Biblioteca INFOTEC

Ciudad de México, a 02 de abril de 2025

VISTO BUENO DE TRABAJO TERMINAL

Maestría en Derecho de las Tecnologías de Información y Comunicación (MDTIC)

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación:

"Propuesta de intervención para la protección de los miembros de la FSFLA contra el seguimiento web"

Desarrollado por el alumno: **Alberto Eleuterio Flores Guerrero**, bajo la asesoría de la **Dra. Evelyn Téllez Carvajal**, cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Dr. Juan Antonio Vega Garfias
Subgerente de Innovación Gubernamental

JAVG/jah

C.c.p. Mtra. Analy Mendoza Rosales. – Encargada de la Gerencia de Capital Humano. - Para su conocimiento.
Alberto Eleuterio Flores Guerrero. – Alumno de la Maestría en Derecho de las Tecnologías de Información y Comunicación. – Para su conocimiento.

jah

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“PROPUESTA DE INTERVENCIÓN PARA LA PROTECCIÓN DE LOS MIEMBROS DE LA FSFLA CONTRA EL SEGUIMIENTO WEB”

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Alberto Eleuterio Flores Guerrero

Asesor:

Mtra. Evelyn Téllez Carvajal

Ciudad de México, febrero, 2023

Agradecimientos

A mis padres

por su inagotable apoyo,

por su paciencia, sabiduría y amor.

Tabla de contenido

Siglas y abreviaturas

CSV	Comma-Separated Values (Valores separados por comas)
EPDPEI	Estándares de Protección de Datos Personales para los Estados Iberoamericanos
EFF	Electronic Frontier Foundation
FSF	Fundación del Software Libre
FSFLA	Fundación del Software Libre América Latina
HTTP	Protocolo de Transferencia de Hipertexto
IETF	Grupo de Trabajo de Ingeniería de Internet
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
IP	Protocolo de Internet
ISP	Proveedor de Servicios de Internet
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
NIST	Instituto Nacional de Estándares y Tecnología de los Estados Unidos
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OEA	Organización de Estados Americanos
PRONADAT	Programa Nacional de Protección de Datos Personales
OS	
RFC	Request for Comments (Petición de comentarios)
RGPD	Reglamento General de Protección de Datos de la Unión

	Europea
RIPD	Red Iberoamericana de Protección de Datos
SNT	Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
TCP	Protocolo de Control de Transición
WWW	World Wide Web (Red Informática Mundial)
XMPP	Protocolo Extensible de Mensajería y Comunicación de Presencia

Introducción

El presente documento tiene un doble objetivo, por una parte, busca informar sobre la práctica del seguimiento web, su panorama actual y cómo puede poner en riesgo la privacidad de los usuarios.

Por otra parte, se realiza una propuesta de intervención[1] con la que se busca que la Fundación Software Libre América Latina (FSFLA) realice una serie de acciones para transformar la realidad digital de sus miembros, con el objetivo de advertir sobre los peligros del seguimiento web, promover y educar sobre cómo proteger la privacidad al navegar en la Web utilizando los programas de Software Libre adecuados.

La FSFLA fue fundada en noviembre de 2003 en Rosario, Argentina,[2] con el objetivo de promover el Software Libre, (es decir el software que respeta la libertad de los usuarios), y para participar e influir en los procesos de políticas públicas en América Latina que afecten los derechos de usuarios y desarrolladores en el desarrollo, uso, redistribución y modificación de todo el software o bien que se vean afectados por el software libre.[3]

Se ha buscado que este trabajo pueda ser leído por todo público, por lo que se ha limitado, en la medida de lo posible, el contenido técnico. Se espera que

---

1 La propuesta de intervención es un trabajo realizado para analizar problemas o situaciones problemáticas y para plantear estrategias que permitan solucionarlo y transformar la realidad. Stagnaro, Daniela y Da Representaçao, Natalia, “El proyecto de intervención”, *En carrera: escritura y lectura de textos académicos y profesionales*, Argentina, Universidad Nacional de General Sarmiento, 2012, pp. 157-178.

2 Busaniche, Beatriz, *FSFLA News Issue #4*, Lista de Correo FSFLA-Anuncio. *https://www.webcitation.org/6AsIccVZH?url=http://mail.fsfeurope.org/pipermail/fsfla-anuncio/2005-November/000036.html* Archivado del original: 22 de septiembre de 2012. (Fecha de consulta: 16 de mayo de 2021).

3 FSFLA, *Constitución*, FSFLA, 2019, *http://www.fsfla.org/ikiwiki/about/constitution.es.html* (Fecha de consulta: 29 de abril de 2021).

pueda ser especialmente útil para el Consejo y los miembros de la FSFLA, quienes en general tienen conocimientos básicos del sistema operativo GNU/Linux, la línea de comandos y la importancia del Software Libre.

El trabajo se ha dividido en tres partes. En la primera parte se analiza el seguimiento web, los métodos para identificar usuarios y la forma en que las compañías de seguimiento web lucran con los datos de los usuarios. También se menciona, de forma breve, cómo el seguimiento web permite realizar predicciones sobre la vida de los usuarios, e incluso, llegar a influir en sus acciones.

En la segunda parte se analiza el derecho a la protección de datos personales, tanto en lo general para América Latina, como en lo específico para algunos de los países más poblados de la zona.

Para el análisis general, se ha tomado como referencia a la Red Iberoamericana de Protección de Datos (RIPD), integrada por Andorra, Brasil, Cabo Verde, Chile, Colombia, Costa Rica, Ecuador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Perú, Paraguay, Portugal, República Dominicana, Santo Tomé y Príncipe, El Salvador y Uruguay.[4]

Se hace especial referencia los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, emitidos en 2017 por la RIPD, ya que los Estados miembros se encuentran en proceso de adaptarlos a su legislación nacional, y en los próximos años los Estándares serán el principal referente en la materia para los países miembros.[5]

Si bien la FSFLA busca tener alcance en toda Latinoamérica, por los límites temporales de esta investigación, solo se analizan con mayor detalle las legislaciones de Argentina, Brasil, Chile, Colombia, México y Perú, al ser los

4 RIPD, “Historia de la Red Iberoamericana de Protección de Datos (RIPD)”, RIPD, https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd (Fecha de consulta: 21 de junio de 2020).

5 *Idem.*

países más poblados de la zona que cuentan con legislación en materia de protección de datos personales.

Como parte de análisis, se hace referencia a las leyes y reglamentos de protección de datos personales de cada país, el fundamento constitucional (cuando existe), y las autoridades de control ante las cuales los ciudadanos pueden ejercer su derecho a la protección de datos personales.

En la tercera y última parte, se propone una estrategia para que la FSFLA informe a sus miembros sobre los peligros del seguimiento en la web y difunda algunas soluciones para disminuir su impacto, y las acciones que puede tomar el Consejo de la FSFLA para promover la privacidad en la web y las tecnologías y servicios respetuosos de la privacidad del usuario, con los que se puede disminuir el impacto del seguimiento web.

Se espera que, tras la lectura de este trabajo, el lector se encuentre capacitado para entender los riesgos del seguimiento web y la forma en la que puede protegerse de las invasiones a su privacidad por parte de estas técnicas. Aunque es importante resaltar que las técnicas y métodos de seguimiento en la web se encuentran en constante cambio, por lo que se recomienda al lector tomar un papel activo en la protección de su privacidad en el mundo digital.

Capítulo 1

Seguimiento Web

Capítulo 1. Seguimiento Web

1.1 Antecedentes

En este capítulo se explicará el seguimiento web: su concepto, funcionamiento, alcance, e impacto individual y social. En caso de que el lector desee protegerse contra este tipo de técnicas, puede consultar el capítulo 2 para aprender sobre sus derechos de protección de datos personales, mientras que en el capítulo 3 se exponen algunas recomendaciones y tecnologías que el lector puede utilizar si desea mitigar el seguimiento a su persona y protegerse.

Debido a limitaciones materiales y temporales, este estudio excluye otras formas de seguimiento comunes en la actualidad: GPS, tarjetas SIM, y otras tecnologías, utilizadas fuera del contexto del seguimiento web.

Para comenzar este trabajo, se explican brevemente los conceptos de Internet, Web, Navegador web y Capa de Internet, términos que son relevantes en esta investigación, pero que no siempre son utilizados de forma correcta en la cultura popular, por lo que pueden causar confusión.

¿Qué es Internet?

El concepto de Internet hace referencia a una red pública para la comunicación de computadoras y dispositivos electrónicos: teléfonos celulares, routers, entre otros. Estos dispositivos se comunican mediante el Protocolo de Control de Transición (TCP) y el Protocolo de Internet (IP), creados para estandarizar el proceso de comunicación entre ordenadores. Para poder conectarnos a Internet se necesita contratar un Proveedor de Servicios de Internet (ISP).[6]

6 Dordal, Peter, *IP - Internet Protocol*, An Introduction to Computer Networks, http://intronetworks.cs.luc.edu/current2/html/intro.html#ip-internet-protocol (Fecha de consulta: 09 de junio de 2021); Peterson, Larry y Davie, Bruce, *Internet (IP)*, Computer Networks: A Systems Approach, https://book.systemsapproach.org/internetworking/basic-ip.html (Fecha de consulta: 09 de junio de 2021) y Kurose, James y Ross, Keith, *Computer Networking*, 6a. ed., Boston, Pearson, 2013. pp. 2-18a.

¿Qué es una Capa de Internet?

Debido a la complejidad de Internet, su funcionamiento y estudio se ha dividido en una arquitectura de capas independientes entre sí. Esto permite realizar innovaciones o modificaciones en una de las capas, sin afectar el funcionamiento de las otras capas. Estas capas se dividen en: capa física, capa de enlace, capa de red, capa de transporte y capa de aplicación.[7]

¿Qué es la Web?

La Web es la forma abreviada de llamar a la World Wide Web (WWW) sistema que funciona en la capa de aplicación de Internet. La Web fue el primer sistema de Internet que llegó al público en general. Se caracteriza por permitir publicar contenido a un bajo costo y de forma sencilla mediante una página web.

Las comunicaciones web se realizan observando el Protocolo de Transferencia de Hipertexto (HTTP), que permite a los usuarios solicitar a un servidor web el contenido que deseen en el momento que así lo requieran.[8]

Diferencias entre la Web e Internet

Internet es una red pública mundial que incluye toda la infraestructura de computadoras y dispositivos, así como sus protocolos y aplicaciones. Mientras que la Web funciona solo en la Capa de Aplicación de Internet, para el intercambio de páginas web. Si bien la Web es uno de los sistemas más conocidos de Internet, no

7 *Ibídem*, pp. 47-55; Dordal, Peter, *Layers*, An Introduction to Computer Networks, http://intronetworks.cs.luc.edu/current2/html/intro.html#layers (Fecha de consulta: 09 de junio de 2021); Peterson, Larry y Davie, Bruce, *Architecture*, Computer Networks: A Systems Approach, https://book.systemsapproach.org/foundation/architecture.html (Fecha de consulta: 09 de junio de 2021)

8 Kurose, James y Ross, Keith, *op. cit.*, pp. 98-110; Peterson, Larry y Davie, Bruce, *Applications*, Computer Networks: A Systems Approach, https://book.systemsapproach.org/foundation/applications.html (Fecha de consulta: 09 de junio de 2021); Bonaventure, Olivier, *The HyperText Transfer Protocol*, Computer Networking: Principles, Protocols and Practice, https://www.computer-networking.info/2nd/html/protocols/http.html (Fecha de consulta: 09 de junio de 2021)

es el único, existen otras aplicaciones de Internet que no utilizan la Web ni el protocolo HTTP.

¿Qué es un Navegador web?

Es un programa especial que nos permite visitar, interactuar y visualizar sitios web con texto, imágenes y vídeo.[9]

De forma general, un navegador web funciona de la siguiente manera:[10]

1. El usuario ingresa una dirección de Internet
2. El navegador realiza una petición de acuerdo con el protocolo HTTP.
3. La petición es procesada como datos y viaja en las diferentes capas de Internet hasta llegar a su destino: el servidor web.
4. Si esta solicitud es satisfactoria, el servidor web responderá con la información solicitada. La respuesta viaja nuevamente a través de Internet, hasta llegar al ordenador.

La respuesta del servidor web puede tener muchas formas: un archivo de texto, una imagen, un vídeo, o cualquier otro tipo de archivo. También puede ser un programa o archivo que se coloca en la computadora con el objetivo de seguir al usuario mientras navega en la Web.[11]

9 Christensson, Per "*Web Browser Definition*", TechTerms, 2014, https://techterms.com/definition/web_browser (Fecha de consulta: 09 de junio de 2021); Dama, Manasa, "Difference Between Search Engine and Browser", *Difference Between Similar Terms and Objects*, Difference Between, 2011, http://www.differencebetween.net/technology/internet/difference-between-search-engine-and-browser/ (Fecha de consulta: 09 de junio de 2021); Extended Learning Institute (ELI) at Northern Virginia Community College (NOVA), *Reading: Web Browser*, Lumen Learning, 2015, https://courses.lumenlearning.com/zeliite115/chapter/reading-web-browser/, (Fecha de consulta: 09 de junio de 2021)

10 Mozilla, *What is a web browser?*, https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/ (Fecha de consulta: 25 de julio de 2020).

11 *Idem.*

El navegador interpreta la respuesta del servidor y utiliza esta información para mostrar el sitio web y ejecutar código en la computadora del usuario de acuerdo a lo ordenado por el servidor.[12]

1.2 Seguimiento Web

El seguimiento web es la práctica por la cual se identifica y recolecta información sobre los usuarios.[13] Esto es posible mediante el uso de rastreadores web. Estos rastreadores ejecutan comandos en el ordenador para obtener datos acerca de la identidad del usuario y la forma en que interactúa con uno o múltiples sitios web.[14] Entre la información recolectada se encuentra: ubicación, intereses, compras, estado laboral, orientación sexual, problemas financieros, estado de salud, entre otros.[15] En la **sección Impacto del seguimiento web** se analiza a detalle cómo se utilizan estos datos y los patrones de comportamiento de cada usuario para inferir todavía más información sobre ellos.

Seguimiento de primeras partes y seguimiento de terceros

Los rastreadores incluidos en los sitios web pueden ser clasificados en dos tipos: de primera parte y de tercera parte.

Los rastreadores de “primera parte”, (first party) son propiedad del sitio web que el usuario desea visitar, estos rastreadores suelen ser utilizados para dar funcionalidad básica al sitio web. Los rastreadores de “terceras partes” (third party) son incluidos por sitios web que utilizan servicios de terceros.[16]

12 *Idem.*

13 R. Mayer, Jonathan y C. Mitchell, John, “Third-Party Web Tracking: Policy and Technology”, *2012 IEEE Symposium on Security and Privacy*, 2012, San Francisco, IEEE, pp. 413-427, https://ieeexplore.ieee.org/document/6234427 (Fecha de consulta: 14 de junio de 2021).

14 Kelly, M.J., *No-judgment digital definitions: What is a web tracker?*, Mozilla, 2019, https://blog.mozilla.org/firefox/what-is-a-web-tracker/ (Fecha de consulta: 25 de julio de 2020)

15 R. Mayer, Jonathan y C. Mitchell, John, *op. cit.*, p. 415.

16 *Idem*.

Los servicios de terceros pueden brindar un valor agregado a los sitios web. Por ejemplo, un negocio puede insertar en su página web un servicio de mapas para indicar a sus clientes la ruta más adecuada para llegar al negocio.[17]

Los servicios de terceros son capaces de seguir e identificar al usuario mientras navega en diferentes sitios web. En la actualidad se encuentra muy extendido el uso de estos servicios, los que suelen obtener tanta información del usuario como les es posible.[18]

Los servicios de terceros también pueden incluir rastreadores que no dan más funcionalidad a los usuarios, por ejemplo, rastreadores con fines publicitarios, de redes sociales, o de analítica (*analytics*).[19]

La sección 1.4 Panorama del seguimiento web muestra a detalle el amplio uso de estos servicios de terceros en los sitios web más visitados del mundo.

Es indiscutible que los servicios de terceras partes pueden ser utilizados para dar mayor valor y utilidad a la Web. Lamentablemente, hoy en día estos servicios son utilizados por las primeras partes sin tomar en consideración privacidad de sus usuarios. Las terceras partes han aprovechado esta situación y

17 El lector que busque conocer más a detalle el uso de servicios de terceras partes en algún sitio web en específico, puede utilizar el navegador Firefox, y abrir las “Herramientas de Desarrollador” (presionando el botón F12 en el teclado), abrir la pestaña “Redes” o “Network” y actualizar la página web visitada. Se recomienda visitar sitios oficiales gubernamentales como el portal www.gob.mx el cual pese a ser un sitio institucional del Gobierno de México, utiliza Google Analytics, es decir tecnologías de seguimiento web de la empresa Google. (Fecha de consulta: 14 de junio de 2021)

18 Roesner Franziska, Kohno Tadayoshi, *et al.*, “Detecting and defending against third-party tracking on the web”, *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, Berkeley, USENIX Association, 2012, https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (Fecha de consulta: 27 de abril de 2021).

19 Lerner, Adam, *et al.*, “Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016”, *25th USENIX Security Symposium (USENIX Security 16)*, USENIX Association, 2016, p. 997. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_lerner.pdf (Fecha de consulta: 29 de abril de 2020)

en sus servicios suelen incluir: rastreadores para la vigilancia y seguimiento de los usuarios, difusión de noticias falsas y, en algunos casos, para utilizar el ordenador del usuario para fines propios, que el usuario no ha autorizado ni necesita.[20]

1.2.1 ¿Cómo funciona el seguimiento web?

El seguimiento web inicia cuando un usuario visita una página web, por ejemplo la página oficial del Gobierno Mexicano `www.gob.mx`, la cual incluye servicios de seguimiento de terceros, como `www.google-analytics.com`.[21]

Entonces, el navegador web llama a `www.google-analytics.com`, para cargar contenido adicional, en este caso un archivo de código, cómo resultado, la empresa Google se entera de la visita del usuario a la página oficial del Gobierno Mexicano.[22]

El servicio de seguimiento utiliza diversos mecanismos rastreadores para continuar identificando al usuario a través de múltiples sitios web. Toda la información es registrada junto con identificadores de los dispositivos del usuario y sus cuentas.[23]

Debido a que los rastreadores son invisibles al usuario, y el usuario no ha visitado de forma intencionada el sitio `www.google-analytics.com`, existe cada vez más preocupación sobre las implicaciones a la privacidad de los usuarios,[24] las cuales mencionaremos más adelante, por ahora examinaremos más a detalle el funcionamiento de estos mecanismos de seguimiento web.

20 Urban, Tobias, *et al.*, “Beyond the Front Page: Measuring Third Party Dynamics in the Field”, 2020, https://arxiv.org/pdf/2001.10248.pdf (Fecha de consulta: 29 de abril de 2020)

21 Lerner, Adam, *et al.*, *op. cit.*, pp. 998-999

22 *Idem*.

23 *Idem*.

24 *Idem*.

1.2.2 Mecanismos de seguimiento web

Para identificar con exactitud a cada usuario y su actividad se utilizan diferentes mecanismos. Estos mecanismos de identificación y para su análisis se clasifican en mecanismos de seguimiento con *estado* y seguimiento sin *estado*.[25]

En el ámbito de un programa informático cuando se habla de estado, nos referimos a que el comportamiento del programa es influenciado por su historial o las actividades realizadas anteriormente por el usuario.[26] La falta de estado índica que el programa no tiene acceso a dicho historial.

En el ámbito específico de la Web, se utiliza el protocolo HTTP, el cual no tiene estado. Esto significa que un servidor web no tiene recuerdos de eventos pasados, al enviar un objeto y olvida este evento inmediatamente. Si el usuario solicita el mismo objeto, el servidor lo envía otra vez, sin recordar que lo había enviado antes.[27]

Para solventar la falta de estado en el protocolo HTTP, se han inventado mecanismos que no necesitan estado para identificar a un dispositivo específico entre miles de millones, aun si el dispositivo se conecta desde diferentes puntos en el mundo. Estos mecanismos permiten identificar al usuario propietario de dicho dispositivo, incluso después de cerrar sesión en el sitio web.[28]

Además, se han inventado mecanismos para preservar el estado para permitir la identificación del usuario guardando en su ordenador los identificadores o rastreadores, para ser consultados y modificados posteriormente.[29]

25 Karaj, Arjaldo, *et al.*, “WhoTracks.Me: Shedding light on the opaque world of online tracking”, *Computing Research Repository*, Cornell University, 2019, p. 3. https://arxiv.org/abs/1804.08959v2 (Fecha de consulta: 29 de junio de 2020)

26 Abelson Harold, *et al.*, *Structure and Interpretation of Computer Programs*, 2a. ed, Cambridge, MIT Press, 1996. p. 296, https://web.mit.edu/alexmv/6.037/sicp.pdf (Fecha de consulta: 29 de abril de 2020)

27 Kurose, James y Ross, Keith, *op. cit.*, pp. 99-100

28 Agencia Española de Protección de Datos, *Estudio Fingerprinting o Huella digital del dispositivo*, 2019, pp. 4-8, https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf (Fecha de consulta: 29 de abril de 2020), pp. 7-9.

29 *Idem*.

Seguimiento sin estado

Este tipo de mecanismos son llamados seguimiento por huella digital del dispositivo (device fingerprinting). Estos mecanismos identifican los atributos del dispositivo que no suele cambiar, por lo que no necesitan conocer el estado de la comunicación entre el usuario y el servidor.

Funcionan recopilando información detallada de cada dispositivo: navegador web, sistema operativo, resolución de pantalla, tipo de procesador, si es una computadora personal o dispositivo móvil, movimientos del ratón, posición y movimientos del dispositivo móvil, entre otras.[30]

Esto permite identificar al dispositivo, al usuario y sus actividades, con el objetivo de perfilar a cada usuario.[31] La cantidad de información que se puede obtener del dispositivo es tan alta, que permite identificarlo con alta precisión entre los miles de millones de dispositivos conectados a Internet, por eso se le denomina huella digital. Una vez que un dispositivo se conecta a un servidor es identificado para siempre, sin importar desde cuál punto en el mundo se conecte en el futuro.[32]

Un ejemplo de estos mecanismos consiste en analizar la forma en que muestra el texto el navegador, para crear, en una fracción de segundo, una huella digital única del dispositivo.

Debido a que un mismo texto se ve diferente en cada dispositivo, conforme al sistema operativo, dimensiones de la pantalla, tarjeta gráfica, controladores de vídeo, tipografías instaladas y navegador web utilizado. Estas diferencias se pueden explotar gracias al elemento “Canvas”, implementado en todos los navegadores web modernos.[33]

30 El lector puede visitar los enlaces https://panopticlick.eff.org/ y https://amiunique.org/fp si desea conocer a mayor detalle algunas de las muchas características que se pueden conocer de su dispositivo.

31 Agencia Española de Protección de Datos, *Estudio Fingerprinting*…, *cit*. pp. 4-8.

32 *Ibídem*, pp. 7-9.

33 Acar, Gunes, *et al.*, “The Web Never Forgets:Persistent Tracking Mechanisms in the Wild”, *CCS ’14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Association for Computing Machinery, 2014, pp. 675-676. https://dl.acm.org/doi/10.1145/2660267.2660347 (Fecha de consulta: 16 de agosto de 2020).

En un estudio “Pixel Perfect: Fingerprinting Canvas in HTML5” de 2012, se utilizaron diferentes métodos para explotar el elemento Canvas. El estudio destacó que incluso una técnica sencilla, consistente en analizar una sola frase, en tipografía Arial tamaño 12, resultaba en una gran cantidad de variaciones entre cada dispositivo. Otros métodos un poco más sofisticados permitían crear huellas digitales con muy alta precisión.[34]

El mismo estudio encontró que la huella digital tenía múltiples propiedades: 1) Consistencia en identificar al mismo usuario en diferentes intentos, 2) Alto nivel de identificación, 3) Independiente y complementario a otras técnicas de huella digital, 4) Es invisible a los ojos del usuario y se realiza en una fracción de segundo y, 5) Se puede ejecutar en cualquier sitio web.

De forma similar, el estudio de 2015 *“Fingerprinting Web Users Through Font Metrics”* analizó más de mil navegadores web, y encontró que incluso métodos sencillos, como el medir la distancia entre el inicio y el fin de un texto, pueden generar una huella digital única que amenaza la privacidad de los usuarios.[35]

Para este método se utilizó el estándar Unicode, en el cual cada carácter, letra o símbolo es representado mediante un número, a estos números se les llama “puntos de código”.[36] En el estudio se utilizó un programa para insertar puntos de código en el navegador y medir la distancia entre sus símbolos correspondientes. El estudio mostró que de los 125,000 puntos de código analizados, bastaba con utilizar 43 para crear huellas digitales rápidas y efectivas.

34 Mowery, Keaton y Shacham Hovav, “Pixel Perfect: Fingerprinting Canvas in HTML5”, *Proceedings of W2SP 2012*, IEEE Computer Society, 2012, pp. 1-10 https://hovav.net/ucsd/papers/ms12.html (Fecha de consulta: 12 de diciembre de 2020).

35 Fifield, David y Egelman, Serge, “Fingerprinting Web Users Through Font Metrics”, *FC 2015: Financial Cryptography and Data Security*, International Conference on Financial Cryptography and Data Security, 2015, pp 107-124, https://link.springer.com/chapter/10.1007%2F978-3-662-47854-7_7 (Fecha de consulta: 12 de diciembre de 2020).

36 W3C, “Appendix E: Accessing code point boundaries” https://www.w3.org/TR/DOM-Level-3-Core/accessing-code-point-boundaries.html (Fecha de consulta: 12 de diciembre de 2020).

Otro análisis, *"Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints"*, de 2016, analizó una gran multitud de métodos de huella digital, y mostró que incluso es posible analizar los emojis, pues al ser parte de Unicode, son tratados como tipografías. Al ser tipografías, la representación de los emojis es diferente en cada sistema, lo que brinda una poderosa herramienta para crear una huella digital única, especialmente en teléfonos móviles, donde cada fabricante tiene una versión propia de emojis.[37]

Incluso los usuarios que tratan de proteger su privacidad se encuentran expuestos a los métodos de huella digital, de acuerdo con datos de la Electronic Frontier Foundation (EFF), organización sin fines de lucro que trabaja en los Estados Unidos para promover la defensa de la libertad de expresión en el contexto de la era digital.

En el estudio *"How Unique Is Your Web Browser?"* la EFF analizó a 470,161 usuarios que habían realizado acciones por defender su privacidad en la web, y encontró que el 83.6% tenían una huella digital única y eran altamente identificables.[38]

Seguimiento con estado

La identificación con estado hace referencia a guardar en el ordenador del usuario los identificadores o rastreadores, para ser consultados y modificados en el futuro.

Muchos sitios web no funcionarían como se espera si no tuvieran estado. El estado permite cuál usuario inició sesión y cuando. Limitando el acceso del usuario exclusivamente a las funciones y contenido que le corresponden.

37 Laperdrix, Pierre *et al.*, "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints", *2016 IEEE Symposium on Security and Privacy*, IEEE, San Jose, 2016, pp. 878-894, https://doi.org/10.1109/SP.2016.57

38 Eckersley, Peter, "How Unique Is Your Web Browser?", *PETS 2010: Privacy Enhancing Technologies. International Symposium on Privacy Enhancing Technologies*, vol 6205. Springer, Berlin, 2010, pp. 1-18, https://doi.org/10.1007/978-3-642-14527-8_1 (Fecha de consulta: 12 de diciembre de 2020)

Uno de los mecanismos de identificación con estado más conocidos y utilizados son las "*Cookies*", sistema de seguimiento de usuarios utilizado por millones de sitios web. Este mecanismo está conformado por dos etapas.

