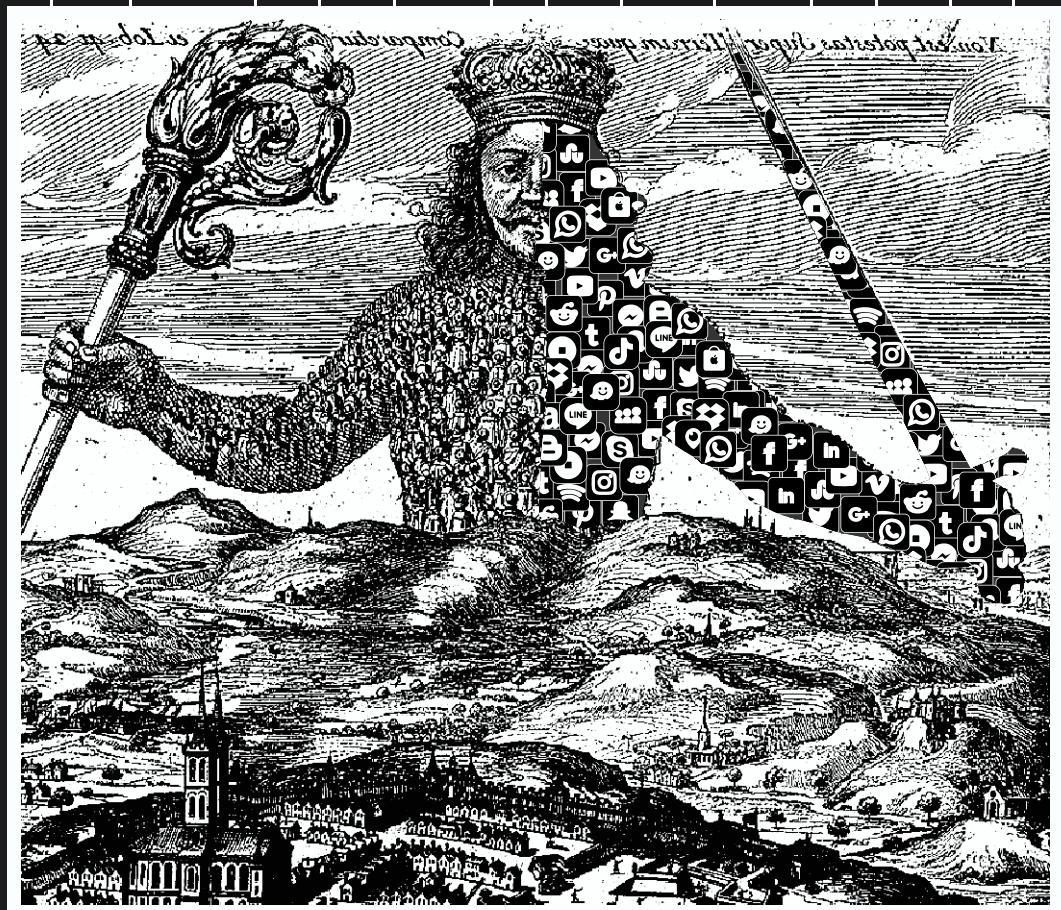


LOS DATOS

EL QUINTO PODER

¿QUIÉNES LE PONEN PRECIO A NUESTRA INFORMACIÓN?



LOS DATOS EL QUINTO PODER

¿QUIÉNES LE PONEN PRECIO
A NUESTRA INFORMACIÓN?



PROGRAMA
SOMOS DEFENSORES

PROGRAMA NO GUBERNAMENTAL DE PROTECCIÓN A
DEFENSORES DE DERECHOS HUMANOS

Los Datos: El Quinto Poder



Calle 19 No. 4-88 Oficina 1302 Bogotá D.C. – Colombia

Tel: (051) 2814010 / www.somosdefensores.org

prensa@somosdefensores.org

2021

El Programa No Gubernamental de Protección a Personas Defensoras de Derechos Humanos – Somos Defensores, es un espacio de protección que busca desarrollar una propuesta integral para prevenir agresiones y proteger la vida de las personas que corren riesgos por su labor como defensores de derechos humanos, cuando resguardan los intereses de grupos sociales y comunidades afectadas por la violencia en Colombia. El Programa Somos Defensores está conformado por:



Asociación MINGA



**Esta edición fue realizada por el Programa Somos Defensores,
bajo la dirección de la Asociación MINGA**

Coordinación Editorial y de Publicación

Leonardo A. Díaz, Sebastián Herrera A., Lourdes Castro

Autor(es)

Leonardo A. Díaz Morales / Sebastián Herrera A.

Diseño, diagramación e impresión

Editorial El Búho S.A.S.

ISBN: 978-958-56838-8-4

Agradecimientos

Este trabajo es gracias al apoyo del equipo de trabajo del Programa Somos Defensores, Lourdes Castro García, Ingrid Beltrán, Sirley Muñoz, Sully Pinzón, Nancy L. Villota, Camila A. Lozano, y a las compañeras de la Asociación MINGA, Diana Sánchez, Martha María Molano, Yolanda Rodríguez y Viviana Hincapié.

El contenido de este informe es responsabilidad de sus autores y no compromete a las organizaciones e instituciones que apoyan esta publicación. Esta publicación es de carácter cultural, pedagógico y su distribución es gratuita. Puede fotocopiarse y reproducirse siempre y cuando se cite la fuente. La impresión de este informe es posible gracias los recursos de la Embajada de Noruega en Colombia.



Embajada de Noruega

El trabajo del Programa Somos Defensores ha sido posible en el 2021 gracias al apoyo de la Embajada de Noruega en Colombia, y las agencias de cooperación internacional Misereor, Pan Para el Mundo, Amnistía Internacional y Diakonia.

ÍNDICE



PRÓLOGO	5
PRESENTACIÓN.....	11

CAPÍTULO I ¿QUIÉNES NOS VIGILAN?

¿Quiénes quieren nuestra información digital?	15
¿Quiénes pueden extraer nuestra información?	18
Tipos de ataque a la información personal	20
Situaciones de ataque a la información personal digital	22
Inteligencia colombiana contra la democracia	35

CAPÍTULO II ¿DÓNDE NOS VIGILAN?

Redes computacionales.....	61
Cronología de internet.....	64
Redes sociales	72

CAPÍTULO III UN CAMPO EN DISPUTA

Internet, redes sociales y política	83
Legislación internacional en materia de derecho a la privacidad ...	98
Legislación en Colombia	116

CAPÍTULO IV ¿CÓMO PROTEGERNOS? UNA SEGURIDAD DIGITAL POSIBLE

Una carta colombiana al Relator Especial sobre el Derecho a la Privacidad.....	135
Reducir los riesgos en un campo minado	138
Recomendaciones para la protección de la información personal y de las organizaciones.....	141
CONCLUSIONES	163



PRÓLOGO

En junio del 2013 un analista de la CIA denunciaba ante el mundo la existencia del primer sistema de espionaje tecnológico de alcance intercontinental, de propiedad estadounidense, operado por la agencia de inteligencia cibernética NSA, y en cuyo intrincado funcionamiento, cooperan las más grandes empresas privadas de la tecnología usamericana en los sectores de sistemas operativos, centros de datos, proveedoras de internet, telefonía celular e infraestructuras de redes telemáticas.

Desde una habitación de hotel en Hong Kong, y luego de una travesía clandestina que le llevó varias semanas de recorrido por varios países, Edward Snowden revelaba a la periodista Laura Poitras y Glenn Greenwald, del periódico The Guardian, un número de pruebas irrefutables que comprometían a las más grandes corporaciones transnacionales tecnológicas usamericanas en el funcionamiento de un potente sistema gubernamental de espionaje masivo subordinado a los intereses geopolíticos de la –hasta el momento– mayor potencia tecnológica del mundo.

El agente de la CIA mostró planos de funcionamiento de ambos sistemas de espionaje digital (PRISM y su proyecto final: XKeyscore) alcances operacionales, responsables gubernamentales y una intrincada red de cooperantes tecnológicos privados.

El escándalo mediático, ciudadano y político no se hizo esperar: CEO's de las más grandes corporaciones tecnológicas, entre ellas Microsoft, Apple, AT&T, Cisco, Google, entre otras corporaciones norteamericanas, salieron presurosos a desmentir la información, a tapar el sol con un dedo, mientras el Departamento de Defensa de Estados Unidos exi-

gía la expedición inmediata de la circular roja de interpol a nombre de Edward Snowden, quien para ese entonces, y dado su conocimiento en geopolítica, ya se encontraba en Rusia, esperando un asilo político que tardaría meses en ser aprobado.

Activistas tecnológicos como Richard Stallman enunciaron una realidad de a puño: el gobierno de estados unidos y aliados (Gran Bretaña, Nueva Zelanda, Canadá y Australia) y corporaciones tecnológicas de USA, han convertido a internet en la extensión virtual de los campos de combate análogos en sujeción a los intereses geopolíticos de la super potencia, en donde, valga decir, la sociedad civil y sus derechos, es la más dignificada.

Sin duda ha sido una década turbulenta en el escenario de la tecnología y la política, es decir, de la tecnopolítica y geopolítica cibernetica. Le debemos a Edward Snowden, Julian Assange, Chelsea Manning, Daniel Heverette Hale, entre otros, la revelación de un escalofriante mundo: el de las guerras de cuarta generación, y por supuesto, gracias a ellos, un nuevo impulso para las diversas luchas hacktivistas en el mundo.

Ya han pasado casi 10 años desde las denuncias de Edward Snowden, y la repercusión de ellas, sin duda, también han tejido interpretaciones y causas en América Latina, escenario histórico de influencia geopolítica estadounidense, en donde, a saber, se han osificado dos tendencias de abordaje respecto al espionaje masivo, aquí un breve esbozo:

1. La tendencia difusionista: la cual, teniendo una lectura juiciosa de la realidad del espionaje masivo en Estados Unidos, extraña dicha realidad al contexto colombiano y de países de periferia, pasando por alto, las profundas asimetrías y brechas en desarrollo tecnológico entre unos y otros, sus concepciones de seguridad nacional, doctrinas de guerra, lógicas de subordinación geopolítica y objetivos locales. Esta lectura asegura la existencia de espionaje masivo, por ejemplo, en Colombia, ubicando todo su andamiaje conceptual desde el derecho y la protección a la intimidad.
2. La tendencia tecnopolítica: desde un análisis de las realidades de infraestructura tecnológica y sus alcances en el espionaje cibernetico, hace un análisis comparativo entre países de centro y periferia. La tendencia tecnopolítica reevalúa (para el caso de la periferia) el concepto de “espionaje masivo”, reemplazándolo por el de “espionaje de segmento”, a saber, como práctica de espionaje tecnológica aplicada

en países de brecha digital, con ausencia de participación en el tejido corporativo tecnológico planetario, estándares de red inferiores al promedio y doctrinas de “enemigo interno” aplicadas en el ámbito cibernético, no en contra de la población toda, sino en contra de grupos activos de la sociedad civil: defensores de derechos humanos, ambientalistas, políticos de oposición, sindicalistas, activistas LGBTIQ, entre otros. Para esta lectura de andamiaje técnico y sociológico, el tema central no está en la privacidad de la información, sino, en el uso de armas de guerra ciberneticas en contra de población civil opositora.

Tendencia difusionista y tendencia tecnopolítica; para unos –en cuestión de tecnologías– Colombia está a la par de Estados Unidos, para otros, la tecnología de espionaje es el resultado de procesos epocales de amplio espectro no homogéneos, con desarrollo diferenciados en nuestros países, y esto exige análisis aterrizados, desde los cuales descubrir sus geografías tecnológicas, y de ahí, sus formas de control social posibles.

No basta con importar software de espionaje “masivo”. Para que exista el espionaje masivo –además– tendrá que haber acceso masivo a las TIC y una capa corporativa tecnológica que respalde; el espionaje masivo es una realidad de pocos países en el mundo (de hecho, USA es el único –en occidente– con la aglutinación de sectores tecnológicos propios y músculo suficiente para consolidar un proyecto de tal magnitud), el espionaje masivo es la corona de un proceso de décadas de desarrollo tecnológico que pasa por la consolidación de empresas TELCO, software, servicios digitales, redes, estructuración de Estado, leyes, entre otros, y eso es importante entenderlo para así hacer las diferenciaciones, estableciendo los hechos reales y límites, desde los cuales se explayan nuevas formas de espionaje en nuestros países y territorios, así mismo los derroteros de protección, temas de delicada importancia en el seno de nuestra sociedad civil.

Colombia es un país en brecha digital, un país que a razón de la guerra le quitó la tierra a millones de campesinos y luego los arrojó a las periferias empobrecidas de las ciudades. Colombia es un país de ciudades desproporcionadas en donde hay más celulares que personas, pero los celulares no están en manos de todos, no, están concentrados (como las tierras) en pocas manos. Colombia es un país con estándares inferiores de red en donde nos venden cable coaxial como si fuera fibra óptica, además con nula participación en el tinglado tecnológico planetario.

Para hacer espionaje tecnológico masivo se necesita de la participación de corporaciones mundiales de la tecnología, que todas se deben a su país: Estados Unidos, no a Colombia. (Ahí el aspecto más poderoso de las revelaciones de Snowden: las empresas tecnológicas no son neutrales, la tecnología no es neutral y ellas se deben al país de donde provienen. Ellas son punta de lanza en el proceso de control geopolítico del siglo XXI, tal cual lo señala Richard Stallman y Julian Assange).

En Colombia no nos espían a todos y todas, para hacerlo, habría de existir un permiso de acceso a los grandes data centers propiedad de las plataformas privadas norteamericanas en donde se depositan los datos de billones de ciudadanos del planeta, incluidos los estadounidenses, o tal vez tener un captador de tráfico parecido al que posee el gobierno Chino, y aunque tengamos que echar mano de teorías de la conspiración, ni aun así nos alcanzaría, y ese ha sido –precisamente– uno de los errores de la lectura difusionista, tal vez, con el ánimo de poner el tema del espionaje tecnológico masivo en centro de debate desde una “pedagogía” un tanto intimidatoria que no ayuda a situar, sino a temer.

En Colombia espían a los que defienden los derechos humanos, a los que hacen oposición política, a los que se organizan por un salario digno y justo, en Colombia no hay sistemas de espionaje “masivos”, pero sí sistemas de espionaje de segmento: como PUMA (Plataforma Única de Monitoreo y Análisis), sistemas acompañados con tecnologías punto a punto o RCS, tales como Pegasus, que no solo captura información, sino que implanta información en equipos de la víctima (y que tampoco es un sistema de espionaje masivo), o Esperanza, (que tampoco es un sistema de espionaje masivo), y que grava conversaciones de objetivos, pero no grava las conversaciones de todos y todas las colombianas, todos los días 24 x 7, en tiempo real, y las deposita en enormes data centers distribuidas desde Leticia a Rioacha con el apoyo de Carlos Slim y los españoles de Telefónica, para luego, ser analizada por cientos de analistas (como Snowden) desde un software de espionaje masivo ubicado en el centro de Bogotá, que en cuestión de segundos, entregue ip, gps, conversaciones y demás, de todos, de todas.

Reitero: PUMA tampoco es una tecnología de espionaje masivo, faltarían varios miles de millones de dólares y empresas emergentes tecnológicas nacionales que arrebaten los usuarios nacionales a Facebook, google, yahoo, Instagram, twitter, entre otros, y que además, acepten o

sean obligadas a entregar datos al sistema de espionaje estatal colombiano. Para eso tendríamos que ser un país que no somos.

Tal vez estemos evadiendo el tema central, tal vez nos obnubilamos en una narración que nos hizo suponer que Colombia está a la par de Estados Unidos, pasando por alto lo que sí nos corresponde: la guerra es hoy análoga y cibernética, es decir: híbrida. Colombia es un país en guerra desde que se hizo su bandera y las tecnologías de espionaje se circunscriben en el segundo brazo de la guerra: el cibernético. Ella –la guerra cibernética en Colombia– se subordina a un paradigma: el modelo de guerra de baja intensidad que busca al “enemigo interno”, fundamentalmente, al interior de la población civil. Insisto: las tecnologías de espionaje son armas tecnológicas que en Colombia se usan en contra de población civil. No nos “chuzaron” el teléfono y “vulneraron nuestra intimidad”, ojalá fuera ese el problema, pero no: nos “bombardearon” nuestras telecomunicaciones, disparan armas de ciberguerra en contra de la población civil organizada vista como objetivo militar.

Ahí el tema central de este debate que va más allá del derecho a la intimidad, que supera la mirada de equiparar a Colombia con Estados Unidos en donde Zuckerberg y Silicon Valley también obedecen al presidente colombiano de turno. Es decir, superando esa narración distorsionante, se presentan temas urgentes y nuevas formas de comprensión, denuncia, reglamentación y protección situadas en nuestra realidad.

FARID AMED
Director
Fundación Casa del Bosque



PRESENTACIÓN

El presente es un documento pedagógico que expone la forma en que el mundo digital, desde el surgimiento del internet como lo conocemos actualmente, ha dado un valor monumental a nuestra información y datos, en términos financieros, culturales, sociales y por supuesto, políticos. Además, pretende alertar sobre los riesgos que se ciernen sobre nuestros datos y el derecho a la privacidad, dada la variedad de actores que están interesados en adquirirla, venderla e incluso, usarla en nuestra contra. Para cumplir estos objetivos y con el fin de ofrecer algunas recomendaciones para la protección y seguridad digitales, especialmente para personas y organizaciones defensoras de derechos humanos, el texto se divide en los siguientes capítulos.

En el **Capítulo I** se mencionan y caracterizan los distintos actores, nacionales e internacionales, públicos y privados, que necesitan nuestros datos; ya sean adquiridos por medios legales o apelando a la trillada minería de datos sin regulación alguna, en un escenario de ilegalidad. Estados y sus agencias de seguridad e inteligencia, corporaciones, empresas privadas dedicadas al desarrollo digital y el aprovechamiento del excedente conductual, agencias de marketing político y otros entes hacen parte de esta lista.

En el **Capítulo II** se aborda la historia de internet desde sus orígenes, haciendo énfasis en los momentos claves de su desarrollo. También se hace referencia a una breve historia de las redes sociales digitales y se ofrece una tipología mínima de las mismas.

En el **Capítulo III** se explica la forma en que internet y todo el campo virtual está en disputa para aprovechar sus beneficios. De un lado, los

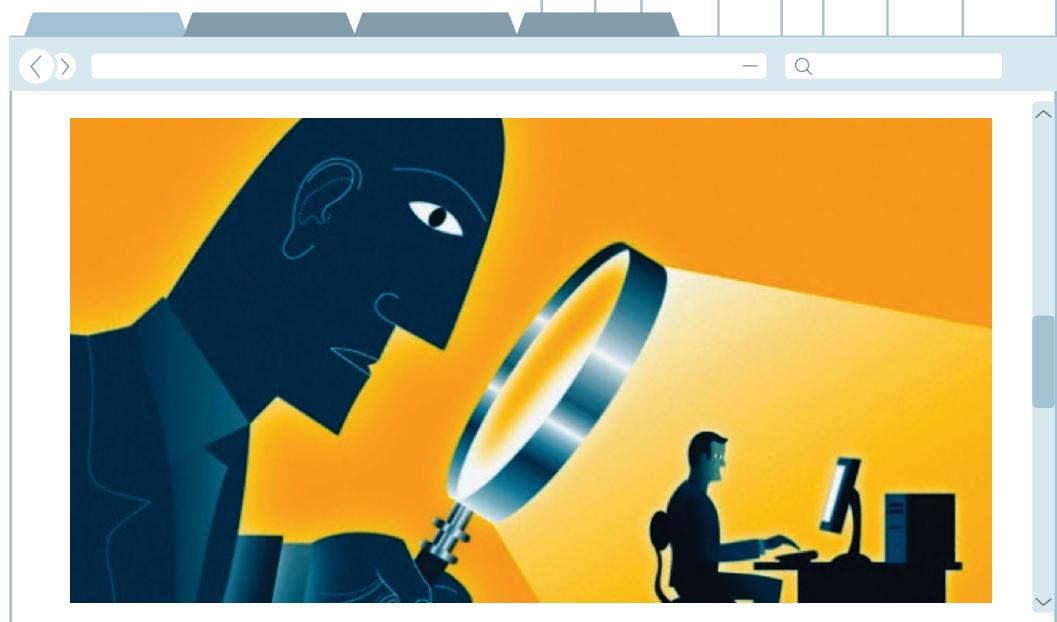
movimientos sociales y los procesos políticos constituyentes; de otro lado, las grandes empresas, los organismos de inteligencia y seguridad estatales junto al aparato jurídico y judicial que los cobija. Aquí se expone también el marco legal internacional y nacional que se relaciona con el derecho a la privacidad y los alcances sobre la información personal.

Finalmente, el **Capítulo IV** es una guía didáctica para poner en práctica los conocimientos técnicos, tecnológicos, jurídicos e históricos esbozados en los capítulos anteriores, con el fin de reducir los riesgos y proteger nuestra información dentro de los límites posibles y con conciencia plena del ámbito donde circula.

CAPÍTULO 1



¿QUIÉNES NOS VIGILAN?





“Internet, nuestra mayor herramienta de emancipación, se ha transformado en la facilitadora más peligrosa del totalitarismo jamás vista.”

JULIÁN ASSANGE

“Los colombianos tenemos derecho a saber quién fue el que convirtió al país en un Estado de policías y terroristas del Estado, quién intentó convertir esto en una nación de espías, quién fue el que concibió el macabro plan de convertir a opositores reales o imaginarios como si fueran delincuentes, quién, quién está detrás de esto. ¿Tres detectives del DAS? No me hagan reír.”

JUAN GOSSAÍN

No hay nada oculto entre el cielo y la tierra, todo lo que se haga es susceptible de conocerse; le ocurrió a la Agencia Nacional de Seguridad Estadounidense (NSA) con Snowden y WikiLeaks; a las FARC-EP con el computador de Raúl Reyes.

En el mundo entero, millones de ciudadanos y ciudadanas que viven sus vidas conforme a las reglas de juego impuestas por distintos régimenes políticos, son vigilados y vigiladas. Las actividades de millones de seres humanos en el mundo son, sin saberlo, permanentemente espiadas, violando leyes nacionales e internacionales, transgrediendo derechos y libertades promulgados por la misma democracia liberal.



¿QUIÉNES QUIEREN NUESTRA INFORMACIÓN DIGITAL?

La respuesta es: ¡todos!

Los dueños de las plataformas digitales, un familiar, una pareja o expareja, un jefe o subordinado, una vieja amistad o enemistad, un delincuente cibernético, un investigador, un político, un comerciante, una corporación, una compañía, etc.

Sin embargo, todos los mencionados no están en el mismo nivel; una expareja, una vieja amistad o un familiar pueden recurrir al nivel pú-



blico de Facebook, donde aparece nuestro nombre, nuestras fotos y la información que hemos hecho pública con cierta conciencia. Nosotros mismos queremos curiosear sobre aquellas personas con las que tuvimos algún vínculo y con quienes quisiéramos establecer nuevamente contacto o saber de ellas simplemente.

Pero los dueños de las plataformas digitales, los gobiernos, las corporaciones y demás actores globales, se encuentran en el nivel de poder suficiente para acceder a información confidencial y utilizarla en su favor, para sostener y recrear el actual estado de cosas en el mundo.

El último informe publicado por Oxfam (Oxford Committee for Famine Relief) señala que la desigualdad en el mundo ha alcanzado niveles preocupantes. Ha aumentado la cifra de mil millonarios que poseen más riqueza que 4.600 millones de personas, es decir, el 60% mundial de la población.

En América Latina y el Caribe, el número de mil millonarios ha pasado de 27 a 104 desde el año 2000. El 20% de la población concentra el 83% de la riqueza; en 2019, 66 millones de personas, esto es el 10,7% de la población, vivía en extrema pobreza, siendo las mujeres el sector más afectado; el trabajo de los cuidados recae sobre las mujeres, por lo que no pueden encontrar fácilmente trabajo remunerado; el 49% de las mujeres que logran acceder a un empleo ganan menos del salario mínimo mensual correspondiente a su país.¹

La Organización de las Naciones Unidas (ONU) advirtió en 2020 que el potencial transformador de las nuevas tecnologías no es aprovechado globalmente, pues el acceso a ellas es restringido aún, generando nuevas divisiones digitales, especialmente en países periféricos y empobrecidos como Colombia.

El segundo hombre más rico del mundo en la actualidad, que aparece como un número en el informe de Oxfam, es Jeff Bezos, presidente de Amazon. Una compañía que ya es mucho más que una tienda digital de libros: tiene la mitad del negocio mundial de la “nube”, es decir, que en sus servidores se encuentra más de un tercio del internet en donde se alojan diariamente 2,5 quintillones de datos. Esos súperservidores,

¹ Oxfam International. 2019. *¿Bienestar público o beneficio privado?* <https://www.oxfam.org/es/informes/bienestar-publico-o-beneficio-privado>

requieren gran cantidad de energía para no recalentarse: ya en 2008 generaban el 2% de gas carbónico que producía el planeta.²

Imagen 1.



Jeff Bezos

El resultado natural de este sistema profundamente desigual, el capitalismo, es la transfiguración de los derechos y servicios sociales en jugosos negocios: la salud, la educación, la vivienda, el agua, los alimentos y también la información, se traducen en mercancías.

Las grandes firmas informáticas como Facebook, Google, Twitter, Amazon, entre otras, tienen un modelo de negocio en el que la más codiciada mercancía son los datos de millones de usuarios y usuarias. Datos que se generan en la cotidianidad de cada persona, en su vida pública y privada. Internet además constituye una vía por la cual circulan mercancías y capitales, es un medio de comercio global.³

En el caso colombiano, en un contexto de conflicto social y armado de más de cinco décadas, el poder del Estado se ha ligado estrechamente

² Peirano, M. 2019. *El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención*. Editorial Debate.

