágil protección de la identidad de la persona:

> El anonimato es débil cuando una persona anónima puede ser desenmascarada mediante métodos sencillos, tales como solicitudes gubernamentales al proveedor de servicio o buscando el nombre asumido en una base de datos existente. (Rodríguez 3)

A diferencia de la segunda, que protege en mayor medida al individuo que la ponga en práctica:

> El anonimato es fuerte cuando existen protecciones técnicas y legales que hacen que sea muy difícil desenmascarar la identidad de una persona anónima. (Rodríguez 3)

A propósito del anonimato débil y fuerte, Young Hyun Kwon en su trabajo *Riffle: An Efficient Communication System with Strong Anonymity* (Riffle: un eficiente sistema de comunicación con un fuerte anonimato), publicado por el Instituto de Tecnología de Massachusetts (MIT por sus siglas en inglés) dice:

> … el anonimato básico que Internet garantiza es demasiado débil para proteger sus identidades incluso de los adversarios más débiles. Como resultado, cada vez más usuarios han adoptado tecnologías que mejoran la privacidad para protegerse. (Kwon 3)

Otra figura señalada regularmente es la del seudoanonimato, que como tal, debe entenderse es la utilización de un alias para no revelar la verdadera identidad. Para la Real Academia de la lengua española un seudónimo es:

> 1. adj. Dicho de un autor: Que oculta con un nombre falso el suyo verdadero.
>
> 2. adj. Dicho de una obra: Firmada con seudónimo.

> 3. m. Nombre utilizado por un artista en sus actividades, en vez del suyo propio. (Real Academia Española, "Seudónimo", párrs.1–3)

El seudoanonimato también puede ser acotado dentro de las categorías fuerte y débil, es decir, puede regirse por los mismos principios de acuerdo a la necesidad de cada usuario, a grandes rasgos, es otra forma de proteger la privacidad a través del ocultamiento de la identidad.

Casi cualquiera podría ejercer un anonimato o seudoanonimato débil y pensarse protegido. Por ejemplo, al crear una cuenta de correo, acceso a un sitio o identidad en redes sociales digitales, bajo cualquier otro nombre o alias, pero aun cuando en apariencia nuestra persona no esté vinculada, hay información que viaja en Internet que puede hacernos identificables:

> Incluso cuando una plataforma le permite a la gente leer y escribir sin adjuntar sus nombres legales a estas actividades, el operador de la plataforma bien puede conocer quiénes son sus usuarios con precisión, así como las ubicaciones particulares desde las cuales se han conectado, mediante el análisis de información como las direcciones del Protocolo de Internet (IP) de los usuarios. (Rodríguez 14)

Al contrario, el anonimato fuerte ofrece mayores ventajas, pero requiere más empeño para poder conseguirlo, así como el uso de ciertas herramientas para lograrlo:

> Estos sistemas van más allá de la simple noción de no solicitar que la gente declare sus nombres; tratan de evitar la creación de un registro significativo que revelaría la identidad de un usuario. (Rodríguez 16)

Al utilizar por ejemplo una cuenta de correo con un nombre falso o alias, aparentemente se protegería la identidad, pero por la correspondencia enviada o recibida podría accederse a información sensible que permitiera la identificación de la persona además de sus intereses. El anonimato fuerte en este caso, buscaría que ni el nombre ni al información hicieran posible conocer al usuario, su círculo social, sus acciones u opiniones.

	Débil	**Fuerte**
Anonimato (ocultamiento del nombre o la identidad) y **seudoanonimato** (alias para ocultamiento del nombre o la identidad). Con base en las definiciones citadas de la RAE.	El anonimato es débil cuando una persona anónima puede ser desenmascarada mediante métodos sencillos, tales como solicitudes gubernamentales al proveedor de servicio o buscando el nombre asumido en una base de datos existente. Autor: Electronic Frontier Foundation	El anonimato es fuerte cuando existen protecciones técnicas y legales que hacen que sea muy difícil desenmascarar la identidad de una persona anónima. Autor: Electronic Frontier Foundation

	El anonimato básico que Internet garantiza es demasiado débil para proteger sus identidades incluso de los adversarios más débiles. Como resultado, cada vez más usuarios han adoptado tecnologías que mejoran la privacidad para protegerse Autor: Young Hyun Kwon	Estos sistemas van más allá de la simple noción de no solicitar que la gente declare sus nombres; tratan de evitar la creación de un registro significativo que revelaría la identidad de un usuario Autor: Electronic Frontier Foundation
	Privacidad en mayor riesgo	Privacidad en menor riesgo

Tabla 13. Anonimato y seudoanonimato fuerte y débil. Elaboración propia.

Tras lo anterior se deduce que, el anonimato o seudoanonimato débil es el simple ocultamiento del nombre o identidad en los entornos digitales y que el anonimato fuerte protege la identidad y nombre más allá de su simple ocultamiento, al evitar la creación de registros significativos de información de nuestras comunicaciones e interacciones.

La protección de datos personales vigente en México, defiende al usuario y su identidad cuando esta información es ingresada en algún sitio o aplicación, pero no existe la figura del anonimato como posibilidad para hacer uso de muchos de estos servicios. Muy al contrario, los esfuerzos en la red se dirigen hoy día a identificar a cada una de las personas que utilizan Internet, por empresas o instituciones gubernamentales y no hay que dejar de considerar los errores, omisiones o usos indebidos que empresas o personas pueden llegar a hacer de la información que generamos.

Luego entonces, una forma de anonimato robusto en Internet, requiere estudio y conocimiento de ciertas herramientas, pero con la posibilidad de lograr mejores resultados al momento de defender nuestra privacidad digital.

II.III. Cómo lograr el anonimato digital

El anonimato como medio de protección de la privacidad digital requiere conocimiento sobre la forma en que funciona Internet, habilidades operativas para ejecutar acciones en su defensa, criterio y disciplina sobre nuestras formas de interacción y comunicación, así como herramientas sin las cuales un usuario promedio no lograría ser anónimo en lo digital.

Sí bien este documento se centra en la conectividad que da Internet y sus peligros. No debieran obviarse las medidas de protección de nuestra identidad que nuestros aparatos electrónicos requieren. Proteger nuestros equipos del acceso de otros físicamente mediante contraseña, así como el cifrado de información (se explicará posteriormente) en dispositivos de almacenamiento extraíbles ante posibles pérdidas o robo es absolutamente necesario. *Una de las principales causas de incidentes a la seguridad de los datos personales, se debe a los dispositivos incorrectamente desechados, reutilizados, perdidos, extraviados y robados.* (INAI, párr.1)

Se reitera entonces, que el objetivo central a abordar en las siguientes líneas, es aprender del anonimato digital en Internet y redes sociales digitales, pues es donde se ha observado los usuarios se desenvuelven más; pese a ello, después de conocer cómo funciona Internet y reconocer sus puntos vulnerables en el apartado siguiente, se recomienda que todo interesado también considere los peligros del Internet de las cosas (aparatos electrónicos, principalmente pensados para el hogar, conectados a Internet o que almacenan información digitalmente), y sistemas de video vigilancia,

que de manejarse equivocadamente, o ser programados por las empresas con intereses particulares ajenos al usuario, pueden agravar nuestra seguridad en lugar de reforzarla.

Como consecuencia de la conectividad a través de Internet, la extracción, intrusión, espionaje y vigilancia son una realidad penosa a considerar y de la cual protegerse es necesario, o incluso una obligación, por ello ha de describirse brevemente el modo en que funciona Internet para tener más claridad de cómo es posible protegerse.

La información a compartir a continuación busca dar luz sobre el modo que trabaja Internet, cómo se obtiene información a partir de ella y la posible utilidad de algunas herramientas pro privacidad y anonimato digital.

Se presentan por ser recomendaciones de personas interesadas en la privacidad digital con experiencia en el campo, como es el caso de Daniel Echeverri Montoya, fundador de *The hacker way* y autor del libro *Deep web: TOR, FreeNET & I2P: privacidad y anonimato*; y el *Manual antiespías: Herramientas para la protección digital de periodistas*, desarrollado por la Fundación para la Libertad de Prensa (FLIP), además de la EFF; reconocidos por su trabajo en pro de la privacidad digital.

Lo importante es conocer que existen alternativas para protegerse y evaluar la validez de las opciones, lo que puede hacerse de participar en foros especializados.

En resumen, son herramientas de protección que demandan un alto grado de confianza, la cual no puede ser total pues no son infalibles; ya sea por el factor humano o por la posibilidad de ser intervenidos, pero si pueden lograr una protección fuerte, si se suman a otras herramientas o procedimientos.

La defensa del anonimato y la privacidad digital, requieren medidas conjuntas, dependientes entre sí.

Lo siguiente se abordará con el fin único de ofrecer un panorama general de Internet que sea asequible al usuario, por lo que no se abundará demasiado en especificaciones técnicas. Las herramientas mencionadas pueden ser no compatibles con todos los sistemas operativos o distribuciones, pero si dar luz sobre su funcionamiento y ventajas, para después ubicar opciones similares de acuerdo a los dispositivos que se utilicen.

La determinación de su funcionamiento en la práctica, es una mera aproximación para ubicar su vigencia, de ahí que se haya realizado en muchas ocasiones, únicamente desde la instalación en un sistema operativo (en este caso Windows 10).

Todo aquel interesado puede referirse a la bibliografía si es su deseo profundizar.

II.III. I. Cómo opera Internet

El protocolo TCP/IP (*Transmission Control Protocol* o Protocolo de Control de Transmisión/*Internet Protocol* o Protocolo de Internet), es el principal estándar de Internet, y permite el entendimiento entre todos componentes de la red. Éste hace posible enlazar diferentes dispositivos, como computadoras a servidores, sin importar el sistema operativo que utilicen (Windows o GNU/Linux, por ejemplo), ya sea sobre redes de área local (casa, oficina) y redes de área más extensas (que abarquen varias ciudades). Es decir, permite la conexión entre equipos a pesar de la distancia geográfica (Peña Ochoa 14):

> …es una aplicación de dos capas: la capa más alta, Transmission Control Protocol, se encarga de mandar los mensajes de la manera más eficiente posible. Así, administra la división de los mensajes o archivos en pequeños paquetes (bits) que son transmitidos a través de Internet y finalmente recibidos por otra capa TCP, que unifica los diferentes paquetes en el mensaje original…la capa más baja, Internet Protocol, administra lo relativo a la dirección de cada paquete que el TCP dicide [sic], para que pueda arribar a su destino correcto. Cada computador que hace de pasarela (router) en la red, examina esta dirección para decidir dónde será derivado el mensaje. Como algunos paquetes del mismo mensaje serán ruteados en forma independiente a la de otros, todos ellos deberán ser nuevamente reunidos en su destino correcto. (Peña Ochoa 14–15)

A partir del protocolo TCP/IP es que funcionan toda clase de servicios, como por ejemplo los de correo electrónico y mensajeria. (Gironés Jesús 2016)

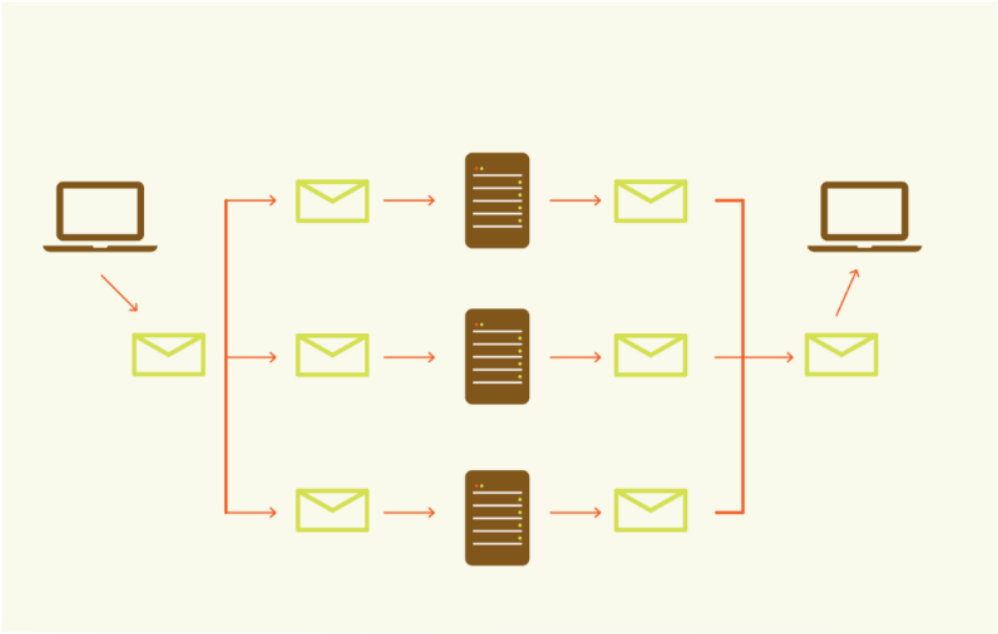

Imagen 26. Descripción del funcionamiento del protocolo TCP/IP según la ONG Derechos Digitales. (Peña Ochoa 15)

El Protocolo de Internet o *Internet Protocol* (IP), permite la identificación y comunicación entre los dispositivos conectados a Internet (celulares, computadoras, tabletas, entre otros), asignándoles números únicos, como si se tratara de números telefónicos.

La llamada IP pública es proporcionada por los Proveedores del Servicio de Internet (ISP por sus siglas en inglés), es visible desde Internet e identifica *router*[10] y *módems*[11]. Por otra parte, la IP privada pertenece a las redes

[10] El *router* o enrutador es un dispositivo que permite que varias redes u ordenadores se conecten entre sí y compartan una misma conexión de Internet. (Bembibre, párr.1)

[11] Un módem es un dispositivo que modula y desmodula (mod=modulador dem=demodulador). Comunica dos ordenadores entre sí, permite el intercambio de datos digitales. (Cano, párrs.1–2)

privadas (por ejemplo, una computadora o impresora conectada a un *router).* (Peña Ochoa 16)

El uso general de este protocolo implica ciertos riesgos, entre los que se encuentran:

- Interceptación de información
- Suplantación de mensajes y direcciones IP, lo que compromete la autenticidad y confidencialidad de los elementos comunicados
- Manipulación de paquetes de datos
- Extracción de información para realizar ataques posteriores
- Incidencia de softwares maliciosos que ocasionen la denegación de servicios como correos electrónicos, compra electrónica, entre otros. (Riffo Gutierrez 195–96)

Un ejemplo de la información que puede obtenerse a través de este protocolo lo dio un experto en seguridad de la United States Military Academy, quién, en un ejercicio, pudo saber que videos visualizaban los clientes de Netflix a partir de un algoritmo, tras analizar por unos minutos las llamadas cabeceras TCP/IP. (Velasco, párrs.1–6)

Luego entonces, nuestra computadora, *Smartphone*, tableta electrónica u otros dispositivos en modalidad WIFI *(Wireless Fidelity)* red inalámbrica de área local, se conectan a Internet mediante un *router* inalámbrico, que a su vez se enlaza con el proveedor de servicios de Internet (ISP por sus siglas en inglés), y éste con los motores de búsqueda de la *World Wide Web*, para finalmente conectarse al servidor donde está alojado el sitio o servicio que queremos utilizar. Cuando se hace una solicitud a los motores de búsqueda, por ejemplo, una dirección web del tipo www.sitio.com, esta viaja a los

Servidores de Nombre de Dominio (DNS, por sus siglas en inglés), que traducen este nombre a la dirección IP para su localización. Si este sitio no hubiera sido visitado previamente y por ende no residiera en la memoria temporal del cliente (nuestro navegador en este caso), enviaría la solicitud al servidor donde se ubica dicha dirección para devolverla al origen de la petición y poder accederlo. (Bejerano, párr.5)

En el caso de la conexión LAN alámbrica (Local Access Network), el dispositivo, nuestra computadora, por ejemplo, se conecta a través de un cable de red al router, que se enlaza con el proveedor de servicios de Internet y este con los motores de búsqueda, que a su vez se enlazan con el servidor donde se aloja el sitio o servicio requerido. Todo esto mediante el protocolo referido inicialmente.

El proceso de conectarse a Internet a través de servicios de telefonía móvil, es muy similar, como se observará en la imagen siguiente. También es posible compartir conexión a Internet a otros dispositivos, si se configura uno de ellos (siempre que lo permita), un *smartphone,* por ejemplo, para funcionar como antena WIFI.

Una precisión importante es que la World Wide Web (www), conocida también como la *red de redes*, que basa su navegación en enlaces que derivan a sitios o documentos, es sinónimo para muchos de Internet, un error, pues en realidad es sólo una parte de él. (Peña Ochoa 23)

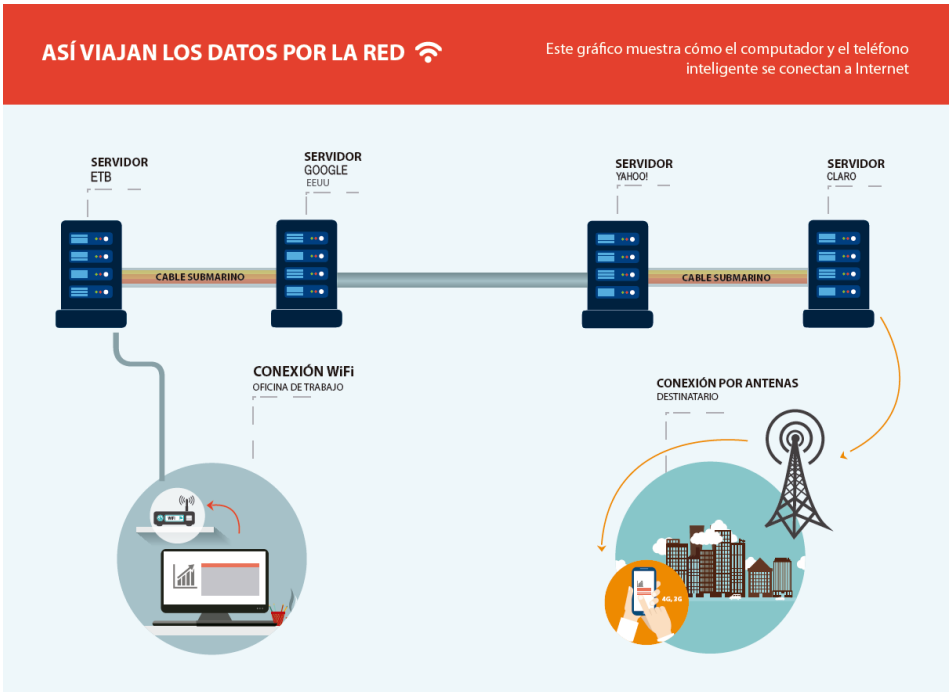

Imagen 27. Descripción de cómo ordenadores y dispositivos se conectan a Internet según Manual Antiespías. (Toledo y Sáenz 18–19)

En este proceso, pueden identificarse cuatro puntos en la comunicación (en el caso de Internet por telefonía móvil son tres): la red local (LAN o Local Area Network) que es la vinculación entre equipos localmente y que se logra mediante, *routers* y repetidores; el proveedor de servicios de Internet, que es quién nos conecta a Internet; los servidores de búsqueda que enlazan todos los contenidos posibles en la Web; y finalmente los servidores donde se alojan los sitios, redes sociales digitales o aplicaciones que queremos utilizar.

> … cuando un usuario utiliza un servicio en línea desde un navegador Web con cualquier tipo de dispositivo, los datos enviados desde el usuario hacia el servicio no viajan en una conexión directa, sino que pasan por medio de varios ordenadores intermedios que componen el entorno de red. (Echeverri 14)

Estos cuatro puntos representan riesgos para la privacidad digital y como consecuencia también para la seguridad, desde la red local (que se vincula desde un *router*), puede intervenirse la comunicación si se logra acceder a ella y obtener información:

> En casi todos los casos estos equipos tienen puertas traseras, entradas remotas que facilitan la administración y actualización de estos equipos por parte de los proveedores. Sin embargo, estas puertas traseras también pueden ser aprovechadas por terceros para monitorear el tráfico que pasa por el *router*. Esta información permite conocer qué páginas se visitan, con quiénes nos comunicamos y con qué frecuencia. (Toledo y Sáenz 22)

Pero en los otros tres puntos puede también almacenarse y accederse a información, como en el caso de los ISP:

> Los servidores de los ISP, como todos los demás equipos, son vulnerables […] almacenan durante años la información de conexiones de sus usuarios. El análisis de datos permite crear perfiles muy precisos de sus usuarios sobre hábitos, gustos e intereses. Bien utilizados sirven para recibir publicidad específica, pero mal utilizados facilitan la identificación de conductas y también ponen en riesgo la privacidad y seguridad de los usuarios. (Toledo y Sáenz 23)

Otro riesgo es el de las denominadas sondas que son capaces de clonar información durante el tránsito de datos:

> Los cables que transportan toda la información entre los grandes servidores y los dispositivos pueden ser atacados. Existen sondas, dispositivos que permiten clonar todo el tráfico que pasa por estos

> cables sin que nadie se dé cuenta. Como sucede con la información almacenada en los ISP, esta gran cantidad de datos puede ser utilizada para crear perfiles y/o hacer seguimientos…este método es utilizado, principalmente, por gobiernos para hacer vigilancia masiva de sus ciudadanos con o sin la participación de los ISP. (Toledo y Sáenz 23)

Por otra parte, los archivos denominados *cookies* también permiten la recopilación de información a partir de nuestra navegación en Internet:

> Muchos sitios web requieren la instalación de una *cookie* en nuestro ordenador. Una *cookie* es una pequeña cantidad de datos que almacena información específica sobre el usuario […] La información puede incluir también los enlaces que hemos seguido para llegar a este o aquel sitio web, o incluso datos personales de nuestros propios ordenadores […] Al acceder a ellas, se puede obtener información acerca de tus intereses y afiliaciones. Una *cookie* en tu ordenador puede actuar como prueba de que has visitado un sitio web particular. (Vitaliev 42)

Luego de conocer la forma en que opera Internet y las zonas de riesgo para la privacidad, debe ser más fácil establecer cuáles son los puntos a considerar para proteger nuestra privacidad y la forma de hacerlo.

En la instancia de lo local con cierto conocimiento y precauciones puede suponerse posible proteger la privacidad, para ello es posible establecer contraseñas seguras, que alternen números, letras, caracteres, mayúsculas y minúsculas (modificándolas periódicamente); elegir con rigor qué redes se comparten con qué personas; proteger nuestros equipos al evitar o permitir su acceso por otros bajo supervisión; actualizar y vigilar con nuestro antivirus los archivos contenidos en dispositivos extraíbles que se

conecten a nuestros aparatos; pero al superar la frontera de nuestra red local todo se complica.

Hay certidumbre, por ejemplo, sobre que la información se traslada en los nodos[12] descritos, pero no así, sobre cómo se protege, qué tanta se almacena, o si lo hacen y el uso que se le da. Ante la difícil posibilidad de monitorear cada uno de esos puntos debe plantearse entonces como proteger nuestra privacidad.

Una de esas posibilidades es desvincular la identidad de la persona sobre lo que hace en Internet para que aun cuando pueda ser leída la información que fluye no sea posible asociarla con ella, lo que funcionaría únicamente cuando esta no permita su identificación, en caso contrario, también habría que hacerla ilegible a terceros, para que sea más complicado conocer los datos que contiene y así lograr el anonimato.

Los dos puntos clave son entonces evitar la identificación expresa y que la información por si misma permita la vinculación. No hay que olvidar que la dirección IP (es el número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella que utilice el protocolo IP (*Internet Protocol*) y dirección MAC (identificador único asignado por el fabricante a una pieza de hardware de red) de nuestro equipo también pueden precisar el origen, destino de la comunicación y por relación, vincularla a una persona específica.

---

[12] Nodo: *punto de intersección o unión de varios elementos que confluyen en el mismo lugar*. (Nuñez Carvonel, párr.1)

Por ello deben considerarse para proteger la privacidad el origen, el destino y la información en tránsito. El ocultamiento de estos tres puntos contribuye al anonimato y como consecuencia a la defensa de la privacidad digital.

Acto seguido, el punto es cómo conseguirlo mientras navegamos en Internet. Con ese pretexto, a continuación, se describirán opciones existentes para lograr el anonimato digital.

II.III. II. Anonimato y sitios web

En el capítulo anterior se han mencionado ya algunos aspectos básicos para proteger nuestra privacidad en lo local, luego entonces falta precisar las opciones realizables mientras navegamos en Internet.

Todo nuestro quehacer en la Web deja un rastro. El buscador de Google por ejemplo es capaz de almacenar nuestro historial de búsqueda indistintamente en un ordenador o dispositivo; acceder a nuestra agenda, conocer que buscamos y a partir de eso perfilar de mejor forma la publicidad que terceros contratan. Por eso no es extraño que los anuncios que se nos muestran en sitios y redes sociales digitales se ajusten a aquello que buscábamos previamente. Esta medición es mejor si tenemos vinculada una cuenta de Gmail, la registramos en nuestro navegador Chrome, el explorador propio de la marca y utilizamos sus distintos servicios (Youtube, Google Maps, Google Plus, etc.), aunque esto es una práctica realizada también por otros navegadores y redes sociales digitales.

Otro punto trascendental es el de las denominadas *cookies*, con las que los sitios web que visitamos rastrean nuestros pasos. Estas se utilizan prácticamente en todos ellos y son distinguibles en algunos casos porque el lugar accedido nos notifica que podemos ser rastreados y solicita aceptar el

uso de las mismas. Si se ignora el anuncio de *cookies*, se considera se ha aceptado tácitamente utilizarlas.