En primer lugar se genera un archivo *cookie*, que contiene un *número de identificación* único asignado por el sitio web, así como información del usuario y su dispositivo. Después, una copia del número de identificación es guardada en el servidor web para identificar y autenticar al usuario, y para dar seguimiento a la actividad que realiza a lo largo del tiempo.[39]

En sus inicios, las cookies eran utilizadas únicamente para brindar funcionalidad básica, como recordar el usuario que inició sesión o recordar los artículos seleccionados para una compra de comercio electrónico. Sin las cookies el usuario tendría que identificarse cada vez, incluso al cambiar de página el navegador olvidaría el inicio de sesión y el usuario tendría que identificarse nuevamente.[40]

Las cookies fueron definidas en 1997 mediante el documento *Request for Comments* (RFC) 2109. Esta primera especificación rechazaba en la sección 4.3.2 el uso de cookies de terceros, para prevenir posibles invasiones a la privacidad y la seguridad del usuario.[41]

En la sección 7 el documento lista los mecanismos que deben existir para que el usuario sea informado y pueda impedir la colocación de cookies de terceros en su ordenador. Esta sección afirma que las cookies de terceros pueden ser vistas como una intrusión, debido la cantidad de información que acumulan sobre los usuarios, aun cuando la identidad del usuario no sea evidente. Además, estas cookies podrían "filtrar" información del usuario a un sitio "incorrecto".

39 Kurose, James y Ross, Keith, *op. cit.*, pp. 108-110

40 Baekdal, Thomas, *The Original Cookie specification from 1997 was GDPR compliant*, octubre 2019, https://baekdal.com/thoughts/the-original-cookie-specification-from-1997-was-gdpr-compliant/ (Fecha de consulta: 18 de mayo de 2020)

41 Kristol, David y Montulli, Lou, "HTTP State Management Mechanism", *Request for Comments 2109*, Grupo de Trabajo de Ingeniería de Internet, febrero 1997, https://tools.ietf.org/html/rfc2109 (Fecha de consulta: 18 de mayo de 2020)

Por último, la sección 8.3 advierte los peligros de usar cookies de terceros y de compartir cookies o su contenido entre diferentes servidores web y servicios. Pues afirma que esto puede problemas severos a la privacidad cuando múltiples partes pueden tener acceso a la información del usuario.

A pesar de lo anterior, las cookies han aumentado su ámbito de aplicación y en la actualidad son utilizadas para objetivos diversos, como análisis del comportamiento o para almacenar información de los hábitos de los usuarios y crear perfiles específicos acerca de ellos.[42] Hoy en día el uso de cookies de terceras partes y el compartir la información obtenida por estas es una práctica común.

De acuerdo con la finalidad y datos que obtienen del usuario, las cookies se clasifican en:[43]1. *Cookies técnicas*: utilizadas para brindar la funcionalidad y servicios básicos de un sitio web: inicio de sesión, realizar una compra o pagos, acceder a contenido restringido por usuario, compartir contenido en redes sociales, entre otros.[44]

2. *Cookies de preferencias*: utilizadas para recordar las configuraciones establecidas por el usuario: idioma, el aspecto del sitio web, cantidad de resultados a mostrar, etcétera.[45]

3. *Cookies de análisis*: No brindan funcionalidad directa al usuario, por el contrario tienen por objetivo analizar su comportamiento, y medir sus actividades.[46]

4. *Cookies de publicidad y perfilamiento*: Tampoco brindan funcionalidad directa al usuario. Se utilizan para la vigilancia y seguimiento al comportamiento

42 Agencia Española de Protección de Datos, *Guía sobre el uso de las cookies*, julio 2020, pp. 11-12, https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (Fecha de consulta: 29 de junio de 2021)

43 Information Commisioner's Office, *What are cookies and similar technologies?*, https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/ (Fecha de consulta: 29 de abril de 2020) Cookiepedia, *How We Classify Cookies*, https://cookiepedia.co.uk/classify-cookies (Fecha de consulta: 29 de abril de 2020)

44 *Idem.*

45 *Idem.*

46 *Idem.*

de los usuarios y permiten desarrollar perfiles específicos de cada uno. Pueden ser utilizadas con fines publicitarios y para recolectar información de personas que han rechazado suscribirse a determinados servicios.[47]

Las cookies suelen ser utilizadas en conjunto con las técnicas de huella digital para guardar y registrar la información que se obtuvo del usuario y sus dispositivos, por ejemplo: tamaño y resolución de pantalla; la posición geográfica incluyendo país, región, ciudad, y coordenadas de GPS de longitud y latitud; fecha y hora de visita. Esto en conjunto con la información que se obtuvo mediante cookies, como páginas visitadas dentro del sitio web, otros sitios web visitados con anterioridad, búsquedas, idioma, entre otros.[48]

Seguimiento con Navegador

En el inicio de la sección **1.2.1 ¿Cómo funciona el seguimiento web?**, se mencionó que el seguimiento web comienza y es ejecutado por la página web que visita el usuario. Si bien esto es correcto, también existen navegadores que, por sí mismos, dan seguimiento a la actividad del usuario.

El navegador web tiene acceso a toda la información del usuario: historial, cookies, sitios donde se inició sesión, contraseñas, etcétera. En años recientes, las compañías que desarrollan navegadores web han comenzado a explotar este acceso para rastrear e informar la actividad de sus usuarios.

Este seguimiento es realizado por los navegadores más importantes a nivel mundial y que cubren casi la totalidad del mercado: Google Chrome, Apple Safari, Mozilla Firefox y Microsoft Edge.[49]

El estudio "*Web Browser Privacy: What Do Browsers Say When They Phone Home?*" publicado en febrero de 2020 explica que el seguimiento con navegadores no suele ser objeto de análisis cuando se investiga el impacto del

47 *Idem.*

48 El lector podrá encontrar interesante leer la política de Cookies con toda la información que recolecta de forma predeterminada incluso por el Comité Europeo de Protección de Datos en su sitio web: https://edpb.europa.eu/cookies_es También la información que recolecta el Supervisor Europeo de Protección de Datos: https://edps.europa.eu/about-edps/legal-notices_en

49 Agencia Española de Protección de Datos, *Estudio Fingerprinting*…, *cit*.pp. 7.

seguimiento web. Pues la mayoría de los investigadores asumen que el navegador es una plataforma confiable.[50]

El mismo estudió encontró que navegadores como Chrome, Edge, Firefox, Safari y Yandex vinculan a cada usuario con un número identificador, informan sobre las páginas visitadas, hardware del usuario, informan a terceras partes, entre otros comportamientos poco éticos. Esta información es transmitida desde que se inicia el navegador por primera vez. Los identificadores son persistentes aun si se reinicia el navegador a los valores de fábrica. También se encontró que estas actividades representan un potencial riesgo para la seguridad y privacidad pues terceras partes pueden ganar acceso a la información de los usuarios.[51]

En este mismo sentido, se ha identificado que el navegador Google Chrome para el sistema operativo Android envía la posición de GPS del dispositivo cada vez que el usuario realiza una búsqueda.[52]

1.2.3 Identificación de Usuarios

Luego de haber explicado los mecanismos de seguimiento web, se explica ahora cómo estos mecanismos son utilizados para identificarnos en la web, aun si no hemos proporcionado nuestro nombre al sitio visitado.

En la web nuestros datos distan de ser anónimos, en realidad son "pseudoanónimos" pues es relativamente sencillo identificar a un usuario, y continuar perfilándolo tanto sus interacciones presentes, pasadas y futuras.[53]

Constantemente se desarrollan nuevas formas de identificación, por lo que es importante tener en cuenta que la siguiente es una lista de ejemplos concretos,

50 Leith, Doug, *Web Browser Privacy: What Do Browsers Say When They Phone Home?*, febrero 2020, https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf (Fecha de consulta: 12 de agosto de 2020)

51 *Idem.*

52 Fowler, Geoffrey, *Goodbye, Chrome: Google's Web browser has become spy software*, The Washington Post, junio 2019, https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch/ (Fecha de consulta: 12 de agosto de 2020)

53 R. Mayer, Jonathan y C. Mitchell, John, *op. cit.*, p. 415.

de los muchos métodos que existen para identificar y dar seguimiento a cada usuario.[54]

1. La tercera parte es también una primera parte

Este tipo de seguimiento web ocurre cuando se utilizan servicios de grandes compañías de rastreo y seguimiento de usuarios como Google o Facebook. Estas empresas son dueñas de sitios web que los usuarios visitan directamente: `google.com`, `youtube.com`, `facebook.com`, `instagram.com`, entre otros.

Pero también funcionan como terceras partes, dando seguimiento a la actividad del usuario en otros sitios web que visita. Estos rastreadores son comunes en páginas web de todo tipo, desde negocios, ocio, noticias, e incluso en escuelas y páginas oficiales de gobierno. En la **sección 1.4 Panorama del seguimiento web**, el lector puede encontrar estadísticas la cantidad de sitios web que utilizan este tipo de rastreadores.

Debido a que las políticas de Facebook y Google cada vez exigen más información a sus usuarios, como nombre completo y número de teléfono celular,[55] en conjunto los mecanismos de seguimiento web; estas empresas pueden identificar de forma precisa cuál usuario ha visitado el sitio web, aun si previamente el usuario cerró sesión y reinició el navegador.[56]

54 Narayanan, Arvind, *There is no such thing as anonymous online tracking*, The Center for Internet and Society, julio 2011, https://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking (Fecha de consulta: 19 de mayo de 2021)

55 En la actualidad ambas empresas son muy estrictas al respecto y no permiten la creación de cuentas sin estos datos. Véanse: Google, *Create a Google Account*, Google Account Help, https://support.google.com/accounts/answer/27441?hl=en&ref_topic=3382296 (Fecha de consulta: 12 de agosto de 2020), y Facebook, *Creating an Account*, Facebook Help Center, https://www.facebook.com/help/570785306433644/?helpref=hc_fnav (Fecha de consulta: 12 de agosto de 2020).

56 R. Mayer, Jonathan y C. Mitchell, John, *op. cit.*, pp. 415-416.

2. Filtros de identificadores de la primera parte a sitios de terceras partes

Existe información que la primera parte no comparte de con los rastreadores de terceras partes. Pero por errores o por negligencia, se pueden filtrar los datos a terceros, incluyendo datos sensibles, lo que también permite identificar al usuario.[57]

Entre estos casos se incluyen:

- El sitio web realiza peticiones HTTP incluyendo el correo electrónico o el número de identificación del usuario.
- La petición HTTP incluye otro tipo de información que puede identificar al usuario, como género, código postal, intereses.
- Los identificadores se incluyen en las cookies compartidas en lugar de en las peticiones HTTP.
- El nombre real del usuario es incluido en el título de la página web.

3. Venta de datos a terceras partes

En los últimos años han surgido negocios en la web dedicados a la recolección y venta de datos de usuarios. Estos datos pueden ser proporcionados de forma voluntaria por los usuarios de la página web, por ejemplo al contestar una encuesta o participar en juego. Los datos también son obtenidos por rastreadores incluidos en el sitio web. Estos datos luego son vendidos a terceras partes.[58]

4. Vulnerabilidades de seguridad

La explotación de vulnerabilidades de seguridad, tanto del navegador, del servidor, o de la comunicación entre estos, también permite identificar a un usuario, aunque este método suele ser ilegal, puede ser explotado por entes maliciosos.

El descubrimiento de vulnerabilidades de seguridad es muy común. Un caso reciente es el Navegador Google Chrome. En 2020 un equipo de investigadores de seguridad descubrió más de 70 extensiones maliciosas que se

57 Narayanan, Arvind, *op. cit.*

58 *Idem*.

podían descargar en la “Tienda Chrome”. Estas extensiones ya superaban 32 millones de descargas y habían filtrado información como las contraseñas almacenadas en el navegador, así como el historial de búsquedas.[59]

5. Desanonimización

Las tercera partes que recibe datos que su supone son “anónimos”, tienen forma de volver a vincular la identidad de los datos con el usuario que los originó, proceso que es conocido como “desanonimizar”.[60]

El proceso puede ser bastante sencillo. Por ejemplo, un usuario visita en un mismo día su sitio favorito de recetas de cocina, lee un artículo acerca de la ciudad donde vive y visita el sitio web de algún amigo, y otros más sitios web. Todas estas actividades son comunes para este usuario en particular. Pero pocos usuarios, probablemente ningún otro, visita estos mismos sitios web. Una tercera parte puede utilizar estos datos para encontrar actividades similares antiguas en sus bases de datos e identificarlo.[61]

Técnicas más avanzadas pueden utilizar la huella digital de dispositivo. Un ejemplo claro se encuentra en las técnicas que permiten desanonimizar mediante el análisis del texto mostrado en el navegador, como se explicó previamente en la **sección 1.2.2 Mecanismos de seguimiento web**.

Otra forma en que una tercera parte puede identificar a un usuario es comparando la hora y lugar en que el usuario visitó un sitio web con los enlaces publicados a este sitio web por usuarios de redes sociales.[62]

59 Menn, Joseph, *Exclusive: Massive spying on users of Google’s Chrome shows new security weakness*, Reuters, junio 2020, https://www.reuters.com/article/us-alphabet-google-chrome-exclusive/exclusive-massive-spying-on-users-of-googles-chrome-shows-new-security-weakness-idUSKBN23P0JO (Fecha de consulta: 20 de mayo de 2021)

60 *Anonimizar y desanonimizar, neologismos válidos*, FundéuRAE, junio 2019, https://www.fundeu.es/recomendacion/anonimizar-desanonimizar/ (Fecha de consulta: 15 de diciembre de 2020)

61 Narayanan, Arvind, *op. cit.*

62 R. Mayer, Jonathan y C. Mitchell, John, *op. cit.*, p. 416.

1.3 Panorama del seguimiento web

1.3.1 ¿Quienes me sigue en la web?

Como parte del estudio *"Beyond the Front Page: Measuring Third Party Dynamics in the Field"* realizado en 2020, analizaron los 10 mil sitios web más visitados y con mayor tráfico en Internet, se encontró que el 99% de las cookies son utilizadas con la intención de rastrear y dar seguimiento a los usuarios, utilizando una clasificación de cookies similar a la explicada anteriormente en la **sección 1.2.2 Mecanismos de seguimiento web**.[63]

Como parte del análisis, se encontró que un 93% de los sitios web utilizaban servicios de terceros, pese a que el uso de estos servicios podrían implicar problemas legales, ya que el estudio encontró que los sitios no suelen cumplir con las legislaciones correspondientes en materias de protección de datos personales.

De la misma forma, en 2016 se realizó un análisis al primer millón de sitios web más visitados, para conocer el estado del seguimiento y vigilancia a usuarios, y en el cual se tomaron en cuenta 15 tipos de técnicas de seguimiento incluidas técnicas con estado basadas en cookies, y sin estado basadas en huellas digitales. Este estudio, llamado *"Online Tracking: A 1-million-site Measurement and Analysis"* encontró que tan solo los rastreadores de la empresa Google se encontraban presentes en casi un 70% de los sitios web. También encontró que la mayoría de las terceras partes realizan "cookie-syncing" es decir que comparten identificadores de usuarios entre ellas, encontrado que la empresa Google compartía 108 diferentes cookies con 118 terceras partes.[64]

Es evidente que el uso de rastreadores para el seguimiento web es algo común, pero para entender a fondo cuáles son sus implicaciones es importante analizar quién da seguimiento a los usuarios y con qué objetivos.

63 Urban, Tobias, *et al.*, *op. cit*., pp. 10-12.

64 Englehardt, Steven y Arvind, Narayanan. "Online Tracking: A 1-million-site Measurement and Analysis", *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, octubre 2016, pp. 1388–1401, https://dl.acm.org/doi/10.1145/2976749.2978313 (Fecha de consulta: 29 de abril de 2020)

Los rastreadores web con mayor alcance son claramente los creados por la industria privada, especialmente los creados por la empresa Google, pues los estudios citados anteriormente han encontrado que los rastreadores de esta empresa se encuentran presentes en la mayoría de los sitios web más visitados.

Aunque, un estudio diferente realizado de 2017 a 2018 en más de mil quinientos millones de páginas visitadas por más de 5 millones de usuarios, encontró que rastreadores de la empresa Google se encontraban presentes en el 82% de los sitios web, mientras que rastreadores de la empresa Facebook se encontraban presentes en casi el 30%, la empresa Amazon llegaba casi al 20%.[65] También se destacaron los rastreadores de ComScore, Twitter, Criteo, Microsoft, Oracle y AppNexus.[66]

1.3.2 El negocio del seguimiento web - ¿Cómo lucran con mis datos?

En la **sección 1.3.1 ¿Quienes me siguen en la Web?**, se listaron cuáles son las principales compañías de seguimiento web, a continuación se listan algunas de las formas en que estos servicios pueden realizan negocios con los datos personales que recaban. Si bien se listan solo algunas, es importante señalar que podrán surgir nuevos métodos a la par del avance tecnológico.

De acuerdo con la Electronic Frontier Foundation, existen dos métodos principales en que las compañías de seguimiento web lucran en la actualidad con los datos de los usuarios.[67] Sin embargo, existen otros tipos negocios que si bien pueden no ser tan lucrativos, también tienen repercusiones a la privacidad de los usuarios. A continuación se listan algunos de ellos.

65 Karaj, Arjaldo, *et al.*, *op. cit.*, pp. 8-3.

66 El lector puede visitar https://whotracks.me/trackers.html para conocer los principales rastreadores web, ordenados por uso o compañía. Este sitio web es creado por los autores del estudio citado. (Fecha de consulta: 27 de junio de 2021)

67 Cyphers, Bennett y Gebhart, Gennie, “Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance”, *Electronic Frontier Foundation*, diciembre 2019, https://www.eff.org/wp/behind-the-one-way-mirror (Fecha de consulta: 29 de junio de 2020)

Subasta en Tiempo Real (*Real-Time Bidding*)

Este modelo de negocios consiste en la subasta de espacios publicitarios específicos a cada usuario. En el modelo tradicional la publicidad se vendía por volumen. En cambio, este novedoso modelo utiliza características exclusivas de cada usuario: demográficas, psicográficas (estudio y clasificación de las personas basado en la personalidad, estilo de vida, actividades, intereses, opiniones, actitudes, aspiraciones y otros criterios psicológicos)[68] y atributos de comportamiento. Para lo cual se analiza a cada usuario, en todos estos rubros y por múltiples compañías, momentos antes de mostrarle publicidad.[69]

El sistema de Subasta en Tiempo Real ocurre en solo unas milésimas de segundo y es posible gracias a la velocidad actual de las computadoras. La subasta funciona de esta forma:[70]

1. Un usuario visita una página web que contiene un espacio donde se le mostrará un anuncio.

2. En ese momento, la empresa de seguimiento web pone en subasta este espacio publicitario.

3. Para lo cual, informa a las compañías interesadas en mostrar la publicidad y participar en la subasta con un paquete de datos.

4. El paquete, en forma de cookie, incluye todos los datos del usuario, de su dispositivo y del tipo de espacio publicitario.[71] La información del usuario incluye:

68 Ciribeli, João Paulo y Miquelito, Samuel, “La segmentación del mercado por el criterio psicográfico: un ensayo teórico sobre los principales enfoques psicográficos y su relación con los criterios de comportamiento”, Visión de Futuro, Vol. 19, N 1, 2015, pp. 33-50, http://www.scielo.org.ar/pdf/vf/v19n1/v19n1a02.pdf (Fecha de consulta: 13 de julio de 2020).

69 Interactive Advertising Bureau, “About OpenRTB”, Interactive Advertising Bureau, https://www.iab.com/guidelines/real-time-bidding-rtb-project/ (Fecha de consulta: 13 de julio de 2020).

70 Cyphers, Bennett y Gebhart, Gennie, *op cit.*

71 La especificación de todos los objetos utilizados por el sistema OpenRTB es amplia. Pero se recomiendan revisar los objetos “Object: User”, “Object: Device” y “Object: Geo”, para conocer todos los atributos de usuario, dispositivo y posición geográfica que son utilizados pero este sistema. La consulta puede realizarse en: Interactive Advertising Bureau, “AdCOM Specification v1.0”, IAB Tech Lab. https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md (Fecha de consulta: 05 de julio de 2020).

número de identificación del usuario en el sitio web, número de identificación del usuario en la compañía publicitaria, año de nacimiento, género del usuario: hombre, mujer, otro; intereses del usuario, consentimiento de transferencia de datos, posición geográfica donde vive el usuario (aun si el usuario se encuentra en otro lugar en ese momento), información adicional del usuario, e incluso, otros identificadores de terceras partes para este mismo usuario.

La información del dispositivo del usuario incluye: Sistema operativo y versión; navegador y versión; dirección IP; fabricante, modelo y versión del dispositivo; largo, ancho y relación de aspecto de la pantalla; lenguaje, proveedor de servicios de Internet o compañía de teléfono celular; tipo de conexión, tipo de red, número de identificación del dispositivo y dirección MAC del dispositivo.

5. La empresa que recibe el paquete analiza al usuario y decide si le interesa o no mostrarle publicidad.

6. Las empresas que tienen interés en mostrar publicidad realizan una oferta o puja, la empresa que gana la subasta es la que muestra publicidad al usuario.

Para fines del presente trabajo, se ha simplificado la explicación del sistema de Subasta en Tiempo Real, pero hoy en día, estos sistemas se han vuelto mucho más complejos, hoy en día hay compañías que al ganar la subasta comienzan su propia Subasta en Tiempo Real, lo que puede llevar a cadenas de transacciones que han vuelto el ecosistema complicado y facilitan múltiples formas de fraudes y vulneraciones de seguridad y a los datos de los usuarios.[72]

Es importante destacar que este tipo de sistemas representan más del 80% de los espacios publicitarios digitales de la actualidad, y que cada año aumenta su alcance y las ventas de estos espacios.[73]

72 Bashur, Muhammad Ahmad, “On the Privacy Implications of Real Time Bidding”, *Tesis de Doctorado*, Northeastern University, 2019, http://www.ccs.neu.edu/home/ahmad/publications/bashir-thesis.pdf (Fecha de consulta: 03 de julio de 2020).

73 Abramovich, Giselle, “15 Mind-Blowing Stats About Programmatic Advertising”, CMO Adobe, 2017, https://cmo.adobe.com/articles/2017/9/15-mind-blowing-stats-about-programmatic-advertising.html#gs.dizpzi (Fecha de consulta: 14 de julio de 2020).

Se ha señalado que es innecesario que sean transmitidos los datos personales del usuario para el funcionamiento ni la efectividad de este sistema, ya que los anuncios podrían ser relevantes de acuerdo al contexto, sin necesidad de analizar datos personales. Sin embargo, estos sistemas continúan utilizando perfiles de los usuarios, pese a la falta de protección a los datos personales.[74]

De acuerdo a una serie de quejas presentadas en 2018 ante las autoridades de protección de datos personales del Reino Unido y de Irlanda, contra las Subastas en Tiempo Real por presuntas violaciones al Reglamento General de Protección de Datos de la Unión Europea (RGPD),[75] en la actualidad existen dos sistemas principales dedicados a la publicidad mediante el sistema de Subasta en Tiempo Real: OpenRTB, utilizado por más de 650 compañías,[76] consideradas las más importantes en el negocio de medios de comunicación y publicidad; y "Authorized Buyers" el sistema creado por Google anteriormente conocido como "DoubleClick Ad Exchange".[77] Aunque Google utiliza tanto OpenRTB como su propio sistema.[78]

Las quejas anteriormente mencionadas, denunciaban que estos sistemas no tienen un control sobre la cantidad de datos íntimos del usuario que son procesados en una solicitud de subasta, lo que, de acuerdo con estas quejas,

74 Ryan, Johny, "Report from Dr Johnny Ryan – Behavioural advertising and personal data", 2018, https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf (Fecha de consulta: 13 de agosto de 2020).

75 Ryan, Johny, "Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR", 2018, https://brave.com/adtech-data-breach-complaint/ (Fecha de consulta: 13 de agosto de 2020).

76 Entre las empresas que lo utilizan se encuentran empresas de cine, televisión, noticias, videojuegos, software, librerías, deportes, bancos, internet, seguros, alimentos, entre otros, para una lista detallada vease: Interactive Advertising Bureau, "Member Directoy", Interactive Advertising Bureau, https://www.iab.com/our-story/ (Fecha de consulta: 13 de julio de 2020).

77 Ryan, Johnny, *et al.*, "Grounds of complaint to the Data Protection Commissioner", 2018, https://brave.com/wp-content/uploads/2018/09/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf (Fecha de consulta: 13 de agosto de 2020).

78 Authorized Buyers, OpenRTB Integration", Google, https://developers.google.com/authorized-buyers/rtb/openrtb-guide (Fecha de consulta: 05 de julio de 2020).

violaría el artículo 5 punto 1 inciso f) del RGPD que indica que los datos personales deben ser:

"*f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad").*"[79]

Publicidad Dirigida por Datos Personales

La Subasta en Tiempo Real no es la única forma en que lucran las empresas de seguimiento web. Otro modelo de negocios de la actualidad es la llamada Publicidad Dirigida, que también puede incluir el uso datos personales.

Las empresas de seguimiento web se dedican, como parte integral de su negocio, a la publicidad basada en comportamientos (*behavioral advertising*), lo que les permite mostrar publicidad personalizada basada en los atributos de los usuarios, desde la orientación sexual, hasta el estado de humor e incluso ciclo menstrual.[80]

Esta práctica se ha extendido al grado de permitir dirigir anuncios a personas en específico. Cualquiera puede utilizar una lista con datos específicos de un grupo de personas, ya sea nombre, correo electrónico, número de teléfono, etcétera, con lo que se puede especificar a quién se va a mostrar la publicidad, aún sin haber obtenido el consentimiento de dichas personas, pues basta tener sus datos para poder mostrarles publicidad. Esta lista se sube directamente a la

79 Diario Oficial de la Unión Europea, "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)", 2016, https://www.boe.es/doue/2016/119/L00001-00088.pdf (Fecha de consulta: 28 de junio de 2020).

80 Edelman, Gilad, "Why Don't We Just Ban Targeted Advertising?", Wired, 22 de marzo de 2020, (Fecha de consulta: 13 de diciembre de 2020).

plataforma de la compañía de seguimiento web. Así es como funcionan tanto los servicios de Google[81] como de Facebook.[82]

Si bien el mostrar publicidad podrá parecer inocente y no malicioso, ya han surgido problemas por el poco cuidado que las empresas de seguimiento web han puesto en proteger a sus usuarios.[83]

Cualquiera puede subir una lista de dispositivos o números de teléfono "anónimos", y, gracias a estos servicios, puede contactar a personas reales en sus dispositivos: teléfonos inteligentes, computadoras, televisiones. Si una persona interactúa con estos anuncios, aún por error, podría entregar sin darse cuenta información cómo: número de identificación de cookie, número de IP, dirección GPS y más.[84]

Este ha facilitado que se filtren datos sensibles de los usuarios, sin que las víctimas puedan protegerse. Todo gracias a que las compañías de seguimiento web guardan información detallada de cada usuario. Se ha demostrado que la plataforma de Facebook ha sido explotada para inferir números de teléfono o direcciones de correo electrónico, incluso sin necesidad de mostrar publicidad a las víctimas, lo que facilitó la violación de la privacidad de celebridades y políticos, la identificación de ciudadanos por parte de gobiernos opresivos y ataques a la intimidad, privacidad y seguridad de los usuarios de esta plataforma.[85]

81 Google Ads Help, "About Customer Match", Google, https://support.google.com/google-ads/answer/6379332?hl=en (Fecha de consulta: 13 de diciembre de 2020).

82 Facebook for Business, "About Lookalike Audiences", https://www.facebook.com/business/help/164749007013531?id=401668390442328 (Fecha de consulta: 13 de diciembre de 2020).

83 Cyphers, Bennett, "Google Says It Doesn't "Sell" Your Data. Here's How the Company Shares, Monetizes, and Exploits It", Electronic Frontier Foundation, 19 de marzo de 2020, https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and (Fecha de consulta: 14 de diciembre de 2020).

84 *Idem*.

85 Venkatadri, Giridhari, *et al.*, "Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface", *2018 IEEE Symposium on Security and Privacy*, San Francisco, 2018, pp. 89-107, https://ieeexplore.ieee.org/document/8418598f (Fecha de consulta: 14 de diciembre de 2020).

Es relevante la anécdota de Brian Swichkow, quien en 2014 detalló como realizó una “broma” a su compañero de cuarto, utilizando la plataforma de anuncios dirigidos de Facebook.[86]

Swichkow creó un archivo CSV (*Comma-Separated Values*) en el que únicamente incluía la dirección de correo electrónico de su compañero. Después, utilizó la plataforma de Facebook para crear una campaña publicitaria, esto le permitió asustar a su compañero de cuarto utilizando bizarros anuncios publicitarios que Swichkow había creado dirigidos específicamente a su compañero.