³ Fuchs, C. 2017. *Hacia un estudio marxiano del internet*. Revista de Ciencias Sociales 155: 63-89. Universidad de Costa Rica.



con la mafia, otro producto natural del capitalismo, a cuyos intereses se oponen las personas que pretenden ampliar la democracia, bajo un modelo ético basado en la exigibilidad de derechos y el liderazgo social para alcanzar el bienestar colectivo.

El Padre Javier Giraldo señala en el informe de la Comisión Histórica del Conflicto y sus Víctimas, que la clase dirigente ha configurado una institucionalidad pública y un Estado “excluyente y elitista”, identificando como enemigo de sus intereses a:

“el sindicalista, el campesino que no simpatiza o se muestra reñiente ante las tropas militares que penetran en su vereda o en su vivienda, el estudiante que participa en protestas callejeras, el militante de fuerzas políticas no tradicionales y críticas, el defensor de derechos humanos, el teólogo de la liberación y en general el poblador inconforme con el statu quo.”⁴

Para el caso de las personas defensoras de derechos humanos, líderes y lideresas sociales, quienes administran el Estado están muy interesados en obtener nuestra información para ejercer vigilancia y control sobre cualquier sujeto, individual o colectivo, que amenace los intereses del capital transnacional y sus adalides nacionales, o que contradiga las ideas de sus portavoces políticos.



¿QUIÉNES PUEDEN EXTRAER NUESTRA INFORMACIÓN?

A continuación, establecemos una categorización técnica y sucinta de qué o quiénes pueden extraer nuestra información:

⁴ Giraldo, J. 2015. *Aportes sobre el origen del conflicto armado en Colombia, su persistencia y sus impactos*, En: *Contribución al entendimiento del conflicto Armado en Colombia*. Comisión Histórica del Conflicto y sus Víctimas.

INFOGRAFÍA 1

AGENTES	FORMAS
Programas y dispositivos 	<p>Software que captura ingentes cantidades de datos, desde la interacción en las redes sociales hasta audios, fotos, documentos, historial de búsquedas y hábitos de conexión.</p> <p>Hardware que apoya este recaudo, como teléfonos inteligentes, cámaras, micrófonos, entre otros.</p>
Hackers 	<p>Contrario a la imagen generalizada, las y los hackers son personas con excelentes conocimientos y habilidades en el ámbito de la computación, orientadas por un código ético que tiene como principio no sabotear ningún sistema, pero sí intentar entrar en él.</p> <p>Pueden incluso ayudarnos a encontrar debilidades en nuestros sistemas. Se puede decir que su interés es cognoscitivo y también político.</p>
Crackers 	<p>Personas con una labor similar a las que son hackers, con la diferencia de tener otras intenciones con nuestra información, de manera que puede atacar el sistema y dejarnos fuera de línea, hurtar datos o daños similares; pueden catalogarse como delincuentes.</p> <p>En Colombia hay experiencias de contratación de <i>crackers</i> para la vigilancia ilegal, como el caso del llamado “hacker de Uribe”, Andrés Sepúlveda.</p>
Script-kiddies 	<p>Principiantes que aspiran ser hackers o crackers y que sin saber realmente lo que hacen, pueden causar mucho daño porque no tienen claridad de sobre su alcance.</p> <p>Este puede ser un mayor número de personas que los dos anteriores (Soriano, sf).</p>
Organismos de inteligencia del Estado 	<p>Vigilancia y actividades de inteligencia a través de programas espía. A nivel mundial, como Prism o Echelon y en territorio colombiano con Puma, Galileo, Esperanza u Hombre invisible.</p>

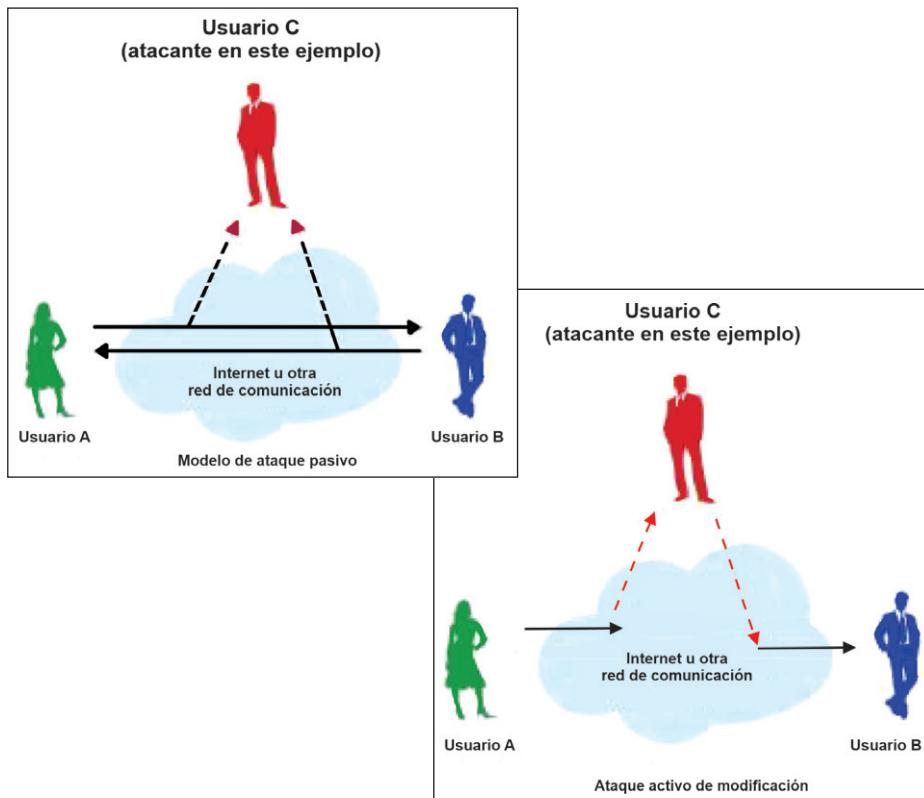


TIPOS DE ATAQUE A LA INFORMACIÓN PERSONAL

Ahora bien, la vigilancia e intromisión en nuestra información se consideran formas de ataque. Luego de importantes luchas para ampliar la juridicidad al respecto en cada país, han empezado a ser penalizados paulatinamente pues constituyen una agresión a la intimidad o a la seguridad de organizaciones y personas que las integran.

En este sentido podemos hablar de dos tipos de ataque: pasivo y activo.

Imagen 2



Fuente: seguridadenlasredesanc.blogspot.com

ATAQUE PASIVO

Se caracteriza por el monitoreo y seguimiento, tanto del flujo de información como de la información en sí misma. Aquí se da lo que llamamos espionaje, que es la observación encubierta de alguien distinto al destinatario de la información enviada de manera abierta (no cifrada).

Otra forma de ataque pasivo es el análisis de tráfico, que consiste en la interceptación y el examen de los mensajes para extraer datos a partir del análisis de los patrones de comunicación. Se puede realizar incluso cuando los mensajes están cifrados. En general, cuanto mayor es el número de mensajes observados, interceptados y almacenados, más se puede inferir del tráfico.

El análisis de tráfico, entre otras cosas, permite a un atacante verificar que dos entidades están manteniendo una comunicación en un determinado momento.

ATAQUE ACTIVO

Es un ataque con el objetivo de modificar o borrar los contenidos de la información y los recursos del sistema, o afectar su funcionamiento. Los ataques activos implican alguna modificación del flujo de datos o la creación de datos falsos.

Este tipo de ataque es común en bases de datos de organizaciones sociales y/o políticas; por ejemplo, las bases de datos de seguimiento a la situación de derechos humanos de un país o territorio, o información sobre hechos y conductas criminales que conlleven efectos judiciales.

En esta modalidad de ataque es posible suplantar la identidad del usuario, modificar el mensaje y reinsertarlo; y/o repetir una transmisión de datos, entre otros. (Soriano, sf).





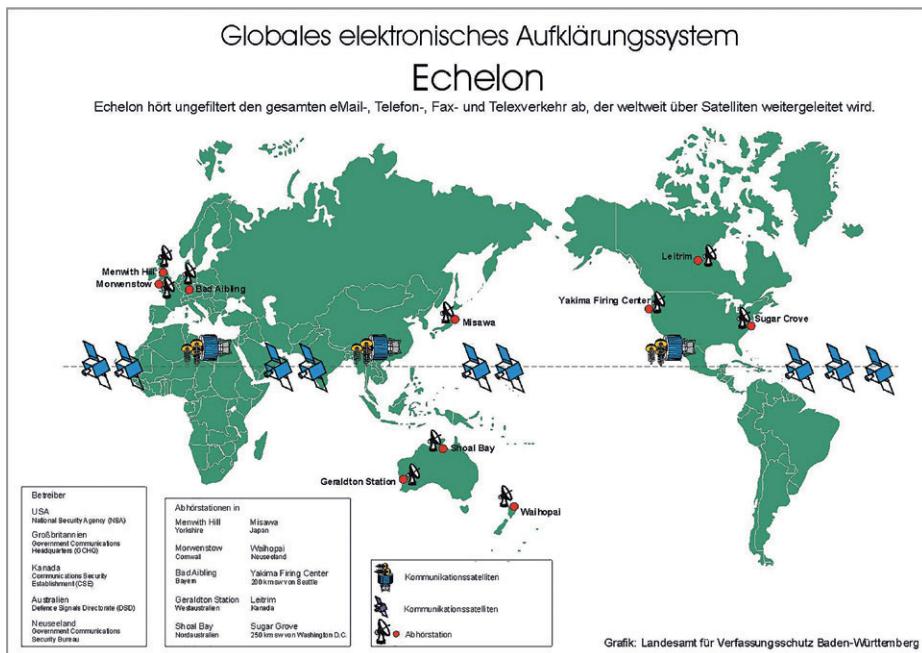
SITUACIONES DE ATAQUE A LA INFORMACIÓN PERSONAL DIGITAL



VIGILANCIA MASIVA EN LA POSGUERRA

Estados Unidos ha intentado, desde hace mucho tiempo, controlar el flujo de información en internet. Ante la imposibilidad de lograrlo, han desarrollado algunos programas 'espías' que monitorean buena parte de lo que circula por internet y según los últimos datos, ya logran grabar, copiar y archivar la información que circula por la red.

Imagen 3.



Fuente: http://www.academia.edu/download/34404651/Le_Monde_124.pdf

Durante la Segunda Guerra Mundial, EE.UU. e Inglaterra firmaron un acuerdo que les permitía compartir información sobre protocolos y cifrado de la máquina japonesa Purple. Una vez terminada la guerra, los dos países establecieron un nuevo acuerdo para la interceptación

de las comunicaciones a nivel mundial, especialmente las de la Unión Soviética.

Este acuerdo, conocido como UKUSA⁵, congregó a otros países dominados por Reino Unido y sus respectivas instituciones de defensa: NSA⁶ de Estados Unidos, GCHQ⁷ de Reino Unido, DSD⁸ de Australia, CSE⁹ de Canadá y GCSB¹⁰ de Nueva Zelanda (Ramonet, 2017).

Esta alianza imperial formó la red de espionaje Echelon, que fue uno de los secretos mejor guardados de la posguerra: se conoció de su existencia en 1976. Se cree que todavía opera en el mundo y que viene recopilando información desde la Segunda Guerra Mundial.

Con el surgimiento y posterior desarrollo del internet, junto a la caída del muro de Berlín y el bloque socialista, se implementaron una diversidad de programas para monitorear las comunicaciones, ya no sólo de otras potencias sino de la ciudadanía en general, carnivore, Dishfire Stoneghost, Frenchelon, Muscular, XKeyscore y Prism son algunos de los más conocidos.



CASO SNOWDEN

En el año 2013, el espía y analista de la Agencia de Seguridad Nacional (NSA), Edward Snowden, filtró a través del Washington Post y Globe, un número indeterminado de documentos que revelaban cómo EE. UU. estaba espiando dentro y fuera de su territorio.

Este hecho tuvo importantes implicaciones en lo político y lo jurídico, en el ámbito nacional e internacional.

⁵ También conocida como Los Cinco Ojos (Five Eyes).

⁶ National Security Agency (Agencia de Seguridad Nacional).

⁷ Government Communications Headquarters (Cuartel General de Comunicaciones del Gobierno).

⁸ Defence Signals Directorate (Dirección de Señales de Defensa), ahora Australian Signals Directorate (ASD).

⁹ Communications Security Establishment (Establecimiento de Seguridad de Comunicaciones).

¹⁰ Government Communications Security Bureau (Oficina de Seguridad de Comunicaciones del Gobierno).

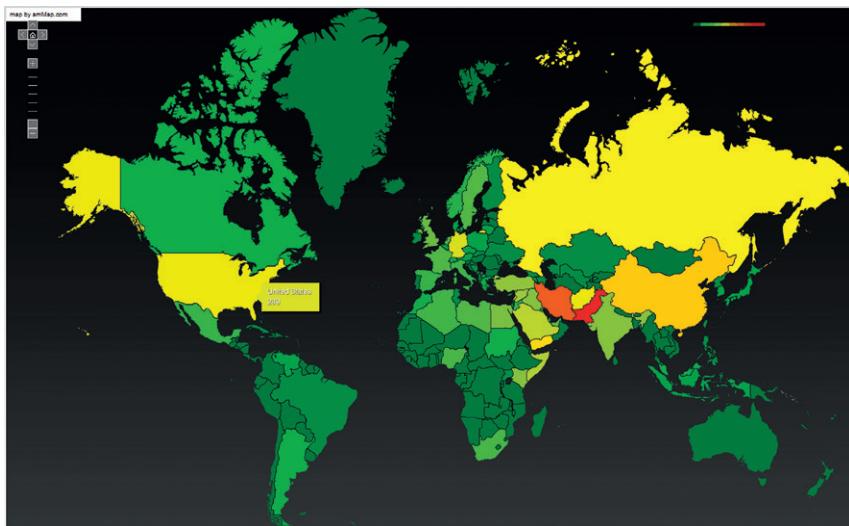
Imagen 4.



Edward Snowden

El joven analista reveló uno de los rostros más ocultos de la potencia norteamericana, demostrando con todo el material publicado que “la vigilancia no tiene que ver con la seguridad, tiene que ver con el poder.”¹¹

Imagen 5.



¹¹ Pérez, J. 2019. *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos*. Universidad de Sevilla.

El esquema va del verde (menor nivel de vigilancia) hasta el amarillo, el naranja y el rojo (mayor nivel de vigilancia).

Los testimonios de Snowden revelaron que la vigilancia masiva por parte de las instituciones gubernamentales estadounidenses se realiza filtrando las acciones en la red móvil y de internet de personas extranjeras, a través de plataformas con vinculación jurídica estadounidense. Estados Unidos vigilaba a líderes mundiales aliados, como Ángela Merkel, y también de aquellos países competidores, como China y Rusia; incluyendo otra multitud de personajes importantes, especialmente del mundo empresarial y financiero, como el presidente de Petrobras.

También se supo que las empresas Google Inc., Facebook, Microsoft, Yahoo!, PalTak, YouTube, Skype, AOL y Apple, compartían información personal y metadatos de sus usuarios con la NSA. Si bien estas empresas negaron dicha información, se ha conocido por otros informes que la agencia les ha solicitado implantar puertas traseras (*backdoors*) en sus sistemas, de tal manera que dichos programas y/o plataformas de servicio puedan ser monitoreadas.



VENTA DE INFORMACIÓN Y DATOS

En el mundo virtual, nuestros datos están alojados en las plataformas de compañías privadas cuyo negocio es “investigar, evaluar, clasificar y empaquetar a los usuarios en categorías cada vez más específicas para vendérselas a sus verdaderos clientes, que incluyen dictadores, empresas de marketing político y agencias de desinformación.”¹²

Es así como la información personal de usuarios y usuarias de internet es permanentemente atacada por estas compañías a través de aplicaciones, tests, formularios, ofertas especiales o rebajas, entre otros mecanismos que estimulan la interacción en la red.

Esta interacción genera una gran cantidad de datos, cuyo procesamiento, mediante algoritmos, permitirá a los comerciantes de la red realizar campañas y estrategias de ventas cada vez más personalizadas (por edad, sexo, clase social, etc.); a los políticos, influenciar la intención

¹² Peirano, M. 2019. *El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención*. Editorial Debate.



de voto; a los crackers, usurpar la identidad para realizar manipulación de información, estafas electrónicas y ataques cibernéticos; a los investigadores, adentrarse más en la intimidad de la persona en cuestión y así, un sinnúmero de posibles maniobras aprovechadas por el tráfico informático.

La utilización globalizada de las diferentes técnicas de marketing digital recopila cada segundo una cantidad impresionante de información privilegiada acerca de los gustos, preferencias, horarios y rutas de ubicación de los usuarios de internet. Esta información es clasificada y segmentada como nunca se había hecho en la historia de la humanidad.

La gran cantidad de datos generados en la red segundo a segundo, por el uso e interacción en ella, origina lo que se ha llamado Big Data y es de tal magnitud, que “superá la capacidad del software convencional para ser capturada, administrada y procesada en un tiempo razonable.”¹³

La utilidad de esa información depende de la velocidad con que se generan y se procesan los datos, así como del volumen y la veracidad de estos.

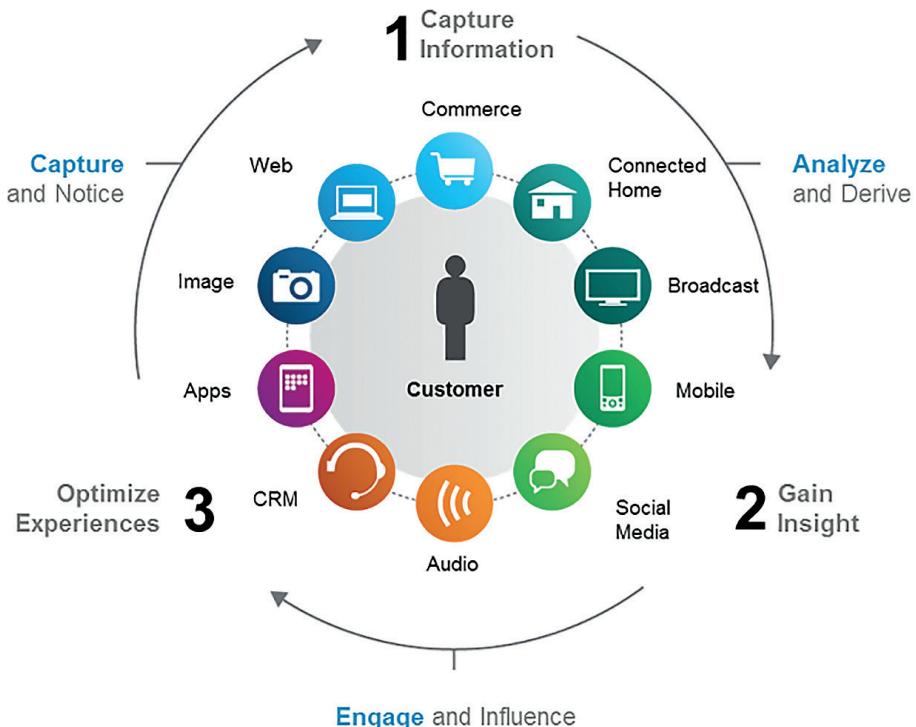
Adsalsa¹⁴ es una de las empresas más grandes en Europa de marketing digital. Su especialidad es la producción de ‘lead generation’, es decir, la creación de fichas de datos reales y verificados. Raúl Abad, director de marketing de Adsalsa, en el año 2015 afirmaba “que el precio de un lead (persona con datos verificados) varía dependiendo de la cantidad de información y puede oscilar entre los 2 y los 10 euros. A 15 euros pueden llegar los leads premium que tienen más información personal.”¹⁵

¹³ Riquelme, R. 2017. *¿Cómo proteger la información en un proyecto de big data?* El Economista. <https://www.eleconomista.com.mx/tecnologia/Como-proteger-la-informacion-en-un-proyecto-de-big-data-20171210-0007.html>

¹⁴ www.adsalsa.com

¹⁵ Contreras, M. 2015. *Así es como las grandes empresas venden tus datos en internet.* El Confidencial. https://www.elconfidencial.com/tecnologia/2015-09-14/asi-es-como-venden-tus-datos-personales-en-internet_1011071/

Imagen 6.



"Los profesionales de marketing pueden obtener datos completos del consumidor en tiempo real y utilizarlos para personalizar sus ofertas según las necesidades de cada cliente".

Fuente: <https://velogig.com/big-data-la-clave-para-entregar-valor-a-los-clientes/>

La forma en la que se consiguen los datos es importante. Por eso estas empresas trabajan con socios o crean sus propios portales para captar personas con intereses concretos, se asocian con marcas reconocidas, creando páginas de aterrizaje (landing pages) con especificaciones de clientes. Gracias a esto se consiguen datos reales y específicos para más tarde venderlos.



CASO FACEBOOK

Esta empresa se ha constituido en un verdadero monopolio de las redes sociales, con la compra de WhatsApp e Instagram es protagonista permanente de diversos escándalos de venta y manipulación de información.



A finales de 2010, el diario estadounidense Wall Street Journal¹⁶ reveló que por lo menos diez de las aplicaciones más populares programadas sobre la red Facebook, transmitieron datos como nombres de usuarios y los de sus amigos a por lo menos 25 empresas.

En 2015, la prensa británica y el diario The New York Times¹⁷ revelaron que Facebook proporcionó acceso a los datos de miles de usuarios, siendo obtenidos posteriormente por la empresa Cambridge Analytica, que a su vez procesó dicha información para orientar la intención de voto del electorado estadounidense a favor de Donald Trump, quien contrató sus servicios.

Imagen 7.



Mark Zuckerberg y Donald Trump.

Mark Zuckerberg, fundador y dueño de Facebook, admitió que hasta 2014 permitía el acceso a los datos de los usuarios con fines investigativos a través de algunas aplicaciones y que otorgó el acceso a un investigador inglés que aplicaba una prueba. El investigador presuntamente vendió los datos a Cambridge Analytica, que los manipuló con fines políticos.¹⁸

¹⁶ <https://www.wsj.com/articles/SB128741022257647963>

¹⁷ <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

¹⁸ González, M. 2018. *Qué ha pasado con Facebook: del caso Cambridge Analytica al resto de polémicas más recientes*. Xataka. <https://www.xataka.com/legislacion-y-de-rechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polémicas-mas-recientes>

Sin embargo, hay serias dudas de la inocencia de Facebook en este escándalo, como lo revelan los testimonios de algunos trabajadores y del mismo ex director de Cambridge Analytica, quien afirma que en la organización de Zuckerberg sabían qué ocurría con la información. A esto se suma que Facebook permitió la difusión de noticias falsas producidas por la firma inglesa, como parte de la campaña electoral y como resultado del análisis de datos de más de 80 millones de estadounidenses. Lo que se reveló en este caso es el modelo de negocio que maneja Facebook.¹⁹

Facebook conoce nuestros datos personales, agenda telefónica, mensajes, fotos y videos (con geolocalización, fechas de publicación o direcciones IP asociadas en muchos casos), chats e la información sobre las sesiones que hemos abierto. Incluso las llamadas y mensajes de texto (SMS, Short Message Service).

“Las empresas que ganan dinero mediante la recolección y venta de registros detallados de vidas privadas fueron descritas una vez claramente como ‘compañías de vigilancia’. Su remarcación como ‘social media’ es el engaño más exitoso desde que el Departamento de Guerra se convirtió en el Departamento de Defensa”, afirmó Snowden en 2018 a través de Twitter, refiriéndose a Facebook.

El diario brasileño O Globo anunció que a través de Prism, que es uno de los programas usados por la NSA y que incursiona en Facebook, Google y YouTube, entre otros sitios web, la agencia estadounidense “obtuvo datos sobre petróleo y adquisiciones militares en Venezuela, energía y narcóticos en México, además de haber mapeado los movimientos de las insurgencias en Colombia.”²⁰

“Los documentos muestran una colecta de información en Colombia con un flujo expresivo y constante”. Estados Unidos estableció un acuerdo de cooperación militar con Colombia, destinado a la lucha contra el narcotráfico y los grupos armados ilegales, inicialmente con el Plan

¹⁹ Riley, Ch. 2018. *Lo que necesitas saber sobre el escándalo de Facebook por la filtración de información*. CNN. <https://cnnespanol.cnn.com/2018/03/19/facebook-trump-filtracion-datos-cambridge-analytica-usuarios/>

²⁰ O Globo. 9 de julio de 2013. *Espionagem dos EUA se espalhou pela América Latina*. <https://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619>



Colombia, por el que se ha recibido desde Washington más de 8.000 millones de dólares desde el año 2000.²¹

En el mes de enero de 2019, la Superintendencia de Industria y Comercio (SIC) exigió a Facebook adoptar medidas para garantizar la seguridad de los datos de más de 31 millones de usuarias y usuarios colombianos que están registrados en la red social. La medida se adoptó, según la Superintendencia, con ocasión de otras investigaciones que cursan en más de 10 países contra Facebook.

El organismo estableció que la compañía debe evitar las siguientes prácticas:

- Acceso no autorizado o fraudulento.
- Uso no autorizado o fraudulento.
- Consulta no autorizada o fraudulenta.
- Adulteración no autorizada o fraudulenta.
- Pérdida no autorizada o fraudulenta.

Imagen 8.



Conexión a nivel mundial de Facebook, actualmente se estima que cuenta con 2.600 millones de usuarios.