Tipos de *Cookies*

***Cookies* de sesión**	Se trata de *cookies* que almacenan información sobre un usuario mientras se encuentra navegando por un sitio web. Suelen tener una duración corta, típicamente hasta que el usuario cierra su navegador o caducan. Son útiles para identificar a un usuario y almacenar información relacionada con sus preferencias. Dicha información es utilizada para ofrecer contenidos personalizados que se ajusten a lo exigido por el cliente.
***Cookies* funcionales**	Son aquellas *cookies* que permiten dotar a la aplicación web de comportamientos personalizados dependiendo de su valor. Algunos ejemplos de este tipo de *cookies* son aquellas que permiten el procesamiento de una operación en la aplicación web o el acceso a funcionalidades concretas. Evidentemente este tipo de *cookies* son definidas y utilizadas por los desarrolladores del sitio web con el fin de cubrir ciertos requisitos funcionales o técnicos exigidos en la aplicación.
***Cookies* de terceros**	Son *cookies* que se crean por un dominio externo al que el usuario se encuentra visitando y en ocasiones son empleadas para hacer un seguimiento de la actividad del usuario.
***Cookies* de personalización**	Aunque son similares a las *cookies* funcionales, las *cookies* de personalización se encargan de establecer valores de carácter general que típicamente afectan a la presentación del sitio web. Algunos ejemplos de personalización de este tipo de *cookies* son aquellas que establecen el idioma en el que se deben enseñar los contenidos del sitio web o el tipo de navegador utilizado por el cliente con el fin de servir los contenidos de forma adecuada.

***Cookies* de análisis**	Se trata de valores que le permiten a una aplicación web analizar el comportamiento de los usuarios y generar patrones. Este tipo de *cookies* pueden contener, entre otras cosas, la hora en la que el usuario entra y sale del sitio web, el navegador utilizado, la dirección IP reportada por el navegador, los enlaces más visitados del sitio, etc. Evidentemente, se trata de *cookies* que intentan perfilar y conocer los hábitos de los usuarios de la aplicación web.

Tabla 14. Tipos de *cookie*s. Elaboración propia. (Echeverri, *Deep Web* 16)

Deshacerse de las *cookies* periódicamente podría hacer pensar que el problema está solucionado, pero hay otras más difíciles de eliminar (prácticamente todos los navegadores permiten su eliminación). *Las cookies* persistentes funcionan de forma más agresivas lo que complica su borrado:

> … cuando se eliminan en uno o varios de los espacios, pero no de todos, el sitio web que ha implementado la *cookie* persistente es capaz de detectar que el usuario ha intentado hacer una limpieza y se encarga de restablecer los valores en cada espacio de almacenamiento, revirtiendo la acción de borrado realizada por el usuario. Esto quiere decir que se debe eliminar la información de la *cookie* persistente de todos los sitios donde se ha guardado y si falta al menos un sitio por limpiar, dichos valores volverán a ser restablecidos. (Echeverri 24)

Podemos entonces eliminar de modo aparentemente sencillo las *cookies* que no son persistentes, pero las últimas requerirán de limpieza exhaustiva. La recomendación preliminar antes de indagar en las formas de lograr el anonimato digital, es averiguar como eliminar estos archivos en su navegador, información que seguramente estará contenida en su sitio de descarga. Deberá realizarse esta acción periódicamente.

II.III.III. HTML 5 y elementos persistentes

Otra forma de almacenaje de la información del usuario se da a través del mecanismo de almacenamiento de HTML5 (lenguaje de marcaje, que se utiliza para estructurar y presentar el contenido para la Web), conocido como *Client-Site storage*. Su principal diferencia sobre las *cookies* es que en este caso no hay fecha de caducidad y que puede almacenar hasta 10 megabytes de información. *El mecanismo de almacenamiento local de HTML5 es una mejora considerable a la hora de guardar datos en el cliente sin depender de las cookies tradicionales y cuenta con una API en Javascript que permite acceder y manipular sus elementos almacenados en el cliente.* (Echeverri, *Deep Web* 17)

Este almacenamiento del lado del cliente o *Client-Site storage*, guarda de manera persistente los datos que no son eliminados de forma automática, por lo que a partir de él también se pueden utilizar (Echeverri, *Deep Web* 17):

> … algunas de las técnicas de seguimiento y vigilancia que se pueden aplicar con las cookies tradicionales y lo que es peor […] son elementos que pueden quedarse de forma indefinida en el navegador del cliente y que le permitan a un servicio web o a terceros, acceder a información sensible sin consentimiento previo. (Echeverri, *Deep Web* 17)

En los últimos dos casos se presume, resultará extremadamente complicado ejecutar las medidas adecuadas por el usuario promedio de Internet, que desconoce esta clase de información.

II.III. IV. Dirección IP

Se menciona nuevamente a manera de recapitulación la dirección IP, que es la dirección asignada por el proveedor de servicios de Internet y mediante la cual se puede conocer diferente información como quién es el proveedor del servicio de Internet, la dirección de la página web de donde se proviene, el navegador utilizado, su versión, si acepta el uso de *cookies*, el sistema operativo del equipo, el *service pack* que tiene instalado (actualizaciones que reparan y mejoran un sistema operativo), y la ubicación geográfica. (Carrodeguas, párr.15)

A través del lenguaje de programación Javascript y la dirección IP, puede conocerse, además, la zona horaria del equipo, el navegador de Internet utilizado, los *pluggins* (complementos), que tiene instalado el navegador, la resolución en pixeles del mismo y parte del historial de navegación. (Carrodeguas, párr.15)

II.III. V. Formularios y registros de acceso

A parte del protocolo TCP/IP, Otras formas de obtención de información de los usuarios son los formularios y registros de acceso de sitios, servicios y redes sociales digitales.

La mayoría de estos, nos obligan a registrarnos para acceder. Es absolutamente necesario en esos casos, estar seguros de la necesidad de utilizarlos y de saber si cumplen con requisitos mínimos de seguridad, pese a ello, ha de preferirse crear un correo electrónico desvinculado de nuestra persona. De acceder con nuestro correo electrónico personal, somos susceptibles de compartir nombre, edad y en algunos casos, el número telefónico (si no hemos configurado correctamente los aspectos de privacidad).

Otro punto importante es jamás vincular estos servicios a nuestras redes sociales digitales, aunque nos simplifique el proceso de registro, porque al hacer esto damos permiso a estas aplicaciones web de acceder a cierta información de las mismas (nombre, edad, fecha de nacimiento, amigos, publicar en nuestro nombre, etc.), datos que pueden utilizarse indebidamente.

Por otro lado, navegar sin vincular una cuenta, en Chrome o servicios similares, no impide que se dé seguimiento de nuestra información. Servicios de métricas, *cookies* y almacenamiento de HTML 5, posibilitan la obtención de la información. Su lectura, incluida la dirección IP, podría ayudar a deducir en algún momento la identidad o al menos los hábitos de una persona para su posterior perfilación. Es decir, no registrarse no es suficiente.

Un ejemplo de rastreo con fines comerciales son los servicios de métricas sobre tráfico web, ampliamente difundidos como Google Analytics, que además de mencionar el lugar de residencia de los visitantes, puede señalar el dispositivo desde el que se accede, el sistema operativo que se utiliza y el tiempo que un usuario permanece dentro de un sitio, las páginas o secciones que visita y en portales de venta, previa configuración, establecer índices de comportamiento (KPI´S) para saber si las personas realizan alguna acción específica.

Luego entonces una posibilidad es ocultar o modificar nuestra dirección IP, bloquear todo aquello que pueda rastrear nuestra información, desvincular nuestra identidad de nuestras acciones en Internet y procurar que la información que compartamos no permita una identificación sencilla. En este punto es igualmente importante considerar que terceros pueden compartir

información propia sin nuestro consentimiento igual que ocurre en el mundo físico.

II.III.VI. Buscadores

Una forma de conseguir el anonimato y evitar el seguimiento de información es la utilización de buscadores o motores de búsqueda (sistema informático que busca archivos almacenados en servidores web) (*EcuRed*, párrs.1–4), que impidan el rastreo y que no guarden historial alguno de nuestras exploraciones.

El primero a mencionar es https://www.ixquick.com/. De acuerdo a su propia descripción, a través de su uso, la información de identificación de la búsqueda es eliminada previamente antes de enviarla anónimamente a Google. (Ixquick, "StartPage", 1–6)

Otra singularidad señalada por Ixquick que puede resultar benéfica es que no memoriza la dirección IP y que no hay filtros por la construcción de perfiles del usuario como existiría en un motor de búsqueda convencional, lo que garantiza resultados indiscriminados y por ende mayor neutralidad y pluralidad. Este buscador cuenta también con una aplicación descargable para dispositivos iOS y Android llamada Ixquick Search. (Ixquick, "Herramientas", párr.1)

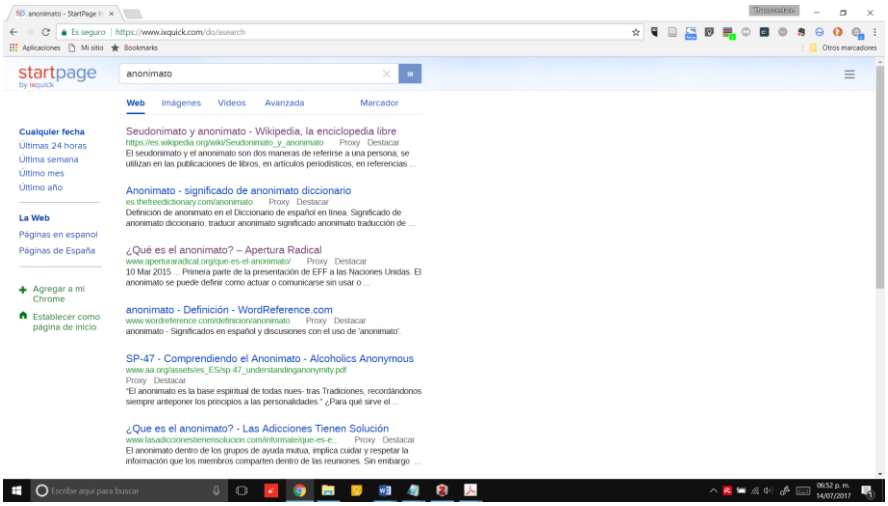

Imagen 28. Apariencia de ixquick.com. Captura de pantalla.

> … es importante anotar que el listado de resultados que arrojan las búsquedas pueden llevar al usuario a sitios que pueden utilizar mecanismos de seguimiento y tracking […] cuando el usuario ingresa en alguna de las páginas contenidas en los resultados de la búsqueda, está abandonando el motor. (Echeverri 28)

Esto quiere decir que al entrar a cualquier sitio se abandona Ixquick, lo que implica protegerse del rastreo en el sitio visitado.

Otro buscador es https://duckduckgo.com/, que presume no recolectar ni compartir información del usuario mientras utiliza sus servicios, no guardar el historial, e incluso, señala no rastrear las búsquedas como lo hacen otros. (DuckDuckGo, párrs.1–4)

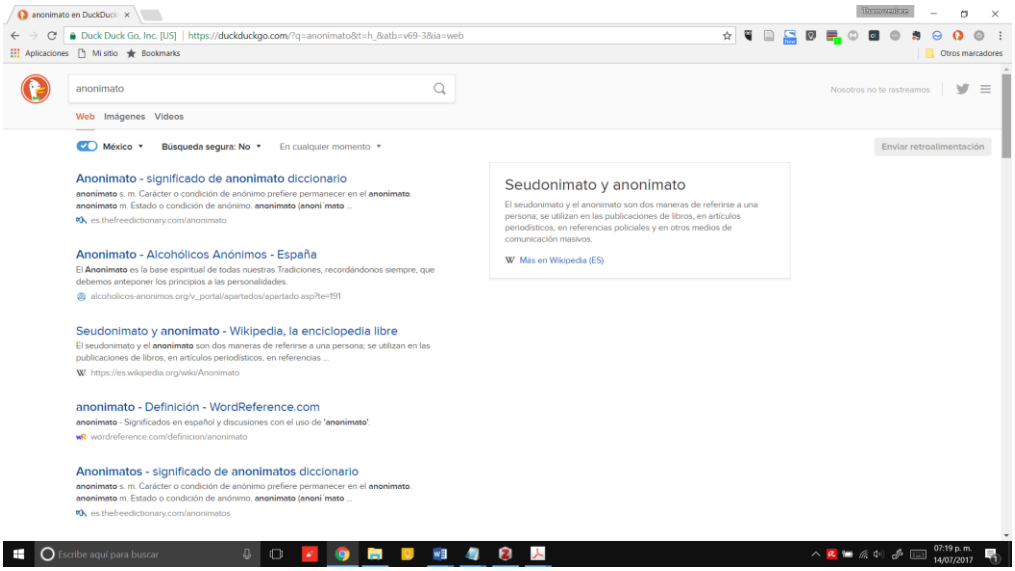

Imagen 29. Apariencia de duckduckgo.com. Captura de pantalla.

En Duck duck go, como en Ixquick, los beneficios se pierden al acceder a cualquier sitio si este rastrea información. Esto es una regla general independiente del buscador que se utilice.

II.III.VII. Complementos para navegadores

También existen complemementos para navegadores o *plugins*[13], que bloquean los rastreadores de la páginas web que visitamos.

Para efectos de esta investigación se analiza Ghostery, porque ha adquirido cierta fama y por ser compatible tanto con el navegador Firefox como Chrome. Este complemento, previamente instalado, *menciona* qué empresas son las que intentan rastrearnos y permite bloquearlas para poder protegernos al navegar directamente en los sitios. (Ghostery, párr.1) El

13 *Plugin: es aquella aplicación que, en un programa informático, añade una funcionalidad adicional o una nueva característica al software. En nuestro idioma, por lo tanto, puede nombrarse al plugin como un complemento.* (Pérez Porto y Merino, párr.2)

inconveniente es que hay que repetir el proceso en cada sitio o crear un perfil para configurar los parámetros. Al acceder directamente a la aplicación nos informa que no estaremos a salvo de sus propios rastreadores:

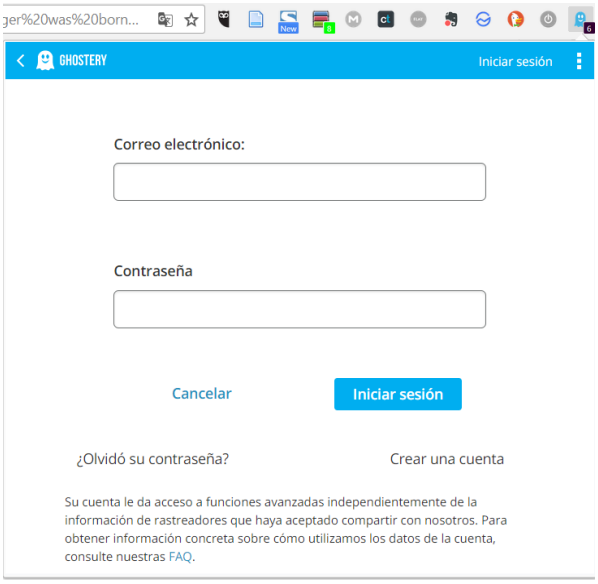

Imagen 30. Ventana de Ghostery en Chrome, para iniciar sesión. Captura de pantalla.

En una pequeña prueba desde el buscador Google, fue posible percatarse que en apariencia no se detectaba ningún rastreador, sin embargo, sí parece hacerlo al acceder a los sitios.

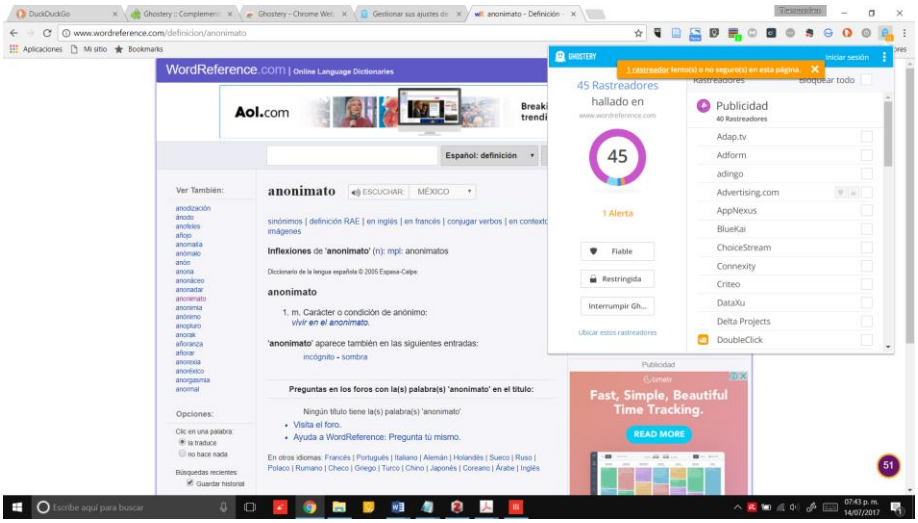

Imagen 31. Detección de rastreadores en Ghostery. Captura de pantalla.

Otra aplicación que nos protege de forma similar es Privacy Badger, *plugin* compatible con los navegadores Firefox y Opera y que tiene como cualidades bloquear anunciantes indeseados e impedir que rastreadores invisibles de terceros nos sigan mientras deambulamos por distintas páginas web. (EFF, "Privacy Badger", párrs.1–3)

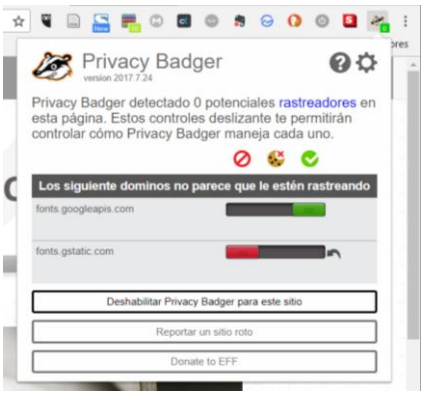

Imagen 32. Ventana de Privacy Badger en Chrome. Captura de pantalla.

Como se aprecia en la imagen, para que el usuario pueda bloquear los rastreadores detectados, debe mover la barra del verde al rojo de cada uno de ellos. Si se muestra en amarillo, el bloqueo es parcial. Puede mostrarse de ese color si el complemento no logra detenerlo totalmente.

Privacy Badger es desarrollado por Electronic Frontier Foundation (EFF), Organización en defensa de la privacidad digital y tiene como punto a favor, sobre muchos otros, el no perseguir fines comerciales que pudieran desvirtuar la razón de este tipo de aplicaciones.

No hay que olvidar que la protección es en ciertos límites falible, debido a las constantes actualizaciones de los sistemas en Internet. Por ello deben tomarse previsiones sobre su utilización. Aquí se propone utilizar mejor aplicaciones como Privacy Badger, que están respaldadas por una organización sin ánimos de lucro, en pie de lucha para defender la privacidad digital, contra aplicaciones que nos protegen de unas, pero no de otras amenazas como es el caso de Ghostery u otras de pago.

Una opción más es HTTPS Everywhere, complemento instalable en Firefox, Chrome y Opera. Este *plugin,* desarrollado también por la propia EFF, promete encriptar[14] las comunicaciones que se tengan con los sitios web a los que accedamos, lo que hace la navegación más segura.

[14] Encriptar: en el ámbito de la informática y las comunicaciones, *es la acción de preparar un archivo o mensaje para que solo pueda interpretarse si se dispone de su contraseña o clave.* (Fundéu BBVA, "encriptar es ocultar un mensaje con una clave", párr.1)

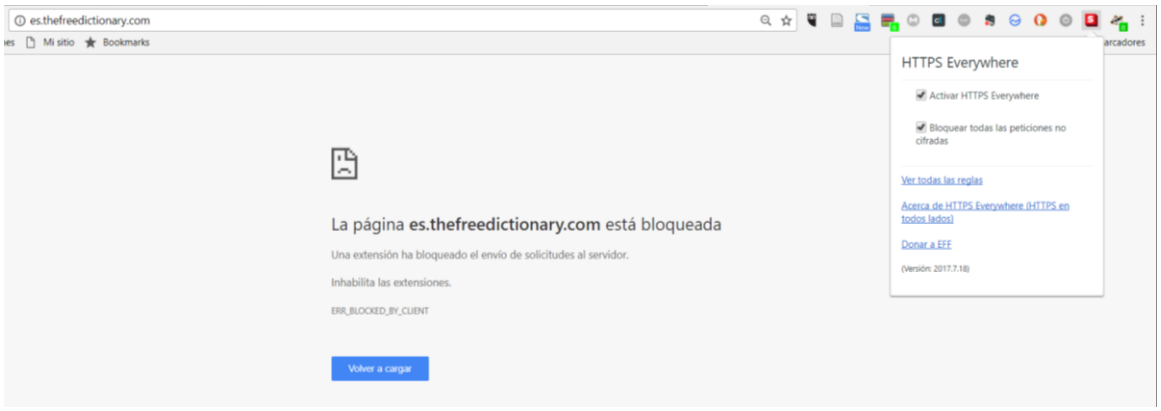

Imagen 33. Sitio bloqueado por HTTPS Everywhere en Chrome. Captura de pantalla.

HTTPS Everywhere cambia miles de sitios del protocolo “http" que son inseguros, a "https", que corresponden a direcciones web que cuentan con el protocolo seguro de transferencia de hipertexto, también bloquea aquellas que no lo tengan, como se aprecia en la imagen anterior. De esta forma se protege al internauta de la posible vigilancia, secuestro de cuentas y algunas formas de censura. Sin embargo, si el servidor web no tiene activado el protocolo https, esto no será posible. (EFF, “HTTPS Everywhere”, párrs.1–2)

Privacy Badger y HTTPS Everywhere cuentan también con versiones instalables compatibles con dispositivos móviles, que tengan instalado el sistema Android y que utilicen como explorador Firefox u Opera.

Los buscadores pro anonimato impedirán la recopilación de información y su almacenamiento, además de que truncarán el acceso a nuestra dirección IP, acto seguido los complementos bloquearan la publicidad y rastreadores invisibles, además de que nulificarán cualquier intento de acceder a un sitio

no seguro (http) y cifrarán[15] la comunicación. Con lo anterior se puede lograr un entorno más o menos seguro en buscadores y sitios web. Aún así no debe olvidarse borrar periódicamente las llamadas *cookies*, para evitar la recopilación sustanciosa de nuestros datos en sitios que para poder usarlos precisen su aceptación.

II.III. VIII. Servidores proxy anónimos y cifrados

Uno de los tantos problemas que acarrea la pérdida de la privacidad es la censura. Hay sitios que son restringidos para ciertas poblaciones o usuarios; en estos casos toma mucha más importancia el anonimato. También es posible que simplemente deseemos estar exentos de ser vigilados y espiados. Los servidores proxy en estos casos se mencionan como la solución.

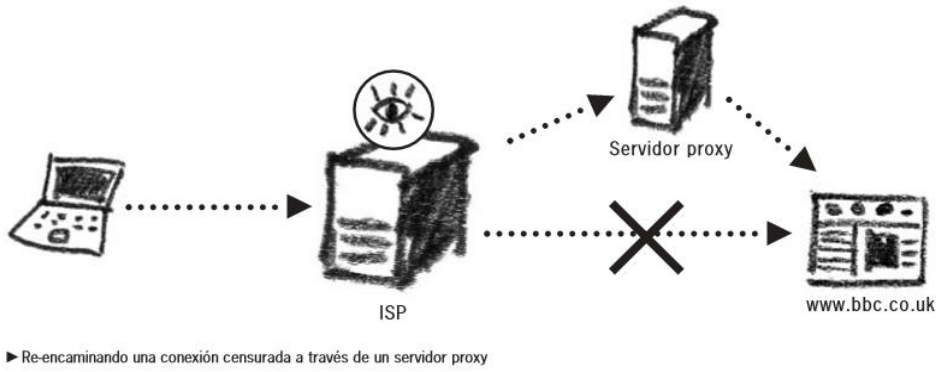

Imagen 34. Funcionamiento de un servidor proxy. (Vitaliev 49)

El servidor proxy en estos casos, recibe la petición del usuario en cuestión, a través del proveedor de servicios de internet o ISP y accede al sitio deseado, tras saltar la prohibición al ordenador o dispositivo original.

---

[15] Los datos son cifrados por un algoritmo para codificarlos, abandonen su formato original y no sea posible verlos. *Los datos solo se pueden decodificar a su forma original aplicando una determinada clave de descifrado.* (Kaspersky Lab, "Qué es el cifrado", párr.1)

Imagen 35. Funcionamiento de un anonimizador. (Vitaliev 49)

Este tipo de servicios están incorporados a una página web mediante la cual se navega y permiten ocultar el origen y el destino solicitado. Pero debe observarse que no hay control sobre el método de comunicación utilizado y como consecuencia sobre la privacidad del enlace entre el servidor proxy elegido y el sitio web deseado:

> ..... muchos de estos servicios implementan rutinas que no favorecen la privacidad de sus usuarios y en algunos casos pueden ser maliciosas. Un servidor proxy recibe y procesa información desde una posición bastante ventajosa, ya que tiene la posibilidad de capturar y manipular los datos de las peticiones y respuestas correspondientes a la comunicación entre un cliente y un sitio web. (Echeverri 43)

Resultará inútil entonces buscar el anonimato en los servidores proxy o anonimizadores, pues representan en alto grado el mismo peligro que se desea evitar, sin embargo, resultan ideales para enfrentar la censura y realizar búsquedas, siempre que no se involucre información sensible que pueda ser capturada y almacenada por otros, aunque algunos países también identifican estos anonimizadores y los incorporan a sus listas negras para que no puedan acceder a determinados lugares.