Swichkow cambiaba los anuncios día con día, haciendo referencia a la vida de su compañero, quien trabajaba en un espectáculo como traga-espadas, y al mismo tiempo, tenía dificultad para tragar incluso pequeñas pastillas. Swichkow diseñó anuncios sobre la ironía de esta situación y otros sucesos de la vida diaria de su compañero.

Pese a ser una simple broma, su compañero de cuarto se llegó a sentir estresado y ansioso al no entender las razones por las que Facebook le mostraba anuncios específicamente dirigidos a su persona y las vivencias de su día a día. Swichkow relata que se sintió culpable de la tortura psicológica a la que había sometiendo a su compañero, quien comenzaba a actuar paranoico. Por lo que, después de 3 semanas de anuncios decidió terminar con la broma. ¿El costo total? Dos dólares.

Si bien este caso resulta chusco y no pasó de simple una broma, también ilustra lo sencillo que es dirigir anuncios a una persona en concreto. Un atacante malicioso podría crear anuncios con los intereses de la víctima, mostrarle anuncios durante algunas semanas y llevarla a hacer click en un sitio web malicioso o realizar alguna acción que podría poner en peligro a la víctima.

86 Swichkow, Brian, “The Ultimate Retaliation: Pranking My Roommate With Targeted Facebook Ads”, Ghost Influence, 6 de septiembre de 2014. https://ghostinfluence.com/the-ultimate-retaliation-pranking-my-roommate-with-targeted-facebook-ads/ (Fecha de consulta: 14 de diciembre de 2020).

Venta de datos

Otro modelo de negocio es la venta directa de datos. En la actualidad, miles de empresas, conocidas como Corredores de Datos (*Data Brokers*), lucran con este tipo de negocios. Los corredores de datos se dedican a recolectar, compilar, comprar y vender datos personales, es decir información sobre quiénes somos y nuestras actividades en línea.[87]

Los corredores de datos no necesariamente se dedican al seguimiento web de forma directa, sin embargo, se dedican a recolectar la información obtenida mediante el seguimiento web por parte de otras empresas. En 2019 el estado de Vermont, en los Estados Unidos, aprobó una ley exigiendo a los corredores de datos registrarse para poder operar. Como resultado 120 compañías se registraron.[88]

Los corredores de datos reportaron tener en sus bases de datos perfiles que incluyen información como edad, género, educación, empleos, opiniones políticas, situación sentimental, número de hijos, prestamos, ingresos, religión, salud, consumo de drogas, alcohol y tabaco, horas de uso en redes sociales, facilidad de ser influenciado, personalidad, e incluso análisis de comportamientos en el día a día.[89]

Entre este tipo de empresas destaca Acxiom, que ha sido calificada como la "más grande empresa de la que nunca has escuchado", una de las empresas

87 Dixon, Pam, "Congressional Testimony: What Information Do Data Brokers Have on Consumers?", World Privacy Forum, diciembre de 2013. https://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/ (Fecha de consulta: 14 de diciembre de 2020).

88 Melendez, Steven y Pasternack, Alex. "Here are the data brokers quietly buying and selling your personal information", Fast Company, 2 de marzo de 2019, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information (Fecha de consulta: 14 de diciembre de 2020).

89 Christl, Wolfie, "Overview: Corporate Surveillance in Everyday Life", Cracked Labs, junio 2017, https://crackedlabs.org/en/corporate-surveillance (Fecha de consulta: 15 de diciembre de 2020).

pioneras en el negocio de comprar información personal, segmentarla, y venderla a negocios para ser usada en el mercado.[90]

De acuerdo con información de Acxiom, en 2017 ya tenía información de más de 2.5 mil millones de personas del mundo, de las 7 mil millones que había vivas. En comparación Facebook reportaba tener 1.32 mil millones de usuarios. Tan solo en México, Axciom reporta tener una alcance de 77 millones de mexicanos, el 84% de la población.[91]

Es posible utilizar la plataforma de Acxiom para consultar información sobre una persona, lugar, casa o entidad. La información de cada persona se clasifica en más de 3 mil categorías, incluyendo:[92]

- Datos de Contacto: Nombre, dirección, código postal, ciudad, correo electrónico, número de teléfono.
- Datos Demográfica: Edad, género, educación, estado laboral, estado civil, número de hijos, etnia, religión, estilo de vida.
- Datos de uso de canales de comunicación: Correo tradicional, mensajes de texto, de internet, radio, revistas, periódicos. Proveedores de dicho servicios. Que tan probable es que la persona utilice Facebook, cuántas horas, probabilidades de responder una publicación en redes sociales, probabilidad de ser influenciado por redes sociales.
- Datos Económicos: Prestamos, ingresos, estabilidad económica, capacidad económica, estado socioeconómico, detalles de uso de bancos y pólizas de seguros, detalles de vehículos, casas y otras propiedades.
- Datos de Actividades e Intereses: Restaurantes visitados, intereses en colecciones, arte, entretenimiento, manualidades, ejercicio, gustos de

90 Marr, Bernard, “Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers”, Forbes, 7 de septiembre de 2017. https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/?sh=7b650fe86c27 (Fecha de consulta: 15 de diciembre de 2020).

91 “Reach Over 2.5 Billion of the World’s Marketable Consumers”, Acxiom, 2017, https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20Global%20Data.pdf (Fecha de consulta: 15 de diciembre de 2020).

92 Data Bundles, Acxiom. https://developer.myacxiom.com/code/api/data-bundles/main (Fecha de consulta: 14 de diciembre de 2020).

comida y bebidas, intereses generales, grupos a los que pertenece, mascotas, lectura, superación personal, viajes, deportes y actividades al aire libre, consumo de alcohol y tabaco, casino y lotería, juegos y videojuegos.

- Datos de Salud: Artritis y movilidad, salud cardiovascular, diabetes, discapacidades, seguro médico.
- Datos de Casa: Número de cuartos, tipo de casa, incluido casa remolque, multifamiliar o en prisión. Si en la casa vive: una mujer embarazada, una persona divorciada, un recién graduado, una persona planeando tener un bebé, una persona planeando adoptar un niño, un futuro abuelo o una persona que cambiará de trabajo.
- Datos de Crédito: Uso de tarjeta de crédito en los últimos 24 meses, limite de crédito, historial crediticio.

Acxiom no es la única que registra este tipo de datos, otra empresa destacada es Oracle, que cuenta con una base de datos con perfiles de más de dos mil millones de personas y más de 30,000 atributos por persona, además de procesar, registrar y guardar más de 700 millones de mensajes de redes sociales cada día; y procesar información de las compañías Facebook, Visa, Mastercard, TransUnion, i-Behavior, Experian, Proxama, VisualDNA, Lotame, entre otras.[93]

En 2014 la Comisión Federal de Comercio de los Estados Unidos publicó un estudio sobre los corredores de datos, donde reconoció la importancia del uso de los datos en la actualidad, pero recordó que la recolección y uso de los datos personales crean riesgos para las personas.[94]

Debido a los riesgos inherentes a que los corredores de datos manejen datos sensibles, como información de salud o financiera, la cual mantienen de forma indefinida y que puede filtrarse a un ente malicioso. O que puede utilizarse para negar a un consumidor el poder realizar una transacción, como comprar un

93 Christl, Wolfie, “Report: Corporate Surveillance in Everyday Life”, Cracked Labs, pp. 54-63 junio 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf (Fecha de consulta: 15 de diciembre de 2020).

94 Federal Trade Comission, “Data Brokers A Call for Transparency and Accountability”, pp. 47-49, mayo 2014, (Fecha de consulta: 15 de diciembre de 2020).

seguro u obtener un préstamo, dañando al consumidor sin que este sepa por qué y sin que pueda tomar acciones para solucionarlo.[95]

1.3.3 ¿Qué pueden saber de mí?

Una vez que se han recolectado datos y huella digital del dispositivo y se ha identificado al usuario, la compañía de seguimiento web o algún ente malicioso, necesita encontrar la información que le es útil entre la gran cantidad de datos. Para esto analizan los datos con diferentes técnicas.

Una técnica eficiente es el *minado web* (*web mining*), consistente en la extracción de información de sitios web, y el *minado de uso web* (*web usage mining*), que solo extrae los datos de usuarios, recolectados al acceder y utilizar un sitio web.[96]

Los datos de los usuarios suelen incluir: detalles de tarjeta de crédito, dirección IP, historial de páginas visitadas, tiempo de visita, sesiones iniciadas, etcétera. Con el minado de uso web se recolecta, analiza y procesa esta información. Métodos matemáticos permiten identificar los comportamientos de los usuarios, e incluso predecir de forma "altamente precisa" sus comportamientos futuros.[97]

Otra técnica muy utilizada en la actualidad es el llamado *minado de datos* (*data mining*) en conjunto con el *análisis predictivo* (*predictive analytics*) estas técnicas son utilizadas por las compañías para predecir múltiples aspectos de la personalidad de los usuarios, incluida información sensible.[98]

95 *Idem*.

96 Michele Facca, Federico y Luca Lanzi, Pier, "Mining interesting knowledge from weblogs: a survey", *Data & Knowledge Engineering*, vol 53, num 3, 2005, pp. 225-226, http://www.sciencedirect.com/science/article/pii/S0169023X04001387 (Fecha de consulta: 29 de junio de 2020).

97 M. John, Joan, *et al.*, "User Profile Tracking by Web Usage Mining in Cloud Computing", *Procedia Engineering*, vol 38, 2012, pp. 3272, 3276, http://www.sciencedirect.com/science/article/pii/S1877705812022916 (Fecha de consulta: 29 de junio de 2020).

98 Christl, Wolfie y Spiekermann, Sarah, *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* Vienna, Facultas, 2016, pp. 11-14

Las conclusiones sobre los usuarios están basadas en estadística, sin embargo, las compañías las consideran lo suficientemente buenas para organizar, calificar y clasificar a las personas de forma automatizada. Aunque mayoría de las compañías mantienen en secreto los detalles de cómo analizan los datos de los usuarios.[99]

Para ilustrar como se pueden predecir comportamientos presentes o futuros de los usuarios, se destacan tres estudios realizados por ingenieros trabajando para Facebook.

El primero: lograron predecir la pareja de sus usuarios, para esto diseñaron un "poderoso método" que les permitió predecir con "gran exactitud", cuanto tiempo duraría una relación de pareja que acababa de comenzar, gracias al análisis de los lazos sociales que tenía cada pareja en la red social.[100] El segundo estudio versó sobre la duración de las relaciones de pareja. Para este estudio, se analizaron las relaciones de parejas de 2008 a 2011, y podían predecir cuantos años duraría dicha relación.[101]

De forma similar, el presidente de Facebook, Mark Zuckerberg ya había declarado en 2010 que podía declarar con un 33% de exactitud que solteros comenzarían una relación en la siguiente semana y con quien.[102] El tercero sobre la cantidad de apoyo y soporte emocional que recibirían los usuarios tras terminar una relación de pareja, por parte de sus amistades y familiares.[103]

http://crackedlabs.org/en/networksofcon (Fecha de consulta: 10 de julio de 2021).

99 *Idem*.

100 Backstrom, Lars y Kleinberg, Jon, Romantic Partnerships and the Dispersion of Social Ties: A Network Analysis of Relationship Status on Facebook, Computing Research Repository, 2013, http://arxiv.org/abs/1310.6753 (Fecha de consulta: 12 de agosto de 2020).

101 State, Bogdan, "Flings or Lifetimes? The Duration of Facebook Relationships", Facebook Data Science, 2014, https://www.facebook.com/notes/facebook-data-science/flings-or-lifetimes-the-duration-of-facebook-relationships/10152060513428859 (Fecha de consulta: 12 de agosto de 2020).

102 Tate, Ryan, "Facebook Knows Who You'll Hook Up With", Gawker, 2010, https://gawker.com/5543723/facebook-knows-who-youll-hook-up-with (Fecha de consulta: 12 de diciembre de 2020).

103 Friggeri, Adrien, "When Love Goes Awry", Facebook Data Science, 2014, https://www.facebook.com/notes/facebook-data-science/when-love-goes-awry/

En este mismo sentido, el sitio web eHarmony, (dedicado a encontrar pareja a sus usuarios), reportó en 2018 en conjunto con la Escuela Imperial de Londres que las tecnologías de reconocimiento de voz que funcionan en asistentes personales conectados a la web, como Alexa o Google Home, pueden utilizarse para detectar cuando una pareja tiene problemas o incluso cuando va a terminar la relación.[104] La aplicación móvil StayGo utiliza la investigación científica en el campo del seguimiento web y predicción del comportamiento de los usuarios para predecir si una pareja se mantendrá unida al largo plazo.[105]

Estos son solo algunos ejemplos sencillos de como el seguimiento web puede predecir nuestros comportamientos, pero sus aplicaciones pueden ser en múltiples campos, para predecir e influenciar nuestros comportamientos. La empresa Google ya ha solicitado algunas patentes relativas a la predicción, detección y corrección de comportamiento de usuarios.[106]

Algunos estudios nos ilustran sobre lo mucho que se puede deducir de una persona con el seguimiento web. El primero, *"Private traits and attributes are predictable from digital records of human behavior"*, realizado en 2013 con la participación de 58,000 voluntarios encontró que analizando las redes sociales es posible predecir datos sensibles de una persona, como la edad, género, orientación sexual, etnia, afinidad política, personalidad, inteligencia, felicidad, uso de drogas, y situación familiar.[107]

10152066701893859/ (Fecha de consulta: 12 de agosto de 2020).

104 Eharmony, "The future of dating report 2018: smart devices will predict if your relationship is on the rocks", Eharmony, https://www.eharmony.co.uk/dating-advice/dating/the-future-of-dating-report-2018-smart-devices-to-predict-if-your-relationship-is-on-the-rocks (Fecha de consulta: 12 de agosto de 2020).

105 Staygo, "Scientific References", Staygo, https://staygoapp.com/references, https://staygoapp.com/references (Fecha de consulta: 12 de agosto de 2020).

106 Davies, Dave, "Patent 1 of 2: How Google learns to influence and control users", Search Engine Land, 2017, https://searchengineland.com/patent-1-2-google-learns-influence-control-users-272358 (Fecha de consulta: 12 de agosto de 2020).

107 Kasinski, Michal, *et al.*, "Private traits and attributes are predictable from digital records of human behavior", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 110, num. 15, 2013, pp. 5733, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3625324/ (Fecha de consulta: 17 de diciembre de

El estudio logró predecir con gran exactitud datos sobre los individuos, entre las predicciones es capaz de predecir: género con un 93% de exactitud. Preferencia sexual (homosexual o heterosexual) en un 88% de precisión. Grupo étnico (afroamericanos y caucásicos) en un 95 por ciento. Preferencia política en un 85%. Religión en un 82%. Consumo de drogas en un 73%. Además de predecir con alta exactitud la personalidad de la persona, atributos como inteligencia, estabilidad emocional, extroversión, empatía, circulo social y amistades.[108]

El estudio *"Computer-based personality judgments are more accurate than those made by humans"* verificó estos hallazgos. Realizado en 2015 con una muestra de 86,220 participantes, el estudio encontró que los análisis de personalidad por computadora, utilizando la huella digital, son más exactos que las percepciones de parejas, familiares, amigos y colegas sobre un mismo individuo. El estudio incluso aseguró que la personalidad se puede predecir mediante un sistema automatizado, sin necesitar habilidades socio-cognitivas humanas. Entre las categorías en que los sistemas de computadora juzgaron con mayor acierto que familiares y amigos tenemos: satisfacción con la vida, depresión, orientación política, valores, intereses, campo de estudio, uso de drogas, salud física, entre otras.[109]

Posteriormente, Michal Kosinski, uno de los investigadores del citado estudio, explicaría que esto demuestra como las características psicológicas de un individuo pueden ser descubiertas analizando los datos personales, sin que intervenga un humano, y que las maquinas pueden saber de nosotros mucho más de lo que creemos.[110]

2020).

108 *Idem*.

109 Youyou, Wu, "Computer-based personality judgments are more accurate than those made by humans", *Proceedings of the National Academy of Sciences*, National Academy of Sciences, Vol. 112, No 4, 2015, pp. 1036-1040. https://www.pnas.org/content/pnas/112/4/1036.full.pdf (Fecha de consulta: 07 de agosto de 2020).

110 Parker, Clifton B., *Michal Kosinski: Computers Are Better Judges of Your Personality Than Friends*, Stanford Business, 2015, https://www.gsb.stanford.edu/insights/michal-kosinski-computers-are-better-judges-your-personality-friends (Fecha de consulta: 07 de agosto de 2020).

El Supervisor Europeo de Protección de Datos ha reconocido que tiene un gran valor para las empresas y gobiernos el acaparar grandes volúmenes de datos obtenidos por diversas fuentes, para posteriormente ser analizados, y así poder supervisar y predecir el comportamiento de las personas, tanto en sus comportamientos individuales como colectivos.[111]

De la misma forma, el Supervisor Europeo de Protección de Datos hace referencia a las declaraciones de la Presidenta de la Comisión Federal de Comercio de Estados Unidos, quien afirmó respecto al seguimiento web y otras técnicas de seguimiento, que es posible combinar datos en línea y no en línea, y acumular "virtualmente cantidades ilimitadas de información sobre los consumidores y almacenarla indefinidamente", y que es posible utilizar estos datos para predecir una cantidad "sorprendente de información sobre cada uno de nosotros".[112]

1.4 Impacto del seguimiento web - ¿Cómo puede afectarme el seguimiento web?

El seguimiento web en la actualidad ya plantea una gran cantidad de problemas éticos y en algunos casos legales, por la forma en la que es utilizado en la actualidad.

Entre algunos de los problemas que se han identificado se encuentran:

Búsquedas Filtradas

Cuando el usuario realiza una búsqueda en la web, la información es filtrada de acuerdo a los intereses y búsquedas anteriores del usuario, si bien a primera vista puede parecer algo útil, efectivamente se está aislando al usuario de

111 Supervisor Europeo de Protección de Datos, *Hacia una nueva ética digital: Datos, dignidad y tecnología*, Dictamen 4/2015, 2015, pp. 7-8, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_es.pdf (Fecha de consulta: 16 de junio de 2020).

112 Edith Ramirez, *Big Data: A Tool for Inclusion or Exclusion?*, Washington, 2014, pp. 2-4, https://www.ftc.gov/system/files/documents/public_statements/582421/140915bigdataworkshop.pdf (Fecha de consulta: 17 de junio de 2020).

opiniones, puntos de vista, eventos e incluso hechos, manteniéndolo en una "burbuja informativa".[113]

Publicidad en línea

Si bien la publicidad por sí misma no causa un daño, la publicidad en la Web, al ser adquirida en forma masiva y sin supervisión humana, permite que se afecte a los usuarios de múltiples formas, por ejemplo, permite que en Facebook se muestren imágenes provocativas con chicas menores de edad,[114] le permite a Google mostrar publicidad fraudulenta durante meses, aún después de haber sido informado, [115] permite la difusión de noticias falsas,[116] incluir software malicioso,[117] entre otros.[118]

113 Bujlow, Tomasz, *et al.*, "A Survey on Web Tracking: Mechanisms, Implications, and Defenses", *Proceedings of the IEEE*, vol. 105, núm. 8, agosto 2017, pp. 1476-1510. https://ieeexplore.ieee.org/document/7872467 (Fecha de consulta: 29 de abril de 2020)

114 Silverman, Craig y Mac, Ryan, *Facebook Gets Paid*, BuzzFeedNews, diciembre 2020, https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam (Fecha de consulta: 17 de junio de 2021).

115 Murphy, Paul, *Exclusive: Google kept scam fishing license ads up for months after being told about them, states say*, CNN Business, febrero 2020, https://edition.cnn.com/2020/02/03/tech/google-fishing-licenses-scam-ads/index.html (Fecha de consulta: 17 de junio de 2021).

116 Relihan, Tom, *Social media advertising can boost fake news — or beat it*, MIT Management Sloan School, diciembre 2018, https://mitsloan.mit.edu/ideas-made-to-matter/social-media-advertising-can-boost-fake-news-or-beat-it (Fecha de consulta: 17 de junio de 2021).

117 Winder, Davey, *Warning: Microsoft Support Scam 'Freezes' Chrome, Edge And Firefox Browsers – How To Defrost Them*, Forbes, abril 2019, https://www.forbes.com/sites/daveywinder/2019/04/30/windows-warning-microsoft-support-scammers-are-freezing-chrome-edge-and-firefox-browsers/?sh=4152586418f1 (Fecha de consulta: 17 de junio de 2021).

118 Wired Staff, *Rogue Ad Attempted to Redirect Wired Readers*, Wired, octubre 2012, https://www.wired.com/2012/04/rogue-ad-wired/ (Fecha de consulta: 17 de junio de 2021).

Discriminación

Existen una gran cantidad de formas en que el seguimiento web puede ser utilizado con fines de discriminación, a continuación se listan algunos ejemplos.

La Presidenta de la Comisión Federal de Comercio de Estados Unidos hace referencia a la "discriminación por algoritmo", que permite a los negocios filtrar a los consumidores de bajos ingresos o de minorías, o que pueden usarse para impactar el acceso a un crédito, casa, empleo, seguro. Incluso asegura que los nombres distintivos de ciertas etnias, pueden ser discriminados por los algoritmos, lo que tiene consecuencias devastadoras, como el limitar acceso a ciertos empleos a una minoría.[119]

La predicción de la personalidad de los usuarios utilizando datos digitales, es cada vez más popular. La agencia GCHQ, del Gobierno Británico, que utilizó la información obtenida de los navegadores Chrome, Firefox, Safari e Internet Explorer, para analizar las correlaciones del uso del navegador con la personalidad. IBM ha analizado las publicaciones de los usuarios de Twitter para determinar su personalidad.[120]

En este sentido, algunas compañías financieras, bancarias y de seguros, ya han comenzado a utilizar la información de los usuarios para crear perfiles que les permitan predecir si una persona es un riesgo crediticio. Por ejemplo la empresa VisualDNA se ha asociado con empresas como MasterCard o Admiral, para "explorar el impacto de la personalidad", utilizando las categorías: demografía, intereses, intenciones y personalidad, para determinar si una persona es digna de obtener un seguro o un crédito.[121]

119 Edith Ramirez, *Big Data: A Tool…*, *op. cit.*, pp. 4-8.

120 Christl, Wolfie y Spiekermann, Sarah, *op. cit.*, pp. 25-27.

121 *Idem*.

Ha sido reportado que el perfil y conexiones de las personas en Facebook puede afectar la calificación crediticia,[122] Admiral utilizaba las publicaciones en Facebook para decidir los costos del seguro de un vehículo.[123]

El uso de la información de los usuarios de la web para clasificar a los individuos y determinar las tasas de interés de un crédito ha comenzado a llamarse "crédito social" haciendo referencia al uso de redes sociales para la determinación. Este nuevo tipo de análisis crediticio ha sido criticado por presentar problemas tanto para el usuario cómo para su círculo social en las redes sociales, quienes pueden ser analizados aún sin haber dado su consentimiento.[124]

Además del proceso de "caja negra" de análisis de los individuos, en el que las compañías pueden tomar decisiones cruciales para las personas, pero ocultan los métodos utilizados para la recolección y análisis de los datos.[125]

Este tipo de discriminación puede extenderse más allá de los servicios bancarios y financieros, también es posible que un sitio web, sin importar su giro comercial, muestre diferentes precios a los usuarios, de acuerdo al perfil del usuario, su ubicación geográfica, entre otros.[126] La empresa Uber es notoria por aumentar sus precios cuando los usuarios tienen mayor necesidad de sus servicios, incluso durante ataques terroristas, desastres naturales y emergencias naturales.[127]La discriminación de precios afecta gravemente a las mujeres, quienes

122 Lobosco, Katie, *Facebook friends could change your credit score*, CNN Business, agosto 2013, https://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html?hpt=hp_t2 (Fecha de consulta: 18 de junio de 2021).

123 Ruddick, Graham, *Admiral to price car insurance based on Facebook posts*, The Guardian, noviembre 2016, https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts (Fecha de consulta: 18 de junio de 2021).

124 Packin, Nizan Geslevich y Lev Aretz, Yafit, "On Social Credit and the Right to Be Unnetworked", *Columbia Business Law Review*,Vol. 2016, Num 2, febrero 2016, pp. 339–347 https://ssrn.com/abstract=2728414 (Fecha de consulta: 18 de junio de 2021).

125 *Ibidem*, pp. 401-406

126 Bujlow, Tomasz, *et al.*, *op. cit.*

127 Hawkins, Andrew, *Uber is overhauling the way it responds to emergencies and natural disasters* The Verge, septiembre 2018, https://www.theverge.com/2018/9/25/17897836/uber-disaster-response-hurricane-price-cap (Fecha de consulta: 18 de junio de 2021). Conger, Kate *Prepare to Pay More for Uber and Lyft Rides*, The New York Times, junio 2021,

suelen tener que pagar más por productos dirigidos al sector femenino, en contrario de los productos dirigidos a los hombres.[128] Las mujeres suelen pagar más por sus primas de seguros,[129] hipotecas,[130] ropa, productos de aseo personal, productos para el hogar, juguetes, entre otros.[131]

Manipulación psicológica y social

Como ya se explicó anteriormente, las empresas de seguimiento web pueden realizar estudios para predecir y manipular los comportamientos de los usuarios. Gracias al seguimiento web pueden predecirse enfermedades

https://www.nytimes.com/article/uber-lyft-surge.html (Fecha de consulta: 20 de junio de 2021).

128 Sanchez, Pilar, *Impuesto rosa: Mujeres pagan hasta 17% más por el mismo producto que un hombre*, Dinero en Imagen, junio 2021, https://www.dineroenimagen.com/economia/impuesto-rosa-mujeres-pagan-hasta-17-mas-por-el-mismo-producto-que-un-hombre/131694 (Fecha de consulta: 20 de junio de 2021).

129 Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, *¿Conoces el impuesto rosa o pink tax?* Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, agosto 2019, https://www.gob.mx/condusef/prensa/conoces-el-impuesto-rosa-o-pink-tax (Fecha de consulta: 20 de junio de 2021).

130 Cheng, Ping, *et al.*, "Do Women Pay More for Mortgages?", *The Journal of Real Estate Finance and Economics*, vol 43, 2011, pp. 423-440, https://www.researchgate.net/publication/225702859_Do_Women_Pay_More_for_Mortgages (Fecha de consulta: 20 de junio de 2021).

131 New York City Department of Consumer Affairs, *From Cradle to Cane: The Cost of Being a Female Consumer*, New York City Department of Consumer Affairs, diciembre 2015, pp. 17-40, https://www1.nyc.gov/assets/dca/downloads/pdf/partners/Study-of-Gender-Pricing-in-NYC.pdf (Fecha de consulta: 20 de junio de 2021). Miller, Zoë, *16 things that are still more expensive for women than for men*, Insider, agosto 2018, https://www.insider.com/women-more-expensive-products-2018-8 (Fecha de consulta: 20 de junio de 2021).

mentales,[132] la depresión a predecirse partir del tiempo de uso de distintos sitos web[133] o por el lenguaje utilizado en las publicaciones de los usuarios.[134]

Pero en la actualidad se ha llegado más allá de las predicciones, el estudio *Psychological targeting as an effective approach to digital mass persuasion*, realizado en 2017, se analizó el efecto de las campañas de persuasión que utilizan el perfil psicológico de los usuarios basado en su huella digital. El estudio analizó la respuesta a la persuasión digital en más de 3.5 millones de usuarios. El estudio encontró que es posible aumentar hasta en un 50% la efectividad de una campaña de persuasión si se aprovecha la huella digital.[135]

Anteriormente se explicó que el seguimiento web se puede utilizar para crear anuncios personalizados y "burbujas informativas", esto ya ha tenido un grave impacto, pues estos problemas en conjunto con la manipulación social, han llevado a la difusión de ideas falsas y teorías conspirativas.[136]

Puede destacarse el caso de la difusión de teorías conspirativas referentes a la pandemia de COVID-19, pues las personas que pasaban más tiempo en redes sociales son las que mayores posibilidades tenían de creer teorías

132 Pantic, Igor, "Online social networking and mental health", *Cyberpsychology, Behavior, and Social Networking*, vol. 17, num. 10, octubre 2014, pp. 652-657, https://www.liebertpub.com/doi/10.1089/cyber.2014.0070 (Fecha de consulta: 22 de junio de 2021).