Fuente: marketingdigital.news

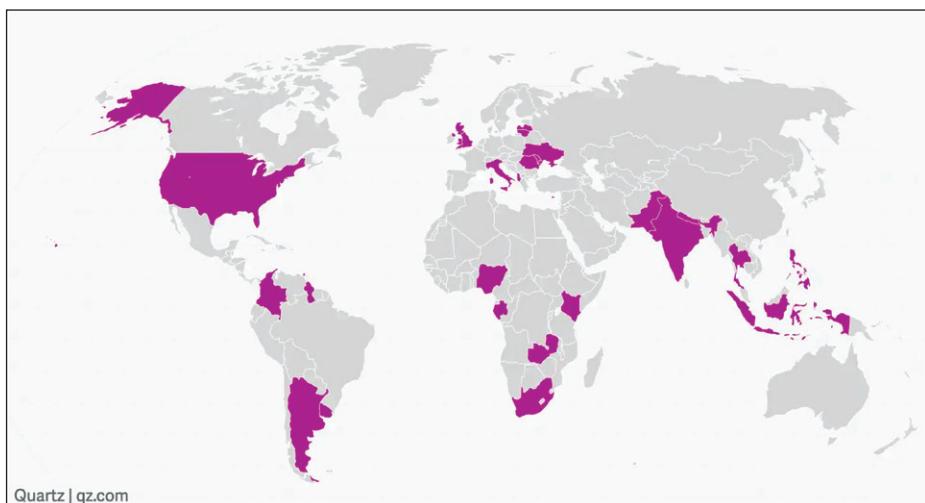
²¹ Semana. 30 de enero de 2014. *Estados Unidos espía los datos de los colombianos en redes sociales*. <https://www.semana.com/estados-unidos-espia-datos-colombianos-redes-sociales/374690-3/>

CASO CAMBRIDGE ANALYTICA

Cambridge Analytica, compañía británica que se derivó de la firma SCL Group, un grupo de contratistas gubernamentales y militares que, trabajaba desde hace más de 25 años en diversos sectores, como la investigación en seguridad alimentaria, la lucha contra los narcóticos y las campañas políticas.

Creada en 2013 por Alexander Nix y financiada por Stephen Bannon, ex asesor de Trump y reconocido político de ultraderecha, esta firma se dedicaba al análisis y ‘minería de datos’ que ofrecía a empresas y campañas electorales “para cambiar el comportamiento de las audiencias.”²²

Imagen 9.



Países en los que Cambridge Analytica trabajó en campañas políticas. En Colombia participó en 2011 con la estrategia de Enrique Peñalosa.

Fuente: ‘The Great Hack’ (Netflix, 2019).

Alexander Nix obtuvo acceso a los datos de 50 millones de estadounidenses y los usó para dirigir la campaña electoral del expresidente Do-

²² Castañeda, J. 2018. *¿Cuál fue el escándalo de Facebook y Cambridge Analytica en época de elecciones?* Fundación Karisma. <https://web.karisma.org.co/cual-fue-el-escandalo-de-facebook-y-cambridge-analytica-en-epoca-de-elecciones/>



nald Trump. Los datos fueron recabados por Aleksandr Kogan, profesor de la Universidad de Cambridge y científico de datos, a través de una aplicación de Facebook para hacer un test de personalidad que para realizarse requería acceso a la información personal y a la red de amigos, sin que estos dieran su consentimiento.

La prueba se realizó a 270.000 usuarios que terminaron enlazando en la interacción propia de la aplicación al 15% de la población estadounidense: 50 millones de personas. Kogan vendió la aplicación y la información a Nix, que a su vez la utilizó para manipular psicológicamente al electorado estadounidense a través del diseño de contenido ajustado a los resultados del test.

La estrategia política usada por Cambridge Analytica ha sido probada en todo el mundo, en especial en América Latina. Luego del triunfo de Trump, en 2017 Cambridge Analytica abrió una filial en Brasil de cara a las elecciones, donde “planeaban aplicar el uso del direccionamiento inteligente de mensajes políticos a WhatsApp”. Esto para beneficiar al candidato de extrema derecha Jair Bolsonaro, que efectivamente llegó en 2018 a la presidencia.

En Argentina diseñaron la campaña de des prestigio al ‘kirchnerismo’, como parte de la estrategia para llevar a Mauricio Macri a la presidencia. Colombia aparecía en la página web de la firma, como uno de los referentes de su trabajo e incluso allí se exhibía una foto del exalcalde de Bogotá Enrique Peñalosa, acompañada de un artículo en el que aseguraban que se trató de una de sus asesorías exitosas. La imagen del alcalde también se ve en el documental ‘Nada es Privado’ (también llamado ‘El Gran Hackeo’ o ‘The Great Hack’) de Netflix, sobre el escándalo de la compañía inglesa. (Netflix, 2018).

Un vocero de la Alcaldía de Bogotá en su momento desmintió el nexo, pero por comunicados oficiales de la propia Cambridge Analytica, de julio de 2017, se sabe que trabajó en alianza con Farrow Colombia S. A. S., una empresa vinculada a la aplicación para celulares Pig.gi. En 2018, la Superintendencia de Industria y Comercio (SIC) ordenó el bloqueo temporal de la aplicación Pig.gi porque podría estar relacionada con Cambridge Analytica y poner en riesgo la información personal de sus usuarios²³.

²³ Para más información: www.sic.gov.co/noticias/como-medida-preventiva-superindustria-ordena-bloqueo-de-aplicacion-pig-gi-por-su-aparente-vinculacion-con-posible-tratamiento-ilegal-de-datos-personales-decolombianos

 CASO GOOGLE

Google y todas las herramientas que ofrece son muy atractivas por su comodidad y utilidad. Por ejemplo, el buscador personaliza las búsquedas de acuerdo con nuestro perfil (ubicación geográfica, horario, intereses personales), el correo nos provee un buen espacio en la nube (15 GB) y una mensajería fácil de usar, una libreta con nuestros contactos, un calendario en el cual hacer anotaciones y dejar recordatorios, una galería de fotos, un espacio de trabajo colaborativo con textos tipo Word y hojas de cálculo tipo Excel, un mapa de todo el mundo para averiguar por la espacialidad de múltiples lugares y otras herramientas más.

Imagen 10.



La investigadora española Marta Peirano presenta a Google como una de las compañías más poderosas de la red cuyo modelo de negocio de venta de datos ha marcado la pauta en el proceso de monopolización de la red, siendo además pieza tecnológica clave en el fenómeno de la vigilancia masiva. Afirma la periodista:



“A Serguéi Brin (presidente de Google) le gusta decir que se ha hecho rico ayudando a millones de personas a hacer las cosas que quieren hacer. Esto es completamente cierto.

Todos los servicios de la empresa son excepcionales. Son útiles, fáciles de usar y ofrecen una nueva relación con el mundo y el espacio. También es cierto que todos están diseñados para la extracción masiva de datos: todo lo que busca, escribe, envía, calcula, recibe, pincha, comparte, lee, borra o adjunta el usuario es digerido por los algoritmos de Google y almacenado en sus servidores para la explotación eterna.

Al principio de todo existía el concepto de que esta información no podía estar vinculada al mundo real. El User ID pertenecía al «mundo digital» de la plataforma y no estaba vinculado a una persona real en el mapa. Después llegaron Google Maps y Google Earth, un modelo de la Tierra creado a partir de un collage de imágenes satelitales, fotografías aéreas y datos SIG, financiado por el programa In-QTel de la CIA. Y, como complemento, un modelo literal a escala del mundo real llamado Google Street View.”²⁴

Peirano reseña la participación de Google en el diseño de tecnologías para el negocio de la guerra: el mejoramiento del video y la orientación de los ataques de los drones estadounidenses; la realización de un buscador especial para la CIA, “en el que escanearon todos los archivos de inteligencia”; “un sistema de inteligencia visual para la Agencia de Inteligencia Geoespacial con las bases militares que tenían en Irak y Afganistán”; el desarrollo de un visualizador del globo en tiempo real, mostrando información clasificada.

²⁴ Peirano, M. 2019. *El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención*. Editorial Debate.

INFOGRAFÍA 2

Herramienta	Descripción	Enlace
Historial de búsqueda	Muestra las búsquedas que hemos hecho en Google, ya sea desde la computadora, tablet o teléfono.	https://www.google.com/history
Historial de ubicación	Nos muestra los sitios en los que hemos estado desde que asociamos el número de teléfono a una cuenta de correo en Gmail.	https://maps.google.com/location/history
Dispositivos desde los que nos hemos conectado	Nos muestra los distintos dispositivos con los que hemos estado conectados a nuestra cuenta Gmail, teléfono, tabletas o computadores. También nos permite la localización y ubicación de dichos dispositivos. En el caso del teléfono celular, permite, además, bloquearlo o borrar la información en caso de robo.	https://security.google.com/settings/security/activity
Historial de publicidad	Podemos ver esos datos de perfil que Google va creando sobre nosotros a partir de nuestras preferencias, por edad, género e intereses generales y así determinar qué anuncios pueden interesarnos.	https://www.google.com/settings/ads/
Permisos otorgados	Aquí podremos ver a qué programas (Facebook, LinkedIn, etc.), de internet hemos dado permisos y accesos a nuestra cuenta Gmail.	https://security.google.com/settings/security/permissions
Datos	Este nos permite descargar los datos obtenidos sobre nosotros a partir de todo lo anterior.	https://www.google.com/takeout

NOTA: El acceso a estos servicios se hacen desde la cuenta Gmail.

Elaboración propia con información de Google.

**INTELIGENCIA COLOMBIANA CONTRA LA DEMOCRACIA**

En Colombia, el ataque a la información y la vigilancia de la ciudadanía en general tiene una larga historia, ha sido un proceso que ha comportado ilegalidad y abuso del poder, a la vez que ha cumplido un papel central en la restricción de la democracia, falazmente considerada la más antigua de América Latina.



Abordar los problemas de seguridad y privacidad nos obliga a remitirnos a la historia reciente para comprender la situación de riesgo y vulnerabilidad de personas defensoras de los derechos humanos en este país.

Revisaremos a continuación algunos momentos de ese desarrollo histórico en el que la interceptación de las comunicaciones y la vigilancia excesiva han sido sucedidos sistemáticamente por la persecución, el hostigamiento y el asesinato de miles de personas, siendo la institucionalidad estatal creada y puesta en ejercicio para esas prácticas que nos alejan de ser un verdadero Estado Social de derecho.



ESBOZO HISTÓRICO

Ante la persistente agresión y asesinato de liderazgos sociales, personas defensoras de derechos humanos y de excombatientes de las FARC-EP (ahora Partido Comunes), Alfredo Molano (2019), señaló que la élite colombiana es heredera de una larga tradición de eliminación física de la oposición política.

Dicha tradición se consolidó en un ejercicio arbitrario de poder, tutelado desde Estados Unidos bajo la Doctrina de la Seguridad Nacional, una visión de las relaciones internacionales que orientó un compendio de directrices para enfrentar el peligro comunista. Dicha doctrina y sus gestores tienen una notable responsabilidad en el desarrollo del conflicto armado en Colombia, sustentando ideológicamente y teóricamente la adecuación de la institucionalidad para el combate del “enemigo interno.”

Esa institucionalidad se puede desglosar así: “las formas institucionales: en primer lugar, las fuerzas armadas, las demás entidades del Estado, las organizaciones de la sociedad (gremios, medios de comunicación, iglesias) y “no institucionales”, representadas en particular por los grupos paramilitares.”²⁵

²⁵ Fajardo, D. 2015. *Estudio sobre los orígenes del conflicto social armado, razones de su persistencia y sus efectos más profundos en la sociedad colombiana*. En: Contribución al entendimiento del conflicto Armado en Colombia. Comisión Histórica del Conflicto y sus Víctimas. Pág. 30.

El “enemigo interno” no se refiere únicamente a los grupos armados subversivos sino a todas aquellas personas que, como enfatizó Giraldo, amenazan el ‘statu quo’; este enemigo interno parece encontrarse en las mayorías nacionales, a juzgar por el número reconocido de víctimas arrojadas por el conflicto (más de ocho millones y medio) y por las masivas protestas que se han tomado las calles de las principales ciudades del país, en contra del régimen político y económico, la represión estatal y la continuación de la guerra después de firmado el Acuerdo de Paz.

Renán Vega Cantor relata parte de la génesis de este proceso en 1959, cuando un equipo especial de la CIA (Central Intelligence Agency) es enviado durante el gobierno de Lleras Camargo para evaluar la seguridad interna en Colombia.

Bajo la supervisión directa del embajador en Colombia, luego de ocho semanas de análisis y revisión de estructuras físicas, componentes y archivos militares, la misión emite una serie de recomendaciones, entre las que se encuentra:

“(...) proporcionar asistencia militar a Colombia de carácter encubierto, de acuerdo a los modelos de Vietnam del Sur y Filipinas, y reforzar la actividad de las agencias de Estados Unidos en el país. Dicha asistencia pretende «establecer una influencia sobre los oficiales» del ejército colombiano y se aconseja convertir al Servicio de Inteligencia Colombiano (SIC) «en una fuente virtualmente dirigida por los Estados Unidos para operaciones de guerra psicológica abierta y encubierta». Lo que Lleras Camargo cumple de manera inmediata, puesto que desarticula al SIC y funda el Departamento Administrativo de Seguridad (DAS), según el modelo de la Oficina Federal de Investigaciones (FBI) de los Estados Unidos.”²⁶

²⁶ Vega, R. 2015. *La dimensión internacional del conflicto social y armado en Colombia. Injerencia de los Estados Unidos, contrainsurgencia y terrorismo de Estado*. En: Contribución al entendimiento del conflicto Armado en Colombia. Comisión Histórica del Conflicto y sus Víctimas. Pág. 23.



Desde entonces, el DAS estuvo legalmente bajo la dirección del poder ejecutivo, que nombraba su mando y orientaba cualquier reestructuración que encontrara necesaria, hasta su cierre en el año 2011. Es así como, década tras década, el DAS cumplió sus tareas de vigilancia, recopilación y sistematización de información, más las que le correspondieron como policía política, antisubversiva y contrainsurgente.

En la década de los sesenta, el DAS tendrá un papel preminente en la vigilancia, recopilación y sistematización de la información requerida para neutralizar la subversión; mediante un decreto será facultado para elaborar listas de sospechosos de actividades subversivas, someterlos a estricta observación y prohibirles ausentarse del lugar sin previo aviso.

A comienzos de los setenta, el DAS y organismos de inteligencia del Ejército comenzarán un proceso histórico de interceptación sistemática de las comunicaciones, antes exclusivamente telefónicas. A finales de esta década, el Departamento fue el brazo ejecutor del Estatuto de Seguridad de Turbay Ayala, junto a la Fuerza Pública. Se enfocó en la persecución a todo lo que se identificara como izquierda, aplicando la tortura como técnica de interrogatorio.

En las dos décadas siguientes, el DAS se vinculó con el narcotráfico y el paramilitarismo. Yair Klein, el mercenario israelí que entrenó paramilitares en Colombia, entre ellos a Carlos Castaño, relata en un largo testimonio que fue recibido en Colombia, la primera vez, por agentes del Departamento y un oficial retirado del Ejército, entre otros.²⁷

El DAS participó en los asesinatos de Gabriel Santamaría, integrante de la Unión Patriótica, en 1989, así como de los candidatos presidenciales Luis Carlos Galán, Bernardo Jaramillo Ossa y Carlos Pizarro, en 1990.²⁸

La cooperación con narcoparamilitares era estrecha: sobre el crimen de Santamaría, ante la Unidad de Justicia y Paz, Don Berna declara que buena parte de los funcionarios de la institución en Antioquia colaboraban

²⁷ Behar, O. 2012. *El Caso Klein: El origen del paramilitarismo en Colombia*. Icono Editorial.

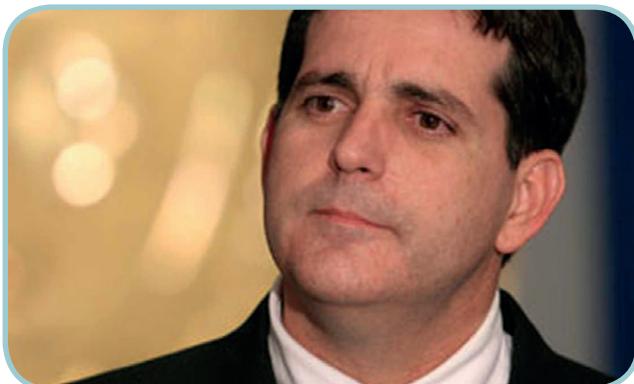
²⁸ Semana. 8 de enero de 2010. *Los magnicidios y el DAS*. <https://www.semana.com/nacion/articulo/los-magnicidios-das/111760-3/>

con los paramilitares y que Carlos Castaño “mantenía una nómina de funcionarios del DAS.”²⁹

En 2005, el director de este organismo, Jorge Enrique Noguera Cotes, fue denunciado por Rafael García, jefe de informática del DAS, de participar en fraude electoral para las elecciones parlamentarias y presidenciales de 2002, de poner la institución al servicio del Bloque Norte de las AUC, proporcionando información e infraestructura para la interceptación, persecución y asesinato de dirigentes estudiantes y líderes sindicales, de organizar un complot para asesinar al presidente Hugo Chávez, infiltrando paramilitares en territorio venezolano y de estar implicado en el asesinato de Danilo Anderson, un fiscal del vecino país.

Desaparecer y manipular información que incriminara a reconocidos paramilitares colombianos también fue una actividad mencionada en la denuncia.

Imagen 11.



Jorge Enrique Noguera

Noguera se encuentra hoy en prisión³⁰, acusado del asesinato del profesor Alfredo Correa de Andreis y de orientar el llamado G3, un organismo clandestino especializado en realizar, incluso fuera de Colombia, espio-

²⁹ El Espectador. 13 de febrero de 2012. *Agentes del DAS habrían participado en asesinato de diputado de la UP.* <https://www.elespectador.com/judicial/agentes-del-das-habrian-participado-en-asesinato-de-diputado-de-la-up-article-326405/>

³⁰ <http://www.cortesuprema.gov.co/corte/wp-content/uploads/2017/09/Sentencia-Jorge-Noguera-6-sep-2017.pdf>



naje y presión a los opositores del gobierno de Álvaro Uribe Vélez. Según él, este organismo fue creado por el subdirector de la entidad, José Miguel Narváez, nombrado directamente por el presidente y hoy condenado por “determinador responsable” del asesinato de Jaime Garzón.³¹

En febrero de 2009, Revista Semana reveló que esta entidad continuaba interceptando ilegalmente comunicaciones, esta vez de 600 figuras públicas entre los que se encontraban defensores de derechos humanos, magistrados, periodistas, congresistas, jueces, generales de la República, entre muchos otros.³²

Representantes de la Corte Suprema calificaron la situación como una empresa criminal dirigida desde la Casa de Nariño. La exdirectora de la institución, María del Pilar Hurtado, fue condenada a prisión en 2014 por abuso de autoridad y violación ilícita de comunicaciones, entre otros. También fue detenido el exsecretario de presidencia, Bernardo Moreno.

Sobre el papel del DAS en el horror padecido por el país, el historiador Renán Vega anota:

No es que el DAS en el camino se tuerce e involucra en actividades dudosas e ilegales, sino que nace como un instrumento diseñado para la «guerra psicológica abierta y disfrazada», según se desprende del documento de la misión militar de 1959. Esta «guerra psicológica» contra la población se traduce directamente en prácticas terroristas por parte del Estado hasta el día de hoy, que han dejado miles de víctimas.³³

³¹ El Espectador. 23 de septiembre de 2018. *Las tareas del G3*. <https://www.elespectador.com/opinion/columnistas/yohir-akerman/las-tareas-del-g3-column-813727/>

³² Semana. 20 de febrero de 2009. *El DAS sigue grabando*. <https://www.semana.com/nacion/articulo/el-das-sigue-grabando/100370-3/>

³³ Vega, R. 2015. *La dimensión internacional del conflicto social y armado en Colombia. Injerencia de los Estados Unidos, contrainsurgencia y terrorismo de Estado*. En: Contribución al entendimiento del conflicto Armado en Colombia. Comisión Histórica del Conflicto y sus Víctimas. Pág. 57.

Con el argumento de que el DAS estaba relacionado con múltiples violaciones de derechos humanos, en el año 2010 el presidente Juan Manuel Santos decide liquidar la entidad. Se abren entonces tres nuevas instituciones que realizarían las labores del departamento: Migración Colombia, la Agencia Nacional de Inteligencia y la Unidad Nacional de Protección (UNP).

El cierre de la institución constituyó, más que un acto de justicia, una acción a favor de la impunidad, una afrenta al derecho de las víctimas y de todo el país a la verdad. En el año 2008, la Corte Constitucional ordenó al DAS, entregar toda la información recopilada de la periodista Claudia Julieta Duque que investigaba el asesinato de Jaime Garzón. Sobre la liquidación del organismo, afirma la periodista:

Nosotros, las víctimas y los defensores de derechos humanos, dijimos desde el comienzo que el cierre de la entidad implicaba el ocultamiento de la verdad sobre lo sucedido, la negación de la verdad y la sistemática estrategia de impunidad. A las víctimas se nos pidió que confiáramos y los archivos fueron entregados en custodia al Archivo General de la Nación, bajo la observación y vigilancia de la Procuraduría General de la Nación.

Además, se creó una junta asesora del director del DAS en supresión, integrada por los ministros de Defensa, del Interior, el Alto Consejero Presidencial para los Derechos Humanos y otros funcionarios. Se nos dijo que con este anclaje la verdad estaba garantizada. Pero esos tres años pasaron en total secretismo, la sociedad civil desconoce lo que sucedió en los últimos tres años del DAS, que finalmente fue desaparecido jurídicamente en julio de 2014. (...) se perdió información desde 1960, cuando se creó el DAS, hasta el 2010 que fue liquidado. Hablamos de información que solo los funcionarios del DAS saben cuánto hubiera podido contribuir a esclarecer múltiples violaciones a los derechos humanos en las que esa entidad estuvo involucrada y que hace parte de la historia reciente del país.³⁴

³⁴ Duque, C. *La desaparición de archivos del DAS o de cómo encubrir violaciones a los derechos humanos en Colombia*. Diálogos de la Memoria. Centro Nacional de Memoria Histórica. <http://www.centrodememoriahistorica.gov.co/descargas/dialogos-memoria/ponencias/021-ClaudiaJulietaDuque.pdf>



Pero los escándalos sobre interceptaciones ilegales no se detuvieron con la liquidación del DAS, ni con el establecimiento de la Mesa de Diálogos en La Habana con las FARC-EP. Le siguieron otros a cargo de distintas agencias de inteligencia del Estado. De hecho, en 2014 la Revista Semana reveló que desde un restaurante en el barrio Galerías de Bogotá, la Central de Inteligencia Técnica del Ejército desarrollaba la Operación Andrómeda, que consistía en el espionaje a los negociadores gubernamentales en La Habana y al presidente de la República, entre otros. Si bien destituyeron al jefe de inteligencia y al director de la Central, el entonces presidente Santos nunca aclaró si la operación fue legal o ilegal y la investigación no prosperó. Por su parte, Univisión también denunció que periodistas que cubrían los sucesos en La Habana también fueron interceptados.³⁵

En ese contexto se conoce que en la Central de Inteligencia y Contrainteligencia Militar (CIME) funciona una ‘sala gris’, “desde la cual se realizan interceptaciones ilegales, cuya información puede ser utilizada para intimidar o hasta asesinar personas. Según un militar de esta unidad, la CIA «suministraba apoyo económico y técnico para que la sala pudiera funcionar. Todo, absolutamente todo lo que aquí ocurre es de conocimiento de ellos. Ellos saben qué, a quién y por qué se intercepta en la sala. En términos prácticos, ellos eran los verdaderos jefes de esta sala».”³⁶



³⁵ Americas Quarterly. 10 de febrero de 2014. *Colombia: Las ‘Chuzadas’ de la era Santos.* <https://www.americasquarterly.org/blog/colombia-las-chuzadas-de-la-era-santos/>

³⁶ Vega, R. 2015. *La dimensión internacional del conflicto social y armado en Colombia. Injerencia de los Estados Unidos, contrainsurgencia y terrorismo de Estado.* En: Contribución al entendimiento del conflicto Armado en Colombia. Comisión Histórica del Conflicto y sus Víctimas. Págs. 56, 57.

Imagen 12.



Nicacio Martínez

El nombre del comandante del Ejército, Nicacio Martínez, salió a relucir en agosto de 2019 por una investigación de la Procuraduría sobre un proceso de cacería al interior de la institución militar, para identificar informantes que revelaban acontecimientos a medios como The New York Times y Semana. Entre los sucesos que buscaban evitar que salieran a la luz, se encuentra una reunión (el 26 de enero de 2019) en Cúcuta, de altos mandos militares (15), para “proteger la zona del Catatumbo”. Finalmente, la información se filtra y la Revista Semana transcribe textualmente una frase del general Diego Villegas, de la Fuerza de Tarea Vulcano, que preside esa reunión:

“El Ejército de hablar inglés, de los protocolos, de los derechos humanos se acabó. Acá lo que toca es dar bajas. Y si nos toca aliarnos con los Pelusos nos vamos a liar, ya hablamos con ellos, para darle al ELN, si toca sicariar, sicariamos y si el problema es de plata, pues plata hay para eso.”³⁷

³⁷ Semana. 25 de agosto de 2019. *El general en su laberinto: los secretos de la cacería que involucra al comandante del Ejército*. <https://www.semana.com/nacion/articulo/investigacion-sobre-la-caceria-en-el-ejercito-involucra-al-general-nicacio-martinez/629193/>



En noviembre de 2019, el periodista varias veces ‘chuzado’, Daniel Coronell, denunció que el exfiscal Néstor Humberto Martínez ordenó la interceptación de personas relacionadas con los diálogos de paz con las FARC-EP. Iván Cepeda, Álvaro Leyva, Diego Martínez, Enrique Santiago y Piedad Córdoba, fueron algunos de los espiados. La información fue proporcionada por Luis Carlos Góngora, jefe de la sala de interceptaciones del búnker de la Fiscalía General de la Nación, preso por las ‘chuza-das’ a los sindicalistas de Avianca.³⁸

De otro lado, Noticias Uno informó sobre el hallazgo de un micrófono escondido en el escritorio del magistrado César Reyes Medina, de un micrófono escondido, siendo él quien lleva el caso contra Álvaro Uribe Vélez.³⁹

El senador Iván Cepeda habla de tres elementos característicos de este nuevo episodio de espionaje que vincula a las agencias estatales de seguridad: una inteligencia ilegal que se practica contra quienes defienden el proceso de paz; un ataque a la prensa que durante el 2019 denunció escándalos en el Ejército y una actividad ilegal de espionaje contra la Corte Suprema de Justicia que lleva el caso de Uribe.⁴⁰

Sin poder profundizar más en otros hechos similares, queremos cerrar esta parte enfatizando en que los conceptos de ciberdefensa y ciberinteligencia plantean nuevos terrenos de combate para los agentes de seguridad y la élite gobernante que ha erigido su poder sobre la barbarie y el terrorismo de Estado.