Algunos opciones son:

https://zend2.com/es/
https://kproxy.com/
https://proxify.com/

Una última recomendación al respecto, es sólo utilizar anonimizadores que utilicen el protocolo HTTPS, o en caso contrario, cualquiera podría vigilar.

La tercera opción son los servidores proxy cifrados: *El cifrado de comunicaciones de punta a punta es el proceso por el cual un mensaje es convertido en un código ilegible, mientras es transmitido por redes de telecomunicaciones.* (Toledo y Sáenz 36)

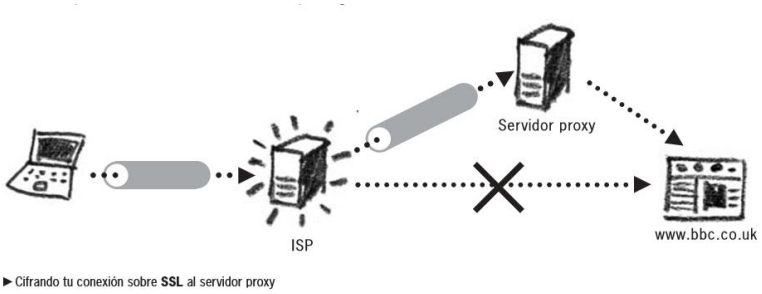

Imagen 36.Funcionamiento de un servidor proxy cifrado. (Vitaliev 50)

En este caso la información es cifrada desde el origen, hasta llegar al servidor proxy, por lo que no puede ser identificada, ni leída, lo que da seguridad en el tránsito, pero hay que tener certeza de que la información no sea utilizada indebidamente una vez que sea descifrada, lo que podría suceder de acuerdo al gráfico anterior al llegar al servidor proxy.

II.III. IX. Circumventores

Una variación de los servidores proxy y servidores proxy cifrados, son los llamados Los circumventores (eludidores), que permiten saltar las restricciones con ayuda de conocidos. La ventaja, que los censores tienen mayor dificultad para descubrir estos servidores. La configuración de esta

aplicación, sin embargo, requiere cierta pericia con nuestro *router.* (Vitaliev 50)

Psiphon.ca ofrece este servicio y puede ser utilizado en dispositivos con sistemas operativos iOS, Android y Windows. Se requiere descarga y en algunos casos instalación, en Windows basta con abrir el fichero ejecutable. El archivo se localiza en el sitio web señalado.

Imagen 37. Funcionamiento de Psiphon. Captura de pantalla.

Tras la descarga y ejecución del archivo, la aplicación comienza a trabajar, incluso la detección de idioma es automática. Acto seguido, puede elegirse el servidor, según el país, desde el que deseamos navegar o permitir que la aplicación elija el más cercano automáticamente, para que la velocidad de navegación se vea menos comprometida.

Psiphon permite también encausar toda nuestra comunicación mediante esta vía o elegir únicamente algunos servicios. El funcionamiento es el mismo desde el teléfono celular.

Finalmente, este servicio tiene como ventajas ser desarrollado con código abierto, con lo que es más fácil determinar vulnerabilidades para los expertos y perfeccionar las operaciones, también, ante la diversificación de servidores se vuelve más complicada la censura; como desventajas, que muestra publicidad, lo que en sí mismo ya es un atentado contra la privacidad, además, requiere cierto conocimiento para la configuración avanzada. Aún así, la comunicación en el trayecto, por estos medios puede resultar anónima para terceros.

El verdadero desalentador sobre esta aplicación se encuentra en sus políticas, que establecen, se utilizan *cookies* en algunos de sus sitios, Google Analytics, e incluso rastreo de información con Amazon S3, lo que puede ir en contra del resguardo de nuestra privacidad, por intrusión e influencia en nuestras decisiones mediante la publicidad. (Psiphon 1–13)

Otra recomendación de circumventores, hallada en la literatura señalada, fue Peacefire, localizable en https://www.peacefire.org/circumventor/ y que:

> ... permite crear tu propio servidor proxy para que puedan utilizarlo los demás. Para poder instalar y mantener este servidor, necesitarás un ordenador dedicado y una conexión a Internet con una IP estática. Es recomendable que tu servidor esté instalado en un país que no ejerce la censura en Internet. (Vitaliev 51)

La primera sorpresa al acceder al sitio, es que no cuenta con una dirección HTTPS, lo que de entrada es inseguro y sólo cuenta con la siguiente descripción:

> This site is used to distribute the location of "Circumventor" URLs like http://www.MouseMatrix.com/, which can be used to get

> around Web blocking software. If MouseMatrix.com is blocked where you are, then you can sign up to receive the URLs of new Circumventor sites every 3 to 4 days, by entering your e-mail address below... (Peacefire, párr.1)

Es decir que debe ingresarse una dirección de correo electrónico para recibir las nuevas direcciones de acceso cada 3 o 4 días. El servicio señala además que no se comparte esta información con terceros y que aún cuando las compañías de *software* de bloqueo puedan inscribir sus propias direcciones de correo electrónico para censurarlas, en la mayoría de lugares tarda entre 3-4 días que los sitios recién publicados en dicho lugar sean bloqueados. (Peacefire, párrs.1–4)

Para configurar este circumventor en nuestro ordenador, hay que seguir los pasos descritos en: https://www.peacefire.org/circumventor/simple-circumventor-instructions.html. Lo importante es que debe ser instalado en un equipo que no haya sido previamente censurado para que pueda funcionar.

De seguir las instrucciones, la instalación se muestra como un proceso sencillo, pese a ello, el manual de instalación está sólo pensado para windows XP y Vista, versiones ya en deshuso. Sin embargo se deja constancia aquí de esta opción para todo aquel que quiera probar verificar si es compatible con su sistema operativo.

De funcionar, la ventaja sustancial en estos casos, es que puede uno ser actor y beneficiario de cierto anonimato. Hay más información disponible en la red sobre circumventores que hay que evaluar según el sistema operativo utilizado, pero estos al no ser considerados en la literatura se han dejado de lado para que el interesado profundice en ello.

II.III. X. Redes privadas virtuales

Las redes privadas virtuales (RPV), comunmente conocidas como VPN (Virtual Private Network), son conexiones privadas entre dos puntos logradas por un red pública como Internet. Así, puede establecerse una conexión directa y cifrada, con la finalidad de hacer anónima la comunicación y mantener la privacidad de los actores de la misma. (Echeverri 41)

Una Red Privada Virtual (RPV o VPN, por sus siglas en inglés), equivaldría a un túnel que comunica dispositivos a través de Internet. Dos son las principales ventajas de su utilización, la primera, que enruta[16] la comunicación (busca y elige un camino), por una dirección IP distinta, lo que hace complicado su rastreo y ubicación. La segunda, que también permite acceder a sitios censurados, en ese sentido, resulta útil como un servidor proxy:

> Las RPV crean conexiones cifradas al servidor central, y a través de esta conexión, mandan toda la información enviada y recibida por el ordenador. Por lo tanto, si tu servidor de RPV se encuentra en un país que no aplica censura en Internet, puedes utilizar este servicio para encaminar el tráfico en Internet a través de el [sic]. (Vitaliev 51)

El principal defecto, al igual que los servidores proxy, es que la información, si bien es innaccesible para terceros, no necesariamente lo es para quiénes ofrecen este tipo de servicios.

---

[16] *Enrutar es redirigir o encaminar una conexión a un equipo en concreto que dispone de un servicio específico o un software que necesita realizar conexiones por un puerto X*. (Alegsa, "¿Qué es enrutar?", párr.1)

Existen versiones gratuitas y de paga para crear redes privadas virtuales (RPV), aquí sólo se han de enumerar algunas a manera de ejemplo.

La primera de ellas es FrootVPN, disponible en https://frootvpn.com/, que ofrece compatibilidad con Windows, iOS, GNU/Linux y Android (en todos los casos tiene que instalarse la aplicación), además de no guardar archivos log, esto significa que no queda registro alguno de nuestra navegación, ni son compartidos nuestros datos con terceros. Como desventaja tiene no ser gratuito, pero ofrece tres opciones de contratación: mensual, trimestral y anual. Su precio base es de 7.99 euros. (FrootVPN, párrs.1–11)

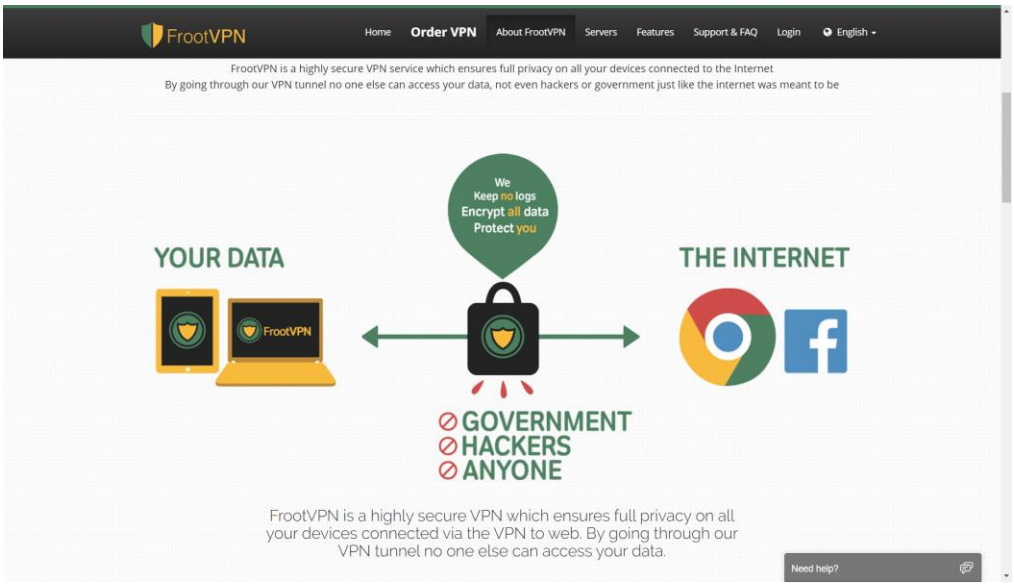

Imagen 38. Descripción del servicio por FrootVPN. Captura de pantalla.

La segunda opción es TunnelBear, disponible en https://www.tunnelbear.com/, que básicamente ofrece navegación segura, sin archivos de registro, compatibilidad con Windows, iOS, GNU/Linux y Android, un par de extensiones para los navegadores Chrome y Opera, además la conexión a su servicio desde un solo clic. Como plus, TunnerBear ofrece una versión gratuita restringida a 500 megabytes (MB) mensuales, suficientes si empleamos poco tiempo para acceder a Internet, si no

requerimos visualizar sitios con demasiado peso (videos, audio, imágenes en alta resolución) o si queremos utilizar nuestros 500 MB en comunicaciones específicas de poco peso. (TunnelBear, párrs.1–11)

El registro comprende únicamente un correo electrónico y contraseña; después es necesario descargar la aplicación, leer y aceptar los términos y condiciones del servicio; elegir la carpeta donde se instalará y acceder con nuestros datos de registro. Después, simplemente hay que elegir la ubicación geográfica desde la que navegaremos.

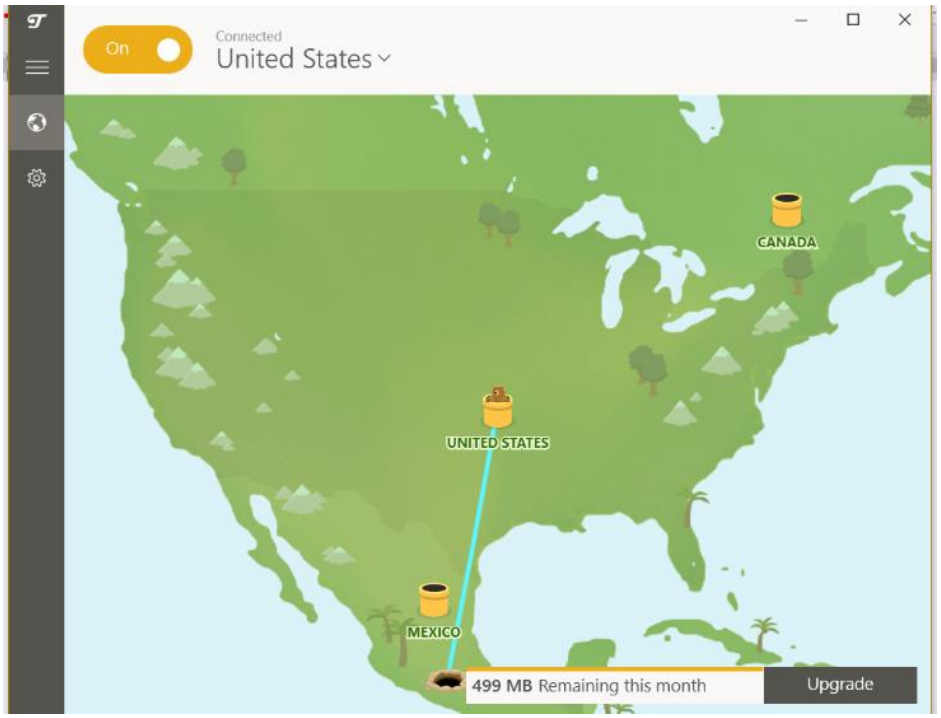

Imagen 39. Interfaz de TunnelBear. Captura de pantalla.

Otro plus de esta aplicación es que intenta ser lo más sencilla e intuitiva posible. La mascota, por ejemplo, te muestra gráficamente la ubicación desde donde navegas y la original cuando está apagada la RPV, así como la cantidad de MB disponibles. Contratar el servicio tiene un costo de 9.99

dólares mensuales o 4.99, si se aseguran 12 meses del servicio, con esto la navegación puede ser ilimitada.

Una tercera opción es Your-freedom, descargable en https://www.your-freedom.net/. Es compatible con Windows, iOS y Android, pero no así con GNU/Linux, su otro inconveniente, desde la óptica del usuario común; es que no es tan intuitivo como los anteriores.

Your-freedom requiere registro e instalación, que consta de muchos pasos y configuraciones que pueden resultar complejas si se está poco familiarizado. Una vez instalado hay que configurar el proxy manualmente, lo que puede resultar tedioso para algunos, aunque ofrece una forma de auto-detección.

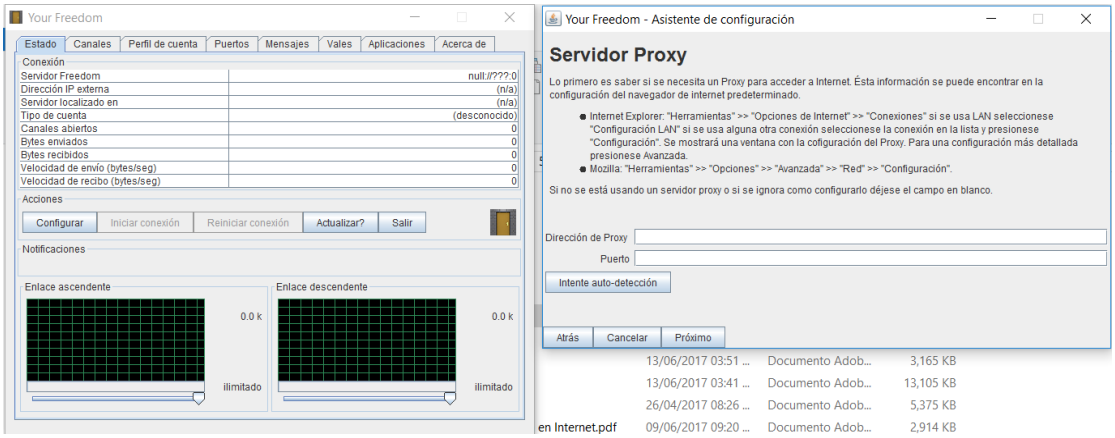

Imagen 40. Interfaz y configuración de Your-freedom. Captura de pantalla.

Acto seguido, puede elegirse un preajuste, que no es más que una lista de los países desde los que se puede navegar en Internet.

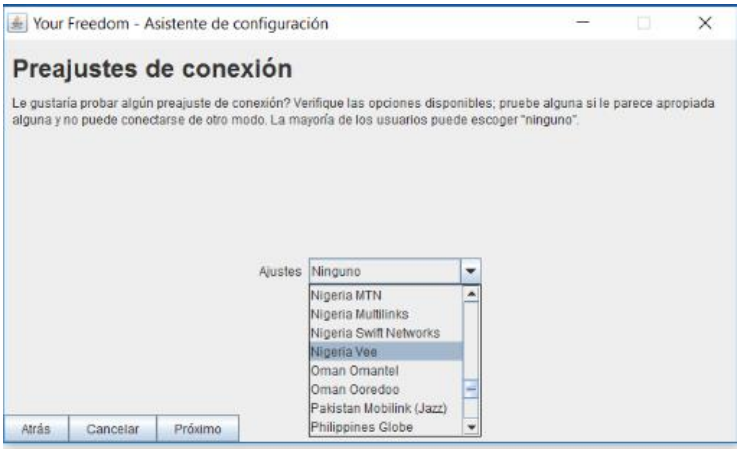

Imagen 41. Selección de protocolos en Your-freedom. Captura de pantalla.

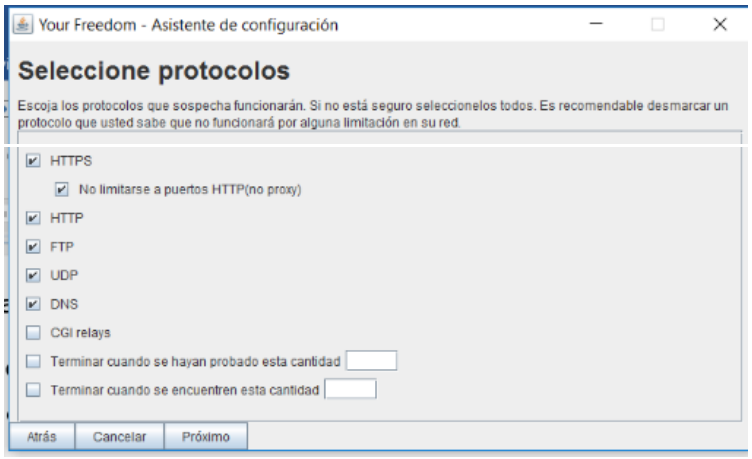

Imagen 42. Preajustes de Your-freedom. Captura de pantalla.

Después todavía hay que seleccionar *que protocolos se sospecha funcionarán.*

Por último, hay que buscar que servidores están disponibles según nuestra configuración y acceder con nuestros datos de registro. Si bien no se duda de las posibilidades que tal nivel de configuración a nivel seguridad otorga, el usuario promedio puede encontrar tantos parámetros confusos, desconocidos e incomprensibles, por lo que de entrada no se traduce en una opción recomendable. Aun así, puede aprenderse más sobre cada uno

de estos parámetros, para qué sirven y utilizar mejor todas sus posibilidades.

A través de las RPV es posible conectarnos a una red local a distancia, como podría ser la de nuestra casa u oficina, una opción valiosa en la que sólo hay que observar que garantías, respecto de la seguridad, ofrecen los proveedores de este tipo de servicios.

Como en los rubros anteriores, estas no son las únicas opciones, existen otras en el mercado y lejos de él, que el interesado puede localizar en una búsqueda rápida por Internet. Las RPV resultan ser una buena opción de anonimato para evitar el monitoreo de nuestra información por terceros y para contrarrestar la censura que puede darse para acceder o difundir cierta información. Para ello es necesario acercarse a la parte técnica.

II.III. XI. Redes anónimas y Web profunda

Una posibilidad más son las redes anónimas, que permiten ocultar nuestra verdadera identidad, a la vez que evitan el filtrado y retención de información que puede darse en la Web tradicional (Vitaliev 51):

> Se trata de las soluciones más avanzadas y maduras que existen actualmente en el campo del anonimato y la privacidad, en consecuencia también las que cuentan con mayor apoyo por parte de la comunidad de usuarios. (Echeverri 49)

La Web consta de diferentes partes con fines distintos, que algunos dividen en: Web profunda o *Deep Web*, donde se ubican bases de datos, investigaciones y documentos gubernamentales; y la Web oscura o *Dark Web*, a la que muchos le dan connotaciones negativas (desde el nombre) y donde coexisten las redes anónimas, usadas entre otras cosas, para

evitar la persecución mediante comunicaciones privadas y la navegación cifrada innacesible para otros:

> ... la web profunda o "deep web" se refiere a contenidos que se encuentran en lnternet pero que no se encuentran indexados por los motores de búsqueda modernos o si lo están, son sumamente difíciles de hallar ... el término "dark web" se refiere a contenidos que no se pueden indexar dado que se encuentran protegidos por sus autores, los cuales se encargan de usar y compartir dichos contenidos en redes privadas/anónimas o en sitios web en Internet que se encuentran protegidos por contraseña. (Echeverri 49–50)

Las razones por las que un sitio puede no estar indexado no necesariamente tienen que ser ilegales, esto puede suceder porque el sitio sea considerado irrelevante, o esté protegido por contraseña y resulte en consecuencia innaccesible. (Echeverri 50)

El caso de la *Dark Web* es el mismo, si bien la imposibilidad de ser accedido y vigilado puede dar pie a prácticas nocivas para la sociedad, también resulta útil para evitar la censura, vigilancia, espionaje y recibir amenazas en actividades como el periodismo y el activismo social, que no exentan al usuario común, que puede encontrar valiosas estas alternativas para proteger su identidad, privacidad e intimidad, sin que esto involucre necesariamente actos delictivos.

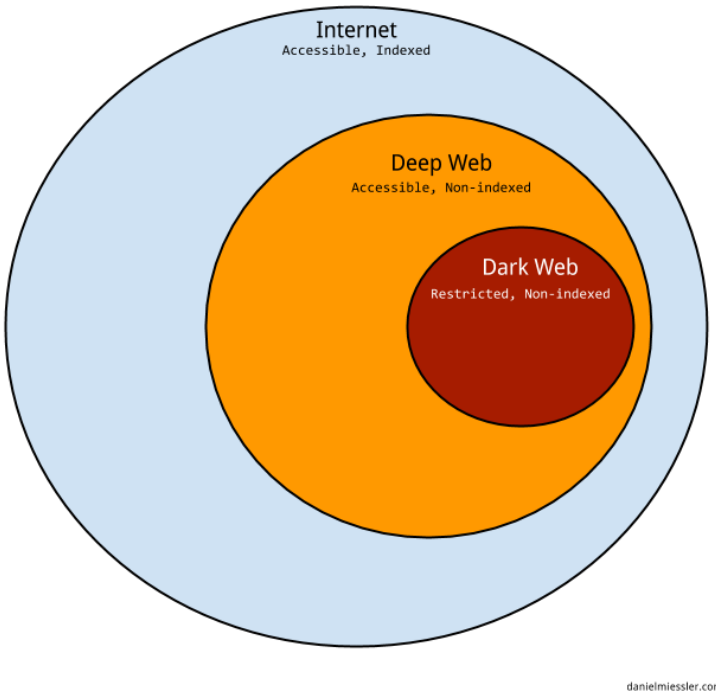

Imagen 43. Surface web vs Deep Web vs Dark Web. (Miessler, párr.1)

En el gráfico anterior se ilustran las distintas partes de la Web, pese a ello, debe considerarse que al no estar indexada la información que existe en la *Deep Web* o *Dark Web*, no puede establecerse su volumen, por lo que hay que ignorar la referencia visual clásica del *iceberg*, que circula en Internet, que puede dar la idea equivocada de que hay más contenido en las dos últimas, que en la primera.

En algún momento de la vida todos podemos requerir de estas herramientas, ya sea por un conflicto laboral, inseguridad, persecución o simplemente porque no queremos ser rastreados por empresas, anunciantes, gobiernos o delincuentes.

Las redes anónimas ocultan la dirección IP y por ende la ubicación real del usuario, además el tráfico pasa por diversos nodos cifrados, lo que dificulta

el rastreo del origen – tránsito (mensaje) - destino y viceversa, de todas las comunicaciones.

Tor (The Onion Router) accesible desde https://www.torproject.org/, es una de las opciones más conocidas de redes anónimas y está disponible para Windows, Mac y GNU/Linux. Utilizar la red Tor requiere descargar el *navegador (software),* dispuesto en su página de Internet.