133 Kim, Jim, *et al.*, "A Systematic review of the validity of screening depression through Facebook, Twitter, Instagram, and Snapchat", *Journal of Affective Disorders* vol. 286, mayo 2021, pp. 360-369, https://www.sciencedirect.com/science/article/abs/pii/S016503272100135X?via%3Dihub (Fecha de consulta: 22 de junio de 2021).

134 Leis, Angela, *et al.*, "Detecting Signs of Depression in Tweets in Spanish: Behavioral and Linguistic Analysis", *Journal of Medical Internet Research*, vol. 2, num. 6, junio 2019, pp. 1-16, https://www.jmir.org/2019/6/e14199/ (Fecha de consulta: 22 de junio de 2021).

135 Matz, Sandra, *et al.*, "Psychological targeting as an effective approach to digital mass persuasion", *Proceedings of the National Academy of Sciences*, vol. 114, num. 48, noviembre 2017, pp. 12714-12719, https://www.pnas.org/content/114/48/12714 (Fecha de consulta: 22 de junio de 2021).

136 Allington, Daniel *Conspiracy Theories, Radicalisation and Digital Media*, The Global Network on Extremism and Technology, febrero 2021, pp. 15-21, https://gnet-research.org/wp-content/uploads/2021/02/GNET-Conspiracy-Theories-Radicalisation-Digital-Media.pdf (Fecha de consulta: 22 de junio de 2021).

conspirativas.[137] Esto ocurre porque los sitios web de redes sociales realizan actividades para perfilar de usuarios con el seguimiento web y permiten la muestra de anuncios, vínculos a páginas web y difusión de noticias falsas a los usuarios más propensos a creer en este tipo de desinformación.[138]

1.5 El seguimiento web y la FSFLA

En lo que compete a la FSFLA, se ha detectado que las preocupaciones sobre el seguimiento web y la privacidad en Internet no son algo nuevo entre sus miembros. Desde hace algunos años existen se han registrado entradas en la lista de distribución de la FSFLA “Discusión”, donde los miembros han planteado su preocupación por temas como: la vigilancia en internet y sus efectos sobre la

137 Allington, Daniel, *et al.*, “Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency”, *Psychological Medicine*, pp. 1-7 https://www.cambridge.org/core/journals/psychological-medicine/article/healthprotective-behaviour-social-media-usage-and-conspiracy-belief-during-the-covid19-public-health-emergency/A0DC2C5E27936FF4D5246BD3AE8C9163 (Fecha de consulta: 22 de junio de 2021).

138 Ahmed, Wasim, *et al.*, “COVID-19 and the 5G Conspiracy Theory: Social Network Analysis of Twitter Data”, *Journal of Medical Internet Research*, vol. 22, num. 5, mayo 2020, pp. 1-9, https://www.jmir.org/2020/5/e19458 (Fecha de consulta: 22 de junio de 2021).

democracia,[139] las redes sociales,[140] las tecnologías de seguimiento web, análisis y la vigilancia,[141] privacidad y anonimato con software libreo,[142] entre otros.

Los miembros de la FSFLA no solo sienten preocupación por el panorama actual de la Web, también han realizado algunas iniciativas para combatir el seguimiento web, como el proyecto “0G” de Alexandre Oliva,[143] y la tesis de maestría de Rafael Bonifaz sobre comunicaciones secretas en Internet.[144]

Las preocupaciones y acciones de los miembros de la FSFLA no se encuentran infundadas, a largo del presente capitulo se mostró el panorama actual del seguimiento web y por qué es un problema actual para la mayoría de los usuarios de Internet.

139 Bonifaz, Rafael, *¿Cuánta vigilancia puede soportar la democracia?*, Lista de distribución FSFLA-Discusión, octubre 2013, https://www.fsfla.org/pipermail/discusion/2013-October/005247.html (Fecha de consulta: 16 de junio de 2021).

140 Ordóñez, Quiliro, *Censura y espionaje en Facebook*, Lista de distribución FSFLA-Discusión, abril 2017, https://www.fsfla.org/pipermail/discusion/2017/005905.html (Fecha de consulta: 16 de junio de 2021); Biasutti Neto, Albino, *Cuenta de FSF Latinoaméricana en Twitter*, Lista de distribución FSFLA-Discusión, mayo 2014, https://www.fsfla.org/pipermail/discusion/2014/005377.html (Fecha de consulta: 16 de junio de 2021).

141 Uebelherr, Willi, *[Internet Policy] The Myth? of analytics*, Lista de distribución FSFLA-Discusión, marzo 2017, https://www.fsfla.org/pipermail/discusion/2017/005803.html (Fecha de consulta: 16 de junio de 2021); Ordóñez, Quiliro, *Usar email con criptografía*, Lista de distribución FSFLA-Discusión, septiembre 2013, https://www.fsfla.org/pipermail/discusion/2013-September/005237.html (Fecha de consulta: 16 de junio de 2021).

142 Bonifaz, Rafael, *Privacidad y Anonimato con Software Libre*, Lista de distribución FSFLA-Discusión, mayo 2018, https://www.fsfla.org/pipermail/discusion/2018/006072.html (Fecha de consulta: 16 de junio de 2021).

143 Oliva, Alexandre, *0G: Escaping the Surveillance Blackhole with Free Mobile Computing*, Norwegian Unix User Group, Oslo, Octubre 2020, https://nuug.no/aktiviteter/20201013-mobile-computing-with-privacy/ (Fecha de consulta: 16 de junio de 2021).

144 Bonifaz, Rafael, *Comunicaciones Secretas en Internet*, Lista de distribución FSFLA-Discusión, marzo 2019, https://www.fsfla.org/pipermail/discusion/2019/006103.html (Fecha de consulta: 16 de junio de 2021).

Es claro que el seguimiento web es un problema que afecta a diferentes sectores de la sociedad, y que, cómo se mencionó en la sección **1.4 Impacto del Seguimiento Web**, puede dar pie a problemas más grandes, en el aspecto personal puede evitar el acceso a oportunidades laborales o financieras, e incluso llegar a la manipulación psicológica, mientras que en el aspecto social puede promover problemas como la desinformación y discriminación.

Por estos motivos, es que surge la presente propuesta de intervención, con la que se busca que el Consejo de la FSFLA realice acciones encaminadas a informar y proteger a sus miembros mediante la difusión de herramientas de Software Libre destinadas a la protección de la privacidad.

Capítulo 2

El Derecho a la Protección de Datos Personales

Capítulo 2. El Derecho a la Protección de Datos Personales

El objetivo del presente capítulo es mostrar, de forma breve, los derechos y principios que nacen del derecho a la protección de datos personales y sus aspectos más relevantes en conexión con el seguimiento web.

Para lo cual se utilizan como referencia los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, emitidos en 2017, ya que este documento fue emitido por la Red Iberoamericana de Protección de Datos (RIPD), con el objetivo de homogeneizar entre sus miembros las reglas, principios, derechos y deberes respecto al derecho de protección de datos personales.[145] Y se espera que en los próximos años, los países miembros de la RIPD adecuen sus leyes a los Estándares.[146]

También se incluyen referencias a los Principios de la Organización de Estados Americanos (OEA) en materia de privacidad y protección de datos personales, ya que la OEA está conformada por todos los países independientes de América.[147]

Además, se analiza con más atención el marco legal en materia de protección de datos personales en seis de los países más poblados de América Latina: Argentina, Brasil, Chile, Colombia, México y Perú,[148] y las autoridades

145 RIPD, "Historia de la Red Iberoamericana…", *op. cit*.

146 RIPD, "Declaración del XV encuentro de la Red Iberoamericana de Protección de Datos", RIPD, https://www.redipd.org/sites/default/files/inline-files/Declaracion_RIPD_XV_encuentro.pdf (Fecha de consulta: 21 de junio de 2020).

147 OEA, "Member States", OEA, http://www.oas.org/en/member_states/default.asp (Fecha de consulta: 10 de julio de 2021).

148 UNdata, "Total population, both sexes combined (thousands)", División de Estadística de la Organización de las Naciones Unidas, 2019, https://data.un.org/Data.aspx?d=PopDiv&f=variableID%3a12%3btimeID%3a83%2c84%3bvarID%3a2&c=2,4,6,7&s=_crEngNameOrderBy:asc,_timeEngNameOrderBy:desc,_varEngNameOrderBy:asc&v=1 (Fecha de consulta: 21 de agosto de 2020).

encargadas de defender este derecho en estos países. Se excluye a Venezuela porque no cuenta con legislación en la materia.[149]

Antecedentes

El derecho a la intimidad o a la vida privada tiene uno de sus primeros antecedentes en el artículo "*The Right to Privacy*" publicado en 1890 en "*Harvard Law Review*". Este documento define al derecho a la vida privada como el "derecho a ser dejado en paz" y considera que la protección de la privacidad es una respuesta a las invenciones tecnológicas y a los nuevos modelos de negocios de la época, por ejemplo las cámaras fotográficas, y el recién surgido periodismo sensacionalista.[150]

Pese a haber sido publicado en el siglo XIX, en el documento ya se hablaba con inquietud por el uso de los avances tecnológico para la intromisión en la vida privada de los ciudadanos y por cómo las terceras partes, por ejemplo el periodismo sensacionalista, podían aprovecharse de esta situación. Incluso, se menciona que si no se debería "reproducir fotográficamente la cara de una mujer sin su consentimiento, mucho menos debería ser tolerado reproducir su cara, su figura y sus acciones".[151]

Más adelante, los horribles eventos de la Segunda Guerra Mundial y el Holocausto, propiciaron que al terminar la guerra, se reconocieran la protección de la dignidad humana y la no injerencia en la vida privada como derechos humanos. Esta protección se materializó en múltiples instrumentos jurídicos internacionales, entre los que destacan la Declaración Universal de los Derechos Humanos de

149 Transparencia, Venezuela, *En Venezuela no existe una Ley que resguarde los datos personales*, Transparencia Venezuela, https://transparencia.org.ve/project/en-venezuela-no-existe-una-ley-que-resguarde-los-datos-personales/ (Fecha de consulta: 21 de agosto de 2020).

150 Warren Samuel D. y Brandeis Louis, "The Right To Privacy". *Harvard Law Review*, Vol. IV, Num 5, 1890, http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm (Fecha de consulta 13 de marzo de 2020).

151 *Idem.*

1948, la Convención Americana de Derechos Humanos de 1966 y el Pacto Internacional de Derechos Civiles y Políticos de 1966.[152]

En los trabajos preparatorios para la elaboración de la Declaración Universal de los Derechos Humanos se consideró que debían proclamarse derechos que permitieran al hombre desarrollar su personalidad y que impidieran que ninguna persona fuese presa o instrumento de otra.[153]

Así, el artículo 12 de la Declaración Universal de los Derechos Humanos indica que: "*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*".[154]

En la década de los ochenta, ante el rápido avance de las tecnologías de la información y la comunicación, aumentó la preocupación por la protección de la privacidad, si bien Internet aún no existía como hoy en día, y las redes de computadoras eran pequeñas, ya se podía vislumbrar que era necesario crear regulación acerca de estas tecnologías.

En 1980 la Organización para la Cooperación y el Desarrollo Económicos (OCDE) emitió las "Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales", a fin de contar con un instrumento internacional que definiera los principios respecto al tratamiento de información personal con medios informáticos.[155]

152 Mendoza Enríquez, Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *Revista IUS*, v. 12, n41, 2018, pp. 267-291, http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es (Fecha de consulta 13 de agosto de 2020).

153 Lefranc Weegan, Federico César, *Holocausto y Dignidad. Sifnificado y fin de la invocación a la dignidad humana en el Preámbulo de la Declaración Universal de Derechos Humanos*, Méxco, Ubijus, 2009, pp. 139.

154 ORGANIZACIÓN de las Naciones Unidas, La Declaración Universal de Derechos Humanos, Organización de las Naciones Unidas, Resolución París, 1948, https://www.un.org/es/universal-declaration-human-rights/ (Fecha de consulta: 23 de mayo de 2020)

155 Organization for Economic Cooperation and Development, *Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, OECD, pp.

En el documento se define a los datos personales como "*cualquier información relacionada con un individuo identificado o identificable (sujeto de los datos)*".[156]

También se destaca el "Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal", primer instrumento internacional jurídicamente vinculante, aunque no es de aplicación directa, pues cada país que lo ratifica debe ajustarlo a su legislación interna. El Convenio protege contra abusos en la recolección y procesamiento de datos personales.[157]

El convenio define los datos personales como "cualquier información relativa a una persona física identificada o identificable (persona concernida)".[158] El tratado ha sido ratificado por los países latinoamericanos Argentina, México y Uruguay.[159]

Definición de datos personales

El artículo 2 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (EPDPEI) define los datos personales como:

2-4. https://www.oecd.org/sti/ieconomy/15590267.pdf (Fecha de consulta: 29 de abril de 2020)

156 Organization for Economic Cooperation and Development, *Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, OECD, p. 2-4. https://www.oecd.org/sti/ieconomy/15590267.pdf (Fecha de consulta: 29 de Abril de 2020)

157 Treaty Office, "Details of Treaty No.108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (Fecha de consulta: 24 de agosto de 2020)

158 Consejo de Europa, "Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal", 1981, http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf (Fecha de consulta: 23 de agosto de 2020)

159 Treaty Office, "Chart of signatures and ratifications of Treaty 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Status as of 24/08/2020", Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=g2DamFix (Fecha de consulta: 24 de agosto de 2020)

"Cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas".[160]

Definición de Datos Personales Sensibles

En el mismo artículo 2, los EPDPEI marcan la existencia de una categoría especial de datos personales, los datos personales sensibles, a los cuales se define como:

"Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física".[161]

En este sentido, la definición de datos personales contrasta con la definición de datos personales sensibles en que esta se refiere a datos que, si se conocen, pueden llegar a afectar la intimidad pues pueden dar origen a discriminación o poner en riesgo a la persona; y aquella se refiere a la información que nos permite identificar a una persona.

Autodeterminación informativa

El concepto de "autodeterminación informativa" se encuentra por primera vez en la jurisprudencia del Tribunal Constitucional Federal de Alemania, que en 1983 declaró como inconstitucionales diversos artículos de la "Ley sobre un censo

160 RIPD, Estándares de Protección de Datos Personales para los Estados Iberoamericanos, RIPD, Santiago de Chile, 2017, https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf (Fecha de consulta: 21 de junio de 2020).

161 *Idem.*

de población, profesión, vivienda y lugares de trabajo", también conocida como, Ley de Censos de 1983.[162]

En la citada resolución, el Tribunal juzga que para proteger el derecho al libre desarrollo de la personalidad es necesaria "*la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales*", esto debido a la alta capacidad para el procesamiento de datos que existe en la actualidad.[163]

El Tribunal manifiesta que se requiere una protección especial ante "*las condiciones actuales y futuras del procesamiento automático de datos*". Por lo que protege la "autodeterminación informativa", es decir, el derecho de los individuos a decidir a quién, cuándo y bajo qué límites desean compartir su vida privada.

Y destaca que la "*autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar*".[164]

La sentencia busca crear un equilibrio entre la autodeterminación informativa del individuo y el beneficio de la comunidad. No garantiza un poder ilimitado sobre los datos personales, ya que algunos datos, como los que tienen fines estadísticos, pueden beneficiar a la comunidad, siempre y cuando se proteja el anonimato del individuo.

Por último, considera que hay datos que nunca deben exigirse a los ciudadanos, incluso ni con fines estadísticos, si son datos que pudieran "*generar el peligro de un etiquetamiento (por ejemplo, como "adicto a las drogas", "persona con antecedentes criminales", "enfermo mental", "persona asocial", etc.)*".[165]

2.5 Importancia de la protección de datos personales

En los años sesenta, Alan Westin, realizó una de las primeras evaluaciones del conflicto entre la privacidad y la vigilancia en la sociedad moderna en el libro

162 Jürgen Schwabe, *Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe*, México, Konrad Adenauer Stiftung, 2009, pp. 95-103

163 *Idem.*

164 *Idem.*

165 *Idem.*

"*Privacy and Freedom*" en el cual considera que tanto la vigilancia como el seguimiento a los individuos, no solo se presentan de forma física, visual o auditiva, también existen tanto la vigilancia psicológica, que puede presentarse utilizando test de personalidad y medios tecnológicos, como la vigilancia de datos personales, mediante la recopilación de información de los individuos en bases de datos.[166]

Westin defiende el valor social de la privacidad, a la que define como el derecho del individuo a controlar la información sobre sí mismo, derecho que, afirma, permite a los individuos y a los grupos de una sociedad el preservar su autonomía. También advierte de los peligros que afronta la sociedad por el aumento de la vigilancia y la perdida de la privacidad, lo cual atribuye a dos razones, primero, los cada vez más bajos costos de la tecnología, y la segunda, que los individuos cada vez están dispuestos a divulgar mayor información sobre sí mismos.[167]

En este orden de ideas, a continuación se analizan cuatro justificaciones morales por las que es importante proteger los datos personales, propuestas por Jeroen Van Den Hoven en el ensayo *"Information technology, privacy, and the protection of personal data"*.[168]

1. *Prevenir un daño*: Si la información es obtenida por criminales, los titulares pueden ser víctimas de diferentes crímenes, como son el robo, suplantación de identidad, fraude, extorsión, entre otros.[169]Las bases de datos con datos personales también pueden ocasionar daño, el Registro de Población de Amterdam contenía datos personales de más de 70,000 judíos viviendo en

166 Alan F. Westin, "Privacy And Freedom", *Washington and Lee Law Review*, No. 166, 1968, https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 (Fecha de consulta: 20 de agosto de 2020).

167 *Idem.*

168 Van den Hoven, Jeroen, "Information technology, privacy, and the protection of personal data", *Information Technology and Moral Philosophy*, Cambridge, Cambridge University Press, 2008, pp. 301–322.

169 *Idem.*

Amsterdam durante la época de la Segunda Guerra Mundial. Las bases de datos incluían: nombre, fecha de nacimiento, profesión, estado civil, familia, y, en el caso de los judíos, contenían una letra "J".[170] Cuando los Países Bajos fueron invadidos por la Alemania Nazi, esta base de datos permitió a los nazis identificar con rapidez a la población judía. En los Países Bajos, tres cuartas partes de la población judía fue aniquilada y enviada a campos de concentración, una mayor proporción que en ningún otro país europeo.[171]

2. *Desigualdad de información*: Debido al gran valor de los datos personales, los individuos se ven en una posición de desventaja en una relación contractual que involucre sus datos personales. Los consumidores no conocen o no entienden las implicaciones de entregar sus datos personales, y, en general, no son capaces de verificar que la otra parte cumpla con sus obligaciones de protección de datos.[172]

3. *Injusticias informativas y discriminación*: La información se ha convertido en un bien económico y, como tal, debe impedirse que se conformen monopolios, es decir entidades que ejercen control social de un bien, en este caso los datos, y explotan su dominación del mercado para obtener ventajas en otros ámbitos, como el monetario o el político. También implica que la información de un ámbito, por ejemplo la información sobre la salud un individuo, no sea utilizada en otro

170 Schlebaum, Pieter, *Raid on the Population Registry of Amsterdam*, trad. de Cor Korpel, Traces of War, septiembre 2019, https://www.tracesofwar.com/articles/5329/Raid-on-the-Population-Registry-of-Amsterdam.htm (Fecha de consulta: 14 de julio de 2021); Boffey, Daniel, *Registration cards of Dutch Holocaust victims to go on display*, The Guardian, enero 2021, https://www.theguardian.com/world/2021/jan/26/registration-cards-dutch-jews-display-holocaust-museum-amsterdam (Fecha de consulta: 14 de julio de 2021)

171 Griffioen, Pim y Zeller, Ron, *The Netherlands: the greatest number of Jewish victims in Western Europe*, Anne Frank House, septiembre 2018, https://www.annefrank.org/en/anne-frank/go-in-depth/netherlands-greatest-number-jewish-victims-western-europe/ (Fecha de consulta: 14 de julio de 2021)

172 van den Hoven, Jeroen, *op. cit.*

sector, por ejemplo el laboral. Pues este cambio de contexto puede ser motivo de discriminación y desventajas para los individuos.[173]

4. *Autonomía moral*: Los individuos tienen derecho a la autonomía en la toma de decisiones sobre su vida privada. Derecho a no tener que preocuparse de la interferencia de otros, ni tener que vivir bajo una presión social de vivir de forma "normal". Cuando la vida privada es expuesta, los individuos realizan acciones y toman decisiones con las que no están de acuerdo, pero a las que se sienten obligados al saberse observados. En este mismo sentido, cuando una entidad toma decisiones sobre una persona basándose en datos, no está aceptando ni respetando la autonomía de esa persona sobre sus propias aspiraciones e identidad. [174]

En México, la importancia de la protección de datos personales también es parte de diversos criterios jurisprudenciales, que resaltan la importancia de:

1) El derecho al honor, la intimidad y la propia imagen, ya que son derechos subjetivos del ser humano inseparables e inherentes al titular y que recaen en la personalidad de los individuos.[175]2) La protección de datos personales como derecho humano, ya que garantiza a los individuos decidir sobre los aspectos de su vida que pueden o no ser conocidos por la sociedad, y es un medio para para salvaguardar otros derechos humanos.[176]3) La protección de los datos personales

173 *Idem.*

174 *Idem.*

175 DERECHOS AL HONOR, A LA INTIMIDAD Y A LA PROPIA IMAGEN. CONSTITUYEN DERECHOS HUMANOS QUE SE PROTEGEN A TRAVÉS DEL ACTUAL MARCO CONSTITUCIONAL. Tesis: 5o.C.4 K (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, Libro XXI, Tomo 2, junio de 2013, p. 1258. https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2003844&Clase=DetalleTesisBL&Semanario=0

176 PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS. Tesis: I.10o.A.5 CS (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, Libro 70, Tomo III, septiembre de 2019, p. 2199, https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2020564&Clase=DetalleTesisBL&Semanario=0

frente a las nuevas tecnologías, ya que por sus características, permiten la difusión y durabilidad de contenido, el cual puede permanecer publicado de forma indefinida y sin restricción de territorio, lo que puede constituir una invasión de los mencionados derechos de intimidad, honor, reputación, vida privada y dignidad humana.[177]

Partes en el derecho de protección de datos

Las dos principales partes participantes en el ejercicio de la protección de datos personales son el *titular* y el *responsable*, y la operación sobre los datos personales es el *tratamiento*.

1. *Titular*: El artículo 2 de los EPDPEI, lo define como la persona física a quien le conciernen los datos personales. Mientras que los Principios de la OEA respecto a la protección de datos personales nos dicen que es la persona cuyos datos personales se recopilan, procesan, almacenan, utilizan o difunden. En resumen, el titular es la persona a la que hacen referencia los datos.

2. *Responsable*: El artículo 2 de los EPDPEI indica que el responsable puede ser tanto una persona física como un colectivo, ya sea en la forma de persona jurídica o moral, autoridad pública, organismo, entre otros. Esta persona decide sobre el tratamiento de los datos personales. Los Principios de la OEA manifiestan que es una persona física o ente colectivo, que se encarga del almacenamiento, procesamiento, uso, protección y difusión de los datos personales del titular, incluyendo a aquellos que se dedican a recopilar datos. Es decir, el responsable es la entidad privada o pública que decide sobre los datos personales.

3. *Tratamiento*: De la misma forma, el artículo 2 de los EPDPEI definen al tratamiento como la o las operaciones que se da a los datos personales del titular,

177 PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO, Tesis: I.10o.A.6 CS (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, Libro 70, Tomo III, septiembre de 2019, p. 2200, https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2020563&Clase=DetalleTesisBL&Semanario=0

ya sea con procedimientos físicos o informáticos, entre estas operaciones se encuentran el almacenamiento, acceso, registro, organización, indexación, consulta, extracción, aprovechamiento, o cualquier otro uso que se dé a los datos personales. Es decir, cualquier operación del responsable concerniente a los datos personales del titular.

El artículo 9 de los EPDPEI establece que a los datos sensibles no se les debe dar tratamiento, salvo las excepciones: A) sean un tratamiento estrictamente necesario, B) se dé cumplimiento a un mandato legal, C) el titular lo autorice de forma explícita y por escrito, y D) sea necesario por razones de seguridad nacional.

2.1 Derechos de los titulares

Para asegurar la protección a los datos personales, las legislaciones han reconocido los derechos de los ciudadanos a ejercer de forma activa su voluntad sobre sus datos personales y tomar decisiones concernientes a su vida privada.

De forma clásica, estos derechos son: Acceso, Rectificación, Cancelación, Oposición y Portabilidad, también llamados Derechos ARCO y se encuentran consagrados en las legislaciones en la materia, incluido el capítulo III de los EPDPEI.

Por su parte, los Principios de la OEA respecto a la protección de datos personales protegen estos derechos en el Principio Ocho: Acceso y Corrección, donde se protege al titular para que pueda acceder, modificar, corregir o eliminar sus datos personales de las bases de datos del responsable.

Dos nuevos derechos que también son protegidos por los EPDPEI son: el derecho de las personas a no ser objeto de decisiones individuales atomizadas y el derecho a la limitación del tratamiento de datos personales.

Estos indican que los titulares tienen derecho a no ser objeto de decisiones que afectarían su vida de forma significativa o que produzcan efectos jurídicos en su contra; si estas decisiones se basan exclusivamente en tratamientos automatizados de datos.

Derecho de Acceso

Este derecho se explica en el artículo 25 de los EPDPEI. Manifiesta el derecho del titular a obtener acceso a sus datos personales. A conocer cualquier información relacionada con su persona en posesión del responsable y las condiciones generales y especificas del tratamiento que se da a sus datos.

Los Principios de la OEA, en el principio ocho, resaltan que tanto el derecho de acceso como el de rectificación, son una de las salvaguardas más importantes para proteger la privacidad de los individuos. Por lo tanto, el derecho de acceso debe poder ejercerse de forma sencilla, sin requerir medidas especiales.

El responsable debe dar acceso en un plazo, precio, manera y forma razonables y proporcionados. Los datos deben ser proporcionados en lenguaje claro y sencillo.

Derecho de Rectificación

De acuerdo al artículo 26 de los EPDPEI, este derecho implica que el responsable tiene la obligación de corregir los datos personales cuando el titular se lo solicite. El responsable también debe corregir los datos cuando sean incompletos, inexactos o anticuados.

De la misma forma, los Principios de la OEA indican que las personas pueden ejercer el derecho a la corrección de sus datos cuando sean incompletos, inexactos, innecesarios o excesivos.

Se debe permitir a la persona proporcionar información para corregir los errores u omisiones. Los Principios de la OEA advierten que no por esto se da el derecho al titular de solicitar que se introduzcan datos inexactos o erróneos.

Derecho de Cancelación

Los EPDPEI garantizan en el artículo 27 el derecho del titular a solicitar la cancelación o supresión de sus datos personales que se encuentren en los archivos, registros y sistemas del responsable. Para que termine el tratamiento y dejen de estar en su posesión.

Los Principios de la OEA no dan el mismo alcance a este derecho, pues afirman que el derecho de cancelación no es absoluto, sino contingente y contextual, ya que puede entrar en conflicto con el derecho de acceso a la verdad, la libertad de información y expresión y la proporcionalidad.

Incluso consideran que el titular no puede pedir que el titular borre datos exactos pero embarazosos de su persona.

Derecho de Oposición

El titular también tiene la libertad de oponerse al tratamiento de sus datos personales, aunque el artículo 28 los EPDPEI permiten solo dos motivos por los que es válida esta oposición:

1. Cuando existe una razón legítima.
2. Cuando el tratamiento tenga por objetivo la mercadotecnia directa y la elaboración de perfiles para la mercadotecnia.

Bajo estas dos razones, el titular puede oponerse y sus datos deberán de ser utilizados para tales fines.

Los Principios de la OEA, al igual que en el ya visto derecho de cancelación, no respaldan el derecho a oponerse o suprimir datos personales, aun si los datos son embarazosos, excesivos o irrelevantes.

Derecho de Portabilidad

El titular puede solicitar que se le entregue una copia de sus datos personales. Para poder utilizarlos para sus propios intereses o ante un tercero. Los datos deben ser entregados en un formato estándar e incluso debe ser posible transmitir los datos de un responsable a otro, si el titular así lo solicita.