La visión del enemigo interno no ha desaparecido totalmente y su consecuencia directa es la amenaza a la información y la vida de personas defensoras de derechos humanos y sus familias, por lo que es imperativo el cuidado de las comunicaciones y el reconocimiento de las instituciones que sabemos nos han espiado, siendo utilizadas en contra de la materialización profundización democracia.

³⁸ Semana. 24 de noviembre de 2019. *¿La paz chuzada?* <https://www.semana.com/opinion/articulo/la-paz-chuzada-por-daniel-coronell/641767/>

³⁹ El Tiempo. 12 de enero de 2020. *Investigan micrófono escondido en despacho de magistrado de la Corte*. <https://www.eltiempo.com/justicia/investigacion/investigan-micronfo-escondido-en-despacho-de-magistrado-de-corte-que-investiga-a-uribe-451098>

⁴⁰ El País. 15 de enero de 2020. *Las escuchas ilegales afloran el pasado más oscuro del uribismo*. https://elpais.com/internacional/2020/01/15/actualidad/1579104554_921897.html



ORGANISMOS DE INTELIGENCIA EN COLOMBIA

A continuación, un listado de los organismos que en Colombia deberían realizar actividades de vigilancia e inteligencia en el marco de la Constitución y las leyes, para la protección y promoción de los derechos de la ciudadanía en su conjunto:

Ejército Nacional

En la estructura de esta institución se encuentran: el Departamento de Inteligencia y Contrainteligencia (CEDE2) y el Comando de Apoyo de Combate de Inteligencia Militar (CAIMI), que contiene 2 brigadas de inteligencia militar: (Brimi1) y (Brimi2). En Brimi1 se encuentran 5 batallones de inteligencia especializada, entre ellos el Batallón de Ciberinteligencia (Bacib). También tiene el Comando de Apoyo de Combate de Contrainteligencia Militar (CACIM), que comprende dos brigadas de contrainteligencia (BRCIM) y (BRCIM2) y se compone de varios batallones, entre ellos, el Batallón de Apoyo de Servicios para la Contrainteligencia (BASCI).

Dirección de Inteligencia Policial (DIPOL)

Es la dirección de policía encargada de producir inteligencia estratégica y operativa relacionada con alteraciones del orden público, la seguridad y la defensa. Fue creada en 1995 en reemplazo del llamado F2, vinculado con innumerables violaciones a los derechos humanos. Debe realizar actividades nacionales de contrainteligencia. Es una de las ocho direcciones policiales responsables ante la Dirección General del Ministerio de Defensa. Tiene las Regionales de Inteligencia Policial (RIPOL) y Seccionales de Inteligencia Policial (SIPOL).

Fue la responsable de los operativos contra Raúl Reyes, el ‘Mono Jojoy’ y Alfonso Cano; en el año 2013, con una inversión de 15 millones de dólares, inauguró la Central de Información más moderna de América Latina, por orden de Juan Manuel Santos. Allí operarían, según Revista Semana, más de 400 analistas.⁴¹

⁴¹ Semana. 31 de mayo de 2013. *El corazón de la inteligencia policial.* <https://www.semana.com/nacion/articulo/el-corazon-inteligencia-policial/345084-3/>



Dirección de Investigación Criminal e Interpol (DIJIN)

Es la dirección policial a cargo de la investigación judicial. Cumple el papel de policía judicial.

Desde la disolución del DAS, asume funciones conforme a convenios del Estado colombiano con la policía internacional (Interpol), por lo que tiene funciones de intercambio de información, cooperación y asistencia recíproca con dicha organización internacional.

Es una de las ocho direcciones de policía responsables ante la Dirección General del Ministerio de Defensa. Su función es apoyar la investigación criminal en áreas técnicas, científicas y operativas, por iniciativa propia o por orden de la Fiscalía. Cuenta con un laboratorio de informática forense que realiza, según la página web de la Policía Nacional, las siguientes actividades:

- Descubrimiento, recolección, procesamiento análisis y preservación de la evidencia física.
- Aplicación de principios y estándares universales.
- Valoración y aprobación probatoria en juicios.
- Reconocimiento y aceptación de la evidencia digital.
- Análisis forenses a computadores, discos duros, memorias USB, equipos terminales móviles, entre otros.
- Extracción y recuperación de archivos borrados, fragmentos de archivos.
- Desciframiento de contraseñas de archivos.
- Reconstrucción de archivos web, historial de archivos ocultos, uso de códigos maliciosos.



Dirección Nacional de Inteligencia (DNI)

Surge en 2011 como reemplazo del DAS, para dirigir el sector de inteligencia y constrainteligen-
cia, dentro de la estructura general del Estado. Responde directamente a los requerimientos de la Presidencia de la
República y las altas instancias de gobierno. Según el Decreto 4179 de
2011, esta agencia está a cargo de:

- i) Desarrollar actividades de inteligencia estratégica y constrainteligen-
cia bajo los principios de necesidad, idoneidad y proporcionalidad,
de conformidad con el marco legal y el objetivo misionero;
- ii) avanzar en acuerdos de cooperación internacional en temas relacio-
nados con inteligencia y constrainteligen-
cia;
- iii) desarrollar sus actividades de inteligencia y constrainteligen-
cia en cooperación con otras agencias de inteligencia nacionales e interna-
cionales, así como con otras entidades del Estado y
- iv) otras funciones relacionadas con las actividades de inteligencia y
constrainteligen-
cia que el presidente pueda asignar de conformidad
con la Constitución y la ley.

Fiscalía General de la Nación

Es la institución encargada de adelantar la investigación penal y la acu-
sación ante los jueces, como parte del Poder Judicial. Posee autonomía
administrativa y presupuestaria. En el marco de su labor investigativa está
facultada para realizar vigilancia de las comunicaciones, garantizar la pro-
tección de víctimas y testigos, así como para dirigir y coordinar las fun-
ciones de la policía judicial. Se encarga también de revisar y aprobar las
órdenes de interceptación de otras agencias, incluida la DNI y la Policía.

Unidad de Información y Análisis Financiero (UIAF)

La UIAF es una unidad administrativa especial del Estado colombiano,
adscrita al Ministerio de Hacienda y Crédito Público. Es un organismo de
inteligencia económica y financiera, que “centraliza, sistematiza y anali-
za la información recaudada en virtud de las leyes 526 de 1999 y 1621
de 2013 suministrada por las entidades reportantes y fuentes abiertas,
para prevenir y detectar posibles operaciones de lavado de activos, fi-
nanciación del terrorismo y sus delitos.”⁴²

⁴² https://www.uiaf.gov.co/nuestra_entidad/quienes_somos



En su página oficial informa que posee tecnología de última generación para la identificación de redes criminales. A partir de la ley 1621 de 2013, integra la comunidad de inteligencia del país.



SISTEMAS DE INTERCEPTACIÓN DE LA INTELIGENCIA COLOMBIANA

Estos organismos reseñados, que han incurrido en el uso abusivo de sus facultades, realizan sus actividades bajo los nuevos esquemas de ciberdefensa y ciberinteligencia, trasladando la confrontación política y social del espacio físico al de las comunicaciones satelitales y virtuales, en donde se utilizan tecnologías de interceptación y espionaje.

El informe ‘The State of Privacy in Colombia’, que realizan Privacy International, Fundación Karisma y Dejusticia, señala que buena parte del equipo de seguridad encargado de la interceptación de las comunicaciones es proporcionada por compañías internacionales, especialmente estadounidenses.⁴³ Si bien existe una ley de contratación que da prioridad a los productos de seguridad y defensa fabricados firmas locales, el acuerdo comercial bilateral entre Estados Unidos y Colombia permite que las empresas estadounidenses sean tratadas como locales cuando participan en ofertas públicas.

Israel también es un importante proveedor militar en Colombia. La compañía israelí-estadounidense Verint Systems proporcionó la infraestructura de interceptación utilizada por el DAS, la DIPOL y la DIJIN alrededor del año 2005. El informe refiere que, durante más de 10 años, en los períodos de gobierno de Uribe, los fondos y la capacitación estadounidenses se utilizaron para espiar a jueces de la Corte Suprema y a opositores del régimen.

De igual modo, asegura que las comunicaciones interceptadas fueron fundamentales para las operaciones encubiertas de la Agencia Central de Inteligencia (CIA) contra las FARC.

Algunas de las tecnologías de interceptación adquiridas por el Estado colombiano son:

⁴³ Dejusticia, Fundación Karisma y Privacy International. 2019. *The State of Privacy in Colombia*. <https://privacyinternational.org/state-privacy/58/state-privacy-colombia>

Análisis Forense Digital

Es un análisis digital realizado mediante un software especializado, como el que realiza el Laboratorio de Informática Forense de la Policía. Este software permite acceder, analizar y manipular la información de computadores, memorias USB, discos duros y demás dispositivos, sin alterar su estado. Además, permite recuperar información vía remota y analizar los datos en vivo, como la memoria del sistema, los volúmenes lógicos y los dispositivos físicos.

El software también burla discos cifrados con el programa PGP. El DAS había comprado, antes de 2010, el Forensic Toolkit (FTK), un software informático forense creado por AccessData, una empresa con sede en EE. UU. Desde entonces fue utilizado por otras agencias de seguridad colombianas.⁴⁴



Colectores IMSI

Los colectores IMSI (International Mobile Subscriber Identity-Catcher; en español, Receptor de Identidad de Suscriptor Móvil Internacional) son dispositivos de vigilancia móvil para identificar un teléfono, el operador y el usuario al que pertenece, suplantando la antena que provee el servicio de telefonía e interceptando la conexión entre el celular y la verdadera torre.

Permiten el acceso a las comunicaciones, acceden a metadatos y proporcionan la ubicación exacta del usuario. Además, pueden obtener información de los móviles cercanos al vigilado, por lo que les resulta útil para recoger información de los asistentes a protestas y manifestaciones.⁴⁵

El aparato puede ser portátil o ensamblado en lugares fijos. En Colombia, en el año 2005, según la investigación de Privacy International⁴⁶, la compañía Spectra Group, con sede en Nueva Zelanda, proporcionó a la

⁴⁴ Ibídem.

⁴⁵ Red en Defensa de los Derechos Digitales. 20 de junio de 2016. *Cinco datos que debes saber sobre los IMSI Catchers*. <https://r3d.mx/2016/06/20/5-datos-que-debes-saber-sobre-los-imsi-catchers-o-stingrays/>

⁴⁶ Privacy International. 2015. *Un estado en la sombra: vigilancia y orden público en Colombia*. https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf. Pág. 42.



DIPOL, a través de la empresa colombiana Maicrotel Ltda., su receptor IMSI. Este sistema monitorea y graba conversaciones telefónicas, también rastrea datos en sistemas de comunicación móvil.

Privacy International documenta que el extinto DAS los usaba y actualmente también la DIJIN. Dada su forma de funcionamiento, es muy difícil reglamentar su uso, pues una vez se activa la falsa antena todos los celulares cercanos se conectan a ella y empiezan a proporcionar información. No está clara su autorización legal.

Intrusión de Malware y Piratería

Hombre Invisible: El escándalo con que inició el año 2020, que le valdría el allanamiento a uno de los batallones de ciberinteligencia del Ejército Nacional, ha develado el uso del software llamado Hombre Invisible. Un software comprado por tres mil millones de pesos a la Mollitian, una empresa española con un contrato que está bajo reserva durante 30 años, de calificación ultrasecreta, dado que podría afectar relaciones diplomáticas con otros países.⁴⁷

Los requerimientos que exigen los compradores en el contrato refieren a malware espía y son:

- Que afecte a sistemas Windows y Apple.
- Proveer persistencia y camuflaje para el malware instalado en el objetivo infectado.
- Ejecutar diferentes tipos de malware sin que el antivirus tenga una reacción hostil.
- Invisible para el 90% de los sistemas de seguridad antimalware y perimetral.
- Acceder o descubrir información borrada u oculta.
- La infraestructura debe estar diseñada para operar con un número infinito de agentes activos (Así funciona hombre invisible, el

⁴⁷ El Espectador. 15 de enero de 2020. *Chuzadas: las exigencias del Ejército en contrato de software de inteligencia.* <https://www.elespectador.com/judicial/chuzadas-las-exigencias-del-ejercito-en-contrato-de-software-de-inteligencia-article-899922/>

software de espionaje con el que habrían realizado nuevas chuzadas).⁴⁸

Un oficial le dijo a la Revista Semana que ‘Hombre Invisible’ le permitía ingresar “a cualquier computador, acceder a llamadas y conversaciones de WhatsApp y Telegram, descargar conversaciones de chat archivadas o borradas, fotos y, en general, lo que tenga almacenado en la memoria de la máquina infectada.”⁴⁹

Galileo: La Policía Nacional adquirió en 2014 a Galileo, un sistema de intrusión producido por Hacking Team. Es un software malicioso o malware espía, con el que se infecta el dispositivo de la persona atacada para manipularlo remotamente. El Sistema de Control Remoto (en inglés, RCS) se puede usar en computadores y dispositivos móviles sin que los usuarios lo detecten, ya que está diseñado para evitar los programas antivirus comunes y el cifrado. Al infectar el dispositivo, la suite RCS puede capturar datos, encender y apagar de forma remota cámaras web y micrófonos, copiar archivos y contraseñas escritas, entre muchas otras posibilidades.

Hacking Team es una empresa italiana ampliamente cuestionada porque su software es contrario a los estándares legales de varios países. En 2013, fueron declarados “enemigos del internet” por vender software a países con gobiernos que violan los derechos humanos, como el colombiano. En 2015, la empresa fue hackeada y fueron puestas a la luz 400 GB de información de la empresa.

La filtración permitió saber que el equipo de esta compañía suministró la tecnología a la DEA, utilizó el software espía para realizar vigilancia desde la Embajada de Estados Unidos en Bogotá. También se supo que, la Dirección de Inteligencia de la Policía (DIPOL) adquirió el software de Hacking Team por 335 mil euros, sirviendo la empresa Robotec como intermediaria. Posteriormente, la DIPOL compró otra li-

⁴⁸ Noticias Caracol. 13 de enero de 2020. *Así funciona hombre invisible, el software de espionaje con el que habrían realizado nuevas chuzadas.* <https://noticias.caracoltv.com/colombia/asi-funciona-hombre-invisible-el-software-de-espionaje-con-el-que-habrian-realizado-nuevas-chuzadas>

⁴⁹ Semana. 13 de enero de 2020. *Chuzadas sin cuartel.* <https://www.semana.com/nacion/articulo/chuzadas-por-que-se-retiro-el-general-nicacio-martinez-del-ejercito/647810/>



cencia de 850 mil euros a la empresa Nice System, una empresa israelí y pagarían además 35 mil euros adicionales por concepto de mantenimiento anual.⁵⁰

Dado el escándalo, la Policía declaró en un comunicado que Galileo fue adquirido por medios legales y que no comprometía la seguridad ni la privacidad de los colombianos.⁵¹

El informe de PI, Karisma y Dejusticia⁵² reseña que una investigación de 2014 realizada por el Citizen Lab de la Universidad de Toronto, concluyó que a partir del año 2012 ese tipo de malware se ha asociado con ataques contra periodistas, activistas y defensores de los derechos humanos.

Interceptación de Red

Sistema Esperanza: Es un sistema de interceptación selectiva de comunicaciones. Es respaldado por la Administración de Control de Drogas de Estados Unidos (DEA). Desde finales de 1990, es la plataforma a través de la cual se efectúan las interceptaciones legales en el país. La Fiscalía General de la Nación lo gestiona y administra; también tienen acceso la Policía y el Ejército.

Requiere que un funcionario de la Fiscalía realice una solicitud formal para la interceptación de una línea telefónica en particular, igualmente requiere presentación electrónica de orden judicial y especificar los jueces de control y garantías. Se encuentra conectada con los operadores de telecomunicaciones del país.

Privacy International explica que la interceptación a través de Esperanza se realiza selectivamente en particulares con el conocimiento y la cooperación del proveedor de servicios de telecomunicaciones, cuyos servidores envían la señal a la plataforma que la reenvía al centro principal

⁵⁰ Derechos Digitales. 20 de abril de 2016. *El auge del software de vigilancia en América Latina*. <https://www.derechosdigitales.org/9880/el-auge-del-software-de-vigilancia-en-america-latina/>

⁵¹ El Tiempo. 8 de julio de 2015. *Policía indicó no tener vínculos comerciales con firma Hacking Team*. <https://www.eltiempo.com/archivo/documento/CMS-16063640>

⁵² Dejusticia, Fundación Karisma y Privacy International. 2019. *The State of Privacy in Colombia*. <https://privacyinternational.org/state-privacy/58/state-privacy-colombia>

de monitoreo, ubicado en el búnker de la Fiscalía. Allí se descompone en paquetes de información en tiempo real para luego transmitirla a una sala central de monitoreo.

En la Fiscalía funcionaban 20 salas en 2012, que recibían la señal para ser procesada por el Cuerpo Técnico de Investigación (CTI) y la Policía (el DAS también cuando existía). PI afirma que seis salas fueron financiadas y asesoradas por la DEA, que tenía allí algunos analistas. Cada sala tiene un coordinador, unas misiones concretas y determinados funcionarios para operar.

El informe revela varios fallos técnicos y recuerda el escándalo de las ‘chuzadas’ del DAS, que se realizaron desde varias salas del sistema. En 2014, la sala gris fue cerrada por 100 escuchas que realizaron los militares y no el CTI, como indica la normatividad. Las víctimas serían nuevamente figuras políticas y altos funcionarios de la Fuerza Pública. La anomalía fue revelada por Semana.

En 2018, Esperanza llama de nuevo la atención porque filtró información a Uribe Vélez en un proceso de interceptación por el caso de los falsos testigos, que lo involucra a él y al senador Iván Cepeda.⁵³



⁵³ Semana. 20 de febrero de 2018. *Esperanza: el misterioso sistema de interceptaciones del caso Uribe- Cepeda*. <https://www.semana.com/nacion/articulo/esperanza-sistema-de-inteligencia-e-interceptaciones-de-la-fiscalia/557768/>



Imagen 13.



Un arcoíris de salas. Las salas conocidas de interceptación del Sistema Esperanza tienen asignados colores; hay 4 principales en la sede central, 15 en las direcciones seccionales de la Fiscalía y 8 salas más de análisis especializado.

Fuente: Privacy International.

Plataforma Única de Monitoreo y Análisis (PUMA): Es un sistema de monitoreo telefónico y de internet, vinculado directamente a la infraestructura de red de los proveedores móviles, a través de una sonda que copia grandes cantidades de datos y los envía directamente a las instalaciones de monitoreo de la Dirección de Investigación Criminal e Interpol de la Policía (Dijin). PUMA puede interceptar y almacenar todas las comunicaciones que pasan por sus sondas. Se concibió como la versión colombiana de PRISMA y una evolución del Sistema Esperanza, dados los fallos de esa plataforma. En el año 2013, la Policía presentó propuestas para extender el sistema, alegando que un PUMA ampliado sería capaz de capturar tres veces más llamadas telefónicas y datos que Esperanza. La Fiscalía, en cabeza de Eduardo Montealegre, aseguró que PUMA “puede conllevar al uso indiscriminado de la interceptación como herramienta de investigación, en casos en los que esa invasión de derechos fundamentales ni siquiera es necesaria en la lucha contra la criminalidad”.⁵⁴ Por ello no fue implementada su expansión, hasta donde se sabe.

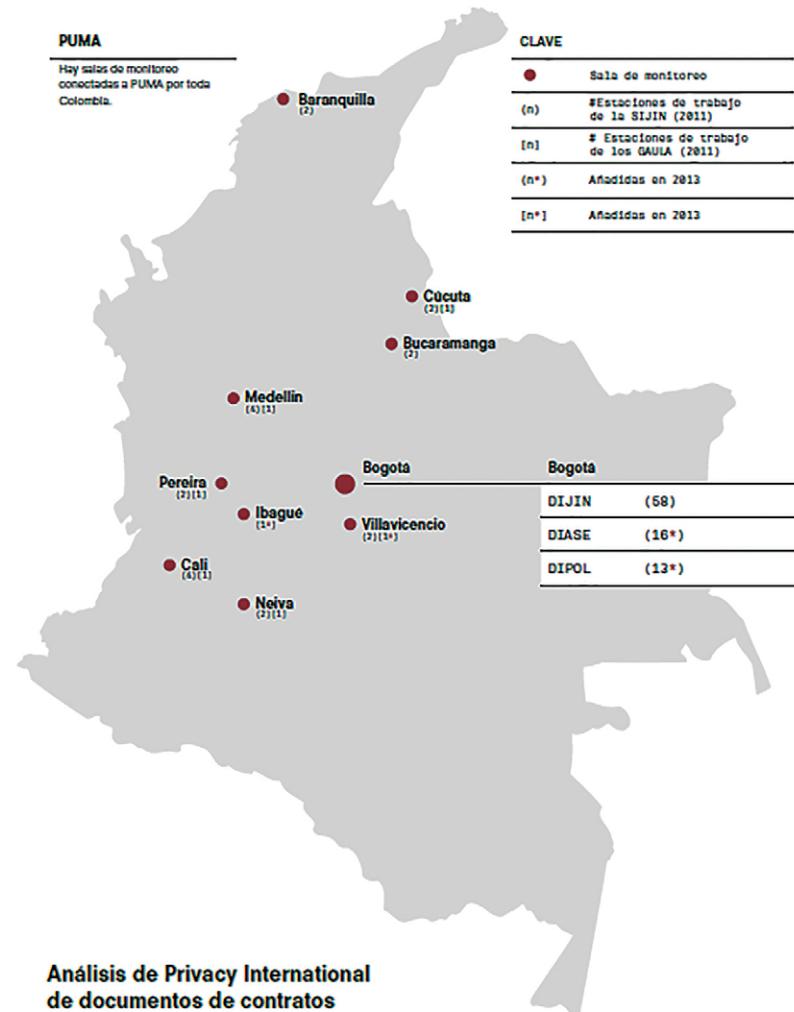


⁵⁴ El Tiempo. 30 de agosto de 2014. *Fiscalía le dice ‘no’ a sistema de interceptación ‘Puma’ de la Policía.* <https://www.eltiempo.com/archivo/documento/CMS-14462092>



Imagen 14.

Plataforma Única de Monitoreo y Análisis (PUMA)



Salas de monitoreo de la Plataforma Única de Monitoreo y Análisis, PUMA.
Fuente: Privacy International

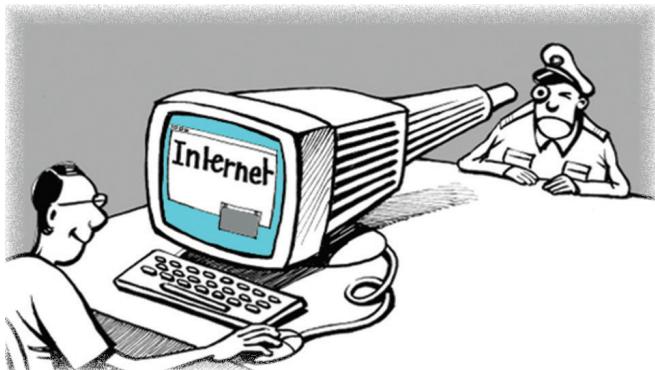


SISTEMA INTEGRADO DE GRABACIÓN DIGITAL (SIGD)

Sobre este sistema, la organización británica reseña que la DIPOL estableció antes que cualquiera un instrumento de vigilancia masiva y automatizada:

"Este centro de monitoreo recibe, procesa y retiene datos recopilados por diversos sistemas de vigilancia, como monitoreo de internet, monitoreo de ubicación, monitoreo de teléfonos y audiovigilancia. Una vez recopilados, estos datos son analizados por potentes ordenadores que muestran conexiones entre personas, sus conversaciones y eventos, y elaboran perfiles de las personas y sus contactos."⁵⁵

Este sistema monitorea el tráfico masivo de comunicaciones a través de líneas E1 y el tráfico de teléfonos móviles 3G y 4G. Puede recopilar 100 millones de registros de datos de llamadas al día e interceptar 20 millones de mensajes de texto diarios. Como PUMA, se configura con el conocimiento de las empresas que proveen el servicio de comunicación.