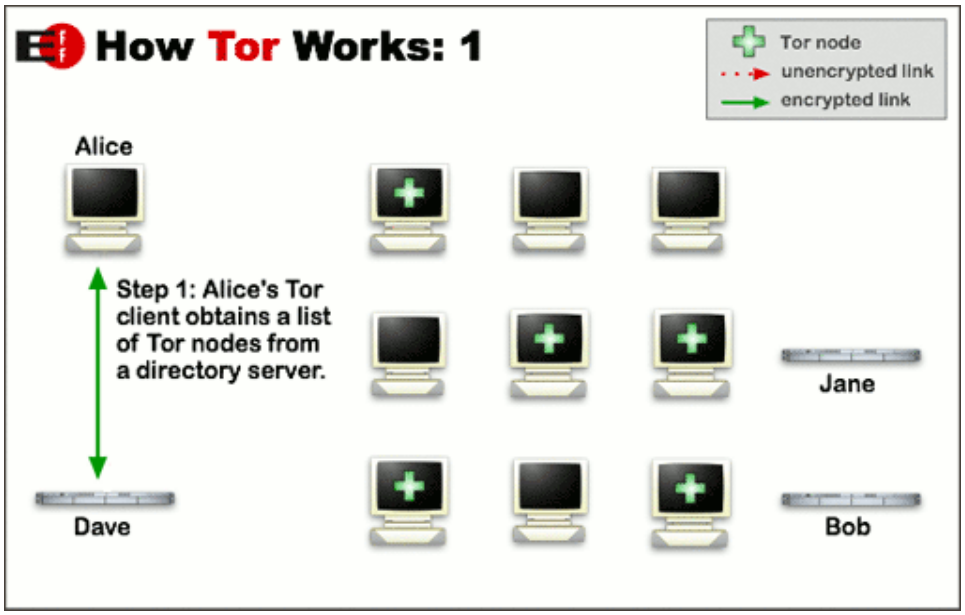

Imagen 44. Modo en que funciona Tor. (The Tor Project Inc, párrs.11–14)

En esta primera imagen, que ilustra el funcionamiento de Tor, se observa, como el navegador de Alice obtiene una lista de los nodos del directorio del servidor (aquellos marcados con una cruz).

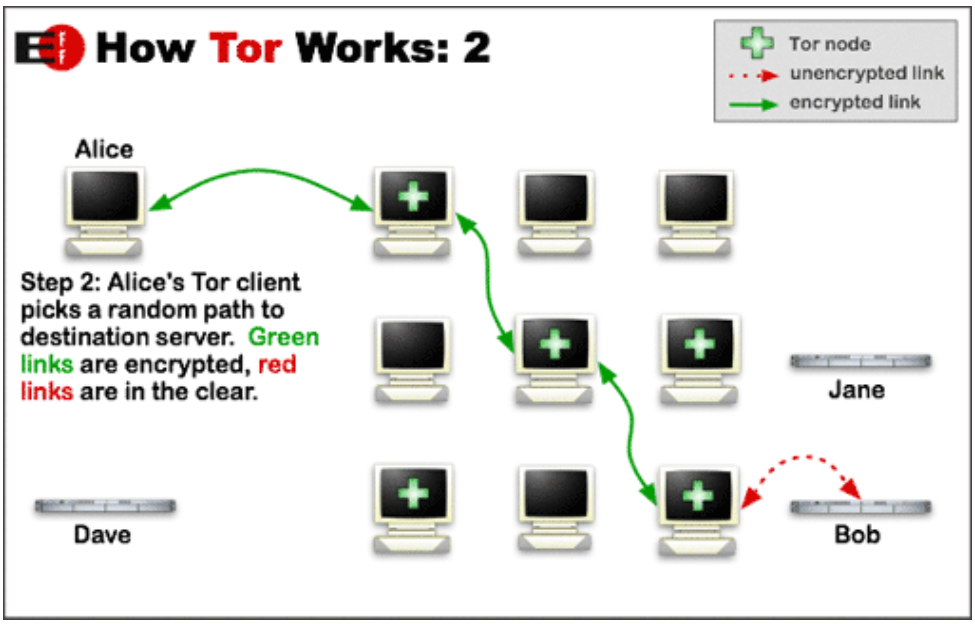

Imagen 45. Modo en que funciona Tor, segunda parte. (The Tor Project Inc, párrs.11–14)

Después, el cliente de Alice (navegador de Tor), envía la información en un patrón aleatorio a través de sus nodos, además de que encripta la información mientras pasa por ellos, hasta llegar a su destino. Donde deja de estar encriptada para poder ser leída. Las flechas verdes indican que se trata de información encriptada, las flechas rojas de información no encriptada.

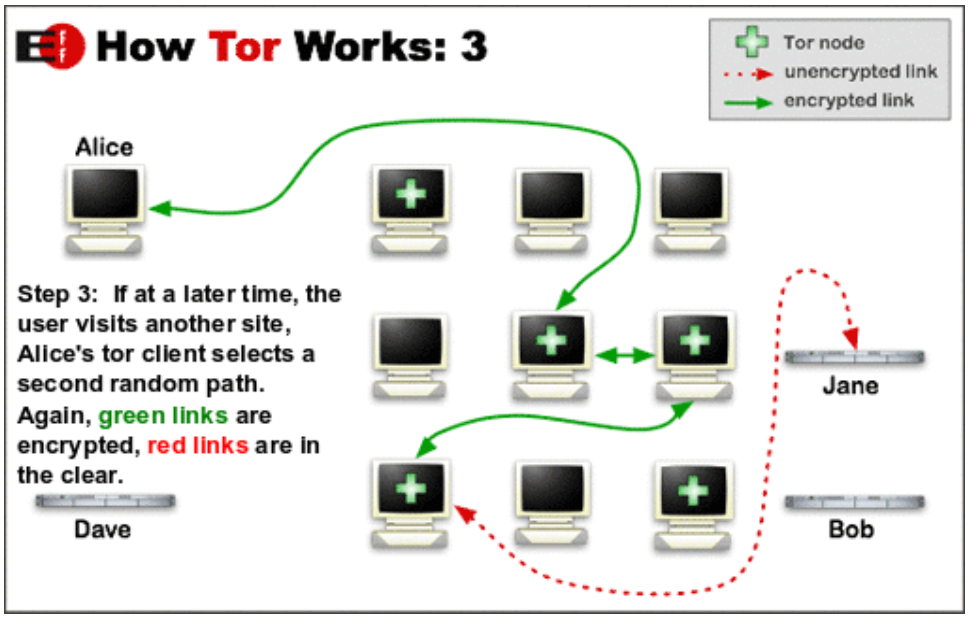

Imagen 46. Modo en que funciona Tor, tercera parte. (The Tor Project Inc, párrs.11–14)

Si tiempo después, el usuario, en este caso Alice, visita otro sitio, su navegador, elegirá otro patrón aleatorio y de igual forma encriptará la información, durante su tránsito entre nodos, para desencriptarla al llegar a su destino.

En resumen, los paquetes de datos en Tor no viajan de forma directa entre emisor y receptor, sino que se desplazan aleatoriamente por diversos nodos para complicar el rastreo de información por terceros. Así estos pueden llegar a conocer la comunicación entre un nodo y otro, pero no el principio y fin de la misma; ningún punto individual conoce la ruta completa que ha tomado un paquete de datos, es decir no puede dar certidumbre sobre el destino. Para mayor seguridad, cada comunicación entre puntos es cifrada para impedir el rastreo de las comunicaciones a medida que suceden. Finalmente, las huellas son borradas periódicamente para que no puedan ser mal utilizadas. (The Tor Project Inc, párrs.11–14)

Una precisión importante, contenida dentro del mismo sitio es que el anonimato no puede ser total al utilizarse The Onion Router, sino que se centra sólo en la protección del transporte de datos, esto implica observar, como se ha reiterado a lo largo de este documento, que información se comparte, también, considerar que los sitios a visitar pueden acceder a información que nos identifique. (The Tor Project Inc, párrs.11–15)

Tras la descarga del archivo según nuestro sistema operativo, en el apartado *downloads*, se ejecuta el fichero en cuestión. La primera ventana permite elegir el idioma deseado para ejecutar el navegador, acto seguido, nos pregunta la carpeta donde se desean ubicar los archivos y finalmente se extraen.

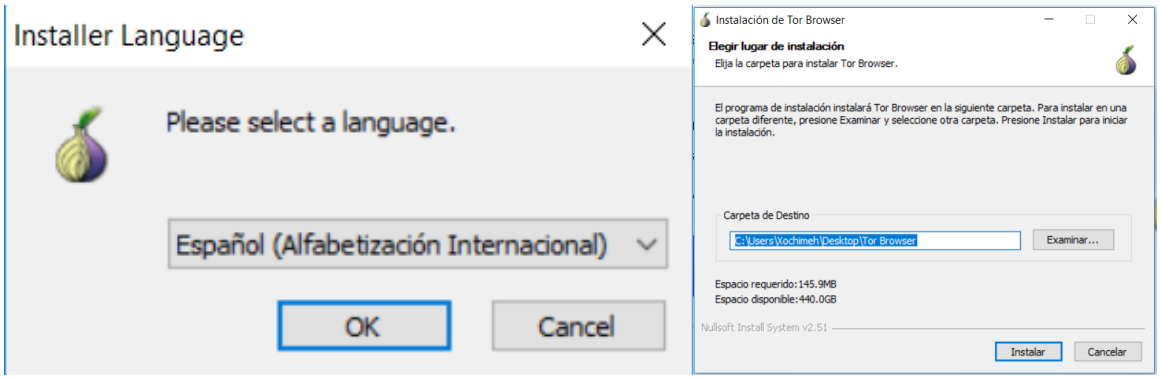

Imagen 47. Proceso de extracción de Tor, primera parte. Captura de pantalla.

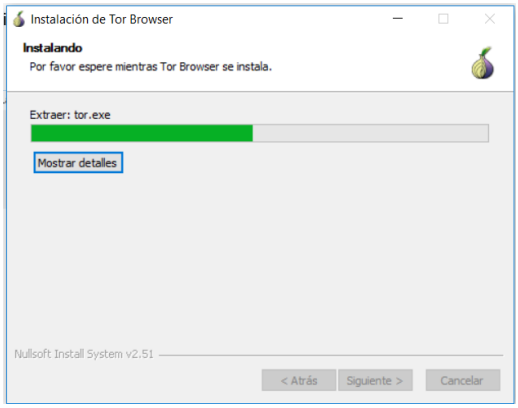

Imagen 48. Proceso de extracción de Tor, segunda parte. Captura de pantalla.

A partir de aquí inicia el proceso de configuración, que arroja dos opciones: la conexión directa a la red Tor y la posibilidad de configurar un servidor proxy. En este caso, se optó por la primera, más accessible al usuario común. Después de esto la conexión se logra.

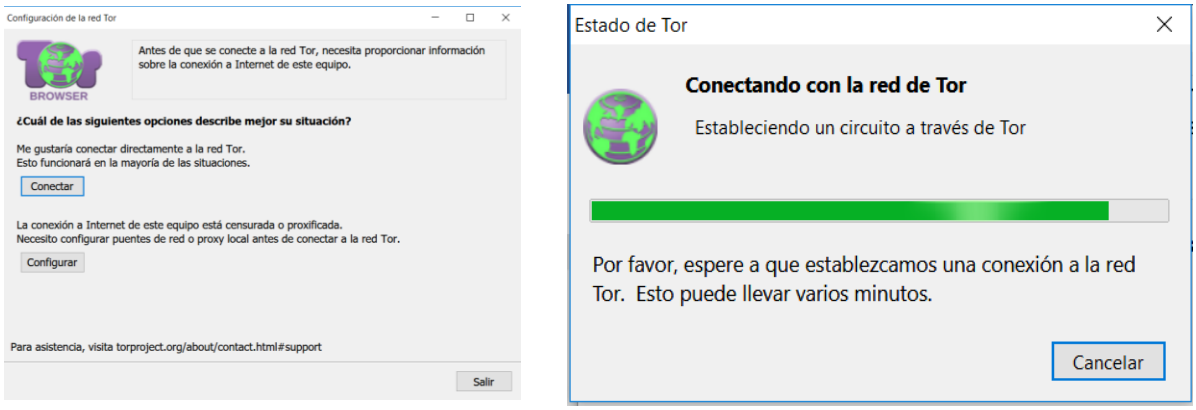

Imagen 49. Proceso de extracción de Tor, tercera parte. Captura de pantalla.

Tras lo anterior el navegador nos da la bienvenida, e incluso nos invita a colaborar como nodo de esta red anónima. Otra precisión importante es que el proceso anterior fue para descomprimir un fichero ejecutable con sus directorios. Tor podrá ser abierto desde esa ubicación.

Imagen 50. El navegador Tor. Captura de pantalla.

La navegación en Tor es diferente a la que se está acostumbrado, para ejecutar búsquedas utiliza Duck duck go, el cual ya hemos referido, pero si

se desea acceder a sitios contenidos dentro de la red anónima es necesario conocer el dominio preciso, estos son distinguibles en lo general por la terminación. onion.

Entre las ventajas del proyecto Tor se encuentran el que no persiga ánimos de lucro y que sea nutrida por una comunidad interesada en la privacidad y anonimato digital. Como desventajas, el que la navegación puede resultar lenta pues depende de los nodos y la cantidad de estos que estén en el medio de una petición. Los sitios regularmente no serán tan estéticos como en la red tradicional (responsabilidad de las páginas .onion y no de la red en sí), pero este es un aspecto menor al que es posible acostumbrarse en muy poco tiempo.

Si desea utilizarse esta red anónima en el sistema operativo Android, puede instalarse la aplicación Orbot, que enruta y cifra nuestras comunicaciones a través de Tor, junto a Orfox, que nos permite ingresar a las direcciones .onion.

Debe de tenerse extrema precaución al utilizar Tor, pues no podrá protegernos de un sitio externo a su red, accedido desde su navegador (de esto ya hemos hablado previamente), pero de igual forma hay que mantenerse exento de sitios que promuevan actividades ilegales, y lo más importante, NO COMPARTIR INFORMACIÓN PERSONAL QUE NOS IDENTIFIQUE en estos lugares. Como siempre, el criterio resulta ser la herramienta más importante para garantizar el anonimato, estas propuestas son únicamente las herramientas y serán tan funcionales como juiciosos seamos de sus posibilidades.

Tails, descargable desde https://tails.boum.org/, es una solución robusta que trabaja con Tor. Se trata de un sistema operativo portable (se puede ejecutar desde medios extraíbles) que promete proteger nuestro anonimato

y privacidad. Es un *software libre* desarrollado con Debian, una distribución de GNU/Linux.

Todas las aplicaciones en Tails están pensadas en torno a la seguridad: el navegador web, el cliente de mensajería instantánea, su aplicación para creación y edición de contenidos (*office suite*), así como sus editores de imagen y sonido, entre otros; están puestos allí por ser considerados seguros, pero su mayor virtud estriba en direccionar todas las comunicaciones a la red Tor y bloquear todo intento de conexión directa. (*Tails - About*, párrs.3–8)

La descarga de tail se lleva a cabo desde https://tails.boum.org/install/index.en.html. Al presionar el botón *let's start the journey!* (comencemos el viaje), se puede elegir desde que sistema operativo se quiere instalar Tails, entre ellas están Windows, MacOS, Debian, Ubuntu, Mint; u otras distribuciones de GNU/Linux como Red Hat, Fedora, etc. A partir de aquí se señalará la forma de descargar e instalar Tails.

Mediante sistemas operativos con estas características se protege, además del navegador, todo nuestro entorno, de posibles intrusiones o bloqueos, lo que lo convierte en una opción sensata a tomar en cuenta.

Una segunda opción de redes anónimas es I2P (Invisible Internet Project) que aparenta ser una solución similar a Tor, pero con sus notables diferencias. Entre sus virtudes se señalan la sencillez de configuración, aunque no se visualiza como una opción real de anonimato, aunque sí de la privacidad:

> I2P no intenta mejorar el anonimato de sus usuarios ocultando a sus participantes, se trata de una red orientada al mensaje donde cada paquete de datos es enrutado a su correspondiente destino

> de forma anónima. Esto quiere decir que cuando un emisor envía un mensaje, los demás participantes en la red pueden conocer la existencia de dicho usuario, pero desconocen el número, contenido y destinatarios de los mensajes que intercambia con otros participantes. (Echeverri 55–56)

Al ser prioridad de este documento el anonimato digital más allá de la privacidad, no se profundizará más en esta alternativa, pero se señala como una opción más, para aquel que quiera proteger la información que envía sin que importe su probable identificación.

II.III. XII. Redes sociales digitales

El análisis de las redes sociales digitales gira más bien en torno a su viabilidad cuando se desea alcanzar el anonimato, pues su propia naturaleza, incita a divulgar información que puede hacernos reconocibles e identificables.

Si bien casi cualquier red social puede ser restringida a un círculo muy cercano y cerrado, algunas de las partes de esa comunicación pueden vulnerar dicha privacidad. Esa información puede ser revelada eventualmente por distracción o mal resguardo de las cuentas propias, de terceros, o incluso por intrusión o mala fe.

En lo que respecta al anonimato, estas redes sociales digitales lo descartan, al obligar a todo aquel que quiera utilizarlas a registrarse. Incluso en el presente algunas solicitan ya la vinculación con otras cuentas y el número de teléfono del móvil para asegurar la identidad de las personas, sin olvidar, que parte de la información de registro queda accesible para cualquiera, como en el caso de Facebook:

> Existen ciertos datos del perfil de cualquier cuenta que son públicos, como por ejemplo el nombre, foto de perfil, sexo, las redes y páginas a las que el usuario le ha dado un "Me gusta", etc. Dicha información en algunos casos es suficiente para identificar inequívocamente a un usuario y junto con otras fuentes de información abierta, perfilar sus gustos o incluso su rutina diaria. (Echeverri 21)

Otro punto a considerar es que, si bien esas redes pueden ser restringidas para usuarios no autorizados o el público en general, no lo son para los proveedores, que perfilan usuarios para ofrecer productos y servicios que más tarde interferirán en el poder de decisión e invadirán sus espacios de navegación, sin olvidar que en algunos casos pueden ser compartidos con otras empresas para mayor análisis y refinamiento de los procesos de venta, en el mejor de los casos. El seguimiento de Facebook, por ejemplo, incluso se da fuera de su propia plataforma:

> … las *cookies* de esta red social se encuentran diseminadas por miles de sitios web en Internet. Puede haber muchas formas para que un sitio web incluya *cookies* de Facebook, sin embargo una de las más comunes es mediante los típicos botones para compartir contenidos. Facebook utiliza estos rastros de navegación para saber con exactitud las páginas visitadas, o al menos, aquellas que están a su alcance por medio de las *cookies.* (Echeverri 20)

Además, cada acción en las redes sociales digitales puede dar a conocer mucho de nosotros; las imágenes, comentarios, ubicaciones y contenidos que se replican y comparten, pueden dar idea clara de nuestras actividades, aficiones, filiaciones, credos, opiniones, estado de salud, etc.

El manual antiespías, previamente comentado, que busca proteger a periodistas y activistas, señala al respecto algunos puntos a considerar al utilizar las redes sociales digitales:

- Ponderar la posibilidad de crear cuentas separadas o perfiles distintos para las actividades personales de las profesionales.
- Al crear un perfil social vinculado con las actividades laborales, hay que evitar mezclar actividades que puedan revelar información personal sensible, estableciendo unas reglas personales sobre qué tipo de interacciones e información se va a mostrar en cada perfil. Es importante ser consciente de los problemas de privacidad y seguridad vinculados con las redes sociales. La información disponible en ellas puede revelar datos sobre el usuario o sobre personas cercanas (ej. familiares, fuentes, contactos, etc.).
- Muchos de los consejos ofrecidos en puntos anteriores son igualmente válidos para la gestión de los perfiles y cuentas en redes sociales: contraseña segura, acceso usando HTTPS, revisión y cambio de los ajustes predeterminados y las configuraciones de privacidad y ubicación, etc.
- Las políticas de privacidad de las redes sociales cambian continuamente. Vale la pena hacer un esfuerzo por actualizarse y entender los cambios de estas políticas.
- Los sitios de redes sociales son propiedad de empresas privadas que hacen negocio con los datos que sus usuarios le ceden y confían. (Toledo y Sáenz 46–47)

Los enunciados anteriores ilustran un poco de lo que previamente se señaló, y puntualizan de manera breve y clara las áreas a proteger, sin embargo,

ninguno arroja luz sobre la posibilidad del anonimato, porque pareciera, lo social y lo anónimo avanzan en sentido contrario. Pese a ello, todo usuario de las redes sociales digitales puede tomar en cuenta estas recomendaciones. Usar cuentas separadas evita que gente indeseada conozca más sobre nosotros, denunciar mediante cuentas alternas puede ayudar a proteger nuestra identidad, aunque no nos libera totalmente de los proveedores del servicio.

Además, hay que procurar evitar dejar abiertas las cuentas en ordenadores o dispositivos no personales, o incluso personales y así prevenir que ante cualquier robo o intrusión otros puedan acceder a ellos. Las contraseñas largas con número y letras que intercalen altas y bajas son una buena opción también, para evitar el robo de identidad. Tampoco hay que dejar de lado que nuestros datos alimentan a estas empresas.

A pesar de la contrariedad que puede involucrar unir los términos redes sociales digitales y anonimato, si existen opciones en ese sentido, pero siempre debe tenerse claro que no basta con proteger el nombre o la apariencia; hay que cuidar que todo lo que compartimos no revele algo de nuestra identidad que no queremos.

Diaspora* es una de esas opciones, que trabaja de modo descentralizado, lo que quiere decir que la información se distribuye en distintos nodos y no en un servidor central que almacene los datos privados, como sucede en las redes sociales digitales convencionales pertenecientes a corporaciones. (Diaspora*, párrs.1–9)

Bajo la idea de alcanzar el anonimato digital, Diaspora* tiene a favor que no precisa datos reales de registro para acceder a ella y que es libre de utilización o modificación. En cuanto a la privacidad, no utiliza la información

para cualquier otro fin que no sea el de comunicar, lo que nos exenta de publicidad en la plataforma. (Diaspora*, “El Proyecto”, párrs.1–10)

Al registrar la cuenta uno decide en que *pod* (nodo), desea estar; esto no representa problema alguno para las conexiones entre ellos, porque todos convergen en la misma red social (diaspora*, “JoinDiaspora*”, párrs.4–6):

> La palabra "diaspora" se refiere al dispersamiento de semillas (o personas) sobre un área amplia. Es por ello que nuestro motivo es el diente de león, y el asterisco en nuestro nombre representa una esponjosa semilla de diente de león. En diaspora* nos referimos a las cuentas individuales como “semillas", y los servidores dónde están almacenadas como “vainas (pods)". ¡Te acostumbrarás pronto! (diaspora*, “Registrarse en diaspora*”, párr.4)

Diaspora* depende de sus miembros que alojan y corren *pods*, por lo que invita regularmente a su comunidad a configurar un nodo en su servidor para que la comunidad se sostenga y crezca. (Diaspora*, “El Proyecto Diaspora*", párr.3)

Un motivador más es el que puedan vincularse algunas redes sociales digitales a Diaspora*, aunque esto probablemente no sea lo más recomendable si consideramos las descripciones anteriores.

Para registrarse, Diaspora* solicita una cuenta de correo electrónico y promete que no será visible para otros usuarios; un nombre de usuario (no necesariamente tu nombre real) y una contraseña.

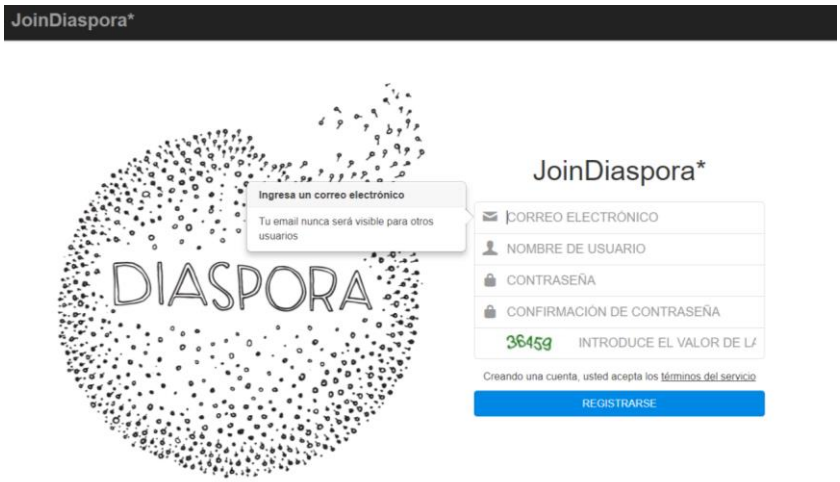

Imagen 51. Registro en Diaspora*. Captura de pantalla.

Ya una vez dentro de la interfaz del sitio tenemos varias opciones, como vincular nuestra cuenta con Facebook, Twitter, Tumblr o WordPress, lo que nos permite publicar desde Diaspora* en estos servicios; algo que pudiera funcionar parcialmente para proteger la privacidad si se discrimina el contenido a compartir entre los distintos servicios, pero no para el anonimato, porque estas redes solicitan nuestras identidades reales para acceder a dichos servicios y cualquiera que busque nuestro nombre de usuario puede visualizarlo y con ello hacer conjeturas.

La apariencia es similar a Facebook, permite elegir si lo que se publica será accesible para el público general, familiares, amigos o conocidos e invitar a contactos a enlazarse contigo. Se pueden compartir desde allí vínculos, imágenes y videos como en redes sociales digitales similares. Por último, permite enviar y recibir mensajes privados; además nos da notificaciones de actividad.