Este derecho es importante en el contexto de los datos personales almacenados en instrumentos electrónicos o automatizados. Este derecho es una respuesta a la existencia de formatos propietarios e incompatibles, creados por algunas empresas de Tecnologías de la Información y Comunicación. Los

formatos propietarios solo impiden que los titulares puedan usar sus propios datos en otros sistemas o ante otros responsables.[178]

El derecho de portabilidad es protegido por el artículo 30 de los EPDPEI, que ordena que los responsables deben entregar los datos personales en un formato electrónico estructurado y de uso común. Sin afectar negativamente otros derechos y libertades. La única excepción es la información inferida, derivada, creada u obtenida mediante el análisis o tratamiento efectuado por el responsable. Por ejemplo los datos referentes a la personalización, recomendación, categorización o creación de perfiles del titular.

Si bien los Principios de la OEA no defienden este derecho, este si es protegido por el artículo 20 del Reglamento Europeo de Protección de Datos, el cual tiene características similares al artículo 30 de los EPDPEI.

Derecho a la Limitación del Tratamiento de los Datos Personales

Este derecho se relaciona con el Principio de Proporcionalidad, que manifiesta que el responsable debe limitar al mínimo necesario la cantidad de datos para el tratamiento. Este principio se encuentra en el artículo 18 de los EPDPEI.

El derecho a la limitación del tratamiento nos dice que cuando los titulares ejerzan su derecho a la rectificación u oposición, el tratamiento de sus datos deberá limitarse al almacenamiento de datos. También se limitará el tratamiento de los datos cuando sean innecesarios para el responsable. Este derecho es titulado por el artículo 31 de lo EPDPEI.

El Principio Cuatro: Uso Limitado y Retención, de los Principios de la OEA, nos dice que los datos personales solo deben destinarse al fin para el que se obtuvieron. Sin mantenerse más tiempo del necesario. Exceptuando si el titular acepta que sus datos sean utilizados para fines distintos.

178 Solange Maqueo, María (coord.), *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada*, México, INAI, 2018, pp. 157-159.

Derecho a No Ser Objeto de Decisiones Individuales Automatizadas

Este es derecho ordena que los titulares no deben ser afectados, de manera significativa, por un tratamiento de datos automatizados, es decir que los algoritmos y los programas de inteligencia artificial no deben ser los que tomen decisiones sobre los seres humanos.

Por lo tanto, este derecho es uno de los de mayor relevancia para nuestra investigación. Este derecho se encuentra titulado por el artículo 29 de los EPDPEI.

El numeral 29.1 de los EPDPEI, dispone que, cuando se afecte la vida íntima o la esfera jurídica de los titulares, el responsable tiene prohibido tomar decisiones automatizadas. Por ejemplo, el responsable no debe tomar decisiones automatizadas sobre el rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento del titular.

Sin embargo, la redacción del artículo solo niega al responsable el derecho a tomar una decisión sin intervención humana. Más no le niega el derecho a apoyarse en estas tecnologías para tomar una decisión que afecte al titular.

En este sentido, el numeral 29.2 explica que si es posible realizar tratamientos automatizados sin intervención humana cuando: 1) sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, 2) que esté autorizado por el derecho interno de los Estados Iberoamericanos, y 3) el titular lo haya consentido.

Pese a lo dispuesto en el inciso 1) anterior, el numeral 29.3 salvaguarda el derecho del titular a solicitar al responsable la intervención humana y a recibir una explicación del responsable, sobre la decisión que se tomó, e incluso permite al titular expresar su punto de vista e impugnar la decisión.

Por último, el numeral 29.4 prohíbe el tratamiento automatizado para la discriminación, por ejemplo: 1) origen racial o étnico, 2) creencias o convicciones religiosas, filosóficas y morales, 3) afiliación sindical, 4) opiniones políticas, 5) datos relativos a la salud, la vida preferencia u orientación sexual, y 6) datos

genéticos o datos biométricos.[179]2.8 Principios de la protección de datos personales

Con respecto a la protección de datos personales se han desarrollado diversos principios que son obligatorios para los responsables, a fin de asegurar el adecuado tratamiento de los datos de los titulares. Debido a su relevancia con respecto al seguimiento web, se analizan los principios de Transparencia y Privacidad por Diseño.

Principio de Transparencia y Aviso de Privacidad

El principio de Transparencia ordena al responsable el informar a los titulares, cuando realizan tratamiento de datos personales y la finalidad de dicho tratamiento. Este principio permite que los titulares puedan tomar decisiones informadas sobre sus datos.

En el contexto del seguimiento web, este principio surge cuando los responsables publican un enlace a su Aviso de Privacidad. El enlace suele encontrarse al final o al pie de los sitios web.

Sobre este principio, el artículo 16 de los EPDPEI establece la información mínima que el responsable debe proporcionar al titular, para dar transparencia al tratamiento de datos.

a) Identidad y datos de contacto del responsable.
b) Finalidades del tratamiento.
c) Comunicaciones de datos a terceros especificando quienes serán los destinatarios y por qué motivo.
d) Los mecanismos y procedimientos por los cuales el titular puede ejercer sus derechos ARCO ante el titular

179 Los datos biométricos son aquellos que permiten la identificación y/o autenticación de una persona mediante sus aspectos físicos y fisiológicos: huellas digitales, reconocimiento de iris, análisis de retina, reconocimiento facial, entre otros; y comportamentales: firma manuscrita, pulsación de teclas, a, forma de caminar, etc. Grupo de Trabajo del Artículo 29, *Documento de trabajo sobre biometría*, agosto de 2003, https://www.apda.ad/sites/default/files/2018-10/wp80_es.pdf (Fecha de consulta: 01 de junio de 2020)

e) Origen de datos personales que no fueron obtenidos directamente del titular.

Toda esta información debe presentarse en un lenguaje claro y sencillo, que incluso debe ser comprensible por niñas, niños y adolescentes cuando sea el caso:

Mientras que los Principios de la OEA marcan en el Principio Ocho: Claridad y Consentimiento, que se debe informar a los titulares de los fines para los cuales se obtienen sus datos personales.

El responsable también debe especificar las prácticas y políticas del tratamiento de datos personales. Estas deben incluir el fundamento jurídico, la forma en que se procesaran los datos, la identidad del responsable incluyendo datos de contacto y los medios por los que el titular puede ejercer sus derechos ARCO.

Principio de Privacidad Por Diseño

Este principio surge a fin de evitar que los titulares vean vulnerados sus derechos solo porque los responsables fallaron en diseñar sus sistemas con buenas prácticas en el tratamiento de los datos personales.

Los EPDPEI contemplan en el artículo 38 la obligación de los responsables de diseñar y aplicar medidas preventivas para salvaguardar la privacidad y seguridad de los datos personales y sus titulares. También marca la obligación de aplicar de forma los principios, derechos y obligaciones que marca la ley. Resaltando la importancia de estas medidas en los sistemas informáticos, que deben ajustarse al principio de privacidad por defecto y dar el mínimo tratamiento posible a los datos personales.

En los Principios de la OEA este principio se encuentra regulado en el Principio diez: Responsabilidad, que dispone la obligación que tienen los responsables de adoptar e implementar sistemas de protección de privacidad desde el diseño y arquitectura, tanto en tecnología como en prácticas comerciales.

El Principio Diez también nos dice que la privacidad y seguridad deben formar parte de todas las etapas de los productos o servicios que ofrecen los responsables. Además, los responsables deben estar preparados para demostrar

que han aplicado estos sistemas de privacidad si la autoridad nacional se los solicita.

2.2 Protección de datos personales en países latinoamericanos seleccionados

A continuación se presentan de forma breve los aspectos más relevantes del derecho a la protección de datos personales en los países seleccionados: Argentina, Brasil, Chile, Colombia, México y Perú, países que se han seleccionado por ser los más poblados de América Latina, con excepción de Venezuela por no contar con legislación en la materia.

Se espera que esto sea de utilidad para la mayoría de los miembros dela FSFLA, para lo cual se expone el fundamento de este derecho, protegido de forma constitucional en la mayoría de los países analizados, las legislaciones y disposiciones más importantes en la materia, así como la autoridad de control ante la cual los particulares pueden solicitar la protección de sus derechos ARCO.

2.2.1 Argentina

El derecho a la protección de datos personales es protegido en la Constitución de la Nación Argentina. Tiene su fundamento en el artículo 43, párrafo tercero. Dicho artículo nos dice que todas las personas tienen derecho a interponer una acción, expedita y rápida de amparo, a fin de conocer los datos concernientes a ella y la finalidad de estos, que se encuentren en registros de o bancos de datos, tanto públicos como privados destinados a proveer informes.[180]

El artículo también da el derecho a las personas de exigir la supresión, rectificación, confidencialidad o actualización de sus datos. Aunque esto no afecta, el derecho a mantener en secreto las fuentes de información periodísticas.

En esta materia son aplicables la Ley 25.326 de Protección de Datos del 2 noviembre de 2000, el Decreto 1558/2001 Reglamentación de la Ley de

180 Constitución de la Nación Argentina reformada en 1994, http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm (Fecha de consulta: 01 de junio de 2020)

Protección de Datos y la Ley 1.845 de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires.

Mediante el artículo 19 del Decreto 764/2017, se estableció que la Agencia de Acceso a la Información Pública es la autoridad encargada de la aplicación de la Ley de Protección de Datos Personales N° 25.326.[181]

La Agencia de Acceso a la Información Pública es la autoridad ante la cual se pueden ejercer los derechos ARCO. Para lo cual la agencia cuenta con diversas guías y documentos para hacer la solicitud correspondiente ante la autoridad, empresa o persona que tenga en su posesión los datos personales.

Además, existe el Registro Nacional de Bases de Datos Personales, el cual permite acceder a la información de los responsables que operan bases de datos personales, la finalidad de estas bases de datos, y el domicilio legal de los responsables. Facilitando el ejercicio de los derechos ARCO a los particulares.[182]

2.2.2 Brasil

En Brasil el derecho a la protección de datos personales es también llamado *habeas data*. Es protegido en el artículo 5 de la Constitución de la República Federal de Brasil (*Constituição da República Federativa do Brasil*). Siendo relevantes los numerales romanos X, LXXII y LXXVII. [183]

El numeral romano X, nos dice que son inviolables la intimidad, vida privada, honra e imágenes de las personas y se da el derecho a recibir una indemnización material o moral en caso de violación.

En el numeral romano LXXII se concede el "*habeas data*", para a) asegurar que el titular pueda tener la información relativa a su persona que conste en

181 Ley de Ministerios. Decreto 746/2017. http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279940/norma.htm (Fecha de consulta: 01 de junio de 2020)

182 Agencia de Acceso a la Información Pública, *Datos Personales: tus derechos* https://www.argentina.gob.ar/aaip/datospersonales/derechos (Fecha de consulta: 01 de junio de 2020)

183 Presidência da República, *Constituição da República Federativa do Brasil de 1988*, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm (Fecha de consulta: 01 de agosto de 2020)

registros o bancos de datos de entidades gubernamentales o de carácter público; y b) para la rectificación de datos, cuando no se quiera hacer mediante un procedimiento secreto, judicial o administrativo.

Por último, el numeral romano LXXVII indica que las acciones de *habeas data* y los actos necesarios para ejercer los derechos de protección de datos son gratuitos.

En cuanto a la legislación específica en la materia, en fecha 14 de agosto de 2018 se aprobó en Brasil la Ley N° 13.709 General de Protección de Datos Personales (*Lei Geral de Proteção de Dados Pessoais*),[184]

Sin embargo, entrará en vigor hasta fecha 3 de mayo de 2021 como se ordenó mediante la Medida Provisional 959/2020, publicada en el Diario Oficial de la Unión el 29 de abril de 2020.[185]

Esta nueva ley manda la creación de la Autoridad Nacional de Protección de Datos (*Autoridade Nacional de Proteção de Dados*) y del Consejo Nacional de Protección de Datos Personales y la Privacidad (*Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*), los cuales fueron ordenados mediante la Medida Provisional N° 869/2018, de conformidad a lo dispuesto en el Capítulo IX de la Ley N° 13.709 mencionada en el párrafo anterior.[186]

La Autoridad Nacional de Protección de Datos ya se encuentra operando, más el portal de Internet aún no cuenta con información sobre cómo realizar una reclamación contra los responsables del tratamiento de datos.[187] Por su parte, el

184 Presidência da República, *LEI Nº 13.709. Lei Geral de Proteção de Dados Pessoais)*, agosto de 2018, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm (Fecha de consulta: 01 de agosto de 2020)

185 Diário Oficial Da União, *Medida Provisória Nº 959*, abril 2020, https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639 (Fecha de consulta: 01 de agosto de 2020)

186 Congresso Nacional, *Medida Provisória n° 869, de 2018 (Proteção de dados pessoais)*, diciembre de 2018, https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062 (Fecha de consulta: 01 de agosto de 2020)

187 Autoridade Nacional de Proteção de Dados, *Reclamação do titular contra controlador de dados*, 05 de febrero de 2021, https://www.gov.br/anpd/pt-br/canais_atendimento/reclamacao-do-titular-contra-controlador-de-dados (Fecha de consulta: 10 de febrero de 2021)

Consejo Nacional de Protección de Datos Personales a la fecha de este escrito se encuentra en convocatoria abierta para su formación, la cual cerrará en marzo de 2021.[188]

También es relevante la Ley N° 12.695 Marco Civil de Internet (*Marco Civil da Internet*), de fecha 23 de abril de 2014, la cual establece los principios, garantías, derechos y obligaciones para el uso de Internet en Brasil.[189]

2.2.3 Chile

La Constitución Política de la República de Chile en el artículo 19, numeral 4°, asegura los derechos de las personas a la vida privada, la honra y la protección de datos personales. Esta protección al tratamiento de datos personales fue agregada a la Constitución mediante la Ley 21.09 el 16 de junio de 2018.[190]

Destaca la Ley 19.628 sobre Protección de la Vida Privada, publicada en 1999, ya que regula la autodeterminación informativa. Su artículo 13, ordena que no deben limitarse por ningún medio, acto o convenio, los derechos de los titulares a la información, modificación, cancelación o bloqueo de sus datos personales. El artículo 3 indica que el titular puede oponerse al uso de sus datos personales cuando el tratamiento tenga fines publicitarios, de investigación de mercado o encuestas de opinión.[191]

188 Autoridade Nacional de Proteção de Dados, *ANPD convoca sociedade para formação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade*, 05 de febrero de 2021, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-convoca-sociedade-para-formacao-do-conselho-nacional-de-protecao-de-dados-pessoais-e-da-privacidade (Fecha de consulta: 10 de febrero de 2021)

189 Câmara dos Deputados, *Lei Nº 12.965. Marco Civil da Internet*, abril de 2014, https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-norma-pl.html (Fecha de consulta: 01 de agosto de 2020)

190 Biblioteca del Congreso Nacional de Chile, *Fija el Texto Refundido, Coordinado y Sistematizado de la Constitucion Politica de la Republica de Chile*, https://www.bcn.cl/leychile/navegar?idNorma=242302

191 Biblioteca del Congreso Nacional de Chile, *Ley 19628 Sobre Proteccion de la Vida Privada*, https://www.bcn.cl/leychile/navegar?idNorma=141599

Esta ley ha sido criticada de ser deficiente y obsoleta para proteger a los ciudadanos contra las prácticas actuales de tratamiento de datos, pues en la ley no se establece una autoridad de control. Por el contrario, el artículo 16 indica que el titular debe recurrir al juez de letras en lo civil para hacer valer sus derechos. Lo que representa costos y gastos innecesarios, limitando el acceso a la protección de los derechos ARCO.[192]

También es importante el Decreto 779 que Aprueba Reglamento del Registro de Bancos de Datos Personales a Cargo de Organismos Públicos, emitido en el año 2000, y que reglamenta el artículo 22 de la ley 19.629.

Tras la reforma a la Constitución de 2018, con motivo de la mencionada deficiencia de la legislación vigente, en la actualidad se discute el proyecto de ley que "Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales", el cual, a la fecha de este escrito, aún se encuentra en el Senado en el Primer trámite constitucional.[193]

2.2.4 Colombia

El artículo 15 de la Constitución Política de la República de Colombia consagra el derecho a la protección de datos personales. Al que define como el derecho de las personas a conocer, actualizar y rectificar la información sobre ellas que se encuentre en bancos de datos y en archivos de entidades públicas y privadas. El artículo indica que en la recolección, tratamiento y circulación de datos deben respetarse la libertad y demás garantías que consagra la constitución.[194]

192 Viollier, Pablo, *El Estado de la Protección de Datos Personales en Chile*, Derechos Digitales América Latina, 2017, pp. 7-9, https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf (Fecha de consulta: 01 de agosto de 2020)

193 Cámara de Diputadas y Diputados, *Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*, 2017, https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07 (Fecha de consulta: 01 de agosto de 2020)

194 Secretaría General del Senado, *Constitución Política de la República de Colombia*, http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html#15 (Fecha de

Las leyes más relevantes en la materia son la Ley Estatutaria 1581 de 2012, la cual dicta disposiciones generales para la protección de datos personales, con fundamento en el mencionado el artículo 15 constitucional y el artículo 20 referente al derecho de acceso a la información.[195]

La ley es complementada por el Decreto número 1377 de 2013. El cual reglamenta parcialmente la mencionada Ley 1581, para regular en lo específico la protección de datos personales.[196]

La autoridad que recibe quejas materia de protección de datos personales es la Superintendencia de Industria y Comercio, de conformidad con el artículo 8 inciso d) de la Ley 1581.

El artículo 19 de la Ley 1581 marca que la autoridad de protección de datos es la SIC mediante la Delegatura para la Protección de Datos Personales. La Delegatura ejerce vigilancia para garantizar el respeto a los principios y derechos de la protección de datos previstos en la ley.

En el mismo sentido, el artículo 25 crea el Registro Nacional de Bases de Datos, que es un directorio público de las bases de datos personales sujetas a tratamiento que operan en el país. Y es operado por la Superintendencia de Industria y Comercio.

2.2.5 México

La Constitución Política de los Estados Unidos Mexicanos fue reformada en 2009 para agregar en los artículos 16 y 73, fracción XXIX-O, el derecho a la protección de datos personales. El artículo 16 le otorga el reconocimiento como derecho fundamental, y concede los derechos de acceso, rectificación, cancelación y oposición al uso de los datos personales, con las excepciones por

consulta: 01 de agosto de 2020)

195 Secretaría General del Senado, *Ley Estatutaria 1581 de 2012*, http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html#15 (Fecha de consulta: 01 de agosto de 2020)

196 Ministerio de Comercio, Industria y Turismo, *Decreto número 1377 de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012* https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf (Fecha de consulta: 01 de agosto de 2020)

razones de seguridad nacional, orden público, seguridad, salud pública y protección de los derechos de terceros.[197]

La reforma dio origen a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) emitida en 2010 y al Reglamento a la LFPDPPP emitido en 2011.

La Autoridad de Control en la materia es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Esto de conformidad con lo establecido en el artículo 6 constitucional tras ser reformado de 2014 mediante el "Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia".[198]

El artículo 6 constitucional, en el apartado A, indica que además, cada entidad federativa, en el ámbito de sus respectivas competencias, puede crear un organismo garante equivalente al INAI.

Esta reforma también ordenó en su artículo transitorio Segundo que se emitieran reformas a la ley en materia de protección de datos personales, en un plazo de un año, es decir el 7 de febrero de 2015.

De esta reforma se origina la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), que es la que regula las actuaciones sobre protección de datos personales para las entidades públicas.

Aún se encuentra pendiente de reformar lo correspondiente a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). La cual hace referencia al otrora Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), que fue derogado por la reforma de 2014, en el artículo transitorio tercero.

197 Cámara de Diputados del H. Congreso de la Unión. *Constitución Política de los Estados Unidos Mexicanos*, http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf (Fecha de consulta: 28 de julio de 2020).

198 Diario Oficial de la Federación, *DECRETO por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia*, DOF, febrero de 2014. http://dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014 (Fecha de consulta: 28 de julio de 2020).

A fin de coordinar, organizar y evaluar las acciones de la política pública en materia protección de datos personales, la LGPDPPSO crea en su Título Primero, Capítulo II; el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (SNT), el cual contribuye a mantener la vigencia del derecho a la protección de datos personales en los tres órdenes de gobierno.

Para lograr esto, fue creado el Programa Nacional de Protección de Datos Personales (PRONADATOS), principal instrumento del SNT para definir y coordinar al sector público, mediante Acuerdo de fecha 21 de enero de 2018.[199]

2.2.6 Perú

En el artículo 2, numeral 6, de la Constitución Política de Perú, se consagra la protección a los datos personales. El cual protege a todas las personas, al prohibir la distribución de información que afecte su intimidad personal y familiar mediante servicios informáticos, públicos o privados, tanto si son computarizados como si no lo son.[200]

Para reglamentar este artículo, se emitió en 2011 la Ley N° 29733, Ley de Protección de Datos Personales, con el objetivo de garantizar este derecho a través de un adecuado tratamiento de los datos, en un marco de respeto a los demás derechos fundamentales protegidos por la constitución.[201]

El artículo 32 de la Ley 29733 indica que el Órgano competente en la materia es el Ministerio de Justicia y Derechos Humanos, que asume la Autoridad Nacional de Protección de Datos Personales.

199 Diario Oficial de la Federación, *ACUERDO mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales*, DOF, enero 2018, https://www.dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018 (Fecha de consulta: 28 de julio de 2020).

200 Congreso de la República del Perú, *Constitución Política de Perú*, diciembre 1993, http://www4.congreso.gob.pe/ntley/Imagenes/Constitu/Cons1993.pdf (Fecha de consulta: 28 de julio de 2020).

201 Congreso de la República del Perú, *Ley N° 29733, Ley de Protección de Datos Personales*, julio 2011, http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf (Fecha de consulta: 28 de julio de 2020).

Esta ley define en el artículo 2 los Bancos de Datos Personales, como el conjunto organizado de datos personales, automatizado o no, independiente del medio físico en que se almacenen, y sin importar la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

En este sentido, el artículo 28 obliga a los encargados de los bancos de datos a proporcionar a la APDP cualquier información que se le requiera. Y a permitir el acceso a los bancos de datos cuando sea solicitado en un procedimiento iniciado por el titular de los datos.

Además, el artículo 34 crea el Registro Nacional de Protección de Datos Personales, el cual está a cargo de la Autoridad Nacional de Protección de Datos Personales y tiene la finalidad de inscribir todos los bancos de datos tanto públicos como privados. A fin de que cualquier persona pueda consultar la existencia de los Bancos de Datos Personales, sus finalidades; la identidad y domicilio de los responsables, e incluso de sus encargados.

Es obligatoria la inscripción de los Bancos de Datos Personales en el Registro Nacional de Protección de Datos Personales, de conformidad con el artículo 38, que califica de infracción grave el incumplir con esta obligación. El Registro Nacional de Protección de Datos Personales puede ser consultado en línea en la Plataforma digital única del Estado Peruano.[202]

La Primera Disposición Complementaria Final de la mencionada ley dispone que se constituya una Comisión Multisectorial, presidida por la Autoridad Nacional de Protección de Datos Personales, para la elaboración del correspondiente Reglamento de la Ley N° 29733, el cual fue emitido en 2013.[203]

202 Plataforma digital única del Estado Peruano, *Consultar el Registro Nacional de Protección de Datos Personales*, https://www.gob.pe/9254-consultar-el-registro-nacional-de-proteccion-de-datos-personales (Fecha de consulta: 28 de julio de 2020).

203 Ministerio de Justicia y Derechos Humanos, *Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales*, marzo 2013, https://www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf (Fecha de consulta: 28 de julio de 2020).

2.3 Protección de datos personales, seguimiento web y la FSFLA

En el marco del seguimiento web, conocer el derecho a la protección de datos personales es importante, ya que en ocasiones, es necesario proporcionar datos personales para utilizar un servicio web, por ejemplo, para realizar compras en un sitio web, suscribirse a una red social, e incluso por motivos laborales o para realizar un trámite en línea ante la autoridad gubernamental.

Estos ejemplos son reales, en 2020 la Secretaría de la Función Pública en México, expuso en la web la declaración patrimonial de 830,000 funcionarios públicos, sin contraseñas ni medidas de seguridad, por lo que el INAI consideró que la Secretaría incumplió con sus obligaciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.[204]

En 2021 la Comisión de Protección de Datos de Irlanda comenzó una investigación en contra de Facebook por la fuga de datos de 533 millones de usuarios, cómo números de teléfono y otros datos que los usuarios no habían hecho públicos en sus perfiles, lo que se encontraría en violación del RGPD.[205]

Las fugas de datos son, relativamente comunes, compañías como Home Depot, UPS, eBay, Yahoo!, entre otras.[206] Tan solo en 2018 se detectaron más de 500 millones de datos personales robados de bases de datos. Las fugas de datos son tan grandes que ya se habla de una “fatiga de fugas de datos”, pues estos eventos se han vuelto tan comunes que la sociedad ya se ha “fatigado” de escucharlos.[207]

204 Soto Galindo, José, *Función Pública incumplió con la ley por fuga de datos personales: Inai*, El Economista, noviembre 2020, https://www.eleconomista.com.mx/politica/Funcion-Publica-incumplio-con-la-ley-por-fuga-de-datos-personales-Inai-20201124-0082.html (Fecha de consulta: 28 de junio de 2021).

205 Holmes, AAron, *Facebook está bajo investigación en la UE por la filtración masiva de datos de 533 millones de personas, y podría enfrentar una multa de miles de millones de dólares*, Business Insider México, abril 2021 (Fecha de consulta: 28 de junio de 2021). https://businessinsider.mx/facebook-investigacion-ue-filtracion-masiva-de-datos-multa/

206 Mendoza, Miguel Ángel, *¿Por qué es importante proteger tus datos personales?*, We Live Security, octubre 2015, https://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/ (Fecha de consulta: 28 de junio de 2021).

El grupo “Privacy Rights Clearinghouse” ha registrado cerca de 20,000 eventos de fugas de datos, siendo víctimas instituciones financieras, negocios, escuelas, centros de salud e instituciones gubernamentales y militares.[208]

Es claro que cuando entrega datos personales, el usuario queda expuesto a los problemas del seguimiento web, afortunadamente, conocer el derecho a la protección de datos permite su ejercicio, por ejemplo, el usuario puede ejercer su derecho a la oposición o a la cancelación.

Basta que se dirija al aviso de privacidad del sitio web, y encuentre la información pertinente para ejercer estos derechos. En caso de una falta de respuesta, de una respuesta negativa, o inapropiada, el usuario siempre podrá acudir ante la autoridad de protección de datos personales de su país, evitando con ello se afecten otros derechos y libertades.

Conocer estos derechos permitirá a los miembros de la FSFLA proteger su privacidad al navegar en la web, no solo haciendo uso de elementos tecnológicos, pues, cómo ya se mencionó, en ocasiones es indispensable el entregar datos personales. Cuando estas situaciones ocurren, los miembros de la FSFLA siempre pueden ejercer sus derechos consagrados en la ley.

207 Zorabedian, John, *Data Breach Fatigue Makes Every Day Feel Like Groundhog Day*, Security Intelligence, febrero 2019, https://securityintelligence.com/data-breach-fatigue-makes-every-day-feel-like-groundhog-day/ (Fecha de consulta: 28 de junio de 2021); Boffey, Daniel, *Registration cards of Dutch Holocaust victims to go on display*, The Guardian, enero 2021, https://www.theguardian.com/world/2021/jan/26/registration-cards-dutch-jews-display-holocaust-museum-amsterdam (Fecha de consulta: 14 de julio de 2021).

208 Privacy Rights Clearinghouse, *Data Breaches*, Privacy Rights Clearinghouse, https://privacyrights.org/data-breaches (Fecha de consulta: 28 de junio de 2021).

Capítulo 3

Sugerencias para los miembros de la FSFLA

Capítulo 3. Sugerencias para los miembros de la FSFLA

3.1 Antecedentes sobre la FSFLA

La Fundación del Software Libre América Latina es una organización creada con el objetivo de promover, defender y difundir las ideas del Software Libre, es decir el software que respeta el derecho de las personas a usar, estudiar, copiar, modificar y redistribuir software. [209]

En este sentido, un programa es considerado Software Libre, cuando respeta las cuatro libertades esenciales de acuerdo con la definición del Software Libre del proyecto GNU, iniciado por Richard Stallman en 1983 para crear un sistema operativo de Software Libre que promoviera el espíritu cooperativo entre la comunidad informática. En la actualidad el sistema operativo funciona en conjunto con el núcleo Linux, por lo que al sistema operativo se le denomina GNU/Linux.[210]

Las cuatro libertades esenciales son:

La libertad de ejecutar el programa como se desee, con cualquier propósito (libertad 0).