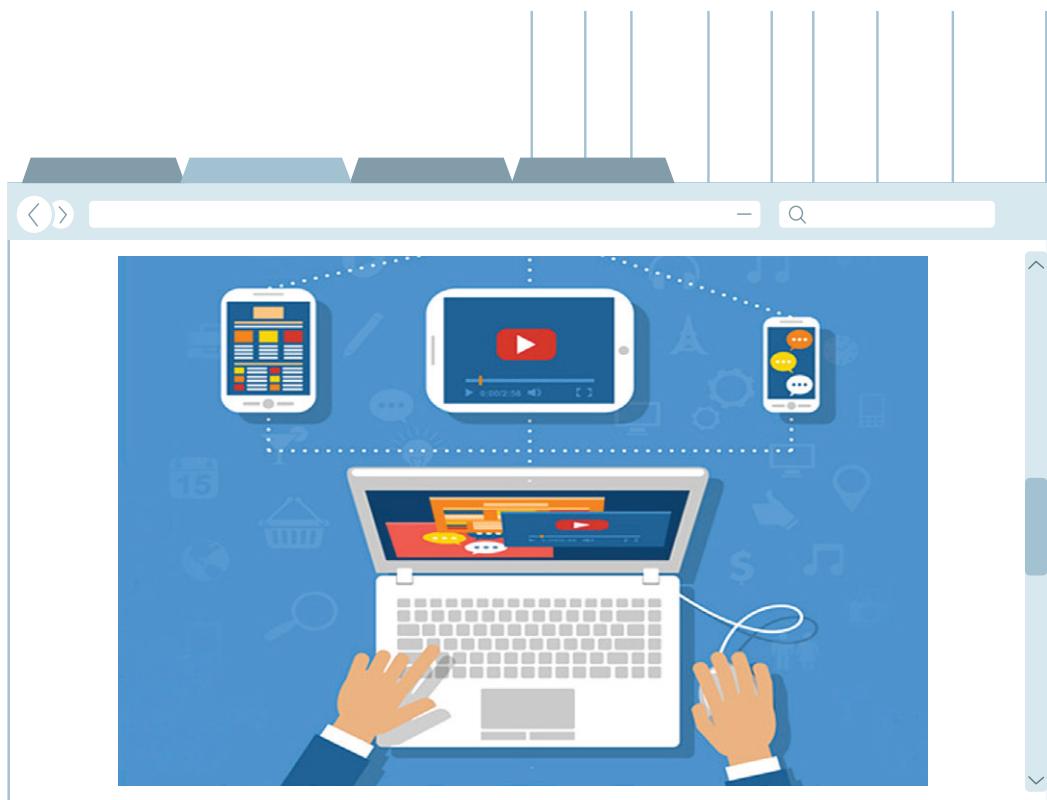


⁵⁵ Privacy International. 2015. *Un estado en la sombra: vigilancia y orden público en Colombia*. https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf. Pág.

CAPÍTULO 2



¿DÓNDE NOS VIGILAN?





*“Me gusta volver al sueño primigenio de internet:
un lugar abierto para un debate abierto, democrático y profundo.”*

JIMMY WALES, fundador de Wikipedia

REDES COMPUTACIONALES

La idea de poder conectar varios equipos entre sí para transmitir y recibir información rápida y precisa fue resultado de una necesidad concreta que, como veremos aquí, no es solamente de origen militar. Atraviesa la esencia relacional del ser humano.

A finales de los años cincuenta del siglo XX, se fueron diseñando algunos bosquejos sobre redes de computadoras pero la consolidación de estas ideas fue materializándose hasta la década siguiente. Las primeras ideas en este sentido consistían en una computadora central, llamada servidor (host), que permitía a otras (terminales) conectarse entre sí.

Las terminales, no eran computadoras como las conocemos hoy: eran enormes máquinas de capacidades muy inferiores a las actuales. La pantalla y el teclado permitían acceder remotamente a la información almacenada en un servidor, que también era una máquina colosal.





Imagen 14.



Primeras terminales.

Hoy en día, cada terminal es una computadora en sí misma, lo que ha permitido el almacenamiento de información de manera descentralizada.

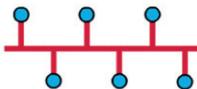
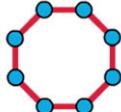
Sin embargo, las formas de conexión de la red no han variado y establecen lo que se llama topología de redes: una arquitectura que ofrece una variedad finita de formas para enlazar los componentes que conforman una red. Dichos componentes son el servidor o nodo central (punto de partida de la conexión), los nodos propiamente hablando (los equipos conectados al servidor), que intercambian información entre sí y el medio de transmisión (tipo de conexión) entre dichos equipos.

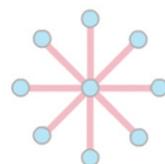
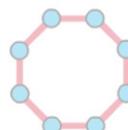
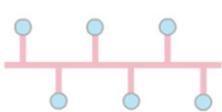
Comprender la configuración de dichas formas nos da una idea general del funcionamiento de internet, entendiendo que es una red de redes.



TOPOLOGÍA DE REDES

INFOGRAFÍA 3

DESCRIPCIÓN	FIGURA
<p>Bus: Se caracteriza por tener un único canal de comunicaciones, denominado bus, troncal o ‘backbone’, el cual es compartido por los diferentes dispositivos que se conectan a él.</p>	 <p>Topología de bus</p>
<p>Estrella: Aquí las estaciones están conectadas a un punto central y todas las comunicaciones se hacen necesariamente pasando por el centro. Los dispositivos no están directamente conectados entre sí.</p>	 <p>Topología en estrella</p>
<p>Malla o punto a punto: Su rasgo característico es que cada nodo está conectado a todos los demás nodos. De esta manera es posible llevar la información por diferentes caminos. Si la red en malla está completamente conectada, no existe ninguna interrupción en la comunicación.</p>	 <p>Topología en malla</p>
<p>Doble anillo y anillo: Son dos anillos concéntricos a los que cada nodo está conectado, aunque los dos anillos no están conectados directamente entre sí. En su variante de un anillo, la diferencia es que hay menos flexibilidad y confiabilidad.</p>	 <p>Topología de anillo</p>





La red de redes

Internet es una red que se desarrolla con el uso y combinación de la topología de redes de manera masiva, permitiendo el almacenamiento no centralizado de la información y con la capacidad de transmitir dicha información de manera cada vez más rápida, de un sitio (servidor) a otro.



Dicha red se relaciona entre sí a través de un lenguaje universal, conformado por los protocolos TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet).

La palabra ‘Internet’ viene del inglés y está compuesta por los vocablos ‘inter’ (entre) y ‘net’ (proveniente de network, que quiere decir ‘red’ en su sentido electrónico).

Existen distintos medios por los cuales se puede obtener conexión a la red de redes. El primero fue la conexión por ‘dial-up’, es decir, tomando la conectividad de una línea telefónica a través de un cable. Los medios evolucionaron y ahora la conexión puede ser por fibra óptica, satélite, redes inalámbricas que sustituyen los cables por señales lumínicas u ondas de radio, líneas eléctricas o telefonía móvil.



CRONOLOGÍA DE INTERNET

Finalizada la Segunda Guerra Mundial, se dio inicio a la llamada Guerra Fría con la Unión de Repúblicas Socialistas Soviéticas (URSS) y Estados Unidos a la cabeza en cada uno de los bloques de poder: una disputa por establecer su hegemonía en todos los niveles territoriales, ideológicos, políticos, militares y tecnológicos.

Para conseguir estos objetivos, ambas potencias protagonizaron una carrera espacial y armamentista que dio inicio también a un complejo proceso de espionaje para obtener información relevante del contendor. Inicialmente, la URSS tomó la ventaja en cuanto a la carrera tecnológica, situando en órbita el primer satélite artificial, en 1957: el **Sputnik**.

Imagen 15



Satélite Sputnik

- **1958:** En Estados Unidos, en respuesta al lanzamiento del Sputnik, se creó la Agencia de Proyectos de Investigación Avanzados (ARPA, por sus siglas en inglés) por orden del presidente Dwight Eisenhower.
- **1959:** En la URSS, Anatoly Kitov, subdirector de un centro de computación del Ministerio de Defensa, propuso la creación de un sistema nacional automatizado de computación y procesamiento de información, con el objetivo de mejorar las comunicaciones de los diferentes ministerios y el desempeño económico de la URSS.

La propuesta no fue desestimada y en el mismo año, el Comité Central del Partido Comunista solicita al gobierno desarrollar la tecnología en computación y la automatización de la producción industrial. Dicha solicitud desemboca en una resolución que orienta la construcción de computadoras para el análisis económico y la planificación (Gerovitch, 2008).

- **1961:** En el XXII Congreso del Partido Comunista de la Unión Soviética (PCUS), el Consejo de Cibernetica de la Academia Soviética de

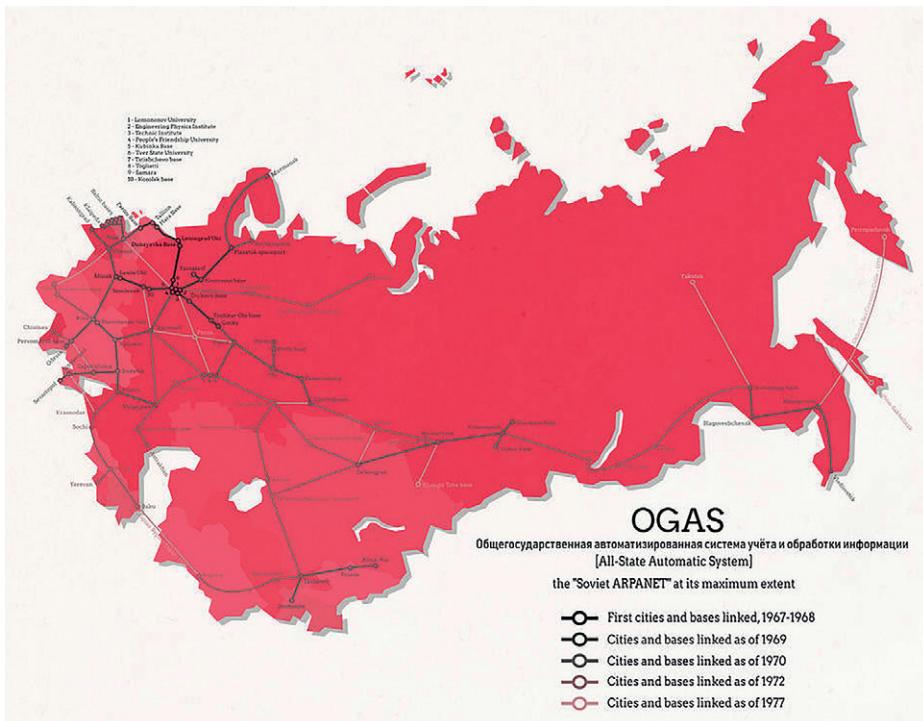


Ciencias publicó un trabajo titulado ‘La cibernetica al servicio del comunismo’, donde se abordan los grandes beneficios de aplicar computadoras y modelos ciberneticos en varias áreas de la vida, desde la biología y la medicina hasta el control de la producción, el transporte y la economía.

- **1962:** Estas noticias soviéticas alarmaron a Estados Unidos y la Agencia Central de Inteligencia (CIA) creó una rama especial para investigar la amenaza de la cibernetica soviética. Arthur Schlesinger Jr., el asesor más cercano del entonces presidente John F. Kennedy, presentó un informe señalando que la Unión Soviética ganaría ventaja si continuaba aquella apuesta tecnológica. El asesor advertía que, si no se decidían a desarrollar seriamente la cibernetica, el país estaría acabado en esta competencia.
- **1962:** Por el lado de la URSS, Víktor Glushkov, uno de los pioneros de la cibernetica y director del Instituto de Cibernetica de Kiev, retomó las investigaciones de Kitov sobre el tema y presenta una nueva propuesta para crear un sistema automatizado de planificación y gestión económica sobre la base de una red informática a escala nacional.
- **1963-1971:** Glushkov le llamaría a esta propuesta Sistema Nacional Automatizado para la Computación y el Procesamiento de Información (OGAS). El proyecto encontró varios opositores dentro del Partido Comunista y las altas instancias del Estado, siendo negado su plan de financiación.

Un proyecto de resolución del XXIV Congreso del Partido, publicado en 1971, autorizó el desarrollo del sistema a gran escala, pero la decisión fue revocada prontamente dentro del Comité Central. La dirigencia soviética vio amenazada su concentración de poder por este proyecto que intentaba conectar toda la extensión territorial de la URSS y además, los economistas liberales que empezaron a tomar protagonismo en la Unión, defendían el mercado como regulador de la producción. El proyecto de OGAS fue finalmente despreciado y archivado.

Imagen 16



Desarrollo territorial del proyecto OGAS entre 1967 hasta 1977.

- **1969:** En Estados Unidos se creó ARPANET, la red de computadoras de ARPA, por pedido del Departamento de Defensa. La red inicialmente conectó a cuatro nodos ubicados en la Universidad de Utah, la Universidad de California (Los Ángeles y Santa Bárbara) y el Instituto de Investigación de Stanford.

ARPANET fue la puesta a prueba de una tecnología para entonces novedosa, llamada ‘comunicación de paquetes’, que divide los datos en pequeños grupos de información para que puedan transmitirse eficientemente a través de la red digital.

- **1971:** En este año ya existían 24 computadoras conectadas a ARPANET, pertenecientes a 15 universidades y centros de educación en distintos estados. Ese mismo año se envió el primer correo electrónico.



nico, creado por Ray Tomlinson, un ingeniero de la empresa Bolt, Beranek y Newman (BBN), encargada de desarrollar la red y su infraestructura.

Este correo usó el símbolo @ que significó ‘en’, de tal manera que la estructura de una dirección electrónica se compuso del nombre de usuario (login) y el servidor en donde se encuentra ubicada (host), quedando así: usuario@servidor.net.

- **1973:** ARPANET se internacionalizó con un enlace satelital que conectaba a Noruega y Reino Unido con los otros nodos en Estados Unidos. Hawái también se unió a la red por satélite. En este punto, la red tenía alrededor de 40 computadoras.
- **1980:** Se inventó Usenet, una red de usuarios que, en un nuevo sistema de presentación de anuncios organizado por temas, permitía el intercambio de consejos de programación, recetas, bromas, opiniones sobre ciencia ficción y mucho más. Dos años más tarde, su popularidad se había extendido rápidamente, llegando a alcanzar las 500 computadoras conectadas.
- **1983:** ARPANET inició su cambio al Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP, por sus siglas en inglés), marcando el nacimiento del internet moderno. Este cambio de protocolo permitía enlazar toda clase de computadoras, aunque tuvieran características diferentes.

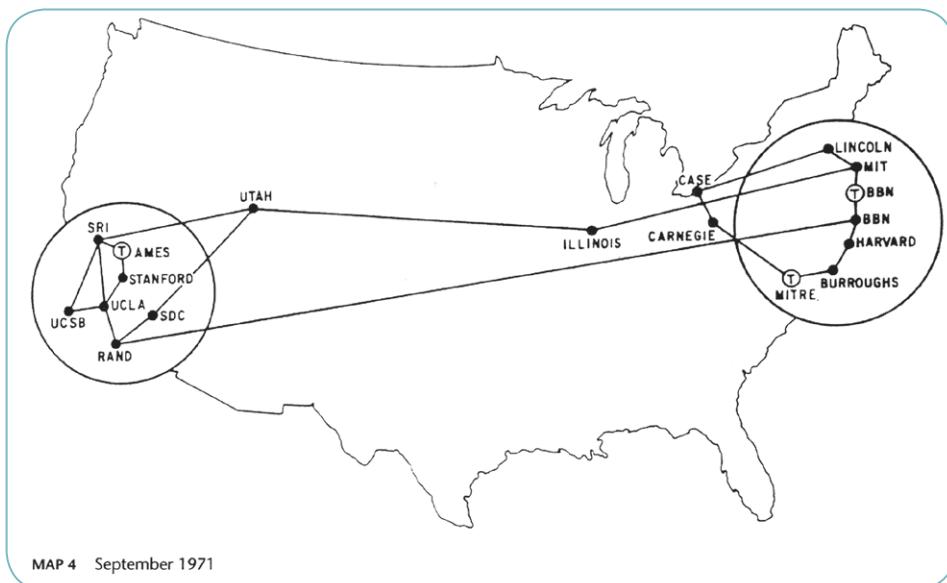
El nuevo estándar allanó el camino para un crecimiento mucho más rápido, al reducir la barrera de entrada para las nuevas redes.

- **1986:** Una de las primeras redes que se conectó a internet fue NSFNET (National Science Foundation Network), fruto de un programa de proyectos coordinados de 1985 a 1995 para promover la investigación avanzada y la creación de redes de educación.

El objetivo principal era permitir a los investigadores en ciencias de la computación iniciar sesión en las supercomputadoras del programa. Como resultado, NSFNET se convirtió en la ‘backbone’ o columna vertebral de internet: la red de alta velocidad y larga distancia que permitía la comunicación de diferentes partes y nodos.

- **1991:** El 26 de febrero de 1991 será recordado como uno de los momentos más importantes de la historia de internet. Ese día fue presentado oficialmente el primer navegador web y editor de HTML en modo gráfico: el World Wide Web, más conocido como WWW. Su creador, Tim Berners Lee, quien es conocido como el padre de la web, publicó el primer sitio en línea que existió en el mundo. Esta página ya no existe, pero se creó una copia en 1992⁵⁶.

Imagen 17



Las redes de ARPANET en 1970.

Las primeras computadoras trabajaban directamente en sistemas operativos por comandos tipo MS-DOS o Unix, no existía el Sistema Operativo de Windows.

Las pantallas de las computadoras eran monocromáticas y las letras que se veían en ellas eran de color verde o naranja; para navegar en internet era necesario saber los comandos de cada sistema operativo.

⁵⁶ Puede visitarse en: <https://www.w3.org/History/19921103hypertext/hypertext/www/TheProject.html>

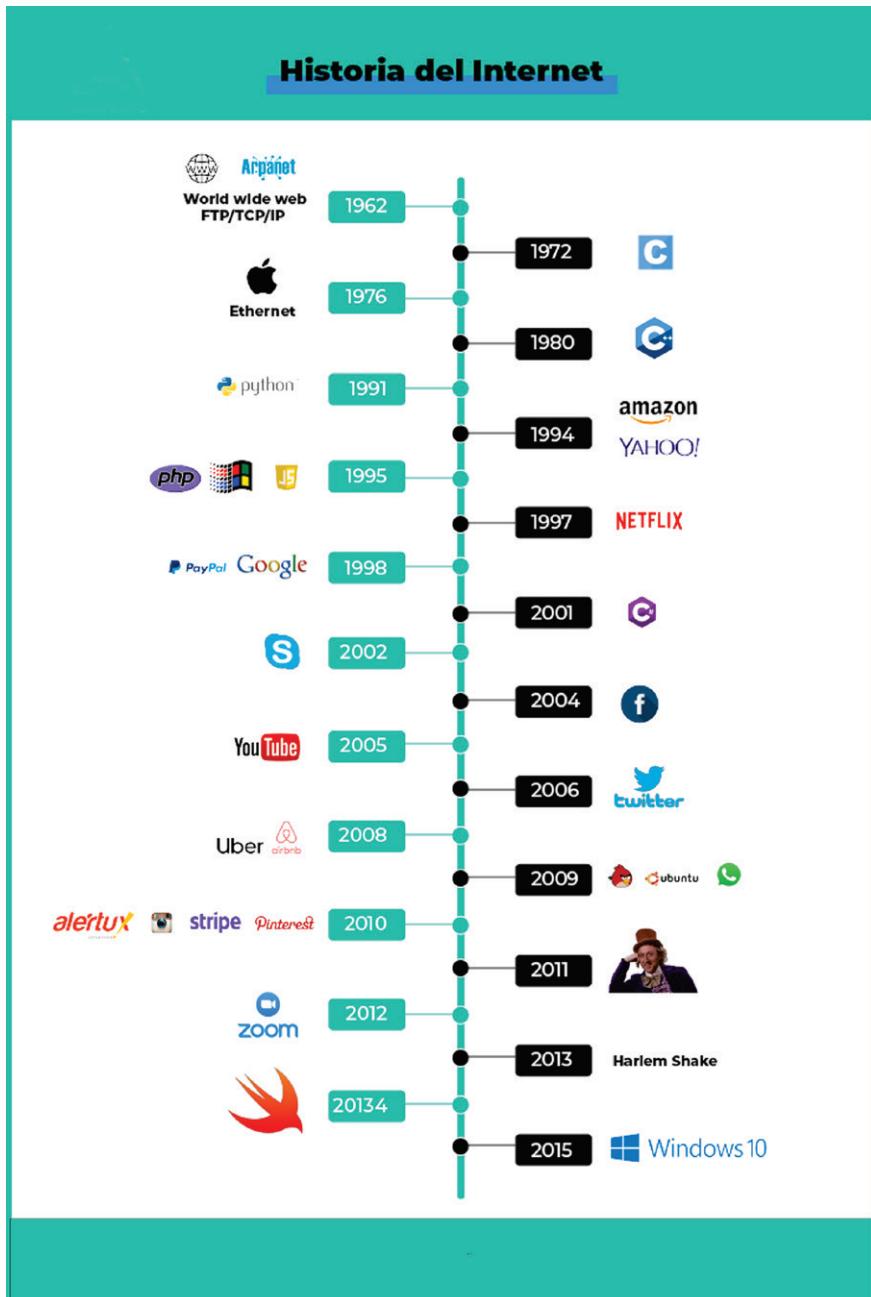
Posteriormente, con el desarrollo de la interfaz gráfica diseñada por Macintosh y Windows, el proceso de trabajo en la computadora se hizo más fácil, más amigable para los usuarios no expertos en programación.

- **1994:** La administración de Bill Clinton privatizó la red troncal de internet. Las empresas comerciales asumieron el trabajo de transportar el tráfico informático a larga distancia, lo que permitió el desmantelamiento de NSFNET, red financiada por el Estado y con recursos públicos.
- **1995:** Con la retirada de la columna vertebral de internet, la NSFNET, el 30 de abril de 1995, la red de redes empezó a ser sostenida por varios proveedores comerciales de internet (ISP, Internet Service Provider) y redes privadas, así como redes entre universidades.

El gobierno se aseguró de que ninguna compañía controlara demasiado la red troncal, ayudando a crear un mercado competitivo para la conexión a internet, que todavía existe en la actualidad.



INFOGRAFÍA 4

Línea del tiempo del desarrollo de internet



REDES SOCIALES



¿QUÉ ES UNA RED SOCIAL?

Comúnmente nos referimos a Facebook, Twitter y a otras plataformas virtuales como redes sociales, pero su significado es mucho más amplio y complejo, pues refiere a la forma misma de vínculos del ser humano, cuya esencia es su carácter relacional.

Es decir, las redes sociales son parte de la vida humana, son la forma en que se configuran las relaciones personales, grupales e institucionales. Estamos enlazados desde mucho antes de alcanzar la conexión a internet.

Los antecedentes conceptuales de red social se remontan a los trabajos de John Arundel Barnes, un antropólogo inglés que hacia 1954 concibió la red como la tribu a la cual pertenece el individuo.

“En todas las antiguas sociedades tribales, más simples y primitivas, la tribu se ocupaba de resolver los problemas existenciales de sus miembros. Los amerindios, los hawaianos, las tribus africanas, los esquimales y otros aún recurren al curandero como una fuente de apoyo social para solucionar los problemas personales.”⁵⁷

Una red social en internet o red virtual se puede definir como un entramado relacional que, mediante plataformas de software, permite a los individuos construir un perfil público o semipúblico dentro de un sistema delimitado, articular una lista de otros usuarios con los que comparten una conexión, ver y recorrer su lista de las conexiones y de las realizadas por otros dentro del sistema.⁵⁸



⁵⁷ Speck, R.V. & Attneave, C.L. 2000. *Redes familiares*. Amorrortu Editores. Pág. 24.

⁵⁸ Flores, J.J., Morán, J.J. & Rodríguez, J.J. 2009. *Las redes sociales*. Universidad de San Martín de Porres. <https://www.usmp.edu.pe/publicaciones/boletin/fia/info69/sociales.pdf>

Entonces, las redes sociales en internet constituyen una estructura social que, desde los recursos de la web y las tecnologías de la información y la comunicación (TIC), promueve la interacción entre personas, grupos y organizaciones bajo uno o varios objetivos comunes. El enlace de las personas mediante una identidad digital permite al usuario expresar ideas, establecer contacto con sus amigos, hacer nuevas amistades, colaborar en producciones grupales, realizar compras y negocios, publicar documentos, fotografías, videos y audios, comentar contenidos y otras múltiples actividades en línea que se basan en la socialización, la colaboración, el aprendizaje, la diversión y el encuentro.



EL PODER DE LAS REDES Y LOS DATOS

Numerosas empresas ofrecen la plataforma tecnológica necesaria para establecer conexiones entre usuarios que comparten las mismas expectativas, necesidades e intereses. Estas empresas de servicios de redes sociales (ESRS) prefiguran, en buena medida, el tipo de relaciones que se establecen desde sus plataformas con la posibilidad de participar como individuo, colectivo, comunidad o empresa.

Un buen número de estas plataformas son de carácter privativo o son de propiedad de las firmas tecnológicas. Esto significa que no permiten el acceso al código fuente, impidiendo total o parcialmente su libre modificación. De otro lado, sus estructuras de red se encuentran fuertemente centralizadas, conteniendo la información de millones de usuarios y usuarias en grandes servidores, que utilizan enormes cantidades de recursos energéticos y son también propiedad suya.

Dado el carácter comercial de dichas empresas, nuestros datos son la mercancía, también denominados ‘el petróleo del siglo XXI’, de donde se generan sustanciosas ganancias. Dicha información y la generación de algoritmos que permiten su clasificación y sistematización de acuerdo con distintos criterios de selección, son la base sobre la que se fundamenta el marketing digital.

Muchos de esos grandes servidores donde se aloja el enorme cúmulo de datos, que son lo que hoy conocemos como ‘la nube’, se encuentran en Silicon Valley, al norte de California en Estados Unidos. Facebook, Apple, Google y otros emporios de alta tecnología tienen allí sus sedes.