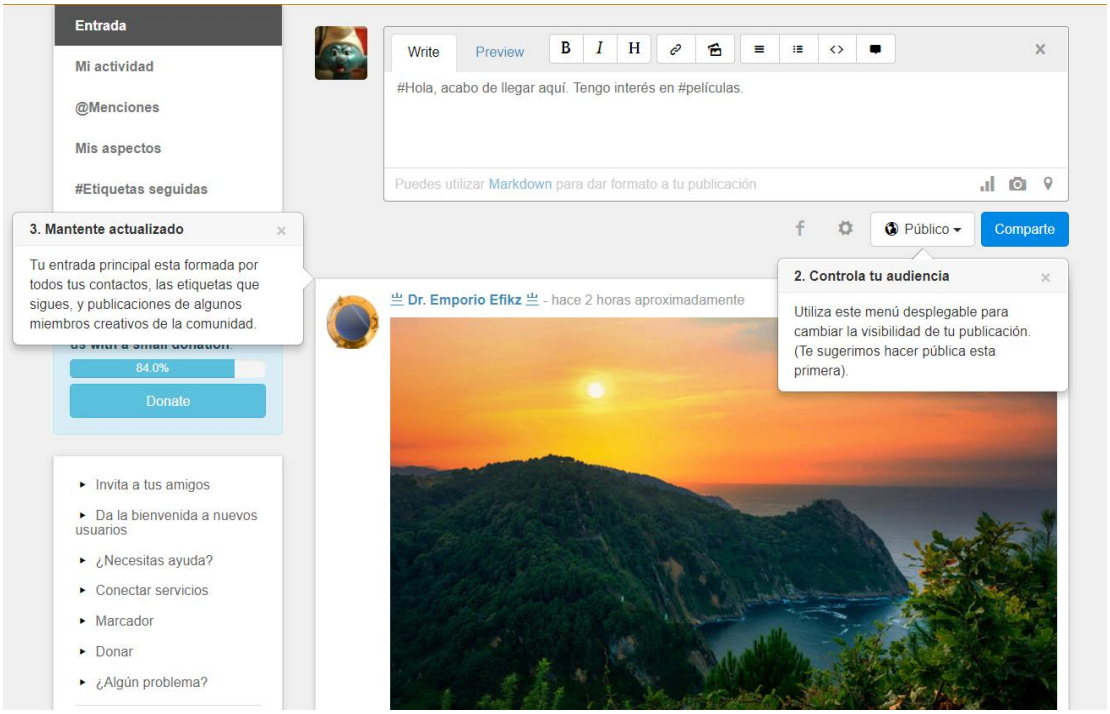

Imagen 52. Interfaz de Diaspora*. Captura de pantalla.

Tras un breve análisis puede decirse que esta red es más eficaz para lograr el anonimato, si no se vincula con otras redes sociales digitales con fines comerciales, toda vez que los contactos aún conocidos pueden mantenerse aquí sin residir en un solo servidor; y sin análisis de nuestra información para perfiles con metas de promoción o venta, también, si se desea, es posible interactuar con otros siempre que nuestra información no dé indicios de nuestra identidad e intereses, esto incluye no proporcionar nuestros datos reales en el registro.

Diaspora* es accesible desde cualquier dispositivo mediante su página web, que tiene versión de escritorio y para móvil.

Estos servicios viven del apoyo de la comunidad y las donaciones, lo que hay que tomar en cuenta si se desea contribuir a su permanencia.

II.III. XIII. Antivirus, *antispyware* y cortafuegos

Si bien, el interés de este documento se centra en el anonimato al navegar en Internet y al usar las redes sociales digitales, en todo caso, es oportuno tomar en cuenta otras necesidades, porque las amenazas pueden tener origen en sitios web, correos electrónicos, publicaciones de redes sociales digitales, aplicaciones o archivos descargables fraudulentos; e incluso en lo local, provenir de medios extraíbles o ficheros transmitidos internamente.

El *software* malicioso, en el presente, busca pasar desapercibido, a diferencia de hace algunos años. Ya no le interesa, en la mayoría de los casos, destruir lo que hay en un ordenador, sino extraer información o instalarse como parásito para que nuestro equipo realice otras actividades, sin que nos demos cuenta, haciéndose de los recursos operativos de la máquina.

Por ello es imperativo; no sólo para lograr el anonimato, sino también la privacidad digital, hacerse de un buen antivirus, *antispyware* y cortafuegos (*firewall*).

A continuación, se hace un desglose para distinguir a detalle las diferencias entre cada concepto:

Antivirus	… es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al Sistema. (Alsina párrs.1–2)
Antispyware	… ayuda a reducir los efectos causados por el *spyware* incluyendo el lento desempeño del equipo, ventanas de mensajes emergentes, cambios no deseados en configuraciones de Internet y uso no autorizado de la información privada. Permite a los usuarios protegerse contra los programas cuya intención es rastrear la información sobre hábitos de consumo y navegación, o peor aún, obtener contraseñas y otros datos sensibles. (Valdés Rodríguez, párr.1)
Firewall	El *firewall* es un dispositivo […] diseñado para impedir de plano el acceso que no se encuentre autorizado y como contrapartida sí permite sin inconvenientes comunicaciones que están autorizadas. (Ucha, párrs.1–2)

Tabla 15. Antivirus, *antispyware* y *firewall*. Elaboración propia.

El antivirus entonces nos protege de cualquier archivo que pueda alterar el funcionamiento de nuestro dispositivo, el *antispyware*, del espionaje o uso secundario no autorizado y el *firewall* o cortafuegos, del acceso a nuestra red por servicios no autorizados.

Una contaminación por *software* malicioso o virus puede suceder mediante un medio extraíble, pero también por la descarga de algún archivo o aplicación aparentemente inofensiva (desde un sitio web, red social o correo electrónico). La lectura de nuestro quehacer en la red también puede suceder cuando algún servicio fuera de nuestra red local se conecta a nuestro dispositivo (como cuando accedemos a terminales de videojuegos para competir con otros usuarios por Internet), es por eso que en el caso

de los cortafuegos sólo debe darse permiso a quiénes se les tenga absoluta confianza.

En el presente algunos servicios de antivirus incluyen *antispyware* y cortafuegos. En la mayoría de estos casos estos servicios serán de pago, aunque cuenten con versiones gratuitas con protección más ligera o poco integral; hay que considerar que estas empresas invierten en investigación para poder mantenerse al día, lo que se traduce en mayor seguridad para los usuarios. Otra opción para aquellos que no deseen desembolsar dinero es usar servicios distintos que cubran cada una de estas áreas.

Bajo la lógica de que hay múltiples ofertas en el mercado, todas similares en su relación costo beneficio, se ha optado aquí por enumerar algunas de las opciones descritas en el sitio https://securityinabox.org, surgido del esfuerzo de la organización Front Line Defenders, nacida para proteger a los defensores de los derechos humanos.

En este mismo sitio existen recomendaciones para otros sistemas operativos, como son Android y GNU/Linux, para todo aquel interesado que desee profundizar en estos temas.

La primera recomendación es Avast, en su versión gratuita, que menciona en su sitio web puede proteger dispositivos de virus, *Malware* (término que engloba todo programa o código informático malicioso) e intrusos en la red.

La instalación de Avast es relativamente sencilla, primero hay que acceder a su sitio https://www.avast.com/, ubicar el área de descarga de la versión gratuita y ejecutar el archivo; después de aceptar los términos y condiciones del servicio, simplemente hay que seguir las instrucciones para que el antivirus quede correctamente instalado y configurado.

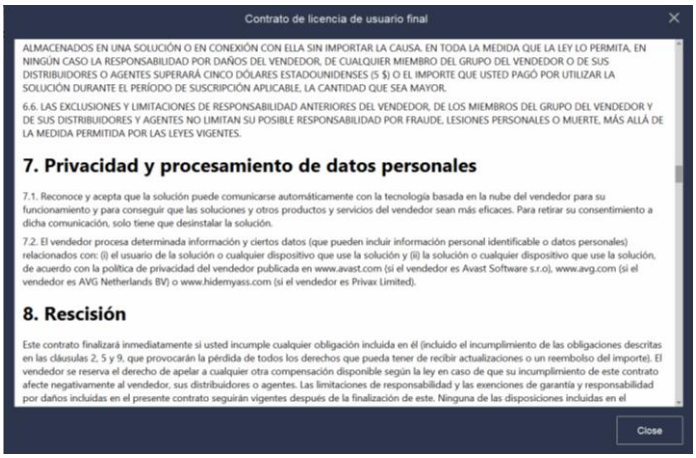

Imagen 53. Acuerdo de privacidad de Avast. Captura de pantalla.

Avast, lamentablemente, como será una constante en estos servicios, dará lectura a nuestra información; en este caso precisa datos personales y de los dispositivos vinculados al mismo. Pese a ello promete respetar nuestra privacidad y jamás compartir nuestra información con terceros.

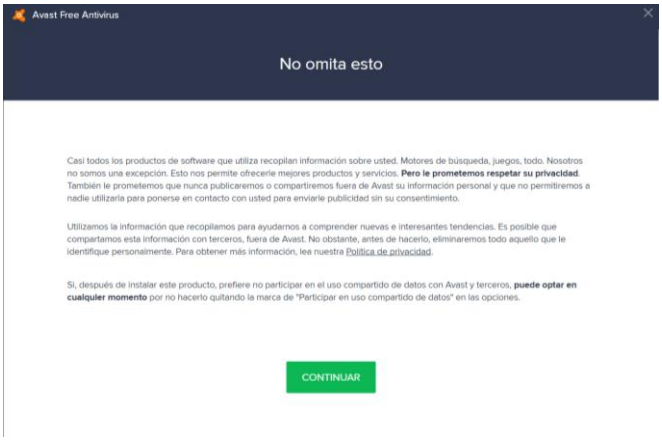

Imagen 54. Aviso sobre privacidad de Avast. Captura de pantalla.

La versión gratuita de Avast incluye la posibilidad de analizar la vulnerabilidad de nuestra propia red, algo que como sabemos es indispensable para protegernos de posibles ataques. También nos permite administrar contraseñas y configurar un VPN o Red Privada Virtual. Para acceder a su servicio de cortafuegos es necesario contratar un plan. Avast

también tiene una versión gratuita para dispositivos móviles y es compatible con dispositivos MacOS y Android.

Spybot es otra recomendación de https://securityinabox.org, para protegernos, en este caso, del posible espionaje, aunque su versión de paga también funciona como antivirus. Se trata de una aplicación gratuita y actualizable; uno de los aspectos más importantes al decidirnos por alguno de estos servicios, que en su versión gratuita nos protege del *Malware* y *Spyware*. Spybot es obtenible desde https://www.safer-networking.org/.

Una vez descargado y ejecutado el archivo, debe elegirse el idioma (no hay opción en español), y el tipo de instalación deseada (para uso personal, empresarial, de pago, donación o evaluación).

Un punto importante es que dentro de la licencia de uso Spybot se asegura no explorar el sistema del Licenciatario, ni buscar específicamente ninguna información de identificación personal.

Una vez finalizada la instalación es posible escanear el sistema en busca de *Malware* y *Spyware*, eliminar archivos temporales para evitar que terceros hagan mal uso de ellos, deshabilitar *cookies* para que no puedan rastrear nuestras acciones y actualizar la base de datos para estar siempre al día frente a posibles amenazas.

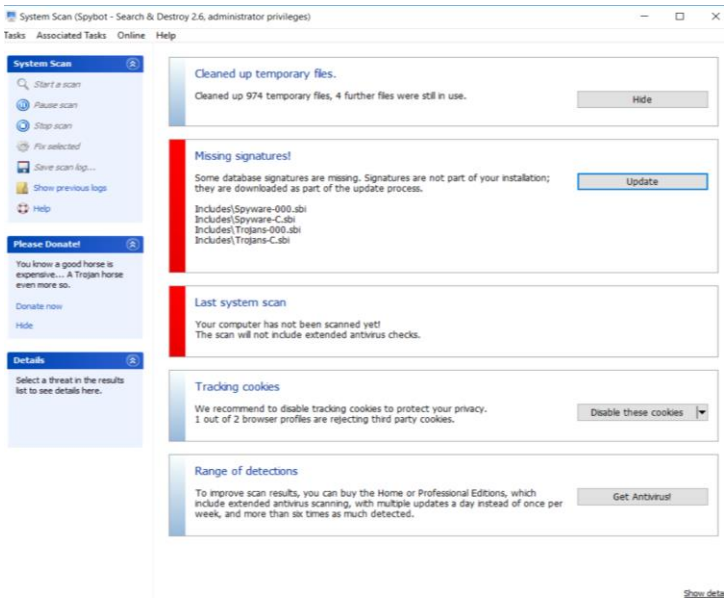

Imagen 55. Apariencia y opciones de Spybot. Captura de pantalla.

La tercera recomendación, en este caso un cortafuegos, es Comodo Firewall, que como las dos opciones anteriores incluye una versión gratuita descargable desde https://personalfirewall.comodo.com/.

El primer punto, posterior a la instalación es seleccionar el idioma, que en este caso es el español, para después leer las condiciones del servicio y el acuerdo de privacidad, que señala no recopilar información sin consentimiento del usuario y esta es sólo referente a las suscripciones deseadas por el mismo y los servicios que involucran (Comodo, "Policies" párr.2):

> La descarga de un producto a menudo requiere la introducción de información personal. Esta información será utilizada por Comodo o sus afiliados para contactar al cliente acerca de los productos y servicios de Comodo, incluyendo actualizaciones de productos y material promocional asociado. Esta información también puede usarse como información demográfica general recopilada para

mejorar los productos y servicios de Comodo. (Comodo, "Policies", párr.3)

Tras aceptar el acuerdo de privacidad y las condiciones del servicio, dicho *software* nos pregunta si queremos utilizar Yahoo como navegador predeterminado, es decir que todas nuestras búsquedas se hagan desde allí y que se vuelva nuestra página de inicio, algo no recomendable si tomamos en cuenta lo expuesto en el apartado de *cookies* y buscadores.

Después nos da a elegir entre las DNS (sistema de nombres de dominio o *Domain Name System)* de Comodo y las preconfiguradas en nuestro equipo, en el caso de utilizar las primeras, la empresa garantiza mayor seguridad y rapidez de navegación. Puede entenderse sencillamente, que, si navegamos desde las DNS de Comodo, lo haremos desde su dirección. Los siguientes dos puntos, que monitorizan el desempeño en la nube y enviar datos de uso, también (como el primero) pueden desmarcarse.

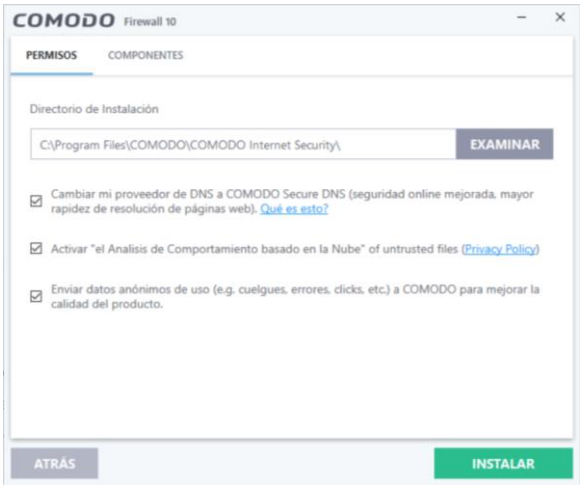

Imagen 56. Opciones de instalación (permisos) de Comodo. Captura de pantalla.

En la pestaña componentes, pueden deshabilitarse también las opciones que da Comodo de manera predeterminada, si no se van a utilizar.

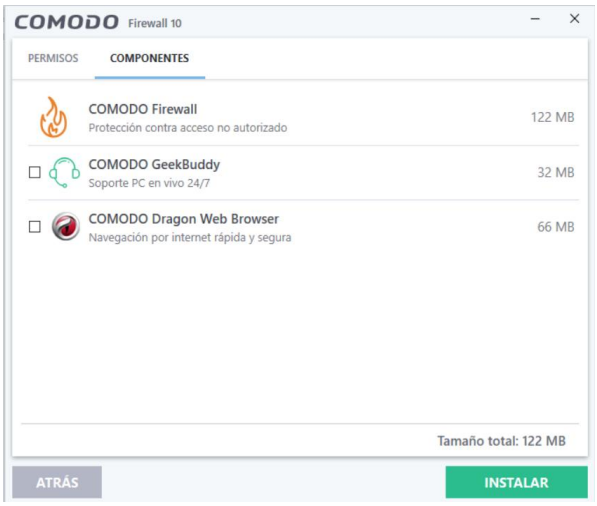

Imagen 57. Opciones de instalación (componentes) de Comodo. Captura de pantalla.

Concluida la instalación, Comodo permitirá administrar redes para impedir el acceso a aquellas que no conozcamos o presumamos inseguras; bloquear y desbloquear aplicaciones; actualizar el *software;* y una cuarta muy interesante, ejecutar aplicaciones virtualmente, lo que nos ayudará a protegernos de instalaciones maliciosas en el sistema, al poder probarlas previamente.

Imagen 58. Apariencia de Comodo Firewall. Captura de pantalla.

Dentro del sitio que hace estas recomendaciones hay otras más respecto del uso correcto de Internet en aras de la privacidad y el anonimato, allí pueden encontrarse guías detalladas de instalación de lo aquí expuesto y de otras opciones más, pensadas para sistemas operativos Windows, MacOs, GNU/Linux y Android, además de otras ejecutables desde la Web.

El usuario puede sentirse libre de buscar otras opciones siempre que se considere necesario, pero se recomienda tomar las previsiones aquí expuestas y otras más que complementen nuestro ejercicio en Internet y redes sociales digitales, como las propuestas dentro del manual Antiespías, elaborado por la Fundación para la Libertad de Prensa (FLIP), que se presentan a continuación:

- Evitar abrir archivos o enlaces enviados por correo electrónico de remitentes desconocidos.
- Revisar el contenido de un archivo adjunto sospechoso con un *software* antivirus y usar el sentido común: los archivos que dicen contener las últimas imágenes de algún famoso o incluso las fotos de supuestas infidelidades de personas cercanas o los anuncios de algún premio son trampas para descargar *software* malicioso o para conocer los datos personales.
- Si para acceder al contenido pide que se registren o ingresen los datos de usuario y contraseña en algún servicio o en una red social, se debe revisar cuidadosamente que no se trate de un sitio falso.
- Instalar y utilizar *software* antivirus y actualizarlo con frecuencia. Estos tendrán la capacidad de detectar casi todo

software malicioso, salvo que se esté ante un ataque dirigido y altamente sofisticado.

- Acudir a expertos informáticos para limpiar los dispositivos de cualquier *software* malicioso. Es necesario crear copias de respaldo antes de iniciar este proceso y asegurarse que la copia no albergue también el *malware.* (Toledo y Sáenz 49)

Y algunas otras más contenidas dentro del mismo sitio https://securityinabox.org, que apuntan la importancia de:

- Proteger su dispositivo contra Malware y piratas informáticos
- Proteger su información de las amenazas físicas
- Crear y mantener contraseñas seguras
- Proteger los archivos confidenciales de su computadora
- Recuperar la pérdida de información
- Destruir información sensible
- Mantener su comunicación en línea privada
- Permanecer anónimo y evitar la censura en Internet
- Protegerse y proteger sus datos cuando utilice sitios de redes sociales
- Utilizar los teléfonos móviles de la forma más segura posible
- Utilizar los teléfonos inteligentes con la mayor seguridad posible (Collective, párrs.1–11)

Si bien todo lo anterior no se asume como la única solución o respuesta a la falta de privacidad digital, se ha expuesto aquí por ser la recomendación de expertos en el área informática, defensores de derechos humanos y periodistas, lo que les hace dignos de ser considerados al menos como un

punto de partida, para saber de las posibilidades que estas herramientas ofrecen y de cómo operan las empresas vinculadas a la Web e Internet mismo.

Si bien es complicado hallar opciones *libres* disponibles para cada uno de los sistemas operativos y dispositivos, la mayoría de los ejemplos (en cuyo caso se ha señalado), son al menos compatibles con Windows, GNU/Linux y algún sistema operativo para dispositivos móviles, lo que debe entenderse como una invitación a incorporar estas medidas en cada uno de los medios de acceso posibles, porque cualquiera puede ser la puerta de entrada a un agente externo indeseado.

Otra consideración derivada del análisis de estas herramientas, es que siempre que sea posible debe privilegiarse el uso de aquellas desarrolladas libremente, que incluso estén respaldadas por organizaciones con renombre, toda vez que, en primer lugar, no persiguen ánimos de lucro en la mayoría de los casos, y en segundo, al ser de código abierto o *software* libre, permiten que cualquiera pueda saber si hay programación mal intencionada en su configuración. Tampoco hay que olvidar, que todas las opciones de pago enunciadas utilizan al menos alguna parte de nuestra información, lo que puede comprometer parcial o totalmente nuestra privacidad y anonimato digital.

En ese tenor, se reitera, es posible explorar también distribuciones de GNU/Linux, muchas de ellas comprendidas dentro del *software* libre *(que por elección manifiesta de su autor, puede ser copiado, estudiado, modificado, utilizado libremente con cualquier fin y redistribuido con o sin cambios o mejoras)* (Cortes Ospina, párr.1), que además de liberarnos de los sistemas operativos de pago; que rastrean el comportamiento de los usuarios y tienden a hacer dependientes a los usuarios de sus programas,

permiten la mejora, modificación y vigilancia de su comunidad, para evitar cualquier uso indebido.

No hay que olvidar que los impulsores del software libre, lo son también de la privacidad digital. Richard Stallman, fundador y representante de la Free Software Fundation, que apela a la democratización de la tecnología y la participación general de la comunidad para la generación de un crecimiento igualitario de Internet, ha cuestionado precisamente, que la aceptación acrítica de todo avance tecnológico; en este caso programas informáticos, aplicaciones y servicios de Internet, con meros intereses comerciales, contribuye a la creación de una sociedad hiper-vigilada. (De Rivera, párrs.1–3)

Finalmente, se establece que, sí es posible lograr el anonimato digital, pero no de una manera infalible y total, porque influye el factor humano del usuario que puede distraerse o actuar irresponsablemente o de mala fe. Porque ninguna de las opciones es plenamente invulnerable, sobre todo si se dieran ataques más sofisticados. Tampoco lo es, porque implica un esfuerzo por abandonar ciertas prácticas asociadas con Internet, que tienen todo que ver con la exposición del individuo y la interacción social.

II.III. XIV. Taxonomía de Solove y anonimato digital

A continuación, se hace un desglose de las herramientas señaladas y la problemática o riesgo que pueden resolver. Sin embargo, debe hacerse énfasis en que el criterio del usuario respecto de su interacción en Internet es la medida de seguridad más importante para alcanzar el anonimato digital.

Se consideran para ello dos puntos clave de la Taxonomía de Solove, comentados en el capítulo uno. Estos son el de la recopilación de

información en la que se da pie a la vigilancia y la interrogación, además del procesamiento de la información, que involucra la agregación, identificación, inseguridad, uso secundario y exclusión. Se deja de lado, la diseminación de la información, porque se considera un momento tardío para protegerse a cabalidad, aunque no deja de ser valioso para prevenir mayores daños, momentos en los que aún son importantes las herramientas previamente descritas.

Los servidores proxy, las redes privadas virtuales y las redes anónimas, resultan idóneas para evitar la recopilación de información porque ocultan de la vista de terceros ese tráfico de la red y porque la hacen accesible sólo a los puntos iniciales y finales, que se asumen son dignos de confianza según la evaluación de cada usuario.

Además, aun cuando cualquiera pudiera obtener un fragmento de esa información; salvo que sea por si misma sensible y personal, difícilmente podría relacionarla con alguna identidad en específico. Aquí se recomendaría no utilizar un solo canal, sino varios, según las circunstancias y gravedad ameriten, para transmitir información.

Al no existir datos que procesar se imposibilita la identificación; la inseguridad derivada de la obtención de nuestra identidad e información; el uso secundario por empresas; y la exclusión, cuando se trata de acceder a ciertos servicios o expresar opiniones.

Justo para lo anterior resultan útiles también los buscadores y complementos para navegadores comentados, pues ellos nos permiten acceder simplemente a la red para buscar información sin que nada de lo que hagamos o veamos se vuelva visible, almacenable e identificable.

Al seguir de entrada estas recomendaciones se resolvería el tercer punto, que habla de la diseminación de información, que involucra el quebrantamiento de la confidencialidad, la divulgación, exposición, accesibilidad incrementada, chantaje, apropiación y distorsión. En este momento se vuelve valiosa la recomendación sobre evitar el uso, en la medida de lo posible, de redes sociales digitales u optar por aquellas descentralizadas, para que nadie pueda apropiarse de los contenidos que compartimos, ni triangular información para identificarnos.

Por último, si se suman los buscadores, complementos para navegadores, redes sociales digitales descentralizadas y el uso crítico de nuestra información en la red, podemos evitar la invasión de nuestros espacios mediante la publicidad que aparece en correos, redes sociales digitales, navegadores y sitios web, además de la interferencia en las decisiones que provoca la perfilación de usuarios.

Pese a ello, para que la protección sea completa se requiere de antivirus, *antispywares* y *firewalls,* que nos ayuden de principio a fin a protegernos dentro y fuera de Internet. Hay que recordar que los riesgos están presentes incluso en lo local y cualquier punto puede ser la entrada.

Una última consideración es sobre los sitios en los que debemos ingresar información, ya sea porque se trata de trámites ante instituciones o sitios de compra, bancos, etc. Está de más decir que allí no es posible el anonimato, salvo que el pago sea en efectivo cuando se trata de compras, algo que da poca certidumbre a muchos sobre la seguridad de una transacción. Luego entonces, la única opción es mantenerse alerta sobre los sitios de riesgo, evitar dar datos reales en los sitios que no lo ameriten, luchar por un sistema que realmente proteja a los usuarios de divulgación o uso indebido de su información y conocer, además de ejercer sus derechos

Arco, para que su información pueda ser eliminada, corregida o modificada según lo considere necesario.