La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello.

La libertad de redistribuir copias para ayudar a otros (libertad 2).

La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3).

Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.[211]

---

209 FSFLA, *Constitución*, FSFLA, 2019, http://www.fsfla.org/ikiwiki/about/constitution.es.html (Fecha de consulta: 29 de Abril de 2020)

210 El Sistema Operativo GNU, *Visión general del sistema GNU*, https://www.gnu.org/gnu/gnu-history.es.html (Fecha de consulta: 28 de julio de 2020).

211 El Sistema Operativo GNU, *¿Qué es el software libre?*, https://www.gnu.org/philosophy/free-sw.es.html (Fecha de consulta: 28 de julio de 2020).

Para que la presente propuesta de intervención sea de utilidad a la FSFLA es necesario que sea ajuste a la Constitución de la FSFLA, es decir que fomente la adopción de Software Libre, las sugerencias propuestas para evitar el seguimiento web, exclusivamente hacen uso de Software Libre.

Debido a la multitud de licencias de software que existen, se tomará de guía las recomendaciones de la Fundación del Software Libre *Free Software Foundation* (FSF), la cual es una organización hermana de la FSFLA y que en su sitio web lista las licencias que cumplen los criterios para ser consideradas Software Libre.[212]

Se considera importante destacar que el software que no es libre, conocido también como software privativo,[213] no puede asegurar la seguridad del usuario, ya que el código fuente del programa normalmente no se encuentra disponible para ser auditado por cualquier persona.

En la ingeniería informática y criptografía, la práctica de esconder, ocultar o mantener en secreto el diseño de un sistema es conocida como “seguridad por obscuridad” esta práctica es considerada débil, incluso el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) recomienda utilizar diseños libres y evitar la seguridad por obscuridad, ya que la “seguridad de un sistema no debe depender en el secreto de su implementación o sus componentes”.[214]

Además, para los usuarios, el software privativo puede traer riesgos, tanto en lo personal como en lo social. Un ejemplo claro viene de Argentina, donde se utilizó software de control de las máquinas de voto electrónico en elecciones de 2017, la empresa MSA, que elaboraba este software mantenía su código oculto,

212 Oficina de Licencias y Cumplimiento de la Fundación del Software Libre, *Lista de licencias con comentarios*, El Sistema Operativo GNU, https://www.gnu.org/licenses/license-list.es.html (Fecha de consulta: 28 de julio de 2020).

213 El Sistema Operativo GNU, *El software privativo a menudo es malware*, https://www.gnu.org/proprietary/proprietary.es.html (Fecha de consulta: 28 de julio de 2020).

214 Scarfone, Karen, *et al.*, “Guide to General Server Security”, *Reccomendations of the National Institute of Standards and Technology*, 2008, pp. 2-4, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf (Fecha de consulta: 28 de julio de 2020).

pero una versión del software fue filtrada a los pocos días de estas elecciones, como la empresa MSA mantenía el código oculto, los ciudadanos no podían verificar si el software utilizado en las computadoras era el oficial.[215]

En 2016, la secretaria del Tribunal Electoral de la Provincia de Salta, Teresa Ovejero, había advertido sobre este problema ante la Cámara de Diputados de la Nación, pues afirmó que fácilmente se podría alterar el software de las máquinas de voto electrónico si este software privativo estuviera en manos de una persona que quisiera alterar los resultados de la elección.[216]

Pues el software privativo impide a los ciudadanos verificar si las máquinas utilizaron el software oficial. Múltiples expertos también pusieron en duda la seguridad del sistema, ya que iba en contra de las buenas prácticas.[217]

En este mismo sentido, la FSF mantiene una lista exhaustiva y documentada de las funcionalidades maliciosas que han sido implementadas en el software propietario por empresas como Adobe, Amazon, Apple, Google y Microsoft, así como las injusticias a las que se puede someter a los usuarios con el software privativo: censura, fraudes, incompatibilidad, inseguridad, intromisión, vigilancia, obsolescencia programada.[218]

---

215 La Nación, “Filtran el software de control de una máquina de voto electrónico usada en Salta”, agosto de 2017, https://www.lanacion.com.ar/tecnologia/filtran-el-codigo-de-una-maquina-de-voto-electronico-de-salta-y-alertan-sobre-los-riesgos-del-sistema-nid2054577 (Fecha de consulta: 28 de julio de 2020).

216 Noticias Iruya, “Una “explicación” de Teresa Ovejero hunde al voto electrónico”, agosto 2016, https://noticias.iruya.com/a/politica/elecciones/17864-una-explicacion-de-teresa-ovejero-hunde-al-voto-electronico.html (Fecha de consulta: 28 de julio de 2020).

217 La Nación, “Dudas entre los expertos por el proyecto para usar una boleta única electrónica nacional”, julio 2016, https://www.lanacion.com.ar/tecnologia/dudas-entre-los-expertos-por-el-proyecto-para-usar-una-boleta-unica-electronica-nacional-nid1921720 (Fecha de consulta: 28 de julio de 2020).

218 El Sistema Operativo GNU, *El software privativo a menudo es malware*, https://www.gnu.org/proprietary/proprietary.es.html (Fecha de consulta: 28 de julio de 2020).

3.2 Propuesta de intervención para la difusión de formas de protección contra el seguimiento web

Cómo se ha mencionado a lo largo de los capítulos anteriores, el seguimiento web se ha convertido en un problema real cuando navegamos en la web.

El presente trabajo busca responder a las inquietudes de los miembros de la FSFLA quienes se preocupan por su privacidad en la web y por cómo defenderse de esta práctica.

Para lo cual, se ha decidido enfocar esta propuesta de intervención en dos aspectos específicos: primero el de informar, tanto del panorama del seguimiento web y su aspecto tecnológico, como del derecho de la protección de datos personales lo que se considera que se ha logrado mediante la información contenida en los capítulos anteriores.

El segundo, aspecto, informar sobre los programas y herramientas de Software Libre que pueden utilizar los usuarios para proteger su privacidad al navegar en la web. Este es quizás el aspecto más relevante para la misión de la FSFLA, pues esta Fundación busca promover el Software Libre en América Latina.

Estos aspectos han sirven de guía para los objetivos y el plan de acción que se presentan a continuación.

Objetivos generales

La presente propuesta tiene por objetivo presentar un plan de acción ante la FSLA para ayudar a sus miembros a proteger su privacidad en la web e incluso mantener el anonimato, mediante el uso de proyectos de Software Libre.

Así como informar y difundir sobre la problemática del seguimiento web, su panorama actual y empedrar a los miembros de la FSFLA para que eviten ser víctimas de vulneración a sus datos personales.

Objetivos específicos

Primera Etapa

Proponer al Consejo de la FSFLA que se incluyan en el artículo 2 de la Constitución el que sea objetivo de esta Fundación el realizar actividades para promover y proteger la privacidad de los usuarios en la web.

Segunda Etapa

Realizar actividades y talleres para la difusión y favorecer el uso de herramientas de Software Libre que ayudan a preservar la privacidad en la web.

Realizar pláticas para la difusión del derecho a la protección de datos personales.

Tercera Etapa

Crear un espacio en el sitio web de la FSFLA para promover la privacidad en la web, informar sobre el seguimiento web y el derecho a la protección de datos personales.

3.3 Plan de Acción

Primera Etapa – 1 a 2 meses

En esta primera etapa se propone que el Consejo discuta y apruebe que en la Constitución de la FSFLA se agregué un apartado al artículo 2, respecto a la defensa de la privacidad y mantener una posición en contra del seguimiento web. Así como la difusión y promoción de herramientas de Software Libre que ayudan a los usuarios a proteger su privacidad y anonimato al navegar en la web.

Segunda Etapa – 2 a 4 meses

En esta segunda etapa se propone, que el Consejo incluya en el sitio web de la FSFLA un apartado para el fomento, difusión y promoción de las herramientas de Software Libre para la protección contra el seguimiento web y

para informar sobre el derecho a la protección de datos personales en América Latina.

Además, que se utilicen las listas de distribución para organizar actividades, conferencias y talleres para la difusión y enseñanza de las herramientas de Software Libre que ayudan a preservar la privacidad y el anonimato en la web, difundir el derecho a la protección de datos personales y resolver dudas e inquietudes de los miembros. Estos talleres se describen más adelante en la sección **3.3.1 Talleres.**

Tercera etapa de 4 a 12 meses.

En esta tercera etapa se deberán impartir los talleres organizados en la etapa anterior por el Consejo de la FSFLA.

Esta tercera etapa requerirá la participación activa de los miembros de la FSFLA, en las formas listadas a continuación:

La primera, participar activamente en los talleres y actividades organizadas por el Consejo, a fin de capacitarse y aprender las formas en las que pueden proteger su privacidad con el Software Libre y aprender los conceptos básicos sobre el derecho de protección de datos personales, a fin de que puedan ejercer este derecho.

La segunda, colaborar con la FSFLA, ya sea creando materiales, documentos, imágenes, vídeos y demás documentos, así como impartiendo talleres y conferencias para ayudar a promover la defensa de la privacidad en la web y compartiendo noticias relevantes, a fin de impulsar estas actuaciones para garantizar que los nuevos miembros, e incluso la sociedad en general, puedan acceder a materiales relevantes en el tema.

La tercera, informarse, promover y difundir la importancia de la privacidad en la web, tanto con otros miembros de la FSFLA, como ante la sociedad en general, ya que la FSFLA cuenta con escasos recursos económicos, y es necesario el apoyo de todos los miembros en este tipo de iniciativas.

Por último, enseñar, en la medida de lo posible, a otros miembros y a la sociedad en general, a utilizar los recursos de Software Libre que se listan más

adelante. Pues estas herramientas en ocasiones no son aprovechadas, ya que son poco conocidas y pueden ser difíciles de entender para personas con pocas habilidades técnicas.

Adoptar nuevas herramientas, puede ser difícil, especialmente para personas que están acostumbradas a utilizar servicios de empresas como Microsoft, Google, Facebook, Apple, entre otras. Si bien adoptar nuevo software y nuevos servicios es proceso es complicado, se sugiere no realizar un cambio radical. Es mejor un cambio en fases, aprendiendo en cada fase una nueva herramienta, sus usos y sus beneficios.

Un cambio completo de la noche a la mañana puede llevar a frustraciones, especialmente cuando se trata de usuarios con pocas habilidades técnicas y digitales que aún no aprenden estas nuevas herramientas ni su forma de trabajo. Pues les puede causar a una sobre saturación de información el tener que aprender muchas herramientas en muy poco tiempo.

3.3.1 Talleres

A continuación se proponen los talleres que deberían impartirse durante la tercera etapa, de manera general, el objetivo de estos talleres deberá ser el de informar a los asistentes para que conozcan sobre el seguimiento web y su impacto, así como capacitarlos para que conozcan y aprendan a utilizar y las herramientas que les permitirán protegerse del seguimiento web, si así lo desean hacer. Respetando siempre los valores del software libre y de la FSFLA.

Taller 1: Introducción al seguimiento web

El objetivo de este taller es informar a los asistentes sobre seguimiento web: qué es, cómo se realiza y su alcance. Para lo cuál se recomienda utilizar el contenido del capítulo 1 de esta investigación, especialmente las secciones 1.1 y 1.2, y hacer referencia a la sección 1.5, sobre como impacta el seguimiento web a la FSFLA.

Taller 2: ¿Quiénes me siguen en la web?

El objetivo de este taller es informar a los asistentes sobre el panorama actual del seguimiento web: los principales actores, el negocio del seguimiento web, el impacto en la vida personales de los asistentes y que se puede saber de ellos gracias al seguimiento web, así como la forma en la que afecta a la FSLA. Para lo cuál se recomienda utilizar el contenido del capítulo 1 de esta investigación, especialmente las secciones 1.3, 1.4 y 1.5.

Taller 3: Introducción al Derecho de Protección de Datos Personales

El objetivo de este taller es introducir a los asistentes el derecho a la protección de datos personales en América Latina, los derechos ARCO y el Aviso de Privacidad. Para lo cuál se recomienda utilizar el contenido del capítulo 2 de esta investigación, especialmente las secciones 2.1 y hacer referencia a la sección 2.3 sobre cómo se relaciona la protección de datos personales con el seguimiento web.

Taller 4: Protección de Datos Personales en América Latina

El objetivo de este taller es informar a los asistentes sobre el derecho a la protección de datos personales en lo particular en los países Argentina, Brasil, Chile, Colombia, México y Perú, cuales leyes brindan está protección, la Autoridad de Control ante la cuál pueden acudir para ejercer sus derechos y la relación de la protección de datos con el seguimiento web y la FSFLA. Para lo cuál se recomienda utilizar el contenido del capítulo 2 de esta investigación, especialmente las secciones 2.2 y 2.3.

Taller 5: Herramientas para la protección contra el seguimiento web

El objetivo de este taller es informar a los asistentes sobre el software libre, los navegadores y extensiones del navegador, así como otras herramientas de software libre que pueden utilizarse para disminuir o limitar el impacto del seguimiento web en las asistentes. Para lo cuál se recomienda utilizar el contenido del capítulo 3 de esta investigación, especialmente las secciones 3.4.1 y 3.4.2.

Taller 6: Servicios Web para la protección contra el seguimiento web

El objetivo de este taller es informar a los asistentes sobre los servicios web que pueden utilizar para sustituir algunos servicios que ya utilizan en la actualidad, los servicios son recomendados por ser respetuosos de la privacidad de los usuarios y porque son software libre. Para lo cuál se recomienda utilizar el contenido del capítulo 3 de esta investigación, especialmente las secciones 3.4.3 y 3.5.

3.4 Herramientas específicas

Para esta propuesta, se han buscado alternativas con las cuales se pueden remplazar populares programas y servicios de software propietario y que suelen dedicarse al seguimiento web y/o a compartir información con empresas de este tipo.

Donde ha sido posible, se han elegido los proyectos de Software Libre considerados de alta prioridad por la FSF[219] que sirven para proteger la privacidad y anonimato de los usuarios, debido a que tienen una importancia estratégica para la adopción de Software Libre en todo el mundo.[220]

Debe hacerse énfasis en que estos servicios y programas por sí mismos no son suficientes para proteger al usuario completamente ni contra todas las técnicas de seguimiento web. Sin embargo, se han elegido herramientas que proporcionan bastante protección con poco esfuerzo y configuraciones por parte del usuario.

Se resalta la importancia de utilizar estos programas y servicios desde una distribución libre del sistema operativo GNU/Linux. Si bien algunos de los programas o servicios mencionados más adelante funcionan en sistemas operativos que no son libres, como Microsoft Windows o Apple MacOS, se

219 Free Software Directory, *Collection:High Priority Projects*, https://directory.fsf.org/wiki/Collection:High_Priority_Projects (Fecha de consulta: 28 de julio de 2020).

220 Free Software Foundation, *High Priority Free Software Projects*, https://www.fsf.org/campaigns/priority-projects (Fecha de consulta: 28 de julio de 2020).

desaconseja su uso debido a que estos sistemas van en contra los principios de la FSFLA.

3.4.1 Navegadores Libres

El primer elemento a considerar para evitar el seguimiento web es tener acceso a un navegador que proteja la privacidad del usuario y por defecto lo proteja contra estas técnicas. Ya en el Capítulo Primero se mostraba como el seguimiento web puede comenzar con el navegador.

Se han identificado tres navegadores de Software Libre y que no tienen ningún costo. Los usuarios pueden utilizar estos navegadores para proteger su privacidad, y pueden reforzarlos mediante la instalación de extensiones y configuraciones de privacidad que se expondrán en las secciones siguientes, los navegadores son:

GNU IceCat

Este navegador es la versión del navegador Firefox, que ha sido modificada por el proyecto GNU para contener exclusivamente software libre, así como para evitar que el usuario instale extensiones que no son Software Libre y por tanto pueden afectar su libertad. El navegador incluye algunas configuraciones de seguridad:[221]

- Extensión *LibreJS*, la cual evita que el usuario ejecute código Javascript que no cuenta con una licencia de Software Libre.
- Extensión *Https-Everywhere*, la cual obliga a los sitios web a utilizar cifrado en las solicitudes HTTP.
- Extensión *SpyBlock*, la cual bloquea los rastreadores utilizados para el seguimiento web y todas las solicitudes de sitios de terceros al navegar en el modo privado.
- Remplazo a la página principal por *about:icecat*, para mostrar al usuario información sobre el software libre y que permite modificar las configuraciones de privacidad del navegador GNU Icecat.

221 El Sistema Operativo GNU, *GNUzilla and IceCat*, https://www.gnu.org/software/gnuzilla/ (Fecha de consulta: 28 de julio de 2020).

- Configuraciones por defecto para deshabilitar el seguimiento web mediante técnicas de *huella digital de dispositivo*.

IceWeasel

Este es un navegador que se incluye en los repositorios de Parábola, una distribución del sistema operativo GNU/Linux aprobada por la FSF, ya en sus repositorios contiene exclusivamente paquetes de software libre.[222]

Uno de estos paquetes es IceWeasel, un navegador basado en Firefox con configuraciones de privacidad y para remover el código y extensoras que no son libres. Para reforzar la privacidad del navegador IceWeasel, Parábola también ofrece paquetes para ofrecer a los usuarios la protección de su seguridad, privacidad y prevención contra los mecanismos de seguimiento web:[223]

- Paquete *iceweasel-hardened-preferencias*, el cual es creado por Parábola para proteger contra ataques de huella digital y privacidad.[224]
- Paquete *iceweasel-noscrpit*, que instala la extensión *NoScript*, el cual bloquea la ejecución de código Javascript mientras el usuario no lo permita, lo que impide la ejecución de rastreadores web.[225]
- Paquete *iceweasel-ublock-origin*, que instala la extensión *Ublock Origin*, el cual bloquea anuncios y rastreadores web.[226]

---

222 Párabola GNU/Linux-libre, *¿Qué es Parabola?* https://wiki.parabola.nu/Main_Page_(Español) (Fecha de consulta: 28 de julio de 2020).

223 Párabola GNU/Linux-libre, *IceWeasel History* https://wiki.parabola.nu/IceWeasel_History (Fecha de consulta: 28 de julio de 2020).

224 Párabola GNU/Linux-libre, *iceweasel-hardened-preferences*, https://www.parabola.nu/packages/nonprism/x86_64/iceweasel-hardened-preferences/ (Fecha de consulta: 28 de julio de 2020).

225 Párabola GNU/Linux-libre, *iceweasel-noscrpit*, https://www.parabola.nu/packages/libre/x86_64/iceweasel-noscript/ (Fecha de consulta: 28 de julio de 2020).

226 Párabola GNU/Linux-libre, *iceweasel-ublock-origin*, https://www.parabola.nu/packages/libre/x86_64/iceweasel-ublock-origin/ (Fecha de consulta: 28 de julio de 2020).

- Paquete *iceweasel-https-everywhere*, que instala la extensión *Https-Everywhere*, el cual obliga a los sitios web a utilizar cifrado en las solicitudes HTTP.[227]

Tor Browser

El Navegador Tor utiliza la red Tor, red de túneles virtuales creada para proteger tanto la privacidad como el anonimato de los usuarios. Este navegador impide que tanto el Proveedor de Servicios de Internet (ISP) como cualquier otro ente que observe la conexión local sea incapaz de conocer la actividad del usuario en la Web, incluyendo los nombres y direcciones de los sitios web visitados; además los sitios y servicios web visitados tampoco pueden conocer la dirección IP del usuario, ya que solo ven una conexión proveniente de la red Tor y no pueden seguir al usuario a menos que se identifique de forma concreta.[228]

Este navegador de forma predeterminada impide que los sitios web realicen seguimiento de huella digital o por la configuración del navegador. Tampoco conserva ningún historial de navegación, y las cookies solo tienen validez durante una sola sesión, siendo eliminadas al cerrar el navegador o al solicitar una nueva sesión.

3.4.2 Extensiones

Si bien existen múltiples extensiones para los navegadores GNU IceCat, IceWeasel y Tor Browser, a continuación se presenta una lista de algunas extensiones disponibles para los tres navegadores y que protegen contra el seguimiento web, aunque no se pretende dar una lista exhaustiva, pues solo se han seleccionado los que brindan la mayor privacidad posible con la menor cantidad de configuraciones y que permiten al usuario, en medida de lo posible,

227 Párabola GNU/Linux-libre, *iceweasel-https-everywhere*, https://www.parabola.nu/packages/libre/x86_64/iceweasel-https-everywhere/ (Fecha de consulta: 28 de julio de 2020).

228 Tor, *Acerca del Navegador Tor*, https://tb-manual.torproject.org/es/about/ (Fecha de consulta: 28 de julio de 2020).

instalar y olvidar, además de ser considerados proyectos de alta prioridad por la FSF.

- Cookie AutoDelete: Extensión que elimina cookies cuando se cierra una pestaña del navegador y todas las cookies que no están en funcionamiento. Permite tener una lista de cookies permitidas y una lista de cookies bloqueadas.
- Decentraleyes: Extensión que impide que se carguen algunas librerías web de terceras partes, para impedir que los sitios web que necesitan estas librerías dejen de funcionar las sustituye por versiones instaladas en el ordenador del usuario.
- HTTPS Everywhere: Extensión que cifra las comunicaciones con múltiples sitios web, impidiendo que terceros observen las comunicaciones del usuario.
- Location Guard: Extensión que oculta la ubicación del usuario y la sustituye por una ubicación falta, además de agregar ruido aleatorio a la ubicación para una mayor privacidad.
- NoScript: Extensión que por defecto impide que los sitios web ejecuten código Javascript en el ordenador del usuario. Permite mantener una lista de sitios web permitidos y bloqueados.
- Ublock Origin: Extensión que bloquea una gran cantidad de rastreadores y anuncios web.

3.4.3 Servicios Web

Es claro que no es suficiente instalar complementos que protegen la privacidad del usuario, ya que muchos servicios no funcionan correctamente si el usuario bloquea rastreadores, anuncios y código Javascript, por ende, es necesario brindar a los usuarios una lista de servicios que pueden utilizar para sustituir los principales servicios web.

Redes Sociales

A continuación se detallan dos estándares ActivityPub y OStatus, que en conjunto con sus implementaciones forman una red mayor llamada “fediverso” por la unión de las palabras “federación” y “universo”, ya que estas plataformas pueden comunicarse unas con otras, a diferencia de plataformas propietarias como Youtube, Facebook o Twitter, que no permiten que sus usuarios interactúen entre sí; en general, los usuarios del fediverso pueden interactuar con usuarios y canales de otros servicios sin tener que visitar o tener cuenta en otro sitio web, por ejemplo, un usuario de Mastodon puede ver y comentar vídeos publicados en un canal de PeerTube, puede observar, comentar y compartir las fotografías de una modelo de PixelFed y puede escuchar la música de sus artistas favoritos en Funkwhale, todo sin salir de Mastodon.[229]

Las implementaciones de estos protocolos son software libre y pueden ser instaladas en el servidor del usuario. Existen diversos protocolos e implementaciones que pueden comunicarse por el fediverso, a continuación se listan algunas de las más sencillas de utilizar.

- ActivityPub: Es un estándar oficial y recomendado del *World Wide Web Consortium*, también llamado Consorcio WWW y W3C, el cual genera los estándares y recomendaciones de la Web. El protocolo ActivityPub es un estándar para la creación de redes sociales descentralizadas, por lo que múltiples servidores y clientes existen y se basa en el estándar de información ActivityStreams 2.0 también publicado por el W3C.[230]

Entre las principales implementaciones destacan Mastodon, Pleroma, Socialhome y Friendica, servidores de redes sociales que se asemejan a Twitter y Facebook, también son similares a diaspora*, aunque esta utiliza el protocolo federado diaspora; PixelFed es una red social similar a Instagram; Funkwhale es similar a SoundCloud; Nextcloud (que será descrito con más adelante a mayor detalle) es un servicio de nube similar a DropBox, Office 365 o Google Drive; y

229 Fediverse, “Fediverse, diversity is strength”, https://fediverse.party/en/fediverse, (Fecha de consulta: 29 de julio de 2020).

230 W3C, “ActivityPub” https://www.w3.org/TR/activitypub/, (Fecha de consulta: 29 de julio de 2020).

Write Freely un servidor para publicar blogs o documentos, similar a Medium y WordPress, este último también puede utilizar el protocolo ActivityPub aunque no de forma predeterminada, sino mediante la instalación de una extensión. Además, el software de WordPress es libre por lo que su uso no causa problemas contra la libertad de los usuarios mientras no se use en conjunto con complementos privativos.

- Ostatus: Otro estándar para redes sociales de microblogging, es decir similares a Twitter. Es un protocolo abierto que utiliza otros protocolos abiertos como Atom, ActivityStreams, WebSub, Salmon y WebFinger.[231] OStatus es soportado por la red social Friendica, la cual fue mencionada anteriormente ya que también soporta ActivityPub; y por GNU Social, una red social que fue creada específicamente para soportar el estándar OStatus. GNU Social es utilizado de forma oficial por la FSF, además, no requiere de Javascript.[232]

Buscadores Web

Searx: es un buscador de internet denominado “metabuscador”, es decir que utiliza información de otros motores de búsqueda, como Google, Yahoo, Bing, entre otros, en la actualidad soporta más de 70 servicios, e impide que los usuarios sean objeto del o de perfilamiento, por defecto no utiliza cookies, además, permite ser utilizado con el navegador Tor o la red Tor para mayor privacidad del usuario.

Searx puede ser instalado en el servidor del usuario, para usarlo desde múltiples dispositivos o se puede utilizar una instancia de alguna organización, las cuales se encuentran registradas en el sitio web del proyecto Searx.[233]

---

231 Prodromou, Evan, *et al.*, “OStatus 1.0 Draft 2”, https://www.w3.org/community/ostatus/wiki/images/9/93/OStatus_1.0_Draft_2.pdf, (Fecha de consulta: 29 de julio de 2020).

232 GNU Social, “The Project”, https://gnusocial.network/ (Fecha de consulta: 29 de julio de 2020).

233 Searx, “Welcome to searx”, https://asciimoo.github.io/searx/ (Fecha de consulta: 29 de julio de 2020).

Comunicación Instantánea y Videoconferencias

- Matrix, Synapse y Element:

Matrix es un protocolo libre para comunicaciones en tiempo real, descentralizadas y seguras. Como protocolo, Matrix no hace referencia a un proyecto de Software Libre en específico, por lo que se han desarrollado múltiples servidores y clientes que utilizan el protocolo de Matrix.[234]

Synapse es la implementación de referencia del servidor de Matrix, es un servidor multiplataforma. Al ser Software Libre cualquier usuario puede instalarlo en un servidor propio y conectarse con otros servidores que utilizan el protocolo Matrix. Synapse soporta mensajes de texto, audio y vídeo, tanto individuales como en grupos, llamadas y vídeollamadas, transferencia de archivos, cifrado de comunicaciones, entre otros.[235]

Element es la implementación de referencia del cliente Matrix, Element es una aplicación existe para los sistemas operativos Android, iOS, GNU/Linux, MacOS y Windows; así como para navegadores web. Los usuarios pueden utilizar el cliente para conectarse a cualquier servidor donde exista una cuenta. Aunque existen muchos más clientes como: Ditto Chat, Nio, Pattle, FluffyChat, SPectral, Fractal, matrixcli, entre otros.[236] Los desarrolladores de Element permiten utilizar el cliente desde su sitio web, donde el usuario puede crear a una cuenta gratuita de matrix.org.[237]

- XMPP:

XMPP es un acrónimo para *Extensible Messaging and Presence Protocol* (Protocolo Extensible de Mensajería y Comunicación de Presencia), el cual es un protocolo abierto y extensible basado en XML. El protocolo es un estándar

234 Matrix, “Frequently Asked Questions”, https://matrix.org/faq/ (Fecha de consulta: 29 de julio de 2020).

235 Matrix, “Synapse” https://matrix.org/docs/projects/server/synapse (Fecha de consulta: 29 de julio de 2020).

236 Matrix, “Clients”, https://matrix.org/clients/ (Fecha de consulta: 29 de julio de 2020).

237 Matrix, “Try Matrix Now”, https://matrix.org/docs/projects/try-matrix-now (Fecha de consulta: 29 de julio de 2020).

formalizado por la *Internet Engineering Task Force* (Grupo de Trabajo de Ingeniería de Internet), Entre las características del protocolo es que es libre, estandarizado, verificado, descentralizado, seguro, extensible, flexible y diverso.[238]

Al igual que en con el protocolo Matrix, múltiples implementaciones del servidor existen para que cualquier usuario pueda instalar en un servidor propio. De la misma forma existen múltiples clientes para todas las plataformas.