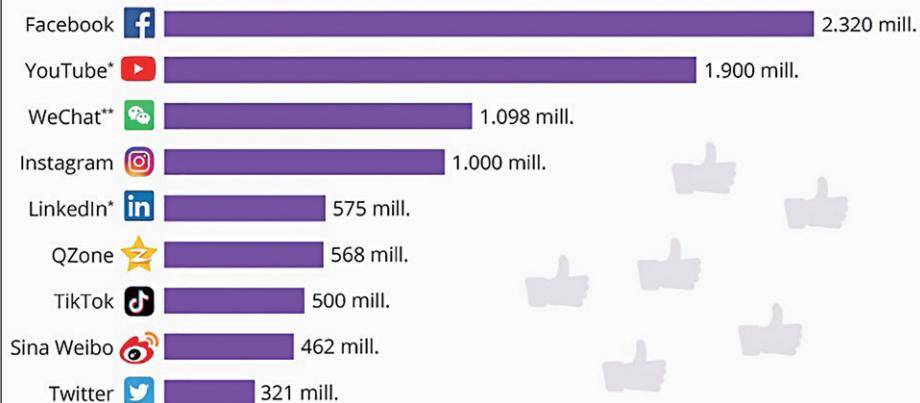


A continuación, una relación entre las redes sociales más populares y el número de usuarios en 2019:

Imagen 18

Las redes sociales preferidas en 2019

Redes sociales con más usuarios activos mensuales en todo el mundo en 2019



Redes sociales seleccionadas. Actualizado en abril de 2019.

Servicios de mensajería tipo WhatsApp excluidos.

* Usuarios registrados totales

** Servicio de mensajería que también cuenta con funciones de red social

Fuentes: Empresas, investigación Statista

statista

En la imagen falta WhatsApp, la aplicación de mensajería instantánea que superó en 2020 los mil millones de usuarios diarios activos. Recientemente comprada por Facebook, es la aplicación de telefonía móvil más popular en el mundo.





BREVE CRONOLOGÍA Y TIPOLOGÍA DE REDES SOCIALES

La historia de las redes sociales tiene los siguientes momentos claves:

- **1994:** Se lanza GeoCities, un servicio para que usuarios y usuarias pudieran crear sus propios sitios web y alojarlos en una especie de ciudadela virtual, donde se podía elegir el “barrio” donde residiría dicha creación, acorde al contenido.
- **1995:** Se crea Classmates.com, una red orientada al reencuentro entre personas que tuvieron un pasado común: compañeros de primaria y secundaria, amistades de infancia, colegas de grupos deportivos o artísticos, etc.
- **1996:** Se estrena ICQ, un servicio de mensajería instantánea con un entorno gráfico agradable y pionero en el ámbito de internet. Su nombre proviene de la pronunciación de la frase ‘I seek you’ (Te busco). Permitió la comunicación por chat y el envío de archivos.
- **1997:** Se lanza Six Degrees, considerada la primera red social en internet, por sus características y finalidad. Andrew Weinreich creó un ‘directorio electrónico’ que conectaba al usuario con sus conocidos y al mismo tiempo, a las personas que estos conocían y así sucesivamente en un crecimiento exponencial.

Lo llamó Six Degrees (Seis Grados) basado en la hipótesis de que cada persona en este planeta está conectada a otra por una cadena de conocidos no mayor a seis personas, o sea, por seis grados de separación.

Ese mismo año se estrena también AOL Instant Messenger, otro servicio de mensajería instantánea, al tiempo que comienza el Blogging con Google.

- **2001:** Se crea Wikipedia bajo el formato ‘wiki’⁵⁹, como una enciclopedia colaborativa de edición abierta. Un proyecto que inició como

⁵⁹ Un wiki es una herramienta colaborativa que permite la edición, modificación y corrección de los contenidos que aloja. Posibilita dar formato, crear enlaces, agregar imágenes y sonidos, etc. Para estructurar el contenido utiliza un sistema basado en hiperenlaces.

un ensayo para agilizar el desarrollo de Nupedia, una enciclopedia escrita por expertos, extinta actualmente. Wikipedia es hoy la mayor y más consultada enciclopedia en el mundo, con ediciones en más de 200 idiomas.

- ❑ **2003:** Nacen dos redes sociales que fueron icónicas en su momento: MySpace y Hi5.
- ❑ **2004:** Como una iniciativa para conectar en un entorno virtual a sus compañeros y compañeras de la Universidad de Harvard, el estudiante Mark Zuckerberg funda Facebook. Con el paso de los años, se convertiría en la red social más famosa de la historia hasta la actualidad.



INFOGRAFÍA 5

endster
living the game

pace 2003

ebook

2005



Instagram



BREVE HISTORIA DE LAS REDES SOCIALES

Hace más de dos décadas que nació la primera red social. Repasamos la evolución del Universo Social Media desde su origen.

sixdegrees®

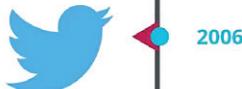
1997 sixdegrees®

friendster living the game 2002

myspace 2003 LinkedIn

facebook 2004

YouTube 2005



WhatsApp 2009

Instagram 2010 Pinterest

G+ 2011

TikTok 2016

mastodon

M4RKETING
E-COMMERCE

ked in

YouTube





Clasificación de redes por su público objetivo y temática

- ❑ **Redes sociales horizontales:** Se dirigen a cualquier usuario, no hay temática definida. Ejemplos: Facebook, Twitter, Instagram, Orkut, Identica.ca.
- ❑ **Redes sociales verticales:** Se conciben alrededor de un eje temático que congrega a las personas interesadas. Su objetivo es agrupar a un colectivo concreto en torno a dicho eje.

En función de su especialización, pueden clasificarse a su vez en:

- ◆ Redes sociales verticales profesionales: Destinadas a enlazar y conectar profesionales. Los ejemplos más representativos son Viadeo, Xing y LinkedIn.
- ◆ Redes sociales verticales de ocio: Congregan colectivos que desarrollan actividades de ocio, deporte, usuarios de videojuegos, fans, etc. Reddit, Twitch, Wipley, Minube Dogster, Last.FM y Moterus son algunas de las más conocidas.
- ◆ Redes sociales verticales mixtas: Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades, tanto profesionales como personales, de acuerdo con sus perfiles. Ejemplos: Yuglo, Unience, PideCita, 11870.

Clasificación de redes por el sujeto principal de la relación

- ❑ **Redes sociales humanas:** Fomentan relaciones entre personas, uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y actividades. Ejemplos: Koornk, Dopplr, Youare y Tuenti.
- ❑ **Redes sociales de contenidos:** Se juntan perfiles a través del contenido publicado, los objetos o archivos que posee el usuario. Ejemplos: Scribd, Flickr, Bebo, Friendster.
- ❑ **Redes sociales de inertes:** Es un sector novedoso en las redes sociales. Su objetivo es unir marcas, automóviles, lugares y otros elementos que no son seres vivos. Entre estas redes sociales destacan

asombrosamente las de difuntos, siendo estos los sujetos principales del entorno digital. El ejemplo más llamativo es Respectance.

Clasificación de redes por la localización geográfica

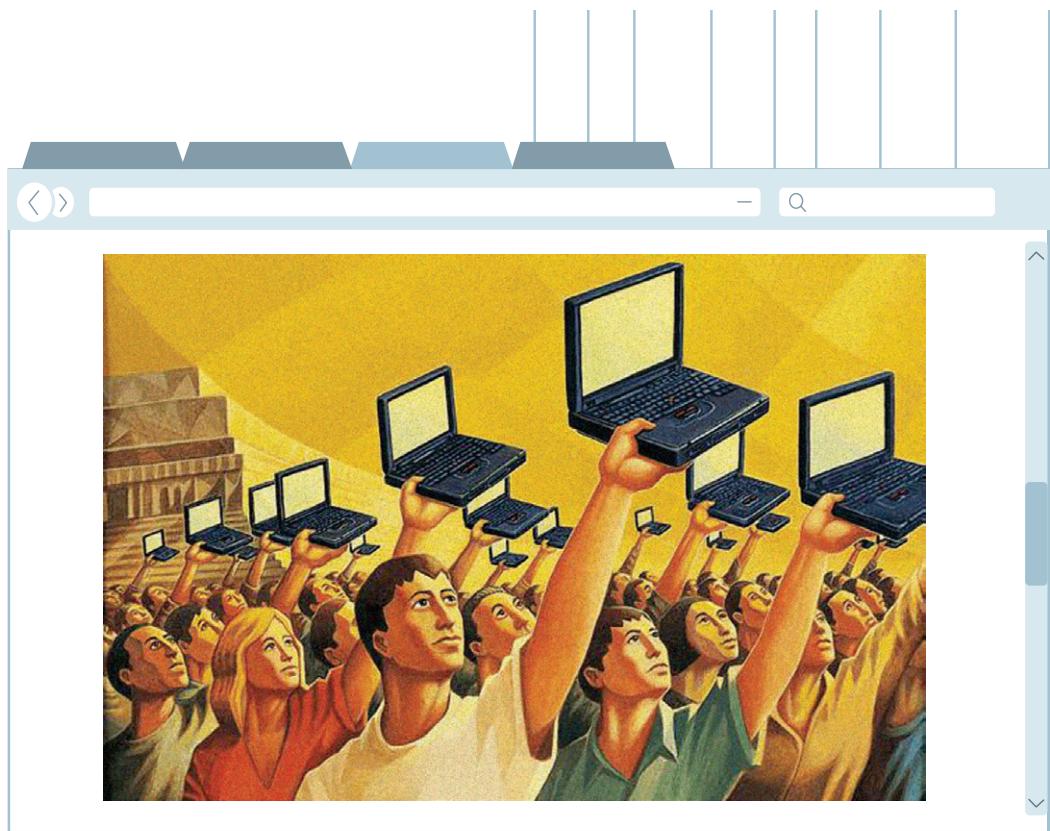
- **Redes sociales sedentarias:** Este tipo de red social se transforma en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Ejemplos: Rejaw, Blogger, Kwippy, Plaxo, Bitacoras.com, Plurk.
- **Redes sociales nómadas:** A las características propias de las redes sociales sedentarias se le suma un nuevo factor de transformación o desarrollo, basado en la localización del sujeto. Se recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Los ejemplos más destacados son Latitud, Brighthkite, Fire Eagle y Scout.



CAPÍTULO 3



UN CAMPO EN DISPUTA





*“¿Privacidad en Internet? Olvídense de eso.
Usted ya ha perdido su privacidad para siempre.”*

SCOTT MCNEALY

*“No puede haber un 100% de seguridad y un 100% de privacidad.
Hay que hacer concesiones y estas pequeñas concesiones
nos ayudan a prevenir ataques terroristas.”*

BARACK OBAMA



INTERNET, REDES SOCIALES Y POLÍTICA

En la denominada sociedad digital, es decir, el mundo de hoy, en donde poco más del 60% de la humanidad se encuentra conectada a internet, tenemos dos espacios fundamentales de interacción social: el espacio online, proporcionado por las plataformas tecnológicas y el espacio offline, que es donde nos encontramos físicamente con nuestros iguales. En ambos espacios, como resultado de lo que somos, tejemos nuestras relaciones a partir del uso de la razón y del lenguaje.

En tal sentido y como afirma Castells⁶⁰, internet no modifica los comportamientos de la gente, no cambia nuestras formas de ser; por el contrario, son los comportamientos, las formas particulares de ser en la cultura y la vida en colectivo los que llegan a la red, que los potencia y amplifica.

La dinámica interactiva y colaborativa que imprimieron los diseñadores de software y los usuarios de la web en la década de los noventa, abrieron el camino hacia la denominada Web 2.0 a donde el público empezó a trasladar una serie de actividades que se tornaron cotidianas.

⁶⁰ Castells, M. 2001. *Internet y la Sociedad Red*. Universidad Nacional Autónoma de México, UNAM. http://fcaenlinea.unam.mx/anexos/1141/1141_u5_act1.pdf



El internet 2.0 será entonces el resultado de la evolución de las herramientas que al principio tenían alta complejidad: las usuarias y usuarios, sin ser expertas/os en los códigos de programación ni en el uso de los distintos sistemas operativos como Unix o Linux, no sólo lograban comunicarse con sus amistades, sino que también podían subir información de cualquier tipo, lo que permitió una mayor interconexión.

El internet 2.0, más que denotar una nueva versión de la red, en realidad se refirió a un nuevo uso, cuya característica principal es la participación colaborativa de usuarios: los autores y los lectores se entremezclan en un entorno participativo. El receptor es activo, busca, investiga, enlaza, opina, contesta, recrea contenidos. El impulsor del código abierto y del concepto de Web 2.0, Tim O'Reilly, afirma:

Web 2.0 es la Red como plataforma, involucrando todos los dispositivos conectados. Aplicaciones Web 2.0 son las que aprovechan mejor las ventajas de esta plataforma, ofreciendo software como un servicio de actualización continua que mejora en la medida en que la cantidad de usuarios aumenta, consumiendo y remezclando datos de diferentes fuentes, incluyendo usuarios individuales, mientras genera sus propios datos en una forma que permite ser remezclado por otros, creando efectos de red a través de una arquitectura de participación y dejando atrás la metáfora de la página del Web 1.0, con el fin de ofrecer experiencias más envolventes al usuario.⁶¹

En esa perspectiva, el internet como espacio de encuentro online, como espacio de articulación y construcción de redes sociales que agrupan una multiplicidad de voluntades a partir de identidades e intereses prefigurados en búsquedas, es también un espacio político que de alguna manera da cuenta de nuestra participación en el devenir de la humanidad. En consecuencia, el acceso a la red de redes debe plantearse como un derecho, como lo es el acceso a la participación en los asuntos

⁶¹ Caldevilla, D. 2010. *Democracia 2.0: La política se introduce en las redes sociales*. Pensar La Publicidad. Revista Internacional De Investigaciones Publicitarias. Universidad Complutense de Madrid. <https://revistas.ucm.es/index.php/PEPU/article/view/PEPU0909220031A>. Pág. 33.

del Estado del que hacemos parte. Y cuando se plantea como derecho, como saben muy bien las personas defensoras de derechos humanos en Colombia, se convierte en motivo de lucha y resistencia.

La idea de la Web 2.0 propendía por un entorno participativo para fomentar la comunicación libre. Esto es, una comunicación no mediada ni determinada por el poder de los gobiernos. El internet se concibe democrático, no como mera representación e inclusión aparente sino como participación y ejercicio del poder por parte de la comunidad.

Dicha intencionalidad, surgida de una ética de la participación y la democratización del acceso, es legítima y por eso fue adoptada retóricamente por los que se adueñaron de las plataformas de redes sociales, que luego convirtieron en poderosas empresas como Facebook, que prometió “socializar la red” y volver “más transparente al mundo”. Una promesa que, como demostramos en este trabajo, es falsa. La red opera bajo la lógica y principios del capital, si se tiene en cuenta la venta de nuestros datos personales al mejor postor. La promesa de Mark Zuckerberg tuvo otra intención: que los usuarios suministren sus datos reales, que valen oro.

Ahora veremos algunos rasgos de esta tensión generada entre dos bandos: de un lado, un conjunto de movimientos online, que impulsan el uso de software libre y el aprovechamiento de internet para causas comunes y del otro lado, los intentos gubernamentales y empresariales por controlar la red, vigilar a la ciudadanía y hacer negocio con la información.



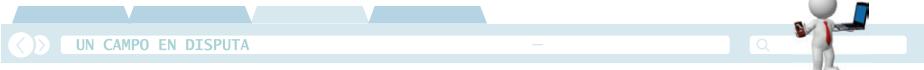
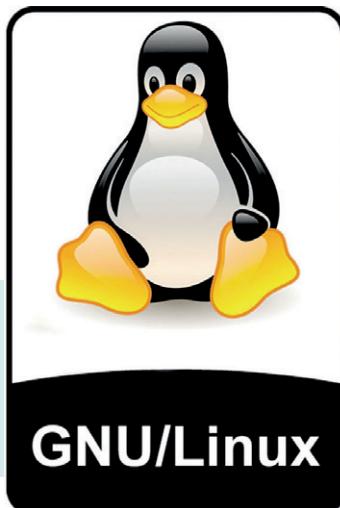


Imagen 19

Logo de GNU/Linux



SOFTWARE LIBRE Y SOBERANÍA

Richard Stallman funda a principios de los ochenta el proyecto GNU, un movimiento de programadores y expertos informáticos que pretendían desarrollar conjuntamente un sistema operativo. Si bien no lo lograron en ese momento, desarrollaron una serie de aplicaciones que darían origen al sistema operativo GNU/Linux que actualmente ya tiene múltiples versiones como Ubuntu, Debian, Fedora, Linux Mint, OpenSuse, entre otras.

Stallman, proclama cuatro libertades que debe tener este tipo de software: 1) la libertad de ejecutar el programa con el fin que se quiera mientras no sea ilegal; 2) la libertad de, en caso de querer y saber, estudiar el código fuente del software y modificarlo; 3) la libertad de crear copias y distribuirlas y 4) la libertad, que parece más un deber, de hacer pública cualquier mejora.

En los tiempos en que se lanza este movimiento, estábamos muy lejos de conocer los escándalos de Facebook y del espionaje de la Agencia de Seguridad de los Estados Unidos (NSA), propiciados a partir del llamado software privativo. El movimiento ha evolucionado e incorporado

la noción de soberanía tecnológica, como expresión de la necesidad de los usuarios y usuarias de tener control de su información, cosa que es posible a través del software libre.

En América Latina, varios países han legislado a favor del software libre. Vale la pena mencionar el caso de Venezuela que, a partir del sabotaje a los sistemas de control digital de la empresa estatal Petróleos de Venezuela, SA. (PDVSA) en el 2002, los cuales eran operados desde Estados Unidos, establece una ley a favor de la utilización del software libre en las instituciones, como parte de una política de recuperación de la soberanía nacional. Posteriormente, se crea el sistema Canaima, basado en el software libre, utilizado en los computadores portátiles (ensamblados en territorio venezolano) que se distribuyen gratuitamente a los niños y niñas en segundo grado de primaria. Esto como parte de una política de democratización de las TICS.⁶²

El movimiento por el software libre no es el único que emerge de las redes. Existe gran diversidad de movimientos de este corte como el hacking-activismo, un acrónimo de hacker y activista, acuñado por un hacker canadiense que busca aplicar la Declaración Universal de los Derechos Humanos a internet. Algunos casos que han tenido resonancia son WikiLeaks, Activismo Hacker y Anonymous.



SOFTWARE PRIVATIVO Y NEocolonialismo

En contraposición al caso venezolano y al movimiento por el software libre, es pertinente recordar que recientemente en Colombia, Mark Zuckerberg, implementó el proyecto Internet.org para facilitar a poblaciones excluidas y sin acceso a la red, la navegación en un número determinado de páginas web, sin pagar un plan o adquirir un servicio de datos móviles.

Entre las 15 páginas a las que se otorga acceso, se encuentran Facebook, El Tiempo y el portal de reparación integral de víctimas. El programa “sin ánimo de lucro” se presenta como una ampliación de la cobertura de acceso a internet en países del tercer mundo. Lo cierto es

⁶² Ágora. 2 de mayo de 2015. *El movimiento del Software Libre*. <http://agorapoliticafilos.blogspot.com/2015/05/el-movimiento-del-software-libre.html>



que representa para la empresa Facebook, por una parte, una jugosa exención de impuestos y por otra, la multiplicación del acceso a la red social en una oferta de sitios web absolutamente restringida.

Este plan, que comenzó como un acuerdo en 2015 con el entonces presidente Santos, no es otra cosa que una violación al principio de ‘Neutralidad de la Red’ (Net neutrality), que establece que los proveedores de internet y los gobiernos no deben restringir de ninguna forma el acceso a ninguna página web.⁶³ En este plan “benéfico” estaría restringiendo el acceso al 99% de las páginas web para una porción de la población, además de agravar la ya débil defensa de la soberanía nacional por parte de los gobernantes colombianos.

Imagen 20



Mark Zuckerberg y Juan Manuel Santos.



PARTIDOS POLÍTICOS Y CAMPAÑAS ELECTORALES

Buena parte de los partidos políticos de todas las tendencias en el mundo hacen presencia en internet y muchos de ellos contratan profesionales para alimentar las redes sociales, especialmente Facebook, Twitter e Instagram; igual ocurre con las instituciones de los diferentes Estados que ofrecen diversos servicios online.

⁶³ Semana. 1 de diciembre de 2015. *La falsa filantropía de los magnates digitales*. <https://www.semana.com/impresa/internet/multimedia/filantropos-tecnologia-bill-melinda-gates-zuckerberg/45279/>

Una amplia gama de negociantes de la red impulsa en la política electoral el uso de estrategias del marketing digital, una versión contemporánea del tradicional marketing. Estas estrategias plantean la generación de anuncios para determinado tipo de personas o consumidores potenciales. Con la gran base de datos que alimentan los dueños de las grandes plataformas de redes sociales, es posible para estos mercaderes diseñar anuncios, mensajes y campañas cada vez más personalizados, lo que se traduce en que publicistas y políticos logren persuadir a cada individuo para que compre determinado producto o vote por tal o cual candidato, a partir del conocimiento profundo de sus intereses, gustos y deseos particulares.

La victoria electoral de Barack Obama en Estados Unidos, se atribuye a una de estas estrategias y se dice que el 60% de los fondos de campaña se recaudaron por internet. El equipo de trabajo del primer presidente negro de EE. UU. lanzó en redes un mensaje viral y personalizado entre sus simpatizantes, en donde invitaba a colocar el nombre de una persona que preferiría hacer otra cosa en lugar de ir a votar.

Esa tendencia marcada por Obama fue bautizada como ‘Política 2.0’ y se refiere al uso de todas las posibilidades que ofrece la Web 2.0 para la política electoral. Si bien, en algunos sitios se habla de la Política 2.0 como la expresión de la nueva forma de hacer política en la red, detrás de este término se encuentra fundamentalmente la venta de servicios de marketing político y el interés natural de los candidatos que buscan acceder a cargos de representación. Igual que en el mundo físico, las y los candidatos electos no recurren posteriormente a la interactividad que propicia el internet para generar diálogos ciudadanos donde se debate o haga veeduría a su desempeño en el cargo.

Luego de la administración demócrata, la Casa Blanca fue habitada por el republicano Donald Trump, el conocido magnate que contrató los servicios de Cambridge Analytica para su campaña, como ya expusimos en el primer capítulo.





Estos ejemplos poco loables de la Política 2.0, no tardaron en imitarse en América Latina. En Colombia, las falsas noticias o ‘fake news’ lograron un amplio despliegue en redes sociales en contra del plebiscito sobre los Acuerdos de Paz entre el Estado y las FARC-EP, en 2016. Juan Carlos Vélez, gerente de la campaña del NO y militante del partido Centro Democrático, en una entrevista al diario La República, declaró que se tergiversó la información y se engaño al electorado con mentiras para lograr la victoria, además de revelar que algunos de sus financiadores públicamente aparecían como simpatizantes del Sí.⁶⁴

Como consecuencia de tal admisión, Vélez debió renunciar luego de que el líder de su partido, Álvaro Uribe, lo amonestara públicamente y emitiera un comunicado desmintiendo sus desafortunadas declaraciones. Pocos meses después, el Consejo de Estado lanzó un dictamen en el que estableció que hubo engaño generalizado en la campaña en lo relativo a: ideología de género, eliminación de subsidios, afectación del régimen pensional, impunidad, víctimas y cambio de modelo económico y régimen político.

No obstante, tanto en el mundo offline como en el online, hay partidos contrahegemónicos, movimientos sociales y otras múltiples manifestaciones de organización y disputa que evidencian el surgimiento de nuevos sujetos colectivos con apuestas políticas admirables que la red de redes permite amplificar y difundir.

Hay una serie de movimientos emblemáticos que se han potenciado desde las redes sociales; vamos a mencionar apenas algunos.

⁶⁴ La República. 4 de octubre de 2016. *El No ha sido la campaña más barata y más efectiva de la historia.* <https://www.asuntoslegales.com.co/actualidad/el-no-ha-sido-la-campana-mas-barata-y-mas-efectiva-de-la-historia-2427891>

Primavera Árabe (2010 -2012)

La ‘Primavera Árabe’ es el nombre que le dieron los medios de comunicación a una serie de manifestaciones multitudinarias en los países del norte de África y Medio Oriente que comenzaron a partir de diciembre de 2010, cuando el joven tunecino de 26 años, Mohamed Bouazizi, se prende fuego como forma de protesta ante el abuso de la policía.

Este movimiento condujo a la caída de las dictaduras de Ben Alí en Túnez y Hosni Mubarak en Egipto, reforzó la violencia en Yemen y derivó en la intervención de Estados Unidos en este y otros “conflictos latentes” en Libia y Siria, que aun hoy no se resuelven. Otros países que vivieron el ‘efecto dominó’ de este movimiento fueron Bahrein y Argelia.

Las revueltas árabes, para algunos analistas, no son levantamientos espontáneos sino parte de dinámicas populares que vinieron de las llamadas ‘revueltas del pan’ en los años setenta y ochenta, en respuesta a los planes de austeridad del Fondo Monetario Internacional (FMI), que agudizaban la profunda dependencia económica y financiera de dichas naciones.

Esta ola democrática tomó por asalto las redes sociales, en donde la indignación se regó como pólvora con la imagen del joven Bouazizi ardiendo, a la que se sumaron imágenes de protesta, de represión policial y los llamados a diversas acciones en plazas y calles. En Facebook y Twitter se comenzaron a comunicar con mayor efectividad las ideas de transformación política que empezaban a retumbar en varios países.