	Momentos	Riesgos	Herramientas para combatirlos
Recopilación de la información	Vigilancia	Vigilancia gubernamental ilegal y legal	Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda
	Interrogación	Almacenamiento de información por las empresas a solicitud del gobierno	Buscadores Complementos Redes sociales digitales descentralizadas
Procesamiento de la información	Agregación	Extralimitación de empresas sobre el uso de datos personales	Buscadores Complementos Redes sociales digitales descentralizadas
	Identificación	Identificación por triangulación de información	Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda Redes sociales digitales descentralizadas

	Inseguridad	Fraude Reemplazo de la identidad Persecución Acoso	Antivirus *Antispyware* *Firewall* Buscadores Complementos Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda
	Uso secundario	Uso de datos personales para fines no autorizados, por empresas	Redes sociales digitales descentralizadas Evaluación de riesgos por parte del usuario Derechos ARCO
	Exclusión	Discriminación en Internet	Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda
Diseminación de la información	Quebrantamiento de la confidencialidad	El nulo resguardo de la información y expansión arbitraria de los límites por empresas	En este punto aún pueden resultar útiles las herramientas mencionadas, pero debe privilegiase la protección en los primeros dos momentos
	Divulgación	Información	
	Exposición	Información privada que se hace pública	
	Accesibilidad incrementada	Minería de datos	
	Chantaje	Extorsión y sextorsión	
	Apropiación	Reutilización de contenidos por las empresas	

	Distorsión	Calumnia y desinformación sobre las personas en sitios web y redes sociales digitales	
Intrusión	Invasión	*Spam*	
	Interferencia de decisiones	Publicidad invasiva	

Tabla 16. Taxonomía de Solove y Anonimato digital. Elaboración propia.

Antes de concluir, se manifiesta aquí, que no es el interés enfrentar al individuo con los esfuerzos colectivos posibles a partir de Internet, pero sí garantizar que nuestra persona, bienes físicos y morales, además de nuestra integridad, no lleguen a verse comprometidos. Cada persona puede tomar su decisión y determinar para qué quiere ser anónimo y para qué no, aunque la mayor cantidad de medidas siempre garantizará mejores resultados.

Preliminares

Aunque el interés por la extensión de temas que abarca Internet, fue centrarse en el uso de sitios web y redes sociales digitales, no se deja de lado la necesidad de ocupar aplicaciones de mensajería. En este caso se recomienda revisar lo que ofrecen Pidgin o Adium, desarrollados con *software* libre, que no muestran publicidad, cifran la comunicación entre origen, destino y viceversa, a la vez permiten gestionar distintos servicios de mensajería y contactos desde el mismo lugar. Estas opciones están disponibles para Windows, GNU/Linux (Pidgin) y MacOs (Adium).

Luego entonces, se infiere:

Que el **anonimato** es el ocultamiento de la identidad o atributos de la misma, por decisión propia y que puede tener muchos orígenes, como el

temor a represalias, la determinación de que las obras u opiniones tengan valor por sí mismas y no sean ponderadas o descalificadas por causa del autor, por ostracismo, etc., todos válidos siempre y cuando no atenten contra la ley.

Que el **anonimato digital**, es un medio para garantizar en Internet la libertad de pensamiento y expresión, para evitar compartir información personal y para protegernos de prácticas nocivas, de vigilancia, intrusión, invasión, suplantación y delitos cibernéticos.

Que el **anonimato digital** puede dividirse en **débil y fuerte**. El primero es más vulnerable pues sólo oculta el nombre, pero no aquello alrededor que puede dar también fe de una persona y su información sensible. El anonimato fuerte, al contrario, protege la identidad y todo aquel contenido que puede vulnerar a una persona en lo que respecta a intimidad y privacidad. El segundo es más difícil de lograr que el primero.

En cuanto a la pregunta principal: **¿qué medidas a considerar por el usuario pueden garantizar su privacidad digital en Internet?** Se señala que el anonimato y privacidad digital, son posibles a través de Servidores proxy anónimos y cifrados, redes privadas virtuales, redes anónimas, web profunda, redes sociales digitales descentralizadas, buscadores y complementos para navegadores, además de antivirus, *antispywares* y *firewalls*; siempre que vayan acompañados de un uso crítico del usuario, quién tiene que ser capaz de evaluar riesgos antes de llevar a cabo cualquier acción en Internet.

Debe considerarse en mayor estima el anonimato digital, pues la imposibilidad de vincular a una persona con cierta información, dificulta cada una de las prácticas señaladas en el apartado de riesgos y Taxonomía de Solove.

Puede decirse entonces, que el anonimato en Internet o digital, fuerte, al navegar en Internet y utilizar redes sociales digitales, será posible si se evita utilizar nombres reales o se adopta la utilización de seudónimos, además de no compartir información públicamente que pueda revelar por asociación nuestra identidad; si nos privamos de utilizar navegadores que se asocien a una cuenta; si se rechazan sitios que utilicen *cookies* y adoptan buscadores que no rastreen información, si se oculta o enmascára nuestra dirección IP y si prescindimos de llenar formularios en sitios web sospechosos, no seguros, pese a la promesa de que nos den algo a cambio. Si saltamos la censura o la vigilancia por medio de redes anónimas o puertas de enlace privado. Por último si evitamos a toda costa descargar archivos de desconocidos y mantenemos actualizado nuestro antivirus, *antispyware* y *firewall* para evitar posibles intrusiones.

Todo lo anterior se traduce en medidas preventivas más que reactivas, que dependen únicamente del usuario y no de los diversos actores de Internet, por lo que se puede decir que la hipótesis que versaba: bajo la figura del anonimato digital puede evitarse que empresas, gobiernos y terceros en México hagan mal uso de los datos personales de los usuarios, previniendo la pérdida de su privacidad digital; queda verificada, aunque debe actualizarse para incluir las consideraciones anteriores. Luego entonces esta versaría: **bajo la figura del anonimato digital sí puede evitarse que empresas, gobiernos y terceros en México hagan mal uso de los datos personales de los usuarios, garantizando a través de medidas preventivas realizadas por el usuario, su privacidad digital.**

Capítulo III. Desarrollo de producto audiovisual de contextualización y acercamiento a las herramientas

Luego de conocer el panorama mexicano respecto de la privacidad en lo digital, los riesgos que derivan de su pérdida, además del anonimato digital y herramientas que lo posibilitan, junto con la valoración de su pertinencia; el paso siguiente es **construir** un video, a propósito del objetivo que dice: **facilitar al usuario la proyección de su anonimato digital con un producto audiovisual que contribuya al conocimiento de estas posibilidades para su ejecución por parte de los usuarios interesados.**

Es decir, este producto audiovisual debe contextualizar al usuario común en esta materia, a la vez que haga de su conocimiento las posibles acciones a emprender para ejercer su derecho a la privacidad.

A continuación, se describe el contenido vertido en dicho producto audiovisual, los elementos que lo componen y aspectos generales de la producción que dan fe del porqué y cómo de su elaboración, así como de los medios para su difusión.

III.I Formato

Bajo la lógica de que el público al que va dirigido este producto es usuario de Internet y que dichos individuos tienen cada vez en mayor estima la brevedad, además de la predilección por productos audiovisuales de fácil lectura y comprensión, se ha optado por condensar lo aquí estudiado y ofrecer sólo lo que pueda resultarle más significativo y de mayor interés.

De tal suerte, se ha optado por desarrollar una serie de cuatro cápsulas. La primera de contextualización sobre los riesgos en México, la segunda de explicación sobre que es la privacidad y el anonimato digital, la tercera que aborda cómo funciona Internet a la vez que menciona las primeras

herramientas pro anonimato, y la cuarta, que comprende más herramientas de protección y otras recomendaciones para el cuidado de la privacidad digital.

El producto ha de ser exhibido en la siguiente dirección de Internet: https://www.youtube.com/channel/UCe6oHm5s_27X_4R1tcmbI4w y compartido en redes sociales digitales, creadas expresamente para la difusión de estas temáticas, donde se considera puede tener mayor penetración.

Pese a que se sabe que estas redes sociales digitales y plataformas de video recopilan y almacenan información, se ha decidido colocarles allí, tras considerar que son puntos de alto riesgo, donde los usuarios pueden encontrar valiosa esta información y actuar en consecuencia.

A continuación, se listan los temas considerados para la elaboración de producto:

Contextualización

- Riesgos en México
- Vigilancia
- Espionaje
- Ciberdelitos
- Empresas y uso indebido
- Usuarios
- Otras consideraciones
- Privacidad digital
- Anonimato digital
- Cómo opera Internet

Herramientas

- Buscadores
- Complementos para navegadores
- Servidores proxy anónimos y cifrados
- Circumventores
- Redes privadas virtuales
- Redes anónimas
- Redes sociales digitales
- Antivirus, *antispyware* y cortafuegos
- Otras recomendaciones

Cierre

- Vinculo al documento
- Sitios de referencia

Con este producto de contextualización e introducción, se busca que el usuario pueda comprender de manera sencilla lo que se señala, y si desea profundizar, acercarse posteriormente a este documento para conocer en mayor medida lo pertinente sobre la privacidad digital, sus riesgos, el anonimato y las herramientas que se han valorado para conseguirlo.

Después de la definición de objetivos y ejes, se ha determinado darle identidad al producto audiovisual, para lo cual se ha elegido el nombre *intus*, adverbio del latín, que, de acuerdo con la Real Academia Española de la lengua (ya mencionado en el capítulo I), significa *dentro de*, acompañado del eslogan, *navega seguro, navega libre*, con la intención de referir de mejor manera al tema que trata el video. Acto seguido nombre y eslogan se han transformado en un logotipo que simula una cerradura que refiere a lo digital, con lo que se busca ser más pregnante. El color elegido ha sido el

azul por su referencia directa a lo tecnológico, acompañado del blanco para mejor lectura. Esto aplicó para el logotipo como para los textos del contenido.

Imagen 59. Logotipo Intus, navega seguro, navega libre. Elaboración propia.

Bajo la misma lógica de la creación de identidad del producto, se han incorporado elementos animados como códigos binarios, rizomas e interfaces digitales.

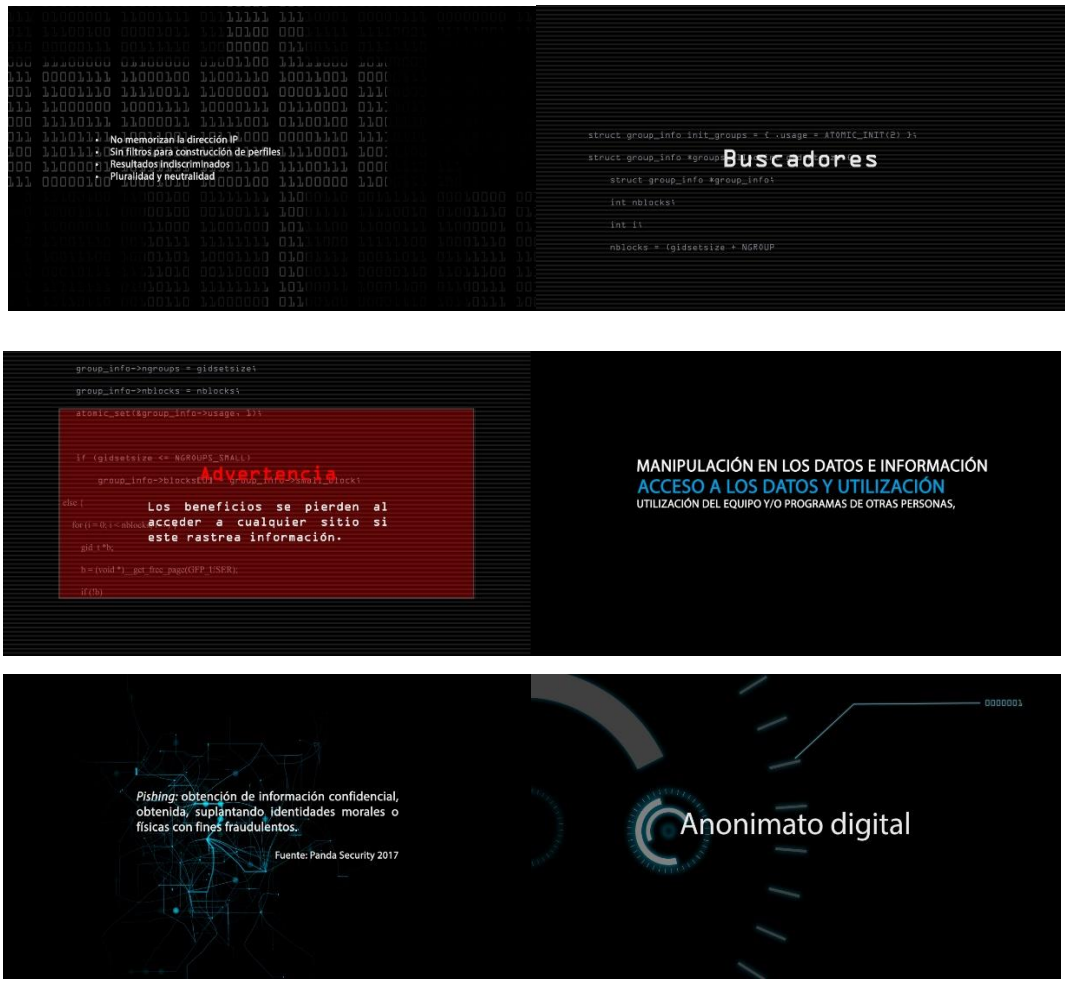

Imagen 60. Elementos gráficos de producto audiovisual. Elaboración propia.

En cuanto al video, se ha optado por utilizar material de *stock* de los sitios https://www.videvo.net/, https://coverr.co/, y https://pxhere.com/, toda vez que el contenido es de alta calidad y refiere a los temas centrales (citados debidamente en los créditos finales del producto audiovisual). En segunda instancia, el material propio ha sido grabado y elegido para mostrar aspectos puntuales que el de terceros no puede, también se han incorporado citas y fuentes de esta investigación para que la credibilidad sobre el contenido aumente. Además, con la intención de que la información sea accesible al grueso de los probables espectadores se han animado gráficos.

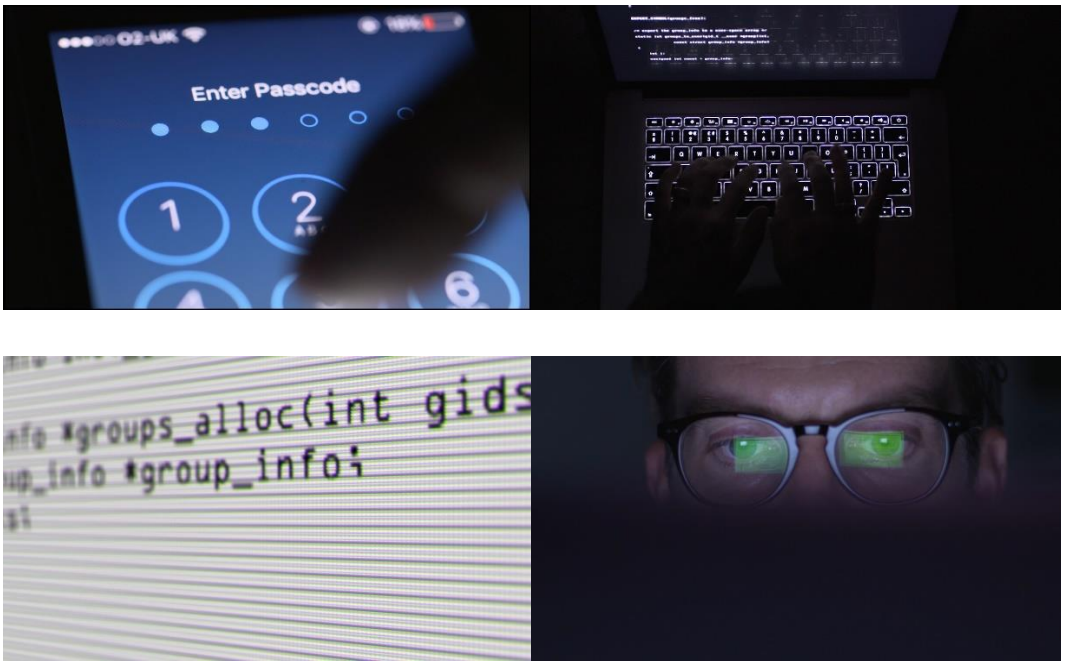

Imagen 61. Material de stock para producto audiovisual. Captura de pantalla.

El producto audiovisual utiliza la narración por medio de la voz en *off,* con la finalidad de evitar que el usuario pueda sentirse o no identificado con una persona por su edad o características, y en su lugar, se logre la sensación de platicar con alguien cercano.

A continuación, se describe de manera más concisa el contenido abordado en cada uno de los puntos señalados anteriormente.

III.II. Contenido del producto audiovisual

La pregunta ¿sabes cómo tu privacidad puede ser vulnerada en Internet? es el punto de partida para hablar de los peligros que involucra nuestra interacción en Internet:

Riesgos en México

Se consideró necesario hablar primero de los riesgos antes que, de las herramientas para lograr la privacidad, con el fin de influir en el usuario y

su probable realidad, antes que pueda sentirse lejano al pensar que sólo se habla de herramientas digitales antes que de problemáticas.

Vigilancia

En este punto se tratan los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y radiodifusión, que obligan a los proveedores de este tipo de servicios a ofrecer información sobre los usuarios a las autoridades cuando les sea solicitado y a almacenar esta hasta por 24 meses sin que exista claridad, ni rendición de cuentas sobre el procedimiento. A la par se enuncian gráficamente algunos de los datos recopilados y almacenados que pueden llegar a solicitar.

Espionaje

En el segundo rubro se habla sobre la adquisición de *software* espía por instituciones gubernamentales mexicanas sin que tengan muchas atribuciones para ello, además de mencionar los datos y comunicaciones que pueden ser intervenidas mediante este tipo de tecnología, para ese fin se consideró el apartado de vigilancia existente en el capítulo II, en el que expertos en derechos humanos como Jesús Robles Maloof analizan estas prácticas. En específico aquí se habla del *software* vendido por la empresa Hacking Team, aunque en el presente ya hay evidencia de otro tipo de servicios del mismo género contratados en el país.

Lo anterior se acompaña de un gráfico que ilustra los clientes de la empresa mencionada en territorio nacional.

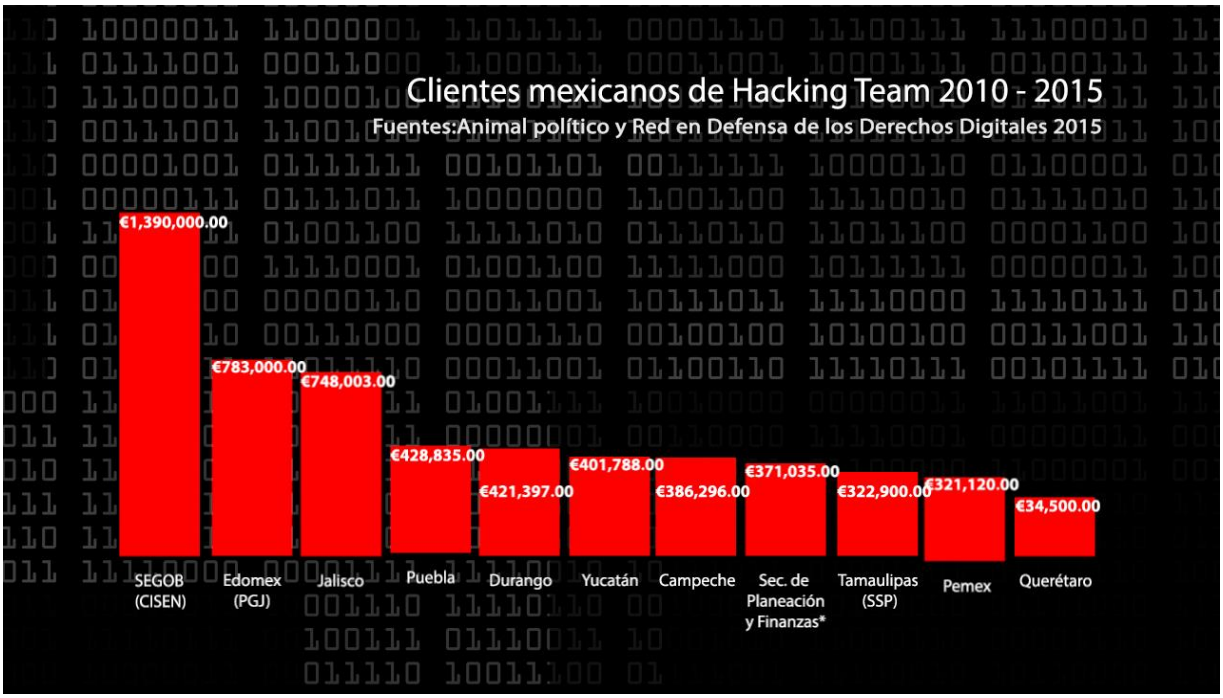

Imagen 62. Producto audiovisual: clientes mexicanos de Hacking Team 2010-2015. Elaboración propia.

Ciberdelitos

Aquí se señalan riesgos y delitos que pueden ser cometidos en nuestro agravio, como son el *phishing*, fraude, extorsión, exhibición, entre otros, mismos que la Alianza por la Seguridad en Internet México determina; a la vez que se arrojan datos estadísticos que mencionan que estas prácticas nocivas dejan cuantiosas pérdidas económicas en México, según datos de la marca Norton by Symantec.

Empresas y uso indebido

En este apartado se menciona el monto total sobre las multas entre que entre 2012 y 2016 el Instituto Nacional de Acceso a la Información y Protección de Datos Personales impuso a empresas por el mal manejo de datos personales, así como qué giros comerciales son los que más incurren en dichas faltas.

Usuarios

En el quinto punto se habla sobre como la propia interacción del usuario puede ponerlo en peligro, a la vez que se enlistan las posibles consecuencias, entre las que se encuentran el acoso, provocación y mensajes de sexo no deseado, todo con base al índice de civismo digital, documento elaborado por la empresa Microsoft.

Otras consideraciones

Es en el sexto rubro que se señala como por medio de nuestra navegación e interacción en sitios web, aplicaciones, redes sociales digitales y empresas, perfilan nuestros intereses y a partir de ello ofrecen publicidad a modo y resultados de búsqueda a medida, lo que interfiere en nuestras decisiones e invade nuestra privacidad.

Además de que toda información vertida en redes sociales digitales o aplicaciones de mensajería, eventualmente puede dejar de ser nuestra y explotada por otros.

Con lo anterior se busca evidenciar la problemática, para hablar después de la privacidad como un derecho a ejercer.

Privacidad digital

Para dar claridad al usuario aquí se define lo que es la privacidad en lo digital, según lo expuesto por la Asamblea General las Naciones Unidas, a la vez que se explica lo que son los datos personales y datos personales sensibles como parte de la privacidad digital. Ambas definiciones son retomadas del ahora llamado Instituto Nacional de Acceso a la Información y Protección de Datos Personales.

Aquí también se presume que, ante lo expuesto, difícilmente la privacidad digital está garantizada, ya que son diversos los actores que intervienen en la comunicación.

Luego entonces, es este el punto de partida para hablar del anonimato digital como probable solución.

Anonimato digital

Acto seguido se retoma la definición de anonimato digital vertida por la Electronic frontier Foundation (EFF), para después comentar algunas de sus bondades, entre las que se encuentran, el ser invisible para delincuentes, empresas y proveedores de servicios, entre otros.

Posteriormente se habla del anonimato débil y sus implicaciones poco seguras para garantizar la seguridad, y su contraparte el anonimato fuerte, que robustece nuestra privacidad digital. Aquí se retoman de igual forma las definiciones y posicionamientos de la EFF.

Cómo opera Internet

Para explicar de manera sencilla cómo funciona Internet se ha elaborado un gráfico que ilustra como todas las conexiones y comunicaciones pasan por distintos momentos y como estos pueden hacernos vulnerables.

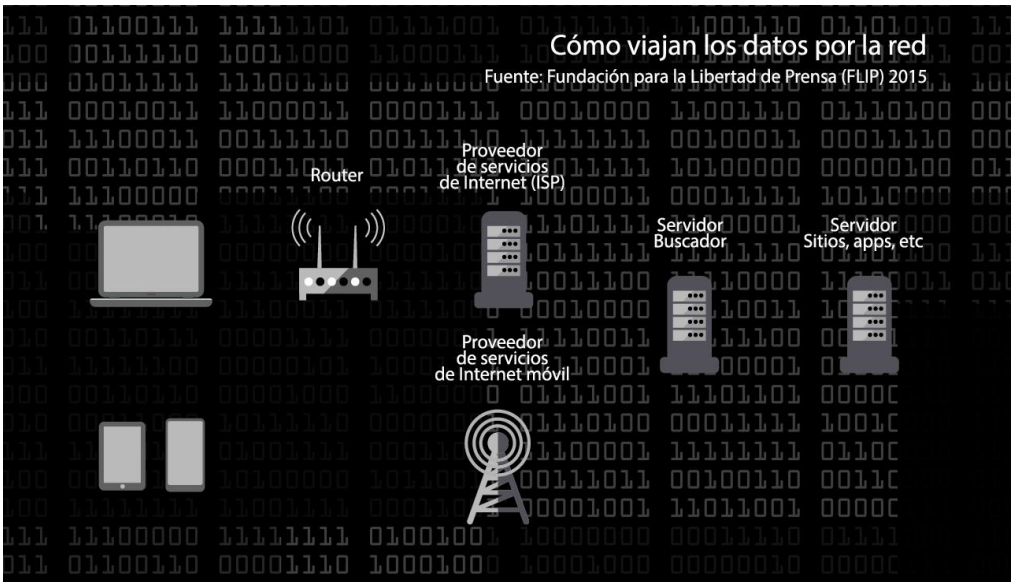

Imagen 63. Producto audiovisual: cómo viajan los datos por la red. Elaboración propia.