Debido a que XMPP es extensible, diversos clientes soportan diferentes características, entre las actividades que son soportadas se encuentran: mensajería de texto, voz y vídeo, transferencia de archivos, cifrado de comunicaciones, entre otros.

- Jitsi Meet

Jitsi Meet es un programa que utiliza otros proyectos de software libre para ofrecer un servidor de vídeoconferencias, incluyendo XMPP. Jitsi Meet puede ser instalado en un servidor con GNU/Linux y de cliente se puede utilizar cualquier navegador así como las aplicaciones disponibles para iOS y Android.[239]

3.5 Eliminar Servicios de Seguimiento Web

El remplazo de los servicios web y del software puede no ser suficiente, ya que las compañías de seguimiento web posiblemente ya tengan mucha información sobre los usuarios y es posible que se desee eliminar esta información.

Una descripción detallada de como eliminar la información de cada servicio supera el alcance de este estudio, sin embargo, de forma general se sugiere revisar el Aviso de Privacidad, también llamado Política de Privacidad o Política de Datos de cada sitio web, normalmente al final de la página, donde cada proveedor de servicios nos explica como ejercer nuestros derechos ARCO explicados en el capítulo II de este trabajo, y también donde se tiene un correo o dirección de contacto para ejercer estos derechos ARCO.

238 XMPP, “An Overview of XMPP”, https://xmpp.org/about/technology-overview.html (Fecha de consulta: 29 de julio de 2020).

239 Jitsi Meet Handbook, “Introduction”, https://jitsi.github.io/handbook/docs/intro (Fecha de consulta: 29 de julio de 2020).

Es posible que algunos usuarios no deseen leer la política de privacidad de cada compañía y prefieran eliminar su información directamente. De ser así, los usuarios pueden visitar el sitio web DeleteMyData que contiene instrucciones claras, sencillas y con ilustraciones, para eliminar nuestra información de los servidores de múltiples compañías. DeleteMyData también ofrece un servicio automatizado para eliminar la información directamente a nuestro nombre, sin embargo, no se recomienda este servicio, ya que DeleteMyData no cuenta con un Aviso de Privacidad.[240]

240 DeleteMyData, “Simplest way to delete your online accounts”, https://deletemydata.io/ (Fecha de consulta: 29 de agosto de 2020).

Conclusiones

Conclusiones

La presente propuesta de intervención fue realizada con el objetivo de que tantos los miembros como el Consejo de la FSFLA enfrenten el problema del seguimiento web.

Si bien los mecanismos de seguimiento web no son inherentemente malos o buenos, en la actualidad estas tecnologías se han destacado por que han sido abusadas para propósitos antiéticos e incluso ilegales.

No es necesario ser experto en el tema del seguimiento web para sentir preocupación al navegar, el hecho de que en cosa de unos días millones de usuarios abandonaran la plataforma WhatsApp, ante los cambios de sus condiciones de sus términos de privacidad, para moverse a plataformas que si protegen la privacidad de sus usuarios, nos indica que existe una preocupación entre los usuarios de la web por proteger su privacidad.[241]

Cómo se comentó en el Capítulo 1 de este documento, la preocupación por defender la privacidad y el anonimato en la web es un tema recurrente entre los miembros de la FSFLA.

Esta propuesta de intervención busca transformar esta realidad, proponiendo acciones en benéfico de los miembros de la FSFLA, y el público en general, para que mediante las herramientas de Software Libre adecuadas, puedan defender su privacidad en la web.

También se ha buscado informar sobre el marco legal del derecho a la protección de datos personales, el cual se puede ejercer en aquellos casos en que mantener el anonimato no es una opción y es necesario proporcionar datos personales en la web.

Se recomienda tomar muy en cuenta el consejo del Capítulo 3 al respecto de la adopción de nuevas herramientas tecnológicas, pues es difícil aprender rápidamente múltiples herramientas y plataformas nuevas, por lo que, ante la

241 Hern, Alex, *WhatsApp loses millions of users after terms update*, The Guardian, enero 2021, https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update (Fecha de consulta: 19 de julio de 2021).

complejidad de este cambio, se sugiere realizar un cambio por fases, aprendiendo una herramienta o plataforma a la vez.

También se recomienda analizar si es una opción el cambio, existen ocasiones, en las que por motivos ajenos a la voluntad del usuario, ya sea por motivos laborales, escolares u otras causas de fuerza mayor, es inevitable el uso de herramientas de seguimiento web, en estos casos pueden adoptarse herramientas, como las extensiones del navegador sugeridas, para bloquear algunos de los rastreadores web más invasivos, sin tener que abandonar la plataforma en su totalidad.

Bibliografía

1. ABELSON Harold, et al., Structure and Interpretation of Computer Programs, 2a. ed, Cambridge, MIT Press, 1996. p. 296, https://web.mit.edu/alexmv/6.037/sicp.pdf (Fecha de consulta: 29 de abril de 2020)
2. ABRAMOVICH, Giselle, "15 Mind-Blowing Stats About Programmatic Advertising", CMO Adobe, 2017, https://cmo.adobe.com/articles/2017/9/15-mind-blowing-stats-about-programmatic-advertising.html#gs.dizpzi (Fecha de consulta: 14 de julio de 2020).
3. ACAR, Gunes, et al., "The Web Never Forgets:Persistent Tracking Mechanisms in the Wild", CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, 2014, pp. 675-676. https://dl.acm.org/doi/10.1145/2660267.2660347 (Fecha de consulta: 16 de agosto de 2020).
4. ACXIOM, "Reach Over 2.5 Billion of the World's Marketable Consumers", Acxiom, 2017, https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20Global%20Data.pdf (Fecha de consulta: 15 de diciembre de 2020).
5. ACXIOM, Data Bundles, Acxiom. https://developer.myacxiom.com/code/api/data-bundles/main (Fecha de consulta: 14 de diciembre de 2020).
6. AGENCIA Española de Protección de Datos, Estudio Fingerprinting o Huella digital del dispositivo, 2019, pp. 4-8,

https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf (Fecha de consulta: 29 de abril de 2020), pp. 7-9.

7. AGENCIA Española de Protección de Datos, Guía sobre el uso de las cookies, julio 2020, pp. 11-12, https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (Fecha de consulta: 29 de junio de 2021)
8. AGENCIA de Acceso a la Información Pública, Datos Personales: tus derechos https://www.argentina.gob.ar/aaip/datospersonales/derechos (Fecha de consulta: 01 de junio de 2020)
9. AHMED, Wasim, et al., "COVID-19 and the 5G Conspiracy Theory: Social Network Analysis of Twitter Data", Journal of Medical Internet Research, vol. 22, num. 5, mayo 2020, pp. 1-9, https://www.jmir.org/2020/5/e19458 (Fecha de consulta: 22 de junio de 2021).
10. ALLINGTON, Daniel Conspiracy Theories, Radicalisation and Digital Media, The Global Network on Extremism and Technology, febrero 2021, pp. 15-21, https://gnet-research.org/wp-content/uploads/2021/02/GNET-Conspiracy-Theories-Radicalisation-Digital-Media.pdf (Fecha de consulta: 22 de junio de 2021).
11. ALLINGTON, Daniel, et al., "Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency", Psychological Medicine, pp. 1-7 https://www.cambridge.org/core/journals/psychological-medicine/article/healthprotective-behaviour-social-media-usage-and-conspiracy-belief-during-the-covid19-public-health-emergency/

A0DC2C5E27936FF4D5246BD3AE8C9163 (Fecha de consulta: 22 de junio de 2021).

12. AUTORIDADE Nacional de Proteção de Dados, ANPD convoca sociedade para formação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, 05 de febrero de 2021, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-convoca-sociedade-para-formacao-do-conselho-nacional-de-protecao-de-dados-pessoais-e-da-privacidade (Fecha de consulta: 10 de febrero de 2021)
13. AUTORIDADE Nacional de Proteção de Dados, Reclamação do titular contra controlador de dados, 05 de febrero de 2021, https://www.gov.br/anpd/pt-br/canais_atendimento/reclamacao-do-titular-contra-controlador-de-dados (Fecha de consulta: 10 de febrero de 2021)
14. AZOULAY, Audrey, Towards an Ethics of Artificial Intelligence, Naciones Unidas, 2019, https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence (Fecha de consulta: 29 de abril de 2020)
15. BACKSTROM, Lars y Kleinberg, Jon, Romantic Partnerships and the Dispersion of Social Ties: A Network Analysis of Relationship Status on Facebook, Computing Research Repository, 2013, http://arxiv.org/abs/1310.6753 (Fecha de consulta: 12 de agosto de 2020).
16. BAEKDAL, Thomas, The Original Cookie specification from 1997 was GDPR compliant, octubre 2019, https://baekdal.com/thoughts/the-original-cookie-specification-from-1997-was-gdpr-compliant/ (Fecha de consulta: 18 de mayo de 2020)

17. BASHUR, Muhammad Ahmad, "On the Privacy Implications of Real Time Bidding", Tesis de Doctorado, Northeastern University, 2019, http://www.ccs.neu.edu/home/ahmad/publications/bashir-thesis.pdf (Fecha de consulta: 03 de julio de 2020).
18. BIASUTTI Neto, Albino, Cuenta de FSF Latinoaméricana en Twitter, Lista de distribución FSFLA-Discusión, mayo 2014, https://www.fsfla.org/pipermail/discusion/2014/005377.html (Fecha de consulta: 16 de junio de 2021).
19. BIBLIOTECA del Congreso Nacional de Chile, Fija el Texto Refundido, Coordinado y Sistematizado de la Constitucion Politica de la Republica de Chile, https://www.bcn.cl/leychile/navegar?idNorma=242302
20. BIBLIOTECA del Congreso Nacional de Chile, Ley 19628 Sobre Proteccion de la Vida Privada, https://www.bcn.cl/leychile/navegar?idNorma=141599
21. BOFFEY, Daniel, Registration cards of Dutch Holocaust victims to go on display, The Guardian, enero 2021, https://www.theguardian.com/world/2021/jan/26/registration-cards-dutch-jews-display-holocaust-museum-amsterdam (Fecha de consulta: 14 de julio de 2021)
22. BONAVENTURE, Olivier, The HyperText Transfer Protocol, Computer Networking: Principles, Protocols and Practice, https://www.computer-networking.info/2nd/html/protocols/http.html (Fecha de consulta: 09 de junio de 2021)
23. BONIFAZ, Rafael, Comunicaciones Secretas en Internet, Lista de distribución FSFLA-Discusión, marzo 2019,

https://www.fsfla.org/pipermail/discusion/2019/006103.html (Fecha de consulta: 16 de junio de 2021).

24. BONIFAZ, Rafael, Privacidad y Anonimato con Software Libre, Lista de distribución FSFLA-Discusión, mayo 2018, https://www.fsfla.org/pipermail/discusion/2018/006072.html (Fecha de consulta: 16 de junio de 2021).
25. BONIFAZ, Rafael, ¿Cuánta vigilancia puede soportar la democracia?, Lista de distribución FSFLA-Discusión, octubre 2013, https://www.fsfla.org/pipermail/discusion/2013-October/005247.html (Fecha de consulta: 16 de junio de 2021).
26. BUITEN, Miriam, “Towards Intelligent Regulation of Artificial Intelligence.” European Journal of Risk Regulation. Cambridge University Press, vol. 10, núm 1, 2019, pp. 41–59. https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-intelligent-regulation-of-artificial-intelligence/AF1AD1940B70DB88D2B24202EE933F1B (Fecha de consulta: 29 de abril de 2020)
27. BUJLOW, Tomasz, et al., "A Survey on Web Tracking: Mechanisms, Implications, and Defenses", Proceedings of the IEEE, vol. 105, núm. 8, agosto 2017, pp. 1476-1510. https://ieeexplore.ieee.org/document/7872467 (Fecha de consulta: 29 de abril de 2020)
28. BUSANICHE, Beatriz, FSFLA News Issue #4, Lista de Correo FSFLA-Anuncio. https://www.webcitation.org/6AsIccVZH?url=http://mail.fsfeurope.org/

pipermail/fsfla-anuncio/2005-November/000036.html Archivado del original: 22 de septiembre de 2012. (Fecha de consulta: 16 de mayo de 2021).

29. CALISKAN, Aylin, et al., "Semantics derived automatically from language corpora contain human-like biases", Science, vol. 356, núm. 6334, abril 2017, pp. 183-186. https://researchportal.bath.ac.uk/en/publications/semantics-derived-automatically-from-language-corpora-necessarily (Fecha de consulta: 29 de abril de 2020)
30. CHENG, Ping, et al., "Do Women Pay More for Mortgages?", The Journal of Real Estate Finance and Economics, vol 43, 2011, pp. 423-440, https://www.researchgate.net/publication/225702859_Do_Women_Pay_More_for_Mortgages (Fecha de consulta: 20 de junio de 2021).
31. CHRISTENSSON, Per "Web Browser Definition", TechTerms, 2014, https://techterms.com/definition/web_browser (Fecha de consulta: 09 de junio de 2021)
32. CHRISTL, Wolfie y Spiekermann, Sarah, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy Vienna, Facultas, 2016, pp. 11-14 http://crackedlabs.org/en/networksofcon (Fecha de consulta: 10 de julio de 2021).
33. CHRISTL, Wolfie, "Overview: Corporate Surveillance in Everyday Life", Cracked Labs, junio 2017, https://crackedlabs.org/en/corporate-surveillance (Fecha de consulta: 15 de diciembre de 2020).
34. CHRISTL, Wolfie, "Report: Corporate Surveillance in Everyday Life", Cracked Labs, pp. 54-63 junio 2017,

https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf (Fecha de consulta: 15 de diciembre de 2020).

35. CIRIBELI, João Paulo y Miquelito, Samuel, "La segmentación del mercado por el criterio psicográfico: un ensayo teórico sobre los principales enfoques psicográficos y su relación con los criterios de comportamiento", Visión de Futuro, Vol. 19, N 1, 2015, pp. 33-50, http://www.scielo.org.ar/pdf/vf/v19n1/v19n1a02.pdf (Fecha de consulta: 13 de julio de 2020).
36. COMISIÓN Europea, (2018). Artificial Intelligence for Europe. Recuperado de: https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe
37. COMISIÓN Europea, (2019). Directrices éticas para una IA fiable. Recuperado de: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
38. COMISIÓN Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, ¿Conoces el impuesto rosa o pink tax? Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, agosto 2019, https://www.gob.mx/condusef/prensa/conoces-el-impuesto-rosa-o-pink-tax (Fecha de consulta: 20 de junio de 2021).
39. CONGER, Kate Prepare to Pay More for Uber and Lyft Rides, The New York Times, junio 2021, https://www.nytimes.com/article/uber-lyft-surge.html (Fecha de consulta: 20 de junio de 2021).
40. CONGRESO de la República del Perú, Constitución Política de Perú, diciembre 1993,

http://www4.congreso.gob.pe/ntley/Imagenes/Constitu/Cons1993.pdf (Fecha de consulta: 28 de julio de 2020).

41. CONGRESO de la República del Perú, Ley N° 29733, Ley de Protección de Datos Personales, julio 2011, http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf (Fecha de consulta: 28 de julio de 2020).
42. CONGRESSO Nacional, Medida Provisória n° 869, de 2018 (Proteção de dados pessoais), diciembre de 2018, https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062 (Fecha de consulta: 01 de agosto de 2020)
43. CONSEJO de Europa, "Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal", 1981, http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf (Fecha de consulta: 23 de agosto de 2020)
44. CONSTITUCIÓN de la Nación Argentina reformada en 1994, http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm (Fecha de consulta: 01 de junio de 2020)
45. COOKIEPEDIA, How We Classify Cookies, https://cookiepedia.co.uk/classify-cookies (Fecha de consulta: 29 de abril de 2020)
46. CYPHERS, Bennett y Gebhart, Gennie, "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance", Electronic

Frontier Foundation, diciembre 2019, https://www.eff.org/wp/behind-the-one-way-mirror (Fecha de consulta: 29 de junio de 2020)

47. CYPHERS, Bennett, "Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It", Electronic Frontier Foundation, 19 de marzo de 2020, https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and (Fecha de consulta: 14 de diciembre de 2020).
48. CÁMARA de Diputadas y Diputados, Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, 2017, https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07 (Fecha de consulta: 01 de agosto de 2020)
49. CÁMARA de Diputados del H. Congreso de la Unión. Constitución Política de los Estados Unidos Mexicanos, http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf (Fecha de consulta: 28 de julio de 2020).
50. CÂMARA dos Deputados, Lei Nº 12.965. Marco Civil da Internet, abril de 2014, https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-norma-pl.html (Fecha de consulta: 01 de agosto de 2020)
51. DAMA, Manasa, "Difference Between Search Engine and Browser", Difference Between Similar Terms and Objects, Difference Between, 2011,

http://www.differencebetween.net/technology/internet/difference-between-search-engine-and-browser/ (Fecha de consulta: 09 de junio de 2021)

52. DAVIES, Dave, "Patent 1 of 2: How Google learns to influence and control users", Search Engine Land, 2017, https://searchengineland.com/patent-1-2-google-learns-influence-control-users-272358 (Fecha de consulta: 12 de agosto de 2020).
53. DELETEMYDATA, "Simplest way to delete your online accounts", https://deletemydata.io/ (Fecha de consulta: 29 de agosto de 2020).
54. DIARIO Oficial de la Federación, ACUERDO mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales, DOF, enero 2018, https://www.dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018 (Fecha de consulta: 28 de julio de 2020).
55. DIARIO Oficial de la Federación, DECRETO por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, DOF, febrero de 2014. http://dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014 (Fecha de consulta: 28 de julio de 2020).
56. DIARIO Oficial de la Unión Europea, "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de

Datos)", 2016, https://www.boe.es/doue/2016/119/L00001-00088.pdf (Fecha de consulta: 28 de junio de 2020).

57. DIXON, Pam, "Congressional Testimony: What Information Do Data Brokers Have on Consumers?", World Privacy Forum, diciembre de 2013. https://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/ (Fecha de consulta: 14 de diciembre de 2020).
58. DIÁRIO Oficial Da União, Medida Provisória Nº 959, abril 2020, https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639 (Fecha de consulta: 01 de agosto de 2020)
59. DORDAL, Peter, IP - Internet Protocol, An Introduction to Computer Networks, http://intronetworks.cs.luc.edu/current2/html/intro.html#ip-internet-protocol (Fecha de consulta: 09 de junio de 2021)
60. DORDAL, Peter, Layers, An Introduction to Computer Networks, http://intronetworks.cs.luc.edu/current2/html/intro.html#layers (Fecha de consulta: 09 de junio de 2021)
61. ECKERSLEY, Peter, "How Unique Is Your Web Browser?", PETS 2010: Privacy Enhancing Technologies. International Symposium on Privacy Enhancing Technologies, vol 6205. Springer, Berlin, 2010, pp. 1-18, https://doi.org/10.1007/978-3-642-14527-8_1 (Fecha de consulta: 12 de diciembre de 2020)
62. EDELMAN, Gilad, "Why Don’t We Just Ban Targeted Advertising?", Wired, 22 de marzo de 2020, (Fecha de consulta: 13 de diciembre de 2020).

63. EHARMONY, "The future of dating report 2018: smart devices will predict if your relationship is on the rocks", Eharmony, https://www.eharmony.co.uk/dating-advice/dating/the-future-of-dating-report-2018-smart-devices-to-predict-if-your-relationship-is-on-the-rocks (Fecha de consulta: 12 de agosto de 2020).
64. ENGLEHARDT, Steven y Arvind, Narayanan. "Online Tracking: A 1-million-site Measurement and Analysis", CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, octubre 2016, pp. 1388–1401, https://dl.acm.org/doi/10.1145/2976749.2978313 (Fecha de consulta: 29 de abril de 2020)
65. EPSTEIN, Brian, "Would you send this postcard in the mail?", https://security.ias.edu/node/22 (Fecha de consulta: 29 de agosto de 2020).
66. EXTENDED LEARNING INSTITUTE (ELI) at Northern Virginia Community College (NOVA), Reading: Web Browser, Lumen Learning, 2015, https://courses.lumenlearning.com/zeliite115/chapter/reading-web-browser/, (Fecha de consulta: 09 de junio de 2021)
67. FACCA Michele, Federico y Luca Lanzi, Pier, "Mining interesting knowledge from weblogs: a survey", Data & Knowledge Engineering, vol 53, num 3, 2005, pp. 225-226, http://www.sciencedirect.com/science/article/pii/S0169023X04001387 (Fecha de consulta: 29 de junio de 2020).
68. FACEBOOK for Business, "About Lookalike Audiences", https://www.facebook.com/business/help/164749007013531?id=401668390442328 (Fecha de consulta: 13 de diciembre de 2020).

69. FEDERAL Trade Comission, "Data Brokers A Call for Transparency and Accountability", pp. 47-49, mayo 2014, (Fecha de consulta: 15 de diciembre de 2020).
70. FEDIVERSE, "Fediverse, diversity is strength", https://fediverse.party/en/fediverse, (Fecha de consulta: 29 de julio de 2020).
71. FIFIELD, David y Egelman, Serge, "Fingerprinting Web Users Through Font Metrics", FC 2015: Financial Cryptography and Data Security, International Conference on Financial Cryptography and Data Security, 2015, pp 107-124, https://link.springer.com/chapter/10.1007%2F978-3-662-47854-7_7 (Fecha de consulta: 12 de diciembre de 2020).
72. FORO Económico Mundial. Informe global de tecnología de la información 2016. (2016) http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf
73. FOWLER, Geoffrey, Goodbye, Chrome: Google's Web browser has become spy software, The Washington Post, junio 2019, https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch/ (Fecha de consulta: 12 de agosto de 2020)
74. FREE Software Directory, Collection:High Priority Projects, https://directory.fsf.org/wiki/Collection:High_Priority_Projects (Fecha de consulta: 28 de julio de 2020).

75. FREE Software Foundation, High Priority Free Software Projects, https://www.fsf.org/campaigns/priority-projects (Fecha de consulta: 28 de julio de 2020).
76. FRIGGERI, Adrien, "When Love Goes Awry", Facebook Data Science, 2014, https://www.facebook.com/notes/facebook-data-science/when-love-goes-awry/10152066701893859/ (Fecha de consulta: 12 de agosto de 2020).
77. FSFLA, Constitución, FSFLA, 2019, http://www.fsfla.org/ikiwiki/about/constitution.es.html (Fecha de consulta: 29 de abril de 2021)
78. FUNDÉURAE, Anonimizar y desanonimizar, neologismos válidos, FundéuRAE, junio 2019, https://www.fundeu.es/recomendacion/anonimizar-desanonimizar/ (Fecha de consulta: 15 de diciembre de 2020)
79. GIL, Elena, Big Data, Privacidad y Protección de Datos, Madrid, Agencia Española de Protección de Datos, 2016, pp. 15-16, https://www.aepd.es/sites/default/files/2019-10/big-data.pdf (Fecha de consulta: 29 de abril de 2020)
80. GNU Social, "The Project", https://gnusocial.network/ (Fecha de consulta: 29 de julio de 2020).
81. GNU, El software privativo a menudo es malware, GNU https://www.gnu.org/proprietary/proprietary.es.html (Fecha de consulta: 28 de julio de 2020).
82. GNU, GNUzilla and IceCat, GNU, https://www.gnu.org/software/gnuzilla/ (Fecha de consulta: 28 de julio de 2020).

83. GNU, Lista de licencias con comentarios, Oficina de Licencias y Cumplimiento de la Fundación del Software Libre, GNU, https://www.gnu.org/licenses/license-list.es.html (Fecha de consulta: 28 de julio de 2020).
84. GNU, Visión general del sistema GNU, GNU https://www.gnu.org/gnu/gnu-history.es.html (Fecha de consulta: 28 de julio de 2020).
85. GNU, ¿Qué es el software libre?, GNU https://www.gnu.org/philosophy/free-sw.es.html (Fecha de consulta: 28 de julio de 2020).
86. GNUPG, "User Guides", https://gnupg.org/documentation/guides.html (Fecha de consulta: 29 de agosto de 2020).
87. GOOGLE Ads Help, "About Customer Match", Google, https://support.google.com/google-ads/answer/6379332?hl=en (Fecha de consulta: 13 de diciembre de 2020).
88. GOOGLE, Authorized Buyers, OpenRTB Integration", Google, https://developers.google.com/authorized-buyers/rtb/openrtb-guide (Fecha de consulta: 05 de julio de 2020).
89. GRIFFIOEN, Pim y Zeller, Ron, The Netherlands: the greatest number of Jewish victims in Western Europe, Anne Frank House, septiembre 2018, https://www.annefrank.org/en/anne-frank/go-in-depth/netherlands-greatest-number-jewish-victims-western-europe/ (Fecha de consulta: 14 de julio de 2021)
90. GRUPO de Trabajo de Ingeniería de Internet, "OpenPGP Message Format", 2007, https://tools.ietf.org/html/rfc4880, (Fecha de consulta: 29 de agosto de 2020).

91. GRUPO de Trabajo del Artículo 29, Documento de trabajo sobre biometría, agosto de 2003, https://www.apda.ad/sites/default/files/2018-10/wp80_es.pdf (Fecha de consulta: 01 de junio de 2020)
92. HAWKINS, Andrew, Uber is overhauling the way it responds to emergencies and natural disasters The Verge, septiembre 2018, https://www.theverge.com/2018/9/25/17897836/uber-disaster-response-hurricane-price-cap (Fecha de consulta: 18 de junio de 2021).
93. HERN, Alex, WhatsApp loses millions of users after terms update, The Guardian, enero 2021, https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update (Fecha de consulta: 19 de julio de 2021).
94. HOFFMAN, Chris, "Why Email Can't Be Protected From Government Surveillance", 2013, https://www.makeuseof.com/tag/why-email-cant-be-protected-from-government-surveillance/ (Fecha de consulta: 29 de agosto de 2020).
95. HOLMES, Aaron, Facebook está bajo investigación en la UE por la filtración masiva de datos de 533 millones de personas, y podría enfrentar una multa de miles de millones de dólares, Business Insider México, abril 2021 (Fecha de consulta: 28 de junio de 2021). https://businessinsider.mx/facebook-investigacion-ue-filtracion-masiva-de-datos-multa/

96. van den HOVEN, Jeroen, “Information technology, privacy, and the protection of personal data”, Information Technology and Moral Philosophy, Cambridge, Cambridge University Press, 2008, pp. 301–322.
97. INFORMATION Commisioner's Office, What are cookies and similar technologies?, https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/ (Fecha de consulta: 29 de abril de 2020)
98. INTERACTIVE Advertising Bureau, "About OpenRTB", Interactive Advertising Bureau, https://www.iab.com/guidelines/real-time-bidding-rtb-project/ (Fecha de consulta: 13 de julio de 2020).
99. INTERACTIVE Advertising Bureau, "AdCOM Specification v1.0", IAB Tech Lab. https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md (Fecha de consulta: 05 de julio de 2020).
100. INTERACTIVE Advertising Bureau, "Member Directoy", Interactive Advertising Bureau, https://www.iab.com/our-story/ (Fecha de consulta: 13 de julio de 2020).
101. JITSI Meet Handbook, "Introduction", https://jitsi.github.io/handbook/docs/intro (Fecha de consulta: 29 de julio de 2020).
102. JOHN, M. Joan, et al., "User Profile Tracking by Web Usage Mining in Cloud Computing", Procedia Engineering, vol 38, 2012, pp. 3272, 3276, http://www.sciencedirect.com/science/article/pii/S1877705812022916 (Fecha de consulta: 29 de junio de 2020).