Antes de dimitir, Mubarak y Ali intentaron bloquear el uso de las redes. Sin embargo, el llamamiento a las protestas en las calles no se detuvo. Cuando los jóvenes activistas no encontraban a sus amigos en Facebook, iban a buscarlos a los lugares más concurridos como la Plaza Tahrir, en El Cairo, “de forma que la falta de información en el mundo virtual impulsó el activismo en el mundo real en vez de frenarlo”, según Sahar Khamis. La televisión satelital jugó un papel importante a través de los canales árabes Al-Arabiya y Al-Jazeera.⁶⁵

⁶⁵ Actual. 17 de enero de 2016. *La Primavera Árabe: más vale lo malo conocido que lo bueno por conocer.* <https://www.actuall.com/democracia/la-primavera-arabe-mas-va-le-lo-malo-conocido-lo-bueno-conocer/>



Imagen 21

Plaza Tahrir,
El Cairo. 2011



15M en España (2011)

El movimiento 15M surgió en medio de la campaña para elecciones autonómicas y municipales en España, en el marco de una fuerte crisis económica, que a su vez generó una creciente molestia por los innumerables recortes presupuestales y de personal que dejaron en la calle a más de cinco millones de desempleados, sumados a las altas hipotecas que dejaron sin vivienda a otros miles de personas.

También fue una muestra de indignación frente al bipartidismo del Partido Socialista Obrero Español (PSOE) y el Partido Popular (PP), profundamente desacreditados y con escándalos de corrupción.

Con una protesta que se lanzó a las calles el 15 de mayo de 2011, convocada por grupos minoritarios que crearon la plataforma ‘Democracia Real Ya’ en Facebook, el conjunto de personas indignadas fue creciendo, desbordando a sus organizadores y manifestándose en diferentes ciudades del país ibérico.

Bajo consignas como “no somos marionetas en manos de políticos y banqueros” o “no somos mercancía en manos de políticos y banqueros”, indignados e indignadas españolas, se organizaron en asambleas y comités temáticos que debatieron en una estructura horizontal diversos

temas de la vida nacional: desde una reforma electoral y aumentos salariales hasta mecanismos de control de la corrupción.

Si bien el proceso de movilización, que duró varios meses, no tenía ningún interés electoral, tuvo un fuerte impacto en el declive del PSOE, sumó importantes votos al partido Izquierda Unida, creó las condiciones para el surgimiento de Podemos, fundado en 2014 y se extendió a otras ciudades en toda Europa, que siguieron el ejemplo de la Puerta del Sol en Madrid.

El 99% o Los Indignados de Wall Street (2011)

El 17 de septiembre de 2011, día del aniversario de la Constitución de Estados Unidos, se inició un campamento ciudadano en Nueva York y con él, el movimiento 'Occupy Wall Street', en contra de las grandes empresas y las corporaciones financieras que, después de la crisis financiera de 2008 y al borde del colapso por su especulación, fueron rescatadas por el gobierno con dineros públicos, mientras que miles de ciudadanos y ciudadanas perdían casas, puestos de trabajo y ahorros en los años anteriores.

La convocatoria arrancó en la revista web Adbusters. También convocaron Ampedstatus.com, cuya página fue saboteada luego de publicar varios especiales sobre el colapso financiero. Anonymous vino en su ayuda y se sumó a la convocatoria, llamando al día del encuentro, igual que en el mundo árabe, el Día de la Ira.

Acudieron alrededor de mil personas al Zuccotti Park en Wall Street. De allí siguieron una serie de manifestaciones que se extendieron a Los Ángeles, Boston, Filadelfia y Washington. Videos de la represión policial fueron difundidos en internet. Se sumaron posteriormente 15 sindicatos de trabajadores de Nueva York.

En el sitio web del movimiento se leía:

"La única cosa que tenemos en común es que somos el 99% de la gente que ya no tolera la codicia del 1%".

El movimiento fue una mezcla de ocupaciones y encuentros cotidianos de carácter asambleario, que establecían acuerdos online y offline. En las ocupaciones más grandes, como la de Nueva York, se levanta-



ron tiendas, bibliotecas, guarderías, antenas wifi, médicos voluntarios, asesoría legal para los detenidos, seguridad y finanzas, entre otros. Eran verdaderos ejercicios de cooperación y gestión comunitaria, o si se quiere, de poder popular.

Al igual que el 15M, no querían líderes locales, nacionales ni mundiales. Fue un ejercicio que merece ser revisado detalladamente, porque tiene mucho que enseñar en cuanto a las posibilidades que ofrecen las redes sociales y el mundo digital para la organización social, la democratización de la información, la difusión amplia de decisiones colectivas, los espacios de intercambio y la deliberación política. El impacto en las políticas financieras del país no fue mayor, dada la ambigüedad de las demandas.⁶⁶

Movimiento de los chalecos amarillos en Francia (2018)

El 17 de noviembre de 2018, comienza la llamada ‘rebelión de los chalecos amarillos’ en contra de un impuesto que aumentó el precio del combustible. Desde las redes sociales se convocó a un masivo bloqueo de rutas por toda Francia. Las protestas encontraron fuerte eco y todos los sábados se convocaron actos a lo largo del territorio nacional.

“Su aparición vino acompañada de varias invenciones sociales: no sólo el chaleco, también la articulación entre las redes sociales y la realidad y esa forma inédita de haber bautizado cada manifestación de los sábados como un «acto». Una forma de decir que la gran pieza de teatro sigue en el escenario.”⁶⁷

No es propiamente un movimiento pacífico, pero tampoco es violento; ha tenido duras confrontaciones con la policía que han arrojado un considerable saldo de detenidos y heridos. El simbolismo de los chalecos, asociados al sector de la construcción y también a conductores y transportadores, ha jugado un papel relevante en la convocatoria y solidaridad de otros sectores de la sociedad francesa.

⁶⁶ Castells, M. 2015. *Redes de indignación y esperanza: los movimientos sociales en la era de internet*. Alianza Editorial. Págs. 158-164.

⁶⁷ Nueva Sociedad. 2019. «Los ‘chalecos amarillos’ se desarrollaron en un desierto político». Nueva Sociedad 280, marzo-abril 2019, ISSN: 0251-3552. <https://nuso.org/articulo/los-chalecos-amarillos-se-desarrollaron-en-un-desierto-politico/>

Las exigencias se han ido diversificando y además de la reducción del precio del combustible se propuso la renuncia de Macron, así como la realización de un referendo de iniciativa ciudadana que permitiría, por ejemplo, formular leyes sin aprobación del Parlamento, el aumento del poder adquisitivo de la clase trabajadora y otras medidas relativas a salud, vivienda y pensiones.

Este movimiento igualmente se declaró sin líderes ni programas, se ha sacudido de la dirección de los sindicatos y escogió como lugar recurrente de protesta el oeste de París, en donde se encuentran las casas, los comercios y los restaurantes de los sectores adinerados de la ciudad. Se ha caracterizado como un movimiento anti-élite y anti-ricos, la composición del movimiento está entre trabajadores pobres y la clase media empobrecida, jóvenes de 20 a 40 años y una fuerte presencia de mujeres.

En la prensa se afirma que gozaban del 70% de apoyo de la población francesa, lo que los convierte en una fuerza social prometedora.

Imagen 22



Protesta de chalecos amarillos en Francia.



Chile despertó (2019)

Con la misma constitución política impuesta por la dictadura de Augusto Pinochet, la democracia chilena, restablecida nominalmente en 1990 pero con una fuerte herencia totalitaria, enfrentó una serie de protestas que comenzaron en octubre de 2019 con la evasión masiva en las estaciones de metro de la capital del país, protagonizada por estudiantes de diversos liceos.

El motivo de descontento inicialmente fue el aumento de los costos de transporte, pero las demandas se diversificaron: pensiones administradas por el Estado y suficientes para sobrevivir, salarios dignos, mejoras en la educación y la salud, terminando por exigir un nuevo proceso constituyente.

El gobierno de Sebastián Piñera derogó el alza del transporte y activó el toque de queda para apaciguar las protestas, pero en vez de conseguirlo, atizó la llama de la indignación. La siguiente consigna fue ampliamente difundida en redes y da una idea de las motivaciones de las y los chilenos para manifestarse: “No son 30 pesos, son 30 años”.

El anhelo de democracia y justicia social del pueblo chileno se ha expresado, además de las protestas, en una serie de encuentros y asambleas que combinan los espacios digitales, los barrios y las plazas públicas de todo el país. Sin liderazgos reconocibles y negándose a aceptar representación de los partidos de izquierda frente al gobierno, el gran sujeto dinamizador de las protestas son la adolescencia y la juventud, millares de estudiantes escolares y universitarios que se convocaron, no tanto por las redes convencionales como WhatsApp, Twitter o Facebook, sino particularmente por los chats de juegos interactivos (Barrera, 2019).

Al contrario del movimiento indignado de Nueva York, las demandas del pueblo chileno no fueron ambiguas: democracia real expresada en un nuevo pacto constitucional, reconstruyendo en todo este proceso movilizador, un tejido social que fue desgarrado con represión y terror en la dictadura de Pinochet.

La gran victoria de este proceso de movilización fue la realización del plebiscito nacional en octubre de 2020, en el que la ciudadanía decidió en las urnas, con una aplastante mayoría del 78%, iniciar un proceso

constituyente y la conformación de una Convención Constitucional para redactar el nuevo texto político.

Paro Nacional 21N en Colombia (2019)

Se podría decir que el país ha estado movilizado en los últimos años, pero el 21 de noviembre de 2019 fue el primer día de una serie de multitudinarias protestas en las que se unificaron diversas plataformas organizativas: de mujeres y diversidades de género, de personas y colectivos defensores de derechos humanos, de indígenas y afros, sindicatos, organizaciones estudiantiles, campesinas y urbanas, etc. Varios partidos políticos apoyaron la movilización.

La convocatoria por redes sociales, bajo el rótulo de ‘Paro Nacional en contra del Paquetazo de Duque y por la Paz’, fue construyendo un pliego de peticiones que comenzó con el rechazo a los anuncios de medidas nefastas para la población y también con la condena al saboteo permanente y deliberado al Acuerdo de Paz. Desde la firma del Acuerdo, en noviembre de 2016 hasta finales de 2019, se registraban más de 800 asesinatos de líderes y lideresas sociales, personas defensoras de derechos humanos, y excombatientes firmantes del Acuerdo.

La llegada de la pandemia apagó el fervor de las movilizaciones de 2019 pero quedó la demostración de la capacidad de convocatoria que genera la desaprobación a la gestión de Iván Duque, uno de los presidentes más rechazados y criticados de la historia de Colombia.





LEGISLACIÓN INTERNACIONAL EN MATERIA DE DERECHO A LA PRIVACIDAD

Numerosos tratados internacionales, algunos de los cuales suscribe Colombia, reconocen la privacidad como un derecho fundamental. Entre ellos están:

- Declaración Universal de los Derechos Humanos, Artículo 12º.
- Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, Artículo 14º.
- Convención sobre los Derechos del Niño, Artículo 16º.
- Pacto Internacional de Derechos Civiles y Políticos, Artículo 17º.
- Convenciones regionales, como la Carta Africana sobre los Derechos y el Bienestar del Niño, Artículo 10º.
- Convención Americana de Derechos Humanos, Artículo 11º.
- Principios de la Unión Africana sobre la Libertad de Expresión, Artículo 4º. Declaración Americana de los Derechos y Deberes del Hombre, Artículo 5º.
- Carta Árabe de Derechos Humanos, Artículo 21º.
- Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.
- Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y Acceso a la Información.
- Principios de Camden para la Libertad de Expresión y la Igualdad, Artículo 8º.



Este derecho es además complementario con los derechos a la información, la libertad de expresión y la libertad de asociación. Un derecho vinculado al de intimidad o privacidad es el de la protección de los datos. La legislación internacional contiene numerosas disposiciones al respecto, partiendo de los retos que supone la obligación de su garantía en la era digital. Por ejemplo, el Comité de Derechos Humanos de la Organización de Naciones Unidas (ONU) en su Observación General No. 16 de 1988, plantea:

(...) para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación.

En 1990, la misma ONU mediante la Resolución 45/95 de la Asamblea General, aprueba las Directrices para la Regulación de los Archivos de Datos Personales Informatizados, que constituyen un conjunto de orientaciones para que los Estados las acojan a la hora de reglar dicha regulación. Contiene dos párrafos:

- A. Principios relativos a las garantías mínimas que deben prever las legislaciones nacionales.
- B. Aplicación de las directrices a archivos de datos personales mantenidos por organizaciones internacionales gubernamentales.

Los principios son, entre otros: el de legalidad y lealtad, el de exactitud, el de especificación de la finalidad (pertinencia y adecuación, no utilización posterior salvo con consentimiento y conservación limitada a lo necesario), el de acceso, el de no discriminación, el de seguridad, el de supervisión y sanción y el de flujo internacional de los datos con



salvaguardas similares, contemplando excepcionalidades en casos de seguridad nacional.

En cuanto al parágrafo B, se plantea la necesidad de establecer una autoridad competente para verificar el cumplimiento de estas directrices.

Imagen 23

ONU.
Relator Especial sobre derecho a la privacidad.



EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL

Desde el año 2013, luego de las revelaciones de Edward Snowden, la ONU, ha lanzado una serie de resoluciones con el nombre de 'El derecho a la privacidad en la era digital'. La primera resolución, del 20 de noviembre de 2013, reafirma los derechos humanos y libertades fundamentales consagrados en la Declaración Universal de Derechos Humanos y otros tratados de la misma índole. Esta necesidad de reafirmar se da en el contexto del ritmo acelerado del desarrollo tecnológico, que amplía el acceso a personas de todo el mundo e incrementa "la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos (...)."

En ese marco, la Resolución reivindica:

(...) el derecho humano a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra esas injerencias, y reconociendo que el ejercicio del derecho a la privacidad es importante para materializar el derecho a la libertad de expresión y para abrigar opiniones sin interferencias, y una de las bases de una sociedad democrática. Destacando la importancia del pleno respeto de la libertad de buscar, recibir y difundir información, incluida la importancia fundamental del acceso a la información y la participación democrática.

Y manifiesta preocupación “por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala”, afirmando que los derechos de las personas también deben estar protegidos en internet, incluido el derecho a la privacidad.





En tal sentido, la ONU exhorta a todos los Estados a que:

- a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales.
- b) Adopten medidas para poner fin a las violaciones de esos derechos y crean las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos.
- c) Examen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando porque se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del Derecho Internacional de los Derechos Humanos (DIDH).
- d) Establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos, capaces de asegurar la transparencia, cuando proceda y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado.

En 2015, el Consejo de Derechos Humanos de la ONU actualiza la anterior resolución, introduciendo un pequeño análisis sobre los metadatos que pueden “revelar información personal y dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona”, sumando a la preocupación antes manifestada la situación de acoso e inseguridad que padecen defensores y defensoras de derechos humanos en muchos países.

Frente a este panorama, se nombra un Relator Especial sobre el Derecho a la Privacidad, entre cuyas funciones se establece: reunir información pertinente sobre juridicidad en la materia en diferentes países, evaluando experiencias y tendencias; formular recomendaciones para garantizar la promoción y protección del derecho; generar conciencia sobre la importancia de la promoción y protección del derecho a la privacidad; denunciar violaciones donde tengan lugar y, por último, presentar un informe anual al Consejo de Derechos Humanos y a la Asamblea General, a partir de sus períodos de sesiones 31º y 71º, respectivamente.

La Resolución de 2018 agrega algunos elementos, haciendo énfasis en el papel que deben jugar las empresas en el respeto del derecho a la privacidad y expresa nuevas preocupaciones porque “con frecuencia las personas no dan o no pueden dar su consentimiento libre, explícito y fundamentado a la venta o la reventa múltiple de sus datos personales, mientras que ha aumentado considerablemente la recopilación, el procesamiento, el uso, el almacenamiento y el intercambio de datos personales, incluidos datos delicados, en la era digital.

Observando con preocupación que la elaboración de perfiles, la adopción automatizada de decisiones y las tecnologías de aprendizaje automático, a veces denominadas inteligencia artificial, pueden, sin las debidas salvaguardas, dar lugar a decisiones que podrían afectar el disfrute de los derechos humanos, incluidos los derechos económicos, sociales y culturales y reconociendo la necesidad de aplicar el derecho internacional de los derechos humanos al diseño, la evaluación y la reglamentación de esas prácticas.”

El texto también plasma la alarma del organismo internacional frente a la difusión en internet de desinformación y propaganda que induce a engaño, incita al odio, la violencia, la discriminación o la hostilidad, por lo que insta a los Estados a que cumplan y hagan cumplir las disposiciones sobre los derechos humanos en este ámbito, siendo que recae sobre aquellos la responsabilidad principal.



RELATOR ESPECIAL SOBRE EL DERECHO A LA PRIVACIDAD

El primer informe del Relator Especial, Joseph Cannataci, presentado en el 31º Período de Sesiones del Consejo de Derechos Humanos de la ONU, el 8 de marzo de 2016, responde al mandato de la resolución del año anterior: el deber de presentar un informe anual.

Comienza planteando la dificultad de ejercer el derecho a la privacidad en el contexto de un desarrollo tecnológico dinámico que presenta permanentemente nuevos problemas. En el documento, el Relator expone sus métodos de trabajo, la situación en que se halla la privacidad en 2016, sus actividades hasta la fecha y un plan de diez puntos con el que pretende esclarecer y elaborar adicionalmente el derecho a la privacidad en el siglo XX. Por último, presenta sus conclusiones.



Entre los estudios temáticos que se ha planteado el Relator se encuentra una aproximación a modelos de negocio en línea de las empresas y uso de los datos personales por parte de ellas.

Aquí un fragmento que vale la pena citar inextenso, para comprender un poco más el trasfondo de la tensión entre economía digital y la protección del derecho a la privacidad y los otros derechos que se relacionan:

Durante los primeros 25 años de su existencia, la World Wide Web ha dado lugar al crecimiento espontáneo y, en gran medida, no reglamentado de empresas privadas, que en ocasiones se han convertido en entidades multinacionales que traspasan las fronteras nacionales y atraen clientes de todo el mundo. Una de las características principales de ese crecimiento ha sido la recopilación y el uso de datos personales; todas las búsquedas, todos los textos leídos, todos los correos electrónicos o cualquier otro tipo de mensaje, todos los productos comprados o los servicios contratados dejan centenares de miles de huellas electrónicas, que se pueden acumular para construir un perfil muy exacto de lo que le gusta o no le gusta a una persona, sus estados de ánimo, su solvencia económica, sus preferencias sexuales, su historial de salud y sus hábitos de compra, así como sus intereses y convicciones intelectuales, políticos, religiosos y filosóficos.

En general, se suscita la pregunta de si ciertos proveedores de servicios en línea tienen derecho a investigar la conducta de las personas, a fin de garantizar una reparación justa. Este mapa de datos sobre el comportamiento de los consumidores, que es cada vez más detallado, ha hecho que los datos personales se conviertan en una mercancía. El acceso a esos datos, o su explotación, es actualmente uno de los mayores negocios del mundo, ya que produce unos ingresos que se calculan en centenares de miles de millones de dólares y se derivan, por lo general, de la publicidad personalizada.

Muy a menudo se tiene la impresión de que, aunque los consumidores sean conscientes de los contenidos que exponen en línea deliberadamente, son mucho menos conscientes de la cantidad, la calidad y los usos específicos de los metadatos que producen cuando navegan, chatean, compran o realizan otras operaciones en línea. Los datos de que se dispone para trazar el perfil de las personas

son actualmente varios órdenes de magnitud mayores que hace 25 años, pero no hay una comprensión cabal de la amplitud de los riesgos que entrañan para la privacidad el uso o el abuso de esos datos.

Hay indicios de que la mercantilización de los datos personales, sobre todo en los sectores considerados sensibles tradicionalmente, como el sector del tratamiento de los datos médicos, ha aumentado hasta el punto de que una persona no es consciente de que esos datos se venden, o se revenden numerosas veces, ni otorga su consentimiento a ello. No hay suficientes pruebas para determinar con exactitud los riesgos inherentes a los datos presuntamente anonimizados, cuyo proceso de anonimización se puede desandar hasta llegar a identificar a la persona.

Este atentado contra la privacidad podría entrañar numerosos riesgos para una persona, así como para su entorno social, sobre todo si se accede a sus datos sin autorización y los que acceden son, por ejemplo, autoridades del Estado que desean adquirir poder o mantenerlo u organizaciones delictivas o sociedades mercantiles que obran ilegalmente. En la primera época de los ordenadores digitales, una de las preocupaciones principales era el uso de los datos personales por parte de los Estados y su capacidad de correlacionar datos de diversas fuentes para trazar un cuadro preciso de las actividades y el patrimonio de una persona.

Sin embargo, en 2016 parece que son las empresas las que tienen muchos más datos que los Estados sobre las personas. Los ingentes ingresos derivados de la monetización de los datos personales hacen que no haya incentivos muy fuertes para cambiar el modelo de negocio en atención exclusivamente a las inquietudes respecto de la privacidad. En realidad, solo cuando en los últimos tiempos, los riesgos para la privacidad han empezado a amenazar las posibilidades que tenía el modelo de negocio de producir ingresos, algunas empresas han adoptado un criterio más estricto y más favorable a la privacidad.



El otro estudio temático que esboza Cannataci es ‘Seguridad, vigilancia, proporcionalidad y paz informática’, señalando el inconveniente de la generación de legislaciones que colocan los servicios de seguridad e inteligencia en una postura de ataque frente a la intimidad, para lo cual él estudia cuatro aspectos que apuntan a evitar cualquier vulneración y a convertir el ciberespacio en otro escenario bélico.

1. Capacidades de vigilancia del Estado que sean proporcionadas en su ámbito de aplicación y estén debidamente limitadas mediante salvaguardias legislativas, procedimentales y técnicas, entre ellas, unos mecanismos de supervisión sólidos.
2. Concentración en la vigilancia específica, en lugar de la vigilancia a gran escala.
3. Acceso de las fuerzas del orden y los servicios de seguridad e inteligencia a los datos personales que estén en posesión de las empresas privadas y otras entidades que no sean públicas.
4. La insistencia renovada en la paz informática.

El relator esboza también los siguientes temas: ‘Análisis de datos abiertos y macrodatos: su repercusión en la privacidad’, ‘Genética y privacidad’, ‘Privacidad, dignidad y reputación: biometría y privacidad’.

En la segunda parte del informe se señalan las dificultades que surgen a la hora de definir la privacidad, pues culturalmente no es aceptado el término desde una sola acepción. Además, se encuentran diversos marcos normativos a los que se suma la heterogeneidad de condiciones socioeconómicas y tecnológicas en los distintos países para promover su protección, por lo que se plantea la necesidad de establecer un mínimo común denominador en la privacidad universal, como el de ser un derecho necesario para la dignidad y libertad personales.

Joseph Cannataci ha trazado un plan de trabajo de diez puntos para cumplir los objetivos que le ha mandatado la Asamblea:



1. Afinar el significado del ‘derecho a la privacidad’.
2. Concientizar a la opinión pública.
3. Mantener de un diálogo estructurado y continuo sobre la privacidad.
4. Crear un enfoque integral de las salvaguardias y los recursos legales, procedimentales y operativos.
5. Insistir redobladamente en las salvaguardias técnicas.
6. Dialogar con el mundo empresarial.
7. Promocionar avances nacionales y regionales en los mecanismos de protección de la privacidad.
8. Aprovechar la energía y la influencia de la sociedad civil.
9. Trabajar los aspectos referidos a ciberespacio, privacidad informática, espionaje informático, guerra y paz informáticas.
10. Aumentar la inversión en el derecho internacional.

El informe concluye que si bien “las tensiones entre seguridad, modelos de negocio de las empresas y privacidad” siguen siendo centrales, el año 2016 ha presentado indicios contradictorios: mientras algunos parlamentos no se muestran muy amigables con el derecho en mención, Estados Unidos y Europa han dado pasos en contra de medidas desproporcionadas como la vigilancia a gran escala, el descifrado o la admisión de las llamadas puertas traseras.

Imagen 24



Unión Europea



REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

El 24 de mayo de 2016 se expidió el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE), que comenzó a aplicarse el 25 de mayo de 2018. Este reglamento constituye una actualización de los principios de la Directiva de Protección de Datos de 1995. Se propone conciliar la protección de los derechos a la intimidad y a la protección de datos personales con el desarrollo económico y la innovación, estableciendo las obligaciones de quienes hacen el tratamiento de datos, el método para el cumplimiento de estas disposiciones y las sanciones frente a la infracción.

Se establecen los siguientes derechos y facilidades para reforzar el control sobre los datos personales:

- La necesidad de un consentimiento claro de la persona respecto del tratamiento de sus datos personales.
- Un acceso más fácil del interesado a sus datos personales.
- Los derechos de rectificación, supresión y olvido.
- El derecho de oponerse al uso de datos personales incluso a efectos de elaboración de perfiles.
- El derecho a la portabilidad de los datos de un prestador de servicios a otro.
- El derecho a recibir información transparente y de fácil acceso a las personas interesadas sobre el tratamiento de sus datos.
- El derecho a presentar una reclamación a la autoridad de control.
- El derecho al recurso judicial, la indemnización y la responsabilidad.
- El derecho a que uno de los órganos jurisdiccionales nacionales revise la decisión de su autoridad de protección de datos.

Entre las obligaciones generales de los responsables y de quienes tratan los datos personales en su nombre se encuentran:



- Aplicar medidas de seguridad adecuadas en función del riesgo derivado de las operaciones de tratamiento de datos que realicen (método basado en el riesgo).
- En ciertos casos, notificar las violaciones de datos personales.
- Todas las autoridades públicas y las empresas que lleven a cabo determinadas operaciones arriesgadas de tratamiento de datos deberán también nombrar un delegado de protección de datos.
- Los Estados miembros deben crear una autoridad de control independiente a nivel nacional.

El reglamento establece sanciones a quienes lo incumplan, como multas de hasta 20 millones de euros o el 4% de su volumen de negocios total anual. Dado que las empresas con filiales en varios Estados tendrán que tratar con las respectivas autoridades de protección de datos, las sanciones las aplican estos mismos entes de control. De igual manera, el reglamento plantea medidas para la transferencia de datos personales a terceros países u organizaciones internacionales.