Por lo que se concluye, existen tres puntos importantes en los que se debe cuidar la privacidad en la comunicación digital: el origen, el tránsito y el destino.

A partir de esto momento, se deja de lado la contextualización para dar espacio a las herramientas que en un momento dado pudieran resultar útiles para alcanzar el anonimato digital y como consecuencia proteger a cabalidad nuestra privacidad.

En resumen, hasta aquí se evidenciaron peligros, se habló del derecho a la privacidad, de cómo el anonimato digital puede ayudarnos a ejercerla y de cómo opera Internet, para poder comprender más adelante de qué manera funcionan las herramientas.

Buscadores

Aquí se define lo que es una *cookie*, de que se trata el rastreo de información al navegar en Internet y que es una dirección IP, para que posterior a su conocimiento, se pueda describir de modo general cuáles son las ventajas

de los buscadores pro anonimato, entre las que se encuentran el no difundir la dirección IP, no mostrar anunciantes y no guardar información de la navegación de los usuarios. A la par de la narración se exponen visualmente algunas opciones y sus características para que el usuario pueda inferirlo, aunque la explicación de su funcionamiento y mayor análisis está contenida en este trabajo. La fuente de estos pronunciamientos es Dmitri Vitaliev, consultor de seguridad digital, ya mencionado en reiteradas ocasiones en el capítulo II.

Complementos para navegadores

En este momento se señalan aplicaciones a instalar en el navegador que evitan el rastreo de terceros y otras que nos facilitan acceder sólo a sitios seguros que utilicen el protocolo HTTPS y que además cifran la comunicación. Parte de las características son tomadas de los sitios web de estas aplicaciones e ilustrados visualmente para mayor claridad. Estas son Privacy Badger y HTTPS Everywhere.

Servidores proxy anónimos y cifrados

Previa explicación gráfica de cómo funcionan los servidores proxy y sus particularidades, se hace lo propio con los servidores proxy cifrados. También se señalan sus beneficios. Se toma como referencia para esta información el trabajo de Dmitri Vitaliev.

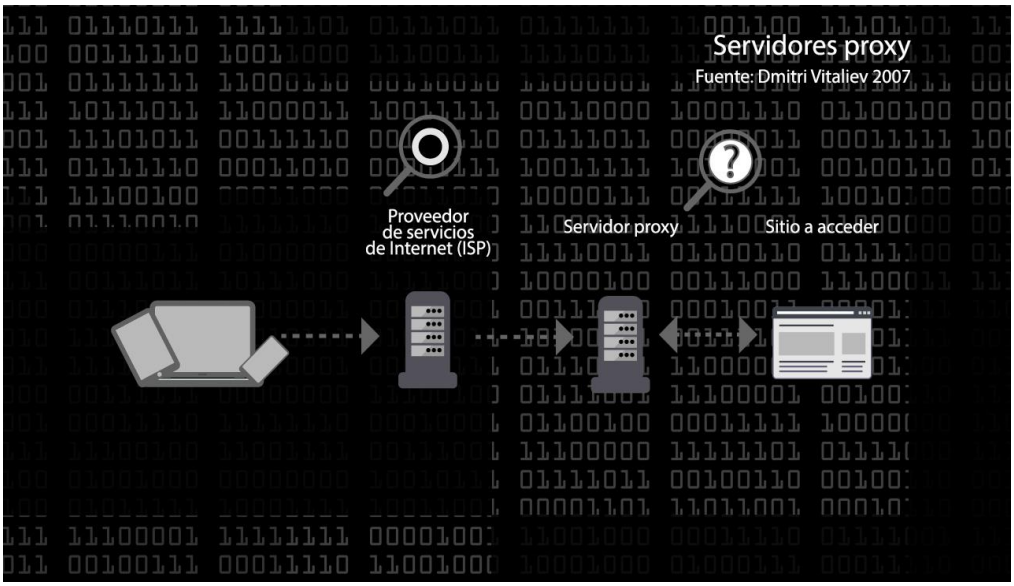

Imagen 64. Producto audiovisual: servidores proxy. Elaboración propia.

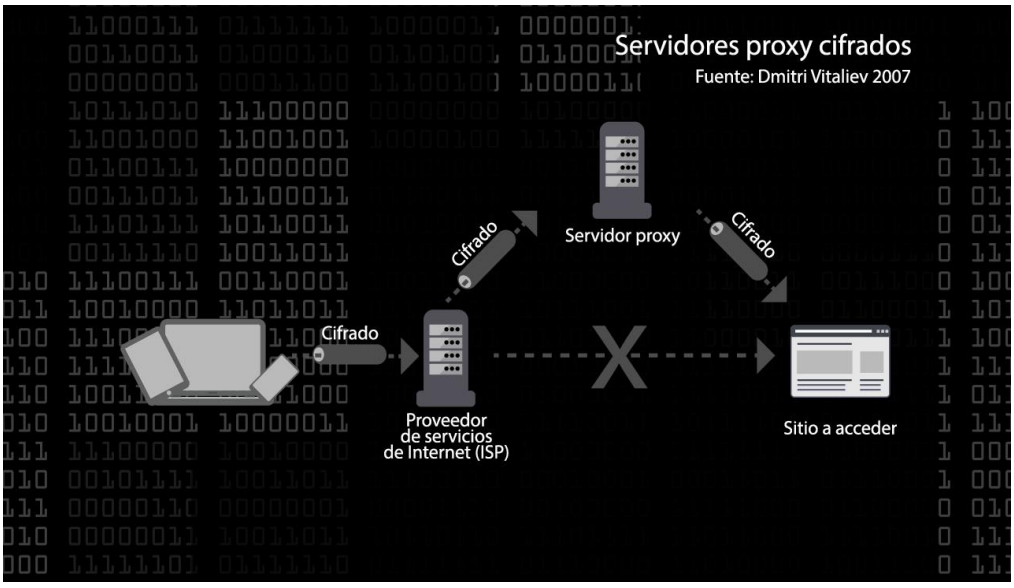

Imagen 65. Producto audiovisual: servidores proxy cifrados. Elaboración propia.

En este punto también se señala su pertinencia para evitar la censura que en ciertos lugares se da. Finalmente, se establecen advertencias sobre su utilización que versan sobre la certidumbre que debe procurarse sobre nuestra información y su utilización al evitar utilizar servidores proxy mal protegidos o fraudulentos.

Circumventores

Un circumventor es en realidad un servidor proxy, con la salvedad que este es gestionado por personas conocidas o que gozan de nuestra confianza, lo que se traduce en mayor seguridad sobre lo que se hace con nuestros datos al llegar a este punto; esto es lo que se expone en este apartado, con la ayuda de su respectivo gráfico, que no se muestra por ser muy similar al inmediato anterior. Fuente: Dmitri Vitaliev.

Redes privadas virtuales

Se explica aquí lo que son las redes privadas virtuales o VPN (Virtual Private Network): conexiones privadas entre dos puntos logradas por una red pública como Internet, así como sus ventajas entre las que se encuentran una comunicación segura conducida por un túnel dentro de la red, con el riesgo que implica respecto del rastreo de información si el proveedor de este servicio no es confiable.

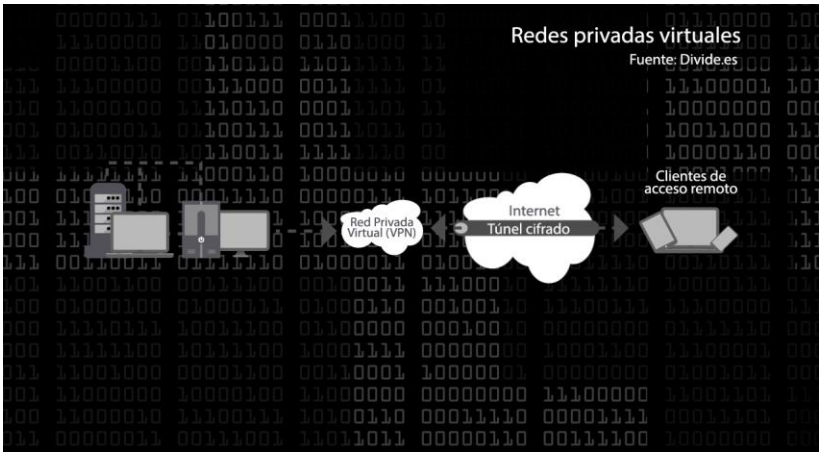

Imagen 66. Producto audiovisual: redes privadas virtuales. Elaboración propia.

Estos conceptos son retomados de lo expresado por Daniel Echeverri en su libro *Deep Web: TOR, FreeNET & I2P: privacidad y anonimato*, localizables en el apartado Redes Privadas Virtuales del capítulo II.

Redes anónimas

Se retoman aquí los pronunciamientos de Dmitri Vitaliev, se explica cómo funcionan las redes anónimas y se enumeran algunas de sus ventajas, entre las que están el ocultamiento de la dirección IP y por ende la ubicación real del usuario, además de que el rastreo de la información se complejiza al pasar por diversos nodos y descifrarse hasta el destino y viceversa la comunicación.

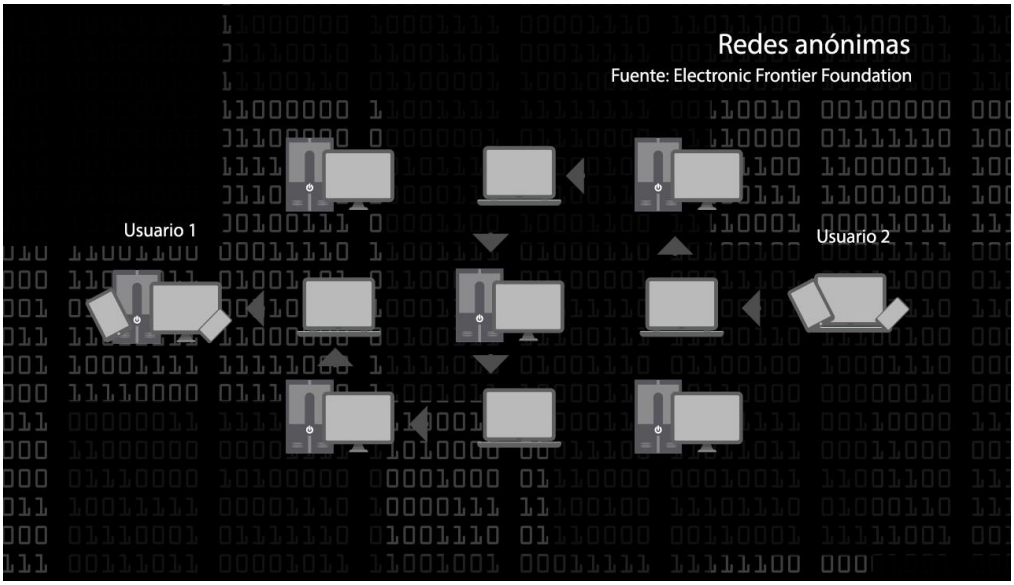

Imagen 67. Redes anónimas. Elaboración propia.

Así, se concluye en este momento su viabilidad tras considerar que cubre los momentos origen – tránsito – destino, señalados anteriormente.

Redes sociales digitales

Aquí se determinan los riesgos derivados de la utilización de las redes sociales digitales; el cómo las empresas que gestionan este tipo de servicios no son pro anonimato; y que la perfilación de los usuarios que sucede a su utilización puede darse incluso fuera de su propia plataforma.

A la par se exponen algunas recomendaciones que versan sobre el establecimiento de contraseñas seguras, crear cuentas distintas según el ámbito social a desenvolverse y evitar compartir información comprometedora, todas elaboradas por la Fundación para la Libertad de Prensa (FLIP).

Por último, se señala que sí existen redes sociales digitales pro anonimato, pero que siempre debe vigilarse y validarse su confiabilidad.

Antivirus, *antispyware* y cortafuegos

Olvidar el entorno de Internet, sin cubrir lo local, representa riesgos, por ello, aquí se define lo que son antivirus, *antispyware* y cortafuegos, para que pueda distinguirse su diferencia y viabilidad. De igual forma se habla de la posibilidad de adquirir un solo producto que involucre los tres beneficios o en su defecto probar con servicios parciales distintos y gratuitos para cubrir las tres áreas.

Otras recomendaciones

Finalmente se hacen algunas recomendaciones vertidas en el sitio https://securityinabox.org, reconocido por impulsar toda clase de herramientas pro privacidad y anonimato digital, que involucran tomar precauciones en lo local y global; entre las recomendaciones aquí encontradas se encuentran: evitar abrir archivos o enlaces enviados por correo electrónico de remitentes desconocidos, revisar el contenido de un archivo adjunto sospechoso con un *software* antivirus y usar el sentido común, destruir información sensible y proveer mecanismos de seguridad también a los dispositivos móviles.

Cierre

El objetivo de este último punto es señalar que el anonimato es posible, aunque no infalible y que involucra no sólo nuestro quehacer en Internet, sino que también obliga a tomar medidas localmente.

Mediante las preguntas ¿necesitas saber cómo instalar y utilizar estas herramientas?, ¿saber más sobre los riesgos en México para la privacidad digital?, ¿o profundizar sobre el anonimato digital?, se buscar enganchar al público para que se dirija a este documento a través de un código QR.

Tras la rúbrica final con nombre y eslogan se colocaron sitios web de referencia que han nutrido esta investigación y que pueden resultar útiles para todo interesado, todos ellos de asociaciones en pro de la privacidad digital.

Preliminares

Tras realizar este producto audiovisual, que ilustra con datos duros e información pública la realidad del Internet en México respecto de la privacidad digital y seguridad, que define lo que es la privacidad en lo digital, el anonimato digital y que describe las herramientas que están disponibles para alcanzarlo; se considera que el objetivo de **construir un producto audiovisual que contribuya al conocimiento de estas posibilidades para su ejecución por parte de los usuarios interesados,** estaría cerca de cumplirse, a reserva expresa, de que el ejercicio que se haga como consecuencia de la difusión de este video y documento, será posterior a su publicación.

Pese a que ciertos temas tecnológicos pueden resultar tediosos, complicados o aburridos para ciertos usuarios, se considera que mediante esta aproximación sencilla se puede alcanzar al menos cierto conocimiento de

cómo opera Internet y las consecuencias que de ello se derivan, para que aun en el caso de no pretender alcanzar el anonimato se haga un uso crítico y consciente del mismo, bajo la aspiración de que el usuario tome conciencia y pueda llevar a la práctica algunas de estas recomendaciones y ser anónimo cuando sea requerido. Eventualmente todos podemos llegar a necesitar de estas herramientas y sus posibilidades.

Una última precisión es que el producto audiovisual ha de ser vinculado a una pequeña página web, alojada dentro de Iconos, Instituto de Investigación en Comunicación y Cultura, acompañada de este documento, y vinculado a las redes sociales digitales convenientes, para la difusión de este proyecto, por considerar que es el medio ideal donde han de ubicarse los usuarios mexicanos de Internet.

Conclusiones

El objetivo general de este proyecto: **identificar los elementos que vulneran la privacidad de las personas en Internet y analizar la pertinencia del anonimato como medio para preservarla**, fue concebido así, con la finalidad de determinar en primera instancia, que riesgos existen para los usuarios de Internet y redes sociales digitales en México; aunque no exclusivos, para después conocer con mayor detalle que es el anonimato y analizar si es posible y suficiente como medio para garantizar la privacidad en lo digital.

Para cumplir esta meta se desarrolló la primera pregunta, eje de trabajo del primer capítulo: **¿qué elementos vulneran la privacidad de las personas en Internet?,** a la que obedeció la hipótesis: **ingresar y divulgar información personal en sitios y redes sociales digitales, por parte de los usuarios en Internet, supone la pérdida del control sobre ella, volviéndola accesible a terceros, posibilitando prácticas fraudulentas, intrusivas, acosadoras y de espionaje, además de limitar su libertad de expresión, en detrimento de su privacidad digital.**

Responder a esta pregunta implicó definir previamente lo que es la privacidad, distinguirla de la intimidad, abundar en lo que es la privacidad en lo digital, que son los datos personales y datos personales sensibles, además de ubicar la privacidad digital como un derecho reconocido en México, para el que incluso existe una dependencia gubernamental (Instituto Nacional de Acceso a la Información y Protección de Datos Personales), que debe hacerlo valer y leyes como la Ley de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), de la que se

derivan los derechos de acceso, rectificación, cancelación y oposición, mejor conocidos como derechos ARCO, para su ejercicio.

Acto seguido, se ubicaron los riesgos en México con base a la taxonomía de Solove, que considera cuatro momentos con sus subdivisiones:

Momentos	Riesgos	Ejemplos
Recopilación de la información	Vigilancia	Vigilancia gubernamental ilegal y legal
	Interrogación	Almacenamiento de información por las empresas a solicitud del gobierno
Procesamiento de la información	Agregación	Extralimitación de empresas sobre el uso de datos personales
	Identificación	Identificación por triangulación de información
	Inseguridad	Fraude Reemplazo de la identidad Persecución Acoso
	Uso secundario	Uso de datos personales para fines no autorizados por empresas
	Exclusión	Discriminación en Internet

Diseminación de la información	Quebrantamiento de la confidencialidad	El nulo resguardo de la información y expansión arbitraria de los límites por empresas
	Divulgación	Información
	Exposición	Información privada que se hace pública
	Accesibilidad incrementada	Minería de datos
	Chantaje	Extorsión y sextorsión
	Apropiación	Reutilización de contenidos por las empresas
	Distorsión	Calumnia y desinformación sobre las personas en sitios y redes sociales digitales
Intrusión	Invasión	*Spam*
	Interferencia de decisiones	Publicidad invasiva

Tabla 11. Taxonomía de Solove y riesgos en México. Elaboración propia.

Así, se determinó que:

- Hay leyes que obligan a los proveedores de servicios de telecomunicaciones y radiodifusión a recopilar, almacenar y facilitar información a las instituciones, sin que haya claridad sobre el procedimiento.
- Que en México se han contratado programas informáticos de espionaje, sin que haya certidumbre sobre quiénes son los investigados, además de que muchas de las dependencias contratantes de estos servicios no tienen facultades para ello.

- Que este tipo de programas pueden insertarse en toda clase de dispositivos y recuperar información incluso de la comunicación por programas de mensajería.
- Que, de acuerdo a empresas desarrolladoras de *software* antivirus y seguridad, en México los ciberdelitos generan cuantiosas pérdidas económicas que pueden hacer desaparecer empresas; por las consecuencias de sus actos, en 6 meses y cuyo costo aproximado es de poco más de 4,000 pesos por víctima.
- Que la interacción en Internet, nos hace susceptibles de ser acosados o chantajeados, discriminados o exhibidos por lo que deben ponderarse medidas que inhiban este tipo de prácticas.
- Que las redes sociales digitales rastrean información dentro y fuera de sus propias plataformas lo que permite la perfilación del usuario para ofrecerle publicidad a modo en los sitios y redes en los que se desenvuelve, lo que puede resultar invasivo.
- Que las empresas también hacen mal uso de nuestros datos personales, haciéndose acreedores a multas, por exceder los límites para los cuales esta información es cedida.

Sumado a esto, fue de nuestro conocimiento que usuarios desconocen total o parcialmente los derechos respecto de su privacidad y datos personales, a la par que las empresas no se muestran facultadas para desempeñarse en la protección de los datos personales de los usuarios, esto de acuerdo a la Asociación Mexicana de Internet (AMIPCI).

Es por lo anterior que se valida la hipótesis creada en consecuencia a nuestra primera pregunta y la tesis versaría entonces:

Ingresar y divulgar información personal en sitios y redes sociales digitales, por parte de los usuarios en Internet sí supone la pérdida

del control sobre ella, volviéndola accesible a terceros, posibilitando prácticas fraudulentas, intrusivas, acosadoras y de espionaje, además de limitar su libertad de expresión, en detrimento de su privacidad digital.

En lo que refiere a los **elementos que vulneran la privacidad digital** de los usuarios de Internet, se asume entonces que su **interacción sin precauciones, el desconocimiento de sus derechos o cómo aplicarlos y el entorno de seguridad de las redes mismas**; que involucran a gobierno, empresas, otros usuarios y delincuencia; son los que la comprometen.

Además, las preguntas derivadas de la primera: **¿se comparte información personal en Internet?** y **¿tiene cabida el concepto de privacidad en sitios web y redes sociales digitales?** también son respondidas, en el primer caso, al señalarse que los usuarios comparten nombre, correo electrónico, información financiera, datos médicos y sensibles; la respuesta es un contundente sí. En el segundo rubro la respuesta es también afirmativa en cuanto a que existen leyes que lo establecen, pero parcial, ante el desconocimiento y desobediencia de las mismas por usuarios, empresas, gobierno y ciberdelincuencia.

Si bien puede decirse que aceptar un acuerdo de privacidad sin leerlo, o utilizar Internet libremente, es ejercicio de este derecho, hacerlo sin alfabetizar o informar a la ciudadanía, en la práctica podría contravenirlo, pues, al asumirse todo como dado, los individuos ignoran que este es un derecho y como tal desconocen cómo ejercerlo.

Ahora bien, aun cuando es posible ejercer los derechos ARCO, estos, como se ha visto, parecen no resultar suficientes al momento de proteger nuestra privacidad digital por los distintos agentes y prácticas señaladas.

Luego entonces, la segunda pregunta, objeto del segundo capítulo de esta tesis fue: **¿qué medidas a considerar por el usuario pueden garantizar su privacidad digital en Internet?,** y que como hipótesis tienen que **bajo la figura del anonimato digital puede evitarse que empresas, gobiernos y terceros en México hagan mal uso de los datos personales de los usuarios, previniendo la pérdida de su privacidad digital.**

Para responder a lo anterior, se definió lo que es el anonimato y el anonimato en lo digital, que *grosso modo*, puede decirse, es la capacidad de ser incognocible por terceros en Internet; se estableció que el anonimato puede ser débil o fuerte, que el primero, al ser prácticamente el simple ocultamiento de nuestro nombre o identidad no es suficiente para hacer valer la privacidad digital, porque las comunicaciones y acciones en Internet todavía podrían ofrecer conocimiento sobre nosotros y nuestros intereses; pero el anonimato fuerte al proteger no sólo el nombre o identidad, sino también el quehacer en Internet por vías legales y herramientas más sofisticadas, resulta más pertinente para lograrlo.

Posteriormente, se consideró a expertos, activistas e impulsores de la privacidad y anonimato en lo digital, para analizar las distintas herramientas que proponen y existen en la actualidad para ejercerlo. De tal suerte se descubrió existen:

- **Buscadores** pro anonimato que no recopilan o almacenan información de nuestra navegación.
- **Aplicaciones o *plugins*** para exploradores web que evitan el rastreo, ocultan la dirección IP, cifran la comunicación y filtran sitios seguros de los no seguros.

- **Servidores proxy cifrados y no cifrados** que dan una solución parcial a la censura y rastreo de nuestra navegación en distintos sitios web, pese a la inseguridad que representan si no son confiables tras pasar por el servidor proxy, por el uso indebido que de la información puede hacerse a partir de ese momento.

- **Circumventores,** que son servidores proxy gestionados por personas de confianza en distintos puntos de mundo, lo que da mayor seguridad aunque requiere cierta pericia para su configuración.

- **Redes privadas virtuales**, que crean un túnel dentro de Internet para comunicar de forma cifrada equipos a distancia, pero que implican verificar que los proveedores de estos servicios no hagan también lectura de nuestros datos.

- **Redes anónimas**, que protegen nuestra navegación y datos al crear recorridos aleatorios de información cifrada que sólo es accesible por el origen y destino, lo que se traduce en una de las opciones más robustas.

- **Redes sociales digitales** pro anonimato, que no precisan nombres reales y que no almacenan información, que trabajan de modo similar a las redes anonimas mediante nodos llamados *pods* y que son impulsadas por un comunidad y no con fines empresariales.

- **Antivirus, *antispyware* y cortafuegos**, que nos protegen de virus, ataques y conexiones no autorizadas en Internet y en lo local, herramientas que pueden estar contenidas en un solo programa o requerir de los tres por separado, pero que también implican indagar en las opciones para cersiorarse de que no rastrean información.

Además, se tomaron en cuenta otras recomendaciones para resguardar esta privacidad, que involucran proteger los equipos localmente, mejorar el uso de contraseñas, crear cuentas distintas para redes sociales digitales y correos electrónicos, de acuerdo a la gravedad de los intereses que allí se manejen, pues la protección de la privacidad debe ser integral para que esta sea posible.