103. KAPLANA, Andreas y Haenleinb, Michael, "Siri, siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence". Business Horizons, vol. 62, núm 1, 2019, pp. 15–25. http://www.sciencedirect.com/science/article/pii/S0007681318301393 (Fecha de consulta: 29 de abril de 2020)

104. KARAJ, Arjaldo, et al., "WhoTracks.Me: Shedding light on the opaque world ofonline tracking", Computing Research Repository, Cornell University, 2019, p. 3. https://arxiv.org/abs/1804.08959v2 (Fecha de consulta: 29 de junio de 2020)

105. KASINSKI, Michal, et al., "Private traits and attributes are predictable from digital records of human behavior", Proceedings of the National Academy of Sciences of the United States of America, vol. 110, num. 15, 2013, pp. 5733, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3625324/ (Fecha de consulta: 17 de diciembre de 2020).

106. KELLY, M.J., No-judgment digital definitions: What is a web tracker?, Mozilla, 2019, https://blog.mozilla.org/firefox/what-is-a-web-tracker/ (Fecha de consulta: 25 de julio de 2020)

107. KIM, Jim, et al., "A Systematic review of the validity of screening depression through Facebook, Twitter, Instagram, and Snapchat", Journal of Affective Disorders vol. 286, mayo 2021, pp. 360-369, https://www.sciencedirect.com/science/article/abs/pii/S016503272100135X?via%3Dihub (Fecha de consulta: 22 de junio de 2021).

108. KRISTOL, David y Montulli, Lou, "HTTP State Management Mechanism", Request for Comments 2109, Grupo de Trabajo de Ingeniería

de Internet, febrero 1997, https://tools.ietf.org/html/rfc2109 (Fecha de consulta: 18 de mayo de 2020)

109. KUROSE, James y Ross, Keith, Computer Networking, 6a. ed., Boston, Pearson, 2013. pp. 2-18

110. LAPERDRIX, Pierre et al., "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints", 2016 IEEE Symposium on Security and Privacy, IEEE, San Jose, 2016, pp. 878-894, https://doi.org/10.1109/SP.2016.57

111. LEFRANC Weegan, Federico César, Holocausto y Dignidad. Sifnificado y fin de la invocación a la dignidad humana en el Preámbulo de la Declaración Universal de Derechos Humanos, Méxco, Ubijus, 2009, pp. 139.

112. LEIS, Angela, et al., "Detecting Signs of Depression in Tweets in Spanish: Behavioral and Linguistic Analysis", Journal of Medical Internet Research, vol. 2, num. 6, junio 2019, pp. 1-16, https://www.jmir.org/2019/6/e14199/ (Fecha de consulta: 22 de junio de 2021).

113. LEITH, Doug, Web Browser Privacy: What Do Browsers Say When They Phone Home?, febrero 2020, https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf (Fecha de consulta: 12 de agosto de 2020)

114. LERNER, Adam, et al., "Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016", 25th USENIX Security Symposium (USENIX Security 16), USENIX

Association, 2016, p. 997. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_lerner.pdf (Fecha de consulta: 29 de abril de 2020)

115. LEY de Ministerios. Decreto 746/2017. http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279940/norma.htm (Fecha de consulta: 01 de junio de 2020)

116. LOBOSCO, Katie, Facebook friends could change your credit score, CNN Business, agosto 2013, https://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html?hpt=hp_t2 (Fecha de consulta: 18 de junio de 2021).

117. MANHEIM, Karl y Kaplan, Lyric. "Artificial Intelligence: Risks to Privacy and Democracy", Yale Journal of Law and Technology, vol 21, núm 106, 2019, pp. 120–122. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016 (Fecha de consulta: 28 de junio de 2020)

118. MARR, Bernard, "Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers", Forbes, 7 de septiembre de 2017. https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/?sh=7b650fe86c27 (Fecha de consulta: 15 de diciembre de 2020).

119. MARTIN, Kirsten, "Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop?", The Information Society, vol. 32, núm. 1, 2016, pp. 51-63, https://kirstenmartin.net/wp-content/uploads/2015/04/Martin-TIS-Tracking-Users-Online-Proof.pdf (Fecha de consulta: 29 de abril de 2020)

120. MATRIX, "Clients", https://matrix.org/clients/ (Fecha de consulta: 29 de julio de 2020).

121. MATRIX, "Frequently Asked Questions", https://matrix.org/faq/ (Fecha de consulta: 29 de julio de 2020).

122. MATRIX, "Synapse" https://matrix.org/docs/projects/server/synapse (Fecha de consulta: 29 de julio de 2020).

123. MATRIX, "Try Matrix Now", https://matrix.org/docs/projects/try-matrix-now (Fecha de consulta: 29 de julio de 2020).

124. MATZ, Sandra, et al., "Psychological targeting as an effective approach to digital mass persuasion", Proceedings of the National Academy of Sciences, vol. 114, num. 48, noviembre 2017, pp. 12714-12719, https://www.pnas.org/content/114/48/12714 (Fecha de consulta: 22 de junio de 2021).

125. MAYER, Jonathan y C. Mitchell, John, "Third-Party Web Tracking: Policy and Technology", 2012 IEEE Symposium on Security and Privacy, 2012, San Francisco, IEEE, pp. 413-427, https://ieeexplore.ieee.org/document/6234427 (Fecha de consulta: 14 de junio de 2021)

126. MCCARTHY, John, What is Artificial Intelligence?, http://www-formal.stanford.edu/jmc/whatisai/node1.html (Fecha de consulta: 29 de abril de 2020)

127. MCCARTHY, Jonh, et al., A proposal for the Dartmouth Summer Research Project on Artificial Intelligence, agosto 1955, http://www-

formal.stanford.edu/jmc/history/dartmouth/dartmouth.html (Fecha de consulta: 29 de abril de 2020).

128. MELENDEZ, Steven y Pasternack, Alex. "Here are the data brokers quietly buying and selling your personal information", Fast Company, 2 de marzo de 2019, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information (Fecha de consulta: 14 de diciembre de 2020).

129. MENDOZA Enríquez, Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", Revista IUS, v. 12, n41, 2018, pp. 267-291, http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es (Fecha de consulta 13 de agosto de 2020).

130. MENDOZA, Miguel Ángel, ¿Por qué es importante proteger tus datos personales?, We Live Security, octubre 2015, https://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/ (Fecha de consulta: 28 de junio de 2021).

131. MENN, Joseph, Exclusive: Massive spying on users of Google's Chrome shows new security weakness, Reuters, junio 2020, https://www.reuters.com/article/us-alphabet-google-chrome-exclusive/exclusive-massive-spying-on-users-of-googles-chrome-shows-new-security-weakness-idUSKBN23P0JO (Fecha de consulta: 20 de mayo de 2021)

132. MILLER, Zoë, 16 things that are still more expensive for women than for men, Insider, agosto 2018, https://www.insider.com/women-more-expensive-products-2018-8 (Fecha de consulta: 20 de junio de 2021).

133. MINISTERIO de Comercio, Industria y Turismo, Decreto número 1377 de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012 https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf (Fecha de consulta: 01 de agosto de 2020)

134. MINISTERIO de Justicia y Derechos Humanos, Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, marzo 2013, https://www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf (Fecha de consulta: 28 de julio de 2020).

135. MOWERY, Keaton y Shacham Hovav, "Pixel Perfect: Fingerprinting Canvas in HTML5", Proceedings of W2SP 2012, IEEE Computer Society, 2012, pp. 1-10 https://hovav.net/ucsd/papers/ms12.html (Fecha de consulta: 12 de diciembre de 2020).

136. MOZILLA, What is a web browser?, https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/ (Fecha de consulta: 25 de julio de 2020)

137. MURPHY, Paul, Exclusive: Google kept scam fishing license ads up for months after being told about them, states say, CNN Business, febrero 2020, https://edition.cnn.com/2020/02/03/tech/google-fishing-licenses-scam-ads/index.html (Fecha de consulta: 17 de junio de 2021).

138. La NACIÓN, "Dudas entre los expertos por el proyecto para usar una boleta única electrónica nacional", julio 2016,

https://www.lanacion.com.ar/tecnologia/dudas-entre-los-expertos-por-el-proyecto-para-usar-una-boleta-unica-electronica-nacional-nid1921720 (Fecha de consulta: 28 de julio de 2020).

139. La NACIÓN, "Filtran el software de control de una máquina de voto electrónico usada en Salta", agosto de 2017, https://www.lanacion.com.ar/tecnologia/filtran-el-codigo-de-una-maquina-de-voto-electronico-de-salta-y-alertan-sobre-los-riesgos-del-sistema-nid2054577 (Fecha de consulta: 28 de julio de 2020).

140. NARAYANAN, Arvind, There is no such thing as anonymous online tracking, The Center for Internet and Society, julio 2011, https://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking (Fecha de consulta: 19 de mayo de 2021)

141. NEW York City Department of Consumer Affairs, From Cradle to Cane: The Cost of Being a Female Consumer, New York City Department of Consumer Affairs, diciembre 2015, pp. 17-40, https://www1.nyc.gov/assets/dca/downloads/pdf/partners/Study-of-Gender-Pricing-in-NYC.pdf (Fecha de consulta: 20 de junio de 2021).

142. NEXTCLOUD, "All Apps", https://apps.nextcloud.com/ (Fecha de consulta: 29 de agosto de 2020).

143. NEXTCLOUD, "Our key differentiators", https://nextcloud.com/about/ (Fecha de consulta: 29 de agosto de 2020).

144. NEXTCLOUD, "What makes Nextcloud the best choice", https://nextcloud.com/compare/ (Fecha de consulta: 29 de agosto de 2020).

145. NOTICIAS Iruya, "Una 'explicación' de Teresa Ovejero hunde al voto electrónico", agosto 2016, https://noticias.iruya.com/a/politica/elecciones/17864-una-explicacion-de-teresa-ovejero-hunde-al-voto-electronico.html (Fecha de consulta: 28 de julio de 2020).

146. OLIVA, Alexandre, 0G: Escaping the Surveillance Blackhole with Free Mobile Computing, Norwegian Unix User Group, Oslo, Octubre 2020, https://nuug.no/aktiviteter/20201013-mobile-computing-with-privacy/ (Fecha de consulta: 16 de junio de 2021).

147. ONIONSHARE, "OnionShare Wiki", https://github.com/micahflee/onionshare/wiki (Fecha de consulta: 29 de agosto de 2020).

148. ORDÓÑEZ, Quiliro, Censura y espionaje en Facebook, Lista de distribución FSFLA-Discusión, abril 2017, https://www.fsfla.org/pipermail/discusion/2017/005905.html (Fecha de consulta: 16 de junio de 2021).

149. ORDÓÑEZ, Quiliro, Usar email con criptografía, Lista de distribución FSFLA-Discusión, septiembre 2013, https://www.fsfla.org/pipermail/discusion/2013-September/005237.html (Fecha de consulta: 16 de junio de 2021).

150. ORGANIZACIÓN Mundial de la Propiedad intelectal, (2018). Índice Mundial de Innovación 2018. Recuperado de: https://www.wipo.int/pressroom/es/articles/2018/article_0005.html

151. ORGANIZACIÓN de Estados Americanos, "Member States", OEA, http://www.oas.org/en/member_states/default.asp (Fecha de consulta: 10 de julio de 2021).

152. ORGANIZACIÓN de Estados Americanos, "Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales", Organización de Estados Americanos, pp. 4-5 https://www.redipd.org/sites/default/files/inline-files/Informe_CJI-doc_474-15_rev2_26_03_15.pdf (Fecha de consulta: 21 de junio de 2020).

153. ORGANIZACIÓN de las Naciones Unidas, La Declaración Universal de Derechos Humanos, Organización de las Naciones Unidas, Resolución París, 1948, https://www.un.org/es/universal-declaration-human-rights/ (Fecha de consulta: 23 de mayo de 2020)

154. ORGANIZATION for Economic Cooperation and Development, Adults, Computers and Problem Solving: What's the Problem?, París, OECD Skills Studies, p. 188. https://www.oecd-ilibrary.org/content/publication/9789264236844-en (Fecha de consulta: 29 de abril de 2020)

155. ORGANIZATION for Economic Cooperation and Development, Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, OECD, pp. 2-4. https://www.oecd.org/sti/ieconomy/15590267.pdf (Fecha de consulta: 29 de abril de 2020)

156. PACKIN, Nizan Geslevich y Lev Aretz, Yafit, "On Social Credit and the Right to Be Unnetworked", Columbia Business Law Review,Vol. 2016, Num

2, febrero 2016, pp. 339–347 https://ssrn.com/abstract=2728414 (Fecha de consulta: 18 de junio de 2021).

157. PANTIC, Igor, "Online social networking and mental health", Cyberpsychology, Behavior, and Social Networking, vol. 17, num. 10, octubre 2014, pp. 652-657, https://www.liebertpub.com/doi/10.1089/cyber.2014.0070 (Fecha de consulta: 22 de junio de 2021).

158. PARKER, Clifton B., Michal Kosinski: Computers Are Better Judges of Your Personality Than Friends, Stanford Business, 2015, https://www.gsb.stanford.edu/insights/michal-kosinski-computers-are-better-judges-your-personality-friends (Fecha de consulta: 07 de agosto de 2020).

159. PETERSON, Larry y Davie, Bruce, Computer Networks: A Systems Approach, https://book.systemsapproach.org/ (Fecha de consulta: 09 de junio de 2021)

160. PETIT, N. (2017). Antitrust and Artificial Intelligence: A Research Agenda. Journal of European Competition Law & Practice, 8(6), 361–362. https://doi.org/10.1093/jeclap/lpx033

161. PLATAFORMA digital única del Estado Peruano, Consultar el Registro Nacional de Protección de Datos Personales, https://www.gob.pe/9254-consultar-el-registro-nacional-de-proteccion-de-datos-personales (Fecha de consulta: 28 de julio de 2020).

162. PRESIDÊNCIA da República, Constituição da República Federativa do Brasil de 1988,

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm (Fecha de consulta: 01 de agosto de 2020)

163. PRESIDÊNCIA da República, LEI Nº 13.709. Lei Geral de Proteção de Dados Pessoais), agosto de 2018, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm (Fecha de consulta: 01 de agosto de 2020)

164. PRIVACY Rights Clearinghouse, Data Breaches, Privacy Rights Clearinghouse, https://privacyrights.org/data-breaches (Fecha de consulta: 28 de junio de 2021).

165. PRODROMOU, Evan, et al., "OStatus 1.0 Draft 2", https://www.w3.org/community/ostatus/wiki/images/9/93/OStatus_1.0_Draft_2.pdf, (Fecha de consulta: 29 de julio de 2020).

166. PÁRABOLA GNU/Linux-libre, IceWeasel History https://wiki.parabola.nu/IceWeasel_History (Fecha de consulta: 28 de julio de 2020).

167. PÁRABOLA GNU/Linux-libre, iceweasel-hardened-preferences, https://www.parabola.nu/packages/nonprism/x86_64/iceweasel-hardened-preferences/ (Fecha de consulta: 28 de julio de 2020).

168. PÁRABOLA GNU/Linux-libre, iceweasel-https-everywhere, https://www.parabola.nu/packages/libre/x86_64/iceweasel-https-everywhere/ (Fecha de consulta: 28 de julio de 2020).

169. PÁRABOLA GNU/Linux-libre, iceweasel-noscrpit, https://www.parabola.nu/packages/libre/x86_64/iceweasel-noscript/ (Fecha de consulta: 28 de julio de 2020).

170. PÁRABOLA GNU/Linux-libre, iceweasel-ublock-origin, https://www.parabola.nu/packages/libre/x86_64/iceweasel-ublock-origin/ (Fecha de consulta: 28 de julio de 2020).

171. PÁRABOLA GNU/Linux-libre, ¿Qué es Parabola? https://wiki.parabola.nu/Main_Page_(Español) (Fecha de consulta: 28 de julio de 2020).

172. RAMIREZ, Edith, Big Data: A Tool for Inclusion or Exclusion?, Washington, 2014, pp. 2-4, https://www.ftc.gov/system/files/documents/public_statements/582421/140915bigdataworkshop.pdf (Fecha de consulta: 17 de junio de 2020).

173. RELIHAN, Tom, Social media advertising can boost fake news — or beat it, MIT Management Sloan School, diciembre 2018, https://mitsloan.mit.edu/ideas-made-to-matter/social-media-advertising-can-boost-fake-news-or-beat-it (Fecha de consulta: 17 de junio de 2021).

174. RIPD, "Declaración del XV encuentro de la Red Iberoamericana de Protección de Datos", RIPD, https://www.redipd.org/sites/default/files/inline-files/Declaracion_RIPD_XV_encuentro.pdf (Fecha de consulta: 21 de junio de 2020).

175. RIPD, Estándares de Protección de Datos Personales para los Estados Iberoamericanos, RIPD, Santiago de Chile, 2017, https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf (Fecha de consulta: 21 de junio de 2020).

176. RIPD, "Historia de la Red Iberoamericana de Protección de Datos (RIPD)", RIPD, https://www.redipd.org/es/la-red/historia-de-la-red-

iberoamericana-de-proteccion-de-datos-ripd (Fecha de consulta: 21 de junio de 2020).

177. RIPD, "Países Miembros", RIPD, https://www.redipd.org/es/enlaces-de-interes/paises-miembros (Fecha de consulta: 21 de junio de 2020).

178. RISEUP, "GPG buenas prácticas", https://riseup.net/es/security/message-security/openpgp/gpg-best-practices (Fecha de consulta: 29 de agosto de 2020).

179. ROESNER Franziska, Kohno Tadayoshi, et al., "Detecting and defending against third-party tracking on the web", Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, Berkeley, USENIX Association, 2012, https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (Fecha de consulta: 27 de abril de 2021).

180. RUDDICK, Graham, Admiral to price car insurance based on Facebook posts, The Guardian, noviembre 2016, https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts (Fecha de consulta: 18 de junio de 2021).

181. RYAN, Johnny, et al., "Grounds of complaint to the Data Protection Commissioner", 2018, https://brave.com/wp-content/uploads/2018/09/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf (Fecha de consulta: 13 de agosto de 2020).

182. RYAN, Johny, "Regulatory complaint concerning massive, web-wide data breach by Google and other “ad tech” companies under Europe’s

GDPR", 2018, https://brave.com/adtech-data-breach-complaint/ (Fecha de consulta: 13 de agosto de 2020).

183. RYAN, Johny, "Report from Dr Johnny Ryan – Behavioural advertising and personal data", 2018, https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf (Fecha de consulta: 13 de agosto de 2020).

184. SANCHEZ, Pilar, Impuesto rosa: Mujeres pagan hasta 17% más por el mismo producto que un hombre, Dinero en Imagen, junio 2021, https://www.dineroenimagen.com/economia/impuesto-rosa-mujeres-pagan-hasta-17-mas-por-el-mismo-producto-que-un-hombre/131694 (Fecha de consulta: 20 de junio de 2021).

185. SCARFONE, Karen, et al., "Guide to General Server Security", Recommendations of the National Institute of Standards and Technology, 2008, pp. 2-4, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf (Fecha de consulta: 28 de julio de 2020).

186. SCHLEBAUM, Pieter, Raid on the Population Registry of Amsterdam, trad. de Cor Korpel, Traces of War, septiembre 2019, https://www.tracesofwar.com/articles/5329/Raid-on-the-Population-Registry-of-Amsterdam.htm (Fecha de consulta: 14 de julio de 2021)

187. SCHWABE, Jürgen, Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe, México, Konrad Adenauer Stiftung, 2009, pp. 95-103

188. SCJN, Derechos Al Honor, A La Intimidad Y A La Propia Imagen. Constituyen Derechos Humanos Que Se Protegen A Través Del Actual Marco Constitucional. Tesis: 5o.C.4 K (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro XXI, Tomo 2, junio de 2013, p. 1258. https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2003844&Clase=DetalleTesisBL&Semanario=0

189. SCJN, Protección De Datos Personales. El Deber Del Estado De Salvaguardar El Derecho Humano Relativo Debe Potencializarse Ante Las Nuevas Herramientas Tecnológicas, Debido A Los Riesgos Que Éstas Representan Por Sus Características. Tesis: I.10o.A.5 CS (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 70, Tomo III, septiembre de 2019, p. 2199, https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2020564&Clase=DetalleTesisBL&Semanario=0

190. SCJN; Protección De Datos Personales. Constituye Un Derecho Vinculado Con La Salvaguarda De Otros Derechos Fundamentales Inherentes Al Ser Humano, Tesis: I.10o.A.6 CS (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 70, Tomo III, septiembre de 2019, p. 2200, https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2020563&Clase=DetalleTesisBL&Semanario=0

191. SEARX, "Welcome to searx", https://asciimoo.github.io/searx/ (Fecha de consulta: 29 de julio de 2020).

192. SECRETARÍA General del Senado, Constitución Política de la República de Colombia, http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html#15 (Fecha de consulta: 01 de agosto de 2020)

193. SECRETARÍA General del Senado, Ley Estatutaria 1581 de 2012, http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html#15 (Fecha de consulta: 01 de agosto de 2020)

194. SILVERMAN, Craig y Mac, Ryan, Facebook Gets Paid, BuzzFeedNews, diciembre 2020, https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam (Fecha de consulta: 17 de junio de 2021).

195. SLOAN, Katherine, The Problem with Data Breach Fatigue, Cybint, marzo 2020, https://www.cybintsolutions.com/the-problem-with-data-breach-fatigue/ (Fecha de consulta: 28 de junio de 2021).

196. SOLANGE Maqueo, María (coord.), Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada, México, INAI, 2018, pp. 157-159.

197. SOTO Galindo, José, Función Pública incumplió con la ley por fuga de datos personales: Inai, El Economista, noviembre 2020, https://www.eleconomista.com.mx/politica/Funcion-Publica-incumplio-con-la-ley-por-fuga-de-datos-personales-Inai-20201124-0082.html (Fecha de consulta: 28 de junio de 2021).

198. STATE, Bogdan, "Flings or Lifetimes? The Duration of Facebook Relationships", Facebook Data Science, 2014,

https://www.facebook.com/notes/facebook-data-science/flings-or-lifetimes-the-duration-of-facebook-relationships/10152060513428859 (Fecha de consulta: 12 de agosto de 2020).

199. STAYGO, "Scientific References", Staygo, https://staygoapp.com/references, https://staygoapp.com/references (Fecha de consulta: 12 de agosto de 2020).

200. SUPERVISOR Europeo de Protección de Datos, Hacia una nueva ética digital: Datos, dignidad y tecnología, Dictamen 4/2015, 2015, pp. 7-8, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_es.pdf (Fecha de consulta: 16 de junio de 2020).

201. SUPREMA Corte de los Estados Unidos, "United States v. Jones (Opinions)" enero 2012. https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf (Fecha de consulta: 28 de junio de 2020)

202. SWICHKOW, Brian, "The Ultimate Retaliation: Pranking My Roommate With Targeted Facebook Ads", Ghost Influence, 6 de septiembre de 2014. https://ghostinfluence.com/the-ultimate-retaliation-pranking-my-roommate-with-targeted-facebook-ads/ (Fecha de consulta: 14 de diciembre de 2020).

203. SYNCTHING, "FAQ", https://docs.syncthing.net/users/faq.html#faq (Fecha de consulta: 29 de agosto de 2020).

204. TATE, Ryan, "Facebook Knows Who You'll Hook Up With", Gawker, 2010, https://gawker.com/5543723/facebook-knows-who-youll-hook-up-with (Fecha de consulta: 12 de diciembre de 2020).

205. TOR, Acerca del Navegador Tor, https://tb-manual.torproject.org/es/about/ (Fecha de consulta: 28 de julio de 2020).

206. TRANSPARENCICA Venezuela, "En Venezuela no existe una Ley que resguarde los datos personales", Transparencia Venezuela, https://transparencia.org.ve/project/en-venezuela-no-existe-una-ley-que-resguarde-los-datos-personales/ (Fecha de consulta: 21 de agosto de 2020).

207. TREATY Office, "Chart of signatures and ratifications of Treaty 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Status as of 24/08/2020", Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=g2DamFix (Fecha de consulta: 24 de agosto de 2020)

208. TREATY Office, "Details of Treaty No.108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (Fecha de consulta: 24 de agosto de 2020)

209. UEBELHERR, Willi, [Internet Policy] The Myth? of analytics, Lista de distribución FSFLA-Discusión, marzo 2017, https://www.fsfla.org/pipermail/discusion/2017/005803.html (Fecha de consulta: 16 de junio de 2021).

210. UNDATA, "Total population, both sexes combined (thousands)", División de Estadística de la Organización de las Naciones Unidas, 2019,

https://data.un.org/Data.aspx?d=PopDiv&f=variableID%3a12%3btimeID%3a83%2c84%3bvarID%3a2&c=2,4,6,7&s=_crEngNameOrderBy:asc,_timeEngNameOrderBy:desc,_varEngNameOrderBy:asc&v=1 (Fecha de consulta: 21 de agosto de 2020).

211. URBAN, Tobias, et al., "Beyond the Front Page: Measuring Third Party Dynamics in the Field", 2020, https://arxiv.org/pdf/2001.10248.pdf (Fecha de consulta: 29 de abril de 2020)

212. VENKATADRI, Giridhari, et al., "Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface", 2018 IEEE Symposium on Security and Privacy, San Francisco, 2018, pp. 89-107, https://ieeexplore.ieee.org/document/8418598f (Fecha de consulta: 14 de diciembre de 2020).

213. VIOLLIER, Pablo, El Estado de la Protección de Datos Personales en Chile, Derechos Digitales América Latina, 2017, pp. 7-9, https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf (Fecha de consulta: 01 de agosto de 2020)

214. W3C, "ActivityPub" https://www.w3.org/TR/activitypub/, (Fecha de consulta: 29 de julio de 2020).

215. W3C, "Appendix E: Accessing code point boundaries" https://www.w3.org/TR/DOM-Level-3-Core/accessing-code-point-boundaries.html (Fecha de consulta: 12 de diciembre de 2020).

216. WAHLSTROM, Kirsten, et al., "On the Ethical and Legal Implications of Data Mining", Technical Report SIE-06-001, School of Informatics and

Engineering, Adelaide, Flinders University, 2006, https://csem.flinders.edu.au/research/techreps/SIE06001.pdf (Fecha de consulta: 29 de abril de 2020)

217. WARREN, Samuel D. y Brandeis Louis, "The Right To Privacy". Harvard Law Review, Vol. IV, Num 5, 1890, http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm (Fecha de consulta 13 de marzo de 2020).

218. WESTIN, Alan, "Privacy And Freedom", Washington and Lee Law Review, No. 166, 1968, https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 (Fecha de consulta: 20 de agosto de 2020)

219. WILNER, Alex, "Cybersecurity and Its Discontents: Artificial Intelligence, the Internet of Things, and Digital Misinformation." International Journal, vol. 73, núm. 2, junio 2018, pp. 308–316, https://journals.sagepub.com/doi/abs/10.1177/0020702018782496?journalCode=ijxa

220. WINDER, Davey, Warning: Microsoft Support Scam 'Freezes' Chrome, Edge And Firefox Browsers – How To Defrost Them, Forbes, abril 2019, https://www.forbes.com/sites/daveywinder/2019/04/30/windows-warning-microsoft-support-scammers-are-freezing-chrome-edge-and-firefox-browsers/?sh=4152586418f1 (Fecha de consulta: 17 de junio de 2021).

221. WIRED Staff, Rogue Ad Attempted to Redirect Wired Readers, Wired, octubre 2012, https://www.wired.com/2012/04/rogue-ad-wired/ (Fecha de consulta: 17 de junio de 2021).

222. XMPP, "An Overview of XMPP", https://xmpp.org/about/technology-overview.html (Fecha de consulta: 29 de julio de 2020).

223. YOUYOU, Wu, "Computer-based personality judgments are more accurate than those made by humans", Proceedings of the National Academy of Sciences, National Academy of Sciences, Vol. 112, No 4, 2015, pp. 1036-1040. https://www.pnas.org/content/pnas/112/4/1036.full.pdf (Fecha de consulta: 07 de agosto de 2020).

224. ZORABEDIAN, John, Data Breach Fatigue Makes Every Day Feel Like Groundhog Day, Security Intelligence, febrero 2019, https://securityintelligence.com/data-breach-fatigue-makes-every-day-feel-like-groundhog-day/ (Fecha de consulta: 28 de junio de 2021).