DIRECTRICES DE LA OCDE SOBRE PROTECCIÓN DE LA PRIVACIDAD Y FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES



La Organización para la Cooperación y el Desarrollo Económicos (OCDE), es tal vez la primera organización de cooperación internacional que construyó una política de protección de la privacidad y los flujos transfronterizos de datos personales.

En 1980 lanzó unas directrices basándose en los principios de democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Dichas directrices han ido actualizándose en diversos años (1995, 1998, 2013), dado el avance acelerado de las tecnologías de la información y las necesidades de negocios de los países miembros.



Para la aplicación nacional de las directrices, la OCDE plantea los siguientes principios:

- Principio de limitación de recogida: obtención con medios legales y justos.
 - Principio de calidad de los datos: limitados para el propósito de su uso.
 - Principio de especificación del propósito: con un objetivo y un tiempo concretos.
 - Principio de limitación de uso: no se usarán con un propósito distinto al establecido sin autorización correspondiente.
 - Principio de salvaguardia de la seguridad: se salvaguardan los datos contra cualquier riesgo.
 - Principio de transparencia: deberá existir una política general sobre transparencia en el manejo de datos.
 - Principio de participación individual: todo individuo tendrá derecho a saber los que datos tienen de él, que le rectifiquen y le informen lo que se hace con ellos.
 - Principio de responsabilidad: el que maneja los datos debe asumir las responsabilidades totales de dicho tratamiento.



Para la aplicación internacional de las directrices, la OCDE plantea los siguientes principios básicos:

- Los países miembros deberán considerar las implicaciones que el procesamiento nacional y la reexportación de datos personales puedan tener para otros países miembros.
- Los países miembros deberán seguir todos los pasos razonables y apropiados para asegurar que el flujo transfronterizo de datos personales, incluido el tránsito a través de un país miembro, se realice de forma ininterrumpida y segura.
- Los países miembros deberán abstenerse de restringir el intercambio transfronterizo de datos personales con otros países miembros, excepto cuando el país receptor todavía no observe de forma sustancial estas directrices o cuando la reexportación de tales datos burle la legislación nacional sobre privacidad.
- Un país miembro también podrá imponer restricciones a ciertas categorías de datos personales sobre las que rijan normativas específicas, contenidas en su legislación nacional sobre privacidad, que por su naturaleza no tienen una protección equiparable en el país receptor.
- Los países miembros deberán evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección.



EL PRECEDENTE DE LA PRIVACIDAD EN ESTADOS UNIDOS

El surgimiento de la noción del ‘derecho a la vida privada’ en Estados Unidos se encuentra en el artículo ‘The Right to Privacy’ de Samuel D. Warren y Louis D. Brandeis, publicado en la revista jurídica Harvard Law Review en 1890. Este escrito formuló y concretó el nuevo derecho ‘a ser dejado en paz’, deslindándolo del resto de los derechos ya conocidos.

El artículo de los abogados Warren y Brandeis no obtuvo una inmediata repercusión en las sentencias de los tribunales estadounidenses, que empezaron a enfrentarse cada vez más con casos de agravio por publicaciones o fotografías indiscretas. Paulatinamente, la opinión pública



fue cada vez más favorable al reconocimiento de este derecho y en los 30 años siguientes fue configurándose como cuerpo de jurisprudencia.

En EE. UU., la privacidad y su derecho a la protección, si bien no se contemplan como tal en la Constitución, se consideran implícitos en la libertad de asociación, garantizada en la Primera Enmienda, también en la Cuarta Enmienda, frente a registros y requisas arbitrarias, se limita la intrusión del gobierno en domicilios, documentos y demás jurisdicciones personales, lo que restringe en cierta medida la vigilancia electrónica. Igualmente, en la Quinta Enmienda, que protege frente a la incriminación contra uno mismo y la obligación de revelar información personal, en la Decimocuarta Enmienda que garantiza el derecho de las personas a tomar las decisiones fundamentales sobre su vida personal, sin injerencia estatal, incluyendo evitar la divulgación de información personal.

Por otra parte, el derecho a la privacidad se considera en el derecho mercantil a través del desarrollo federal de normas de diversa índole, incluso desde el derecho contractual⁶⁸ y de propiedad⁶⁹. Hay una doble dimensión de las personas estadounidenses frente a las leyes: de un lado, como ciudadanos y de otro, como consumidores. Todo consumidor es ciudadano y como tal, tiene unos derechos que le son inherentes, pero hay unas particularidades referidas a la relación del ciudadano o la ciudadana con el ente en cuestión, si derivó en la violación a un derecho. Por ejemplo, una entidad bancaria, una corporación privada o un poder público, administrativo o gubernamental. En este último aspecto se presentan grandes limitaciones y contradicciones de las normativas y líneas definitorias, ya que por razones de seguridad nacional y orden público se pierde el equilibrio entre seguridad, libertad, ejercicio y protección de derechos.⁷⁰

⁶⁸ El derecho contractual es el área del derecho que se encarga de las promesas o acuerdos que tienen dos o más personas y cuándo son ejecutables. Esencialmente, el derecho contractual permite a las partes llegar a un acuerdo para hacer que la ley los cubra, lo cual el tribunal luego ejecutará, siempre y cuando se sigan las leyes y se cumplan los requisitos.

⁶⁹ El derecho de propiedad es el poder legal e inmediato que tiene una persona para gozar, disponer y reivindicar sobre un objeto, sin afectar los derechos de los demás ni sobrepasar los límites impuestos por la ley.

⁷⁰ Pérez, J. 2019. *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos*. Universidad de Sevilla.

Encontramos que en el marco legal de Estados Unidos hay tres conjuntos de leyes que abordan de alguna manera la protección a la privacidad: 1) las referidas a la protección de la privacidad de consumidores, propietarios y clientes, 2) las contemplaciones indirectas de las enmiendas constitucionales y 3) las que preponderan los intereses del Estado y la seguridad nacional sobre los derechos ciudadanos (como la USA PATRIOT Act o Ley Patriota y la USA Freedom Act o Ley Libertad).

Imagen 25



Protestas contra la Ley Patriota.



LA LEY PATRIOTA Y LA LEY LIBERTAD

Esta ley fue promulgada en el año 2001 y justificada en la ‘nueva amenaza global del terrorismo’, luego de los atentados del 11 de septiembre. Permite la intervención en la privacidad de ciudadanos y ciudadanas por parte del Estado para proteger la seguridad nacional, sobre la base de la “legítima defensa del Estado y la guerra preventiva frente a la lucha contra el terrorismo.”⁷¹

⁷¹ Espino, A. 2014. *La ley “Patriot Act” y el estado de excepción según Agamben*. <http://www.pensamientopenal.com.ar/system/files/2014/07/doctrina39412.pdf>



La ley amplió las facultades de las agencias de seguridad estadounidenses para establecer la vigilancia necesaria a nacionales y extranjeros, buscando impedir cualquier delito de terrorismo. Así se modificó parte de la legislación referida a la privacidad, incluyendo las garantías constitucionales.

Permite las interceptaciones telefónicas y electrónicas masivas, el almacenamiento de metadatos telefónicos, la revisión de la correspondencia, la restricción a sistemas de encriptación de empresas para permitir a las agencias de seguridad acceder a la información requerida.⁷²

Permite registros domiciliarios secretos, impone censura en medios de comunicación, juzga sospechosos en tribunales militares secretos, concede poderes extraordinarios a la policía, entre otras muchas disposiciones de este corte.⁷³

Edward Snowden, el ex analista de la Agencia Nacional de Seguridad (NSA), lanzó en 2016 la siguiente opinión sobre la legislación de su país en materia de protección a la privacidad de la ciudadanía:

“Desafortunadamente, ninguna de las reformas que ha llevado a cabo el Gobierno de Estados Unidos desde 2013 ha tenido en cuenta que, con la ley vigente, el gobierno puede monitorizar las actividades privadas de todo el mundo de manera indiscriminada, también a los ciudadanos estadounidenses (...). Bajo este paradigma, llamado “recolección a granel” por el gobierno y vigilancia masiva por el resto del mundo, no se necesita una orden judicial individual para interceptar y archivar secretamente tus actividades. (...) En los Estados Unidos no tenemos una ley de protección de datos: lo que hay son unas pocas leyes que regulan la privacidad en sectores muy particulares. El sector de servicios financieros y la industria de servicios médicos tienen alguna pequeña protección para el consumidor, pero, a no ser que se utilicen esos datos en un contexto muy específico, hay barra libre para manejar los datos. En vez de una legisla-

⁷² Pérez, J. 2019. *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos*. Universidad de Sevilla. Pág. 250.

⁷³ Espino, A. 2014. *La ley “Patriot Act” y el estado de excepción según Agamben*. <http://www.pensamientopenal.com.ar/system/files/2014/07/doctrina39412.pdf>

ción, lo que tenemos son esos contratos en los que cada proveedor de servicios establece los términos de servicio. Y en esos acuerdos de términos de uso, estás comprando software donde los términos pueden ser modificados unilateral e inmediatamente por el proveedor de servicio en cualquier momento. Usando ese servicio, estás de acuerdo con que te estafen y abusen de ti de manera permanente.”⁷⁴

Como consecuencia de las famosas revelaciones de Snowden, se aprobaron una serie de reformas materializadas en la Ley Libertad, sancionada en junio de 2015, poniendo freno a la recopilación masiva de datos realizada por el gobierno estadounidense.

El 1 de enero de 2019, entró en vigencia en el estado de California la primera ley de privacidad de datos en los Estados Unidos, otorgando a los californianos y californianas la propiedad sobre su información personal. Esto se traduce en que la ciudadanía de este estado tiene el poder de revisar qué información personal ha sido recabada por empresas en todo el mundo y puede obligar a dichas empresas a dejar de vender la información personal, igual que solicitar que se eliminen sus datos.

La nueva ley de privacidad de California (California Consumer Privacy Act, CCPA) plantea la protección de jóvenes usuarios de la red entre los 13 y los 15 años, pues las empresas deben obtener el consentimiento de sus padres o responsables, para vender la información que tienen de ellos.⁷⁵



⁷⁴ Pérez, J. 2019. *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos*. Universidad de Sevilla. Pág. 249.

⁷⁵ Univisión. 31 de diciembre de 2019. *Si vive en California, desde el 1 de enero una ley protegerá su privacidad en internet*. <https://www.univision.com/noticias/estados-unidos/si-vive-en-california-desde-el-1-de-enero-una-ley-protegera-su-privacidad-en-internet>



LEGISLACIÓN EN COLOMBIA



CONVENIOS INTERNACIONALES

Colombia participa en varios tratados internacionales de derechos humanos que contienen, de alguna forma, el derecho a la privacidad, la intimidad y la propiedad sobre la información. Según lo establecido en el Artículo 93 de la Constitución Política, los tratados y convenios ratificados por Colombia en materia de derechos humanos tienen rango constitucional, por lo que son de obligatorio cumplimiento y prevalecen sobre otras disposiciones legales.

Algunos de estos compromisos adquiridos son:

- La Declaración Universal de Derechos Humanos, que en su Artículo 12 establece:

“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.”

- El Pacto Internacional de Derechos Civiles y Políticos, ratificado por el Congreso de la República mediante la Ley 74 de 1968, que en el Artículo 17 señala:

“Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”

- El Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales, que indica en el Artículo 8.1: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.”

- La Convención Americana sobre Derechos Humanos, Pacto de San José de Costa Rica, ratificada por Colombia mediante la Ley 16 de 1972, que en su Artículo 11 establece:

“Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su

familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honor o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”

- La Convención Internacional para la Protección de Todas las Personas contra las Desapariciones Forzadas, que señala en el Artículo 19:

“1. Las informaciones personales, inclusive los datos médicos o genéticos, que se recaben y/o transmitan en el marco de la búsqueda de una persona desaparecida no pueden ser utilizadas o reveladas con fines distintos de dicha búsqueda. Ello es sin perjuicio de la utilización de esas informaciones en procedimientos penales relativos a un delito de desaparición forzada, o en ejercicio del derecho a obtener reparación.

2. La recopilación, el tratamiento, el uso y la conservación de informaciones personales, inclusive datos médicos o genéticos, no debe infringir o tener el efecto de infringir los derechos humanos, las libertades fundamentales y la dignidad de la persona.”

- La Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, de 1990, que plantea en su Artículo 14:

“Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques.”





CONSTITUCIÓN POLÍTICA DE COLOMBIA

La Carta Magna tiene en su articulado tres disposiciones referidas al derecho a la privacidad y a la información. El Artículo 15, el Artículo 20 y el Artículo 28, que plantea:

“Toda persona es libre. Nadie puede ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley.

La persona detenida preventivamente será puesta a disposición del juez competente dentro de las treinta y seis horas siguientes, para que este adopte la decisión correspondiente en el término que establezca la ley.

En ningún caso podrá haber detención, prisión ni arresto por deudas, ni penas y medidas de seguridad imprescriptibles.”

Imagen 26



Imagen alusiva a datos y metadatos.

HABEAS DATA

Habeas Data es una acción constitucional que confirma el derecho de todos los ciudadanos y ciudadanas para obtener, actualizar y rectificar toda la información recaudada sobre ellos en bancos y bases de datos; incluso solicitar borrarla. También refiere a los demás derechos, libertades y garantías constitucionales relacionados con la recolección, tratamiento y circulación de datos personales, como se expresa en el Artículo 15 de la Constitución.

En el año 2003 y cursando el primer mandato de Álvaro Uribe, el texto de este artículo fue modificado, introduciendo las líneas que se resaltan en negrilla y que responden al ‘espíritu antiterrorista’ de la Ley Patriota de EE. UU., la cual condujo a innumerables arbitrariedades.

“Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones, el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.”

De igual forma, el Habeas Data trata del derecho a la información establecido en el Artículo 20 de la Constitución Política, que reza:

“Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.”



Con la Ley 1266 de 2008 o Ley de Habeas Data, establecida por el Gobierno Nacional, se desarrollan los derechos constitucionales consagrados en los Artículos 15 y 20, particularmente en relación con la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. En el Decreto 2592 de 2010 se reglamentan los Artículos 12 y 13 de la Ley de Habeas Data; mediante el Decreto 1727 de 2009 se determina la forma en que los operadores de los bancos de datos deben presentar la información de los titulares.

De otro lado, la Ley Estatutaria 1581 de 2012 o Ley de Protección de Datos Personales dicta disposiciones generales para la protección de datos personales y es reglamentada parcialmente por el Decreto 1377 de 2013. Esta ley se plantea, igual que la Ley de Habeas Data, como

desarrollo de los derechos establecidos en los artículos ya mencionados de la Constitución. No obstante, señala que no se aplica a las bases de datos y archivos regulados por la Ley 1266 de 2018, relativas a Seguridad y Defensa de la Nación, a las que contengan información de inteligencia y contrainteligencia, ni a archivos mantenidos en un ámbito personal y doméstico.

En el Artículo 5º de la Ley 1581 de 2012 se definen los datos sensibles como “aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.”

La ley en mención es limitada en lo que se refiere a los datos personales en internet y por lo mismo, no contempla en sus definiciones toda la dimensión de lo que podrían constituir los datos personales en la era digital. Por tanto, la ley adolece de especificidad respecto a disposiciones que puedan impedir abusos por parte de empresas que prestan servicios de redes sociales o buscadores, u otras que utilizan esos datos personales para distintos fines, como la comercialización, la generación de propaganda personalizada, etc.

Tampoco está normado el uso de las llamadas ‘cookies’, software que permite la recolección de todo tipo de datos, desde la dirección IP hasta los hábitos de navegación de usuarios y usuarias de internet.

Otra limitación de la ley es el ámbito de aplicación territorial: se han presentado demandas de usuarios que no pueden ser procesadas por los organismos competentes pues plataformas de redes sociales como Facebook o buscadores como Google, alojan los datos de los usuarios en servidores que se encuentran fuera del país. Además, los medios con los cuales esas empresas dan tratamiento a la información se encuentran fuera del ámbito de aplicación de la ley. No hay mecanismos legales claros para que esas empresas, que gozan de millones de usuarios de nacionalidad colombiana, rindan cuentas del manejo que dan a los datos personales.



CÓDIGO PENAL

Sobre la comercialización de datos personales hay una sola normativa legal y es señalada en el Código Penal, que en el Artículo 269F impone pena de prisión a quien incurra en violación de datos personales:

“El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.”

Este artículo pertenece a una serie titulada ‘De la Protección de la Información y los Datos’, que va desde el Artículo 269A al 269J, imponiendo penas para las siguientes tipificaciones: obstaculización ilegítima de sistema informático o red de telecomunicación, daño informático, suplantación de sitios web para capturar datos personales, hurto por medios informáticos y semejantes, transferencia no consentida de activos.

El problema histórico de la seguridad de Estado en Colombia, con las transformaciones propias de la era digital, es tratado en el Artículo 269C:

“Interceptación de datos informáticos. El que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.”

El uso de software malicioso, utilizado como una forma de ataque a la información personal y usado sistema de interceptación por parte de la inteligencia colombiana es tratado en el Artículo 269E:

“Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.”



CÓDIGO DE PROCEDIMIENTO PENAL

El respeto al derecho a la intimidad de los colombianos y colombianas es establecido también por el Código de Procedimiento Penal, que en su Artículo 14 establece:

“Toda persona tiene derecho al respeto de su intimidad. Nadie podrá ser molestado en su vida privada. No podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos en este código. Se entienden excluidas las situaciones de flagrancia y demás contempladas por la ley. De la misma manera deberá procederse cuando resulte necesaria la búsqueda selectiva en las bases de datos computarizadas, mecánicas o de cualquier otra índole, que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones.”





El Artículo 235 del Código estipula las condiciones bajo las cuales la Fiscalía General de la Nación, autorizada por la Constitución en su Artículo 20, puede ordenar la interceptación de comunicaciones telefónicas y similares:

“El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación, así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación. En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva. Por ningún motivo se podrán interceptar las comunicaciones del defensor. La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron. La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.”



LEYES DE INTELIGENCIA

Luego del escándalo de las interceptaciones ilegales o ‘chuzadas’ del Departamento Administrativo de Seguridad (DAS), el entonces presidente Juan Manuel Santos expidió el Decreto 1704 de 2012, que autoriza realizar interceptación legal de las comunicaciones. El Artículo 1 del decreto define la interceptación legal de comunicaciones como “un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la ley”.

Este decreto obliga a los proveedores de telecomunicaciones (como Eme cali, Telebucaramanga, ETB y EPM) y a las redes de datos móviles (como

Claro, Tigo, Avantel y Movistar) a facilitar la monitorización del servicio por parte del Estado, como garante de la seguridad y la lucha contra el terrorismo, así como a colocar a disposición de las autoridades las diferentes herramientas tecnológicas, y el acceso a la información que recopilan de sus clientes. En ese sentido, el Artículo 2 de este decreto establece:

“Los proveedores de redes y servicios de telecomunicaciones que desarrollen su actividad comercial en el territorio nacional deberán implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de Policía Judicial cumplan, previa autorización del Fiscal General de la Nación o su delegado, con todas aquellas labores inherentes a la interceptación de las comunicaciones requeridas.”

En 2013, se adoptó la nueva Ley de Inteligencia y Contrainteligencia (1621 de 2013), regulada por el Decreto 857 de 2014. Esta ley controla a los organismos facultados para realizar actividades de inteligencia y contrainteligencia y establece lo pertinente a esas funciones. En el Artículo 2º se define la función de inteligencia y contrainteligencia como:

“(...) aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta Ley.”

En el Artículo 4 se definen los límites y fines de la función de inteligencia y contrainteligencia, señalando que:



"La función de inteligencia y constrainteligencia estará limitada en su ejercicio al respeto de los derechos humanos y al cumplimiento estricto de la Constitución, la Ley y el Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos. En especial, la función de inteligencia estará limitada por el principio de reserva legal que garantiza la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso."

El Artículo 5, referido a los principios de las actividades de inteligencia y constrainteligencia, es totalmente transgredido por las llamadas 'chuzadas' y en particular, el uso de software espía que permite la interceptación masiva:

"Principio de necesidad: La actividad de inteligencia y constrainteligencia debe ser necesaria para alcanzar los fines constitucionales deseados; es decir que podrá recurrirse a ésta siempre que no existan otras actividades menos lesivas que permitan alcanzar tales fines.

Principio de idoneidad: La actividad de inteligencia y constrainteligencia debe hacer uso de medios que se adecuen al logro de los fines definidos en el artículo 4 de esta Ley; es decir que se deben usar los medios aptos para el cumplimiento de tales fines y no otros.

Principio de proporcionalidad: La actividad de inteligencia y constrainteligencia deberá ser proporcional a los fines buscados y sus beneficios deben exceder las restricciones impuestas sobre otros principios y valores constitucionales. En particular, los medios y métodos empleados no deben ser desproporcionados frente a los fines que se busca lograr."

Con preocupación se observa que no existe un dictamen legal explícito que impida la vigilancia masiva, ejercida por las fuerzas de seguridad colombianas, a través de diversos sistemas de interceptación de comunicaciones. Tampoco hay una disposición que norme la adquisición y

el uso de tecnologías intrusivas de la vida privada de los ciudadanos y ciudadanas.

El superior jerárquico, establecido en el Artículo 15, no está facultado para ordenar interceptaciones de las comunicaciones sino, como lo plantea el Artículo 17, para el monitoreo del espectro electromagnético. La interceptación de comunicaciones sigue bajo el dictamen del Código Penal Procesal.

Privacy International, revisa el contenido de la Ley 1621 de 2013 y plantea que “el monitoreo del espectro electromagnético”, establecido en el artículo 17, carece de una definición precisa que puede conducir a equívocos, pues podría incluir monitorear correos electrónicos, mensajes de texto y llamadas telefónicas, interfiriendo en la privacidad de las personas.⁷⁶



⁷⁶ Privacy International. 2015. *Un estado en la sombra: vigilancia y orden público en Colombia*. https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf.



Aunque la Corte Constitucional, luego de evaluar dicha ley, ratificó que se encuentra conforme a la Constitución y ceñida a las obligaciones internacionales sobre derechos humanos, Privacy afirma que:

“La decisión de la Corte se basa en la idea de que hay una forma de “monitorear” el espectro electromagnético que no comporta interferencia en la privacidad de las comunicaciones. Es decir que los mensajes de correo electrónico y de texto y las llamadas de teléfono transmitidas por el espectro electromagnético pueden filtrarse, analizarse y monitorearse sin violar la integridad de la comunicación ni, por tanto, la privacidad de la persona que envía o recibe la comunicación. Tal conclusión no es del todo incorrecta, pero se aplica a un conjunto sumamente limitado de actividades. Las únicas acciones en que posiblemente se podría “monitorear” el espectro electromagnético sin interferir de ningún modo en la privacidad de la comunicación serían las de los detectores térmicos y los instrumentos de orientación y antenas, por ejemplo. Todas las demás formas de “monitoreo” del espectro electromagnético hacen necesaria una interferencia (con una comunicación) de un tipo que sólo permite concluir que el monitoreo ha resultado en la intercepción de la comunicación.”⁷⁷

Imagen 27



Labores de inteligencia y contrainteligencia de los organismos colombianos.

⁷⁷ Ibídem. Pág. 36.



CÓDIGO DE POLICÍA Y CONVIVENCIA

El nuevo Código de Policía (Código Nacional de Policía y Convivencia para Vivir en Paz), que empezó a regir en enero de 2017, ha sido fuertemente criticado y ha recibido alrededor de 151 demandas, presentadas a la Corte Constitucional, por sus diversas irregularidades.⁷⁸

En lo que se refiere al derecho a la privacidad, el Código plantea en el Artículo 32 la siguiente definición de privacidad de las personas:

“(...) el derecho de ellas a satisfacer sus necesidades y desarrollar sus actividades en un ámbito que le sea exclusivo y por lo tanto considerado como privado. No se consideran lugares privados:

1. Bienes muebles o inmuebles que se encuentran en el espacio público, en lugar privado abierto al público o utilizados para fines sociales, comerciales e industriales.
2. Los sitios públicos o abiertos al público, incluidas las barras, mostradores, áreas dispuestas para: almacenamiento, preparación, fabricación de bienes comercializados o utilizados en el lugar, así como también las áreas dispuestas para el manejo de los equipos musicales o disc jockey y estacionamientos a servicio del público.”



⁷⁸ El Espectador. 11 de junio de 2019. *¿Cómo ha cambiado el Código de Policía por decisiones de la Corte Constitucional?* <https://www.elespectador.com/judicial/como-ha-cambiado-el-codigo-de-policia-por-decisiones-de-la-corte-constitucional-article-865310/>



Esta definición ha resultado estrecha para algunas organizaciones de defensa de la privacidad, asegurando que:

“(...) la disposición parece confundir el derecho a la privacidad con el derecho al desarrollo sin trabas de la personalidad, así como con el derecho a la inviolabilidad del hogar. Por lo tanto, al vincular el derecho a la privacidad con la existencia de espacios físicos privados, excluye de la protección de la privacidad a cualquier persona o activos (como automóviles o dispositivos electrónicos como computadoras portátiles o teléfonos celulares) colocados en lugares públicos, incluidos bares, restaurantes, etc., dejando también en un área gris legal actos privados que pueden tener lugar en un espacio público.”⁷⁹

La caracterización de ‘espacio público’, en el Artículo 139, resulta demasiado amplia cuando establece que el espectro electromagnético hace parte de esta esfera. El espacio público es definido previamente por la ley como “el conjunto de muebles e inmuebles públicos, bienes de uso público, bienes fiscales, áreas protegidas y de especial importancia ecológica y los elementos arquitectónicos y naturales de los inmuebles privados, destinados por su naturaleza, usos o afectación, a la satisfacción de necesidades colectivas que trascienden los límites de los intereses individuales de todas las personas en el territorio nacional.”

Hay una preocupante relación entre la anterior