En comparación con la taxonomía de Solove, estos son los rubros para los que resultan útiles:

	Momentos	**Riesgos**	**Herramientas para combatirlos**
Recopilación de la información	Vigilancia	Vigilancia gubernamental ilegal y legal	Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda
	Interrogación	Almacenamiento de información por las empresas a solicitud del gobierno	Navegadores Complementos Redes sociales digitales descentralizadas

Procesamiento de la información	Agregación	Extralimitación de empresas sobre el uso de datos personales	Navegadores Complementos Redes sociales digitales descentralizadas
	Identificación	Identificación por triangulación de información	Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda Redes sociales digitales descentralizadas
	Inseguridad	Fraude Reemplazo de la identidad Persecución Acoso	Antivirus *Antispyware* *Firewall* Navegadores Complementos Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda

	Uso secundario	Uso de datos personales para fines no autorizados por empresas	Redes sociales digitales descentralizadas Evaluación de riesgos por parte del usuario Derechos ARCO
	Exclusión	Discriminación en Internet	Servidores proxy anónimos y cifrados Redes privadas virtuales Redes anónimas y web profunda
Diseminación de la información	Quebrantamiento de la confidencialidad	El nulo resguardo de la información y expansión arbitraria de los límites por empresas	En este punto aún pueden resultar útiles las herramientas mencionadas, pero debe privilegiase la protección en los primeros dos momentos
	Divulgación	Información	
	Exposición	Información privada que se hace pública	
	Accesibilidad incrementada	Minería de datos	
	Chantaje	Extorsión y sextorsión	
	Apropiación	Reutilización de contenidos por las empresas	

	Distorsión	Calumnia y desinformación sobre las personas en sitios y redes sociales digitales	
Intrusión	Invasión	*Spam*	
	Interferencia de decisiones	Publicidad invasiva	

Tabla 16. Taxonomía de Solove y Anonimato digital. Elaboración propia.

Tras lo anterior se concluye, respecto del segundo apartado y a manera de respuesta a su pregunta matriz: **¿qué medidas a considerar por el usuario pueden garantizar su privacidad digital en Internet?**, que el anonimato es una posibilidad real y viable para protegerla, puesto que, según las herramientas que se utilicen, protege la identidad, como las comunicaciones y el origen, tránsito y destino de las mismas.

Que el anonimato digital es la capacidad de ser incognoscible por terceros en Internet, que el anonimato débil es una protección parcial, que sólo oculta el nombre o la identidad, pero no las comunicaciones; que el anonimato fuerte es la mejor opción para resguardar el nombre la identidad y datos en tránsito. Que el anonimato digital resulta la vía idónea para proteger la privacidad digital porque dificulta la obtención de información y que aun cuando esta pueda ser conocida complica asociarla con una identidad. Por último, que el anonimato digital implica tomar medidas preventivas como usuario, por lo que la hipótesis que versaba: bajo la figura del anonimato digital sí es posible evitar que empresas, gobiernos y terceros en México hagan mal uso de los datos personales de los usuarios, previniendo la pérdida de su privacidad digital**;** se verifica, aunque debe ser reformulada para mayor precisión, por lo que ahora diría: **bajo la figura del anonimato digital sí puede evitarse que empresas, gobiernos y**

terceros en México hagan mal uso de los datos personales de los usuarios, garantizando a través de medidas preventivas realizadas por el usuario, su privacidad digital.

Aunque con las siguientes atenuantes:

Si se registran datos personales en sitios web o redes sociales digitales, se cede esta información y con conocimiento o desconocimiento puede hacerse mal uso de ella, en este punto no sería posible, al menos en ese campo, lograr el anonimato, sobre todo cuando se trata de registros obligatorios donde se precisan datos reales como en las plataformas gubernamentales. Sin embargo, puede tenerse una identidad para estos fines y procurar vigilar el desempeño de las mismas para ejercer nuestros derechos por las vías legales de ser necesario; y tener identidades secundarias para los distintos ámbitos de nuestra vida en Internet.

Aunque el anonimato digital es posible, no es infalible, porque hay medios sofisticados para romper candados e intervenir comunicaciones, además de que hay diversos factores a tener presentes que en ciertas ocasiones pueden escapar de nuestro control. Por ejemplo si un dispositivo es utilizado por diferentes personas cualquiera de ellas puede por desatención permitir la instalación de un archivo malicioso, es probable acceder a redes gratuitas no seguras o ser contaminados por archivos en medios extraibles. Aquí la recomendación sería entonces, de acuerdo a la gravedad de los datos, cifrarlos y revisar siempre con nuestro *software* toda aquella información que se ingrese por medios extraíbles y electrónicos.

Otro punto importante es privilegiar el uso de *software* libre, que sí puede ser auditado por una comunidad y por consecuencia, ser conocidas sus vulnerabilidades. Los sistemas operativos comerciales en ese sentido son innacesibles por lo que no hay certeza de que información es rastreada.

En lo que respecta a las redes sociales digitales, la invitación es compartir sólo aquella información que no represente peligro, por el simple hecho de que perdemos el control sobre ella al publicarla, como pudo observarse en este apartado del capítulo dos, pese a los acuerdos aceptados por el usuario que estos servicios redactan y actualizan periódicamente.

Luego entonces, el anonimato digital es más completo en la medida en que se utilizan más herramientas y se obedecen ciertos protocolos (ya enunciados como recomendaciones al final del capítulo II).

El tercer capítulo de este trabajo ha sido trazado a partir del objetivo de **elaborar un producto audiovisual que contribuya al conocimiento de estas posibilidades para su ejecución por parte de los usuarios interesados,** el cual ya fue descrito en el capítulo III, donde se ha contextualizado la problemática con evidencias de riesgos en territorio nacional, a la vez, que se ha mencionado que es la privacidad y anonimato digital, para finalmente explicar cómo funciona Internet y las herramientas que existen para lograr el anonimato y como consecuencia la privacidad digital, por lo que se considera cumplido parcialmente, a reserva de conocer las consecuencias de la difusión del producto señalado y su vinculación a este documento, lo que será posterior a su publicación. Al cierre de este trabajo se ha revelado nueva información sobre la adquisición de *software* espía utilizado para intervenir las comunicaciones de periodistas, por lo que no debe pensarse que es un problema solucionado y del pasado, por el contrario, es necesario reactualizar la información para saber qué tanto se ha avanzado, lo que puede ser un nuevo objetivo a desarrollar en respuesta a este trabajo.

En el caso del uso indebido de nuestra información por empresas, se hace énfasis que esta no necesariamente pudo ser obtenida a través de Internet,

pero que finalmente está contenida allí. Es el caso del trámite de una tarjeta de crédito por ejemplo, que requirió un trámite personal, pero que mediante la vinculación con nuestro correo electrónico posibilita el *spam.*

Algunas de las aplicaciones revisadas son compatibles con diversos sistemas operativos lo que facilita su incorporación a tabletas y teléfonos inteligentes. La mayoría, en la medida de lo posible también han sido seleccionadas por ser elaboradas por asociaciones sin fines de lucro, por lo que se deben utilizar estas últimas en la medida de lo posible, en lugar de las de pago, e instalarlas no sólo en computadoras, sino en todos los dispositivos posibles.

Otro punto importante, que pudiera derivar en posibles investigaciones posteriores, es el uso de aplicaciones para dispositivos móviles, que solicitan permisos para obtener información de contactos, ubicación, mensajes y archivos contenidos dentro de los mismos. Mientras tanto aquí se extiende la invitación a utilizar sólo aquellas validadas por las distintas tiendas de descarga que los sistemas operativos tienen y cerciorarse de que los permisos no exceden las funcionalidades de estas *apps*, como en el caso de un cronómetro digital que quiera tener acceso a nuestras comunicaciones sin que tenga la opción de compartir ciertas alarmas con nuestros contactos.

De la misma forma, puede abordarse que tan pertinente es utilizar *software* privativo y sus consecuencias para la privacidad de los usuarios, además de cómo el sistema educativo, en todos sus niveles, ha privilegiado su uso por encima del *software* libre, que parece ser más seguro. Conocer de este último y evaluar sus posibilidades y pertinencia para el cuidado de la privacidad, abundar sobre los retos de su incorporación en los dispositivos digitales mexicanos, y precisar si la filosofía que involucra, pudiera permitir un uso mejor de Internet.

Averiguar que medidas pudieran dar certidumbre real sobre el cuidado de la privacidad, por parte de gobiernos, empresas y servicios de Internet, además de usuarios, a fin de abonar a la confianza.

Indagar con mayor profundidad, que tanto ha perjudicado a la sociedad mexicana, la vigilancia y espionaje desde Internet, si ha interferido en las decisiones y de qué manera, además de sus probables causas y consecuencias, ya sean nocivas o positivas.

Descubrir que tanto se han ponderado las opiniones de expertos, más allá del plano legal, a la hora de determinar medidas de protección de la privacidad en lo digital y cómo pudieran ser incorporadas.

Un último tema digno de explorar, no contenido en este trabajo y del que pudieran derivarse también posibles investigaciones, es qué tanto se protege, a través de nuestros dispositivos electrónicos, nuestra privacidad digital en lo local. Por ejemplo, al configurar un *router* inalámbrico sin el cifrado de contraseña correcto se facilita su obtención, lo que a su vez hace posible conocer la información que va y viene en ese lugar de conexión. Algo similar a lo que sucede cuando se deja abierta una conexión a Internet, ante lo que cualquiera que logre ingresar a esa red podrá obtener, con ciertos conocimientos, toda la información concerniente a la navegación de los usuarios que la utilizan.

El anonimato digital es satanizado por algunos, al señalar que implica actos delictivos, pero también resulta necesario cuando del activismo social y periodismo se habla, sin olvidar aquellos perseguidos por desaveniencias de la vida, pese a ello el usuario que no se considere en peligro también puede servirse de este para no ser agraviado por delincuentes y gozar de un Internet realmente neutro y plural, lejos de la burbuja que la perfilación de usuarios nos fabrica. Las herramientas, como todo en la vida pueden usarse

para el bien o para el mal, el proposito aquí ha sido empoderar positivamente a la sociedad.

Fuentes de consulta

Alegsa. "Definición de Indexar". *Alegsa.com.mar*. Web. 04-06-2018. <URL>.

Alegsa. "¿Qué es enrutar?" *Alegsa.com.ar*, 22-09-2010. Web. 04-06-2018. <URL>.

Alsina González, Guillem. "Antivirus". *Definición ABC*, 30-12-2008. Web. 13-09-2017. <URL>.

AMIPCI, Asociación Mexicana de Internet. *Estudio de Protección de Datos Personales entre Usuarios y Empresas*, 2012. Web. 02-10-2017. <URL>.

Animal Político. "Gobierno de Puebla usó el software de Hacking Team para espionaje político". *Animal Político*, 22-07-2015. Web. 20-04-2017.<URL>.

Animal Político. "IFAI multa a Banamex por divulgar datos personales". *Animal Político*, 06-09-2013. Web. 24-05-2017. 24-05-2017. <URL>.

Animal Político, y Arturo Angel. "México, el principal cliente de una empresa que vende software para espiar". *Animal Político*, 07-07-2015. Web. 20-04-2017. <URL>.

Animal Político, y Arturo Angel. "Sedena negoció compra de software a Hacking Team en 2015 para espiar a 600 personas". *Animal Político*, 21-07-2015. Web. 20-04-2017. <URL>.

Animal Político, y Nayeli Roldán. "113 empresas hicieron mal uso de datos personales de 2012 a 2016". *Animal Político*, 26-01-2017. Web. 15-05-2017. <URL>.

Aponte Núñez, Emercio José. "La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano". *Revista de Derecho Privado*, vol. 12–13, enero-diciembre de 2007, pp. 109–24. Impreso.

ASI-México, Alianza por la Seguridad en Internet. "Internet S.O.S." *El efecto Internet*, vol. 1, 200d. C., pp. 4–7. Impreso.

ASI-México, Alianza por la Seguridad en Internet. "Radiografía del SPAM en México". *ASI-México*. Web. 01-06-2017. <URL>.

Bejerano, Pablo G. "Qué son las DNS". *Blogthinkbig.com*, 15-07-2014. Web. 17-05-2018. <URL>.

Bembibre, Victoria. "Router". *Definición ABC*, 01-06-2009. Web. 30-10-2017. <URL>.

Bertoni, Eduardo A. *Hacia una Internet libre de censura: propuestas para América Latina*. Editado por Universidad de Palermo (Palermo, Buenos Aires, Argentina), Universidad de Palermo, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información, 2012. Impreso.

Cano, Francisco. "Definición de Modem". *Definición ABC*, 08-11-2014. Web. 17-05-2018. <URL>.

Cárdenas, Sánchez, Sandra. *Necesidad de crear una regulación específica en México sobre Protección de Datos Personales en el sector privado*. Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, septiembre de 2010 . Web. 21-09-2016. <URL>.

Carrodeguas, Norfi. "Datos del usuario que se obtienen con la dirección IP y el navegador". *NorfiPC.* Web. 17-05-2018. <URL>.

Collective, Tactical Technology. *All Tactics guides*. https://securityinabox.org. Web. 4-11-2017. <URL>.

Comodo. "Policies and Practices of the Comodo Companies". *Comodo*. Web. 13-09-2017. <URL>.

Condusef, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. "Fraude". *Proteja su dinero*. Web. 02-11-2017. <URL>.

Condusef, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. "Protege tu identidad". *Condusef*. Web. 26-04-2017.<URL>.

Cortes Ospina, Mateo. "¿Qué es software libre?" *MindMeister*. Web. 21-05-2018. <URL>.

De Rivera, Javier. "Richard Stallman, el Software Libre y la Libertad en la Red". *Sociología y redes sociales*, 31-08- 2011. Web. 21-05-2018. <URL>.

Derechos Digitales, Derechos Humanos y Tecnología en América Latina, et al. *Internet en México. Derechos Humanos en el Entorno Digital*. Editado por Juan Carlos Lara, Derechos digitales, 2016. Web. <URL>.

Diario Oficial de la Federación. *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. 07-05-2010. Web. 28-09-2016. <URL>.

Diario Oficial de la Federación. *Ley Federal de Telecomunicacines y Radiodifusión*. 14-07-2014. Web. 29-10-2017. <URL>.

Diaspora*. "El Proyecto diaspora*". *diaspora* social network*. Web. 27-05-2017. <URL>.

Diaspora*. "JoinDiaspora*". *diaspora* social network*. Web. 09-09-2017. <URL>.

Diaspora*. "Registrarse en diaspora*". *diaspora* social network*. Web. 06-09-2017. <URL>.

Díaz Rojo, José Antonio. "Privacidad: ¿neologismo o barbarismo?" *Espéculo. Revista de estudios literarios*, vol. 21, septiembre de 2016. Web. 02-11-2017. <URL>.

Dinero en Imagen. "Lanzan alerta de 'Sextorsión' en las redes". *Dinero en Imagen.com*, 22-09-2012. Web. 25-05-2017. <URL>.

DuckDuckGo. "DuckDuckGo". *DuckDuckGo*. Web. 14-07-2017. <URL>.

Echeverri, Daniel. *Deep Web: TOR, FreeNET & I2P: privacidad y anonimato*. Oxword, 2016. Web. <URL>.

Ecured. "Motor de búsqueda - EcuRed". *Ecured*. Web. 18-05-2018. <URL>.

EFF, Electronic Frontier Foundation. "HTTPS Everywhere". *Electronic Frontier Foundation*, 07-10-2011. Web. 08-08-2017. <URL>.

EFF, Electronic Frontier Foundation. "Privacy Badger". *Electronic Frontier Foundation*, 24-04-2013. Web. 08-08-2017. <URL>

El economista, y Ana Langner. "Ley de Telecomunicaciones no viola privacidad: SCJN". *El Economista*, 04-05-2016. Web. 23-03-2017. <URL>.

Encuentro jurídico, y Graciano Ambar. "Los derechos humanos de tercera y cuarta generación". *Encuentro jurídico*, 04-01-2013. Web. 29-10-2017. <URL>.

Escalante Gonzalbo, Fernando. *El derecho a la privacidad*. ifai, Instituto Federal de Acceso a la Información Pública, 2007. Impreso.

Etimologías. "Anónimo". *Etimologías de Chile*, 06-02-2017. Web. 02-06-2017 <URL>.

Facebook. “Declaración de derechos y responsabilidades”. *Facebook*, 30-01-2015. Web. 26-05-2017. <URL>.

Facebook. “Política de datos”. *Facebook*, 29-09-2016. Web. 26-05-2017. <URL>.

FrootVPN. “Best VPN - Fast, Encrypted to Surf Anonymously”. *FrootVPN*. Web. 04-11-2017. <URL>.

Fundéu BBVA. “encriptar es ocultar un mensaje con una clave”. *Fundéu BBVA buscador urgente de dudas*, 01-12-2015. Web. 18-05-2018. <URL>.

Fundéu BBVA. “hacker y cracker, diferencias de significado”. *Fundéu BBVA buscador urgente de dudas*. Web. 04-06-2018. <URL>.

Fundéu BBVA. "Stalkear". *Fundéu BBVA buscador urgente de dudas*. Web. 29-10-2017. <URL>.

Fundéu BBVA. "*Troleo*". *Fundéu BBVA buscador urgente de dudas*. Web. 29-10-2017.<URL>.

García, González, Aristeo. “La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado”. *Boletín Mexicano de Derecho Comparado*, núm. 120, 2007, pp. 743–78. Impreso.

Garrido, Rodrigo. “Facebook es la red social preferida de los mexicanos, pero Instagram y Snapchat ganan terreno”. *Xataka.com.mx*, 05-12-2016. Web.04-11-2017. <URL>.

Garzón Valdés, Ernesto. *Lo íntimo, lo privado y lo público*. 3. ed, ifai, Instituto Federal de Acceso a la Información Pública, 2007. Impreso.

Ghostery. “Bienvenido a Ghostery”. *Ghostery*. Web. 04-11-2017. <URL>.

Gironés Jesús, Tomás. *Modelo de referencia TCP/IP*. Universitat Politècnica de València UPV, 2016. Web. 20-05-2018. <URL>.

González Marcos, Ana. "Desarrollo de técnicas de minería de datos en procesos industriales: Modelización en lineas de produccion de acero". *Universidad de La Rioja*, 2007. Web. 15-05-2018. <U"RL>

Hacking Team. “Solutions”. *Hacking Team*. Web. 20-04-2017. <URL>

INAI, Instituto Nacional de Acceso a la Información. "Dispositivos incorrectamente desechados, perdidos y robados, principales causas de vulneración de datos personales, alerta INAI". *INAI.* 25-07-2016. Web. 25-04-2017 <URL>.

InfoSpyware. “¿Qué es el Phishing?” *InfoSpyware*. Web. 29-10-2017. <URL>.

Instituto Federal de Acceso a la Información Pública. *Protección de Datos Personales. Compendio de Lecturas y Legislación*. Primera edición, Tiro Corto Editores, 2010. Impreso.

Ixquick. "Herramientas". *Startpage by Ixquick*. Web. 04-11-2017. <URL>.

Ixquick. "StartPage by Ixquick". *Startpage by Ixquick.* Web. 14-07-2017. <URL>.

Kaspersky Lab, et al. "El spam en 2016". *Secure List*, 20-02-2017. Web 01-06-2017. <URL>.

Kaspersky Lab, et al. "Sextorsión: una amenaza para todos, en especial para los adolescentes". *Kaspersky Lab Daily*, 02-08-2016. Web. 25-05-2017. <URL>.

Kaspersky Lab, LATAM. "¿Qué es el cifrado?". *Kaspersky Lab*. Web. 20-05-2018. <URL>.

Krogerus, Hannes Grassegger &. Mikael. "The Data That Turned the World Upside Down". *Motherboard*, 28-01-2017. Web. 15-05-2018. <URL>.

Kwon, Young Hyun. *Riffle : An Efficient Communication System with Strong Anonymity*. Massachusetts Institute of Technology, 2015. *dspace.mit.edu*. Web. 15-06-2017. <URL>.

Lucas Murillo de la Cueva, Pablo Lucas, y José Luis Piñar Mañas. *El derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo, 2009. Impreso.

Lucena Cid, Isabel Victoria. "La protección de la intimidad en la era tecnológica: hacia una reconceptualización". *Revista internacional de pensamiento político*, vol. 7, 2012, pp. 117–44. Impreso.

Luchadoras, Mx, et al. *La violencia en línea contra las mujeres en México: Informe para la Relatora sobre Violencia contra las Mujeres Ms. Dubravka Šimonović*. 2017.*Sontusdatos.org.* Web. 15-05-2018. <URL>.

Miessler, Daniel. "The Internet, the Deep Web, and the Dark Web". *Daniel Miessler*, 08-07-2015. Web. 18-05-2018. <URL>.

Migliorisi, Diego Fernando. *Internet profunda: anonimato, libertad de expresión y censura en Internet*. 1a ed., 2015. Impreso.

Naciones Unidas, Asamblea General. *El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.* 30-06-2014. Web. 31-10-2017. <URL>.

News Center LATAM, y Jacquelin Beauchere. "Microsoft lanza Índice de Civismo Digital; desafía a la gente a ser más empática en línea". *News Center Latinoamérica*, 07-02-2017. Web. 25-05-2017. <URL>.

Norton by Symantec. *Reporte Norton 2013. México*. septiembre de 2013. Web. 15-05-2017. <URL>.

Nuñez Carvonel, Gustavo. "Nodo - EcuRed". *Ecured.cu*. Web. 20-05-2018. <URL>.

Panda Security. "Phishing". *Panda Security*. Web. 15-05-2017. <URL>.

Panda Security. "¿Qué es un Ransomware y cómo actúa?" *Panda Security Mediacenter*, 15-11-2013. Web. 15-05-2017. <URL>.

Peacefire. "Circumventor Central". *Peacefire.org*. Web. 30-10-2017. <URL>.

Peña Ochoa, Paz. *¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos*. ONG Derechos Digitales, 2013. Web. 20-05-2018. <URL>.

Pérez Porto, Julián, y María Merino. "Plugin". *Definición.de*, 2013. Web. 30-10-2017. <URL>.

Proceso, y Emilio Godoy. "El data mining invade México, a costa de los usuarios". *Proceso.com.mx*, 15-05-2015. Web. 26-05-2017. <URL>.

Psiphon. "Política de privacidad". *Psiphon*. Web. 12-08-2017. Web. <URL>.

Real Academia Española. "anonimato". *Diccionario de la lengua española.* Web. 04-11-2017. <URL>.

Real Academia Española. "Anónimo". *Diccionario de la lengua española*. Web. 02-06-2017. <URL>.

Real Academia Española. "Dato". *Diccionario de la lengua española*, 12-10-2016. Web. <URL>.

Real Academia Española. " Intimidad". *Diccionario de la lengua española,* 30-09-2016. Web. <URL>.

Real Academia Española. "Seudónimo". *Diccionario de la lengua española*. Web. 13-06-2017. <URL>.

Riffo Gutierrez, Marcelo Alejandro. *Vulnerabilidades de las redes TCP/IP y principales mecanismos de seguridad*. Universidad Austral de Chile, 2009. Web. 20-05-2018. <URL>.

Rodríguez, Katitza. *Anonimato y cifrado*. 10-02-2015. *www.eff.org.* Web. 06-02-2017. <URL>.

Secretaría del Gobierno Digital. "¿Qué son los Metadatos?" *Secretaría del Gobierno Digital*. Web. 30-10-2017. <URL>.

SonTusDatos. "Ante vulneraciones de datos personales ¿Qué hacen las empresas en México?" *SonTusDatos.org*, 18-01-2017. Web. 04-06-2018. <URL>.

SonTusDatos.org, y Daniel Villegas. "Varias multas del INAI por violación de datos personales nunca se pagarán". *SonTusDatos.org*, 16-06-2016. Web. 15-05-2017. <URL>.

Tails - About. Web. 06-09-2017. <URL>.

Tecnología & Informática. "El sistema binario". *Tecnología & Informática*, 13-02-2018. Web. 12-05-2018. <URL>.

Telefónica, Data Warden. "Telefónica y Data Warden ofrecen servicios de seguridad". *Telefónica*, 31-01-2017. Web. <URL>.

Tenorio Cueto, Guillermo A., y Ana Cristina González Rincón. "Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares". *Cuestiones Constitucionales*, vol. 28, junio de 2013, pp. 391–406. Impreso.

Tenorio Cueto, Guillermo A., y María Rivero del Paso. *Los datos personales en México: perspectivas y retos de su manejo en posesión de particulares*. Editorial Porrúa : Universidad Panamericana, 2012. Impreso.

The Tor Project Inc. "Tor Project: Overview". *Tor*. Web. 25-08-2017. <URL>.

Toledo, Amalia M., y Pilar Sáenz. *Manual Antiespías. Herramientas para la protección digital de periodistas*. Fundación para la Libertad de Prensa, 2015. Web. 08-08-2017. <URL>.

TunnelBear. “TunnelBear: Secure VPN Service”. *TunnelBear*. Web. 04-11-2017. <URL>.

Twitter. “Política de Privacidad de Twitter”. *Twitter*, 18-06-2017. Web. 26-05-2017. <URL>.

Twitter. “Términos de servicio”. *Twitter*, 30-09-2016. Web. 02-11-2017. <URL>.

Ucha, Florencia. “Firewall”. *Definición ABC*, 23-01-2014. Web. 13-09-2017<URL>.

Valdés Rodríguez, Miriam. “Antispyware: Protegiéndote de los Espías”. *.Seguridad*, 2017. Web. <URL>.

Velasco, Rubén. “Las cabeceras TCP/IP filtran lo que estás viendo en Netflix”. *Redes Zone*, 12-04-2017. Web. 13-09-2017. <URL>.

Vitaliev, Dmitri. *Seguridad y privacidad digital para los defensores de los derechos humanos*. Front Line, 2007. *libros.metabiblioteca.org*. Web. 21-09-2016. <URL>.

Warren, Samuel, et al. *El derecho a la intimidad - the right to privacy*. Civitas, 1995. Impreso

WikiLeaks. “The Hacking Team Archives”. *WikiLeaks*, 08-07-2015. Web. 20-04-2017. <URL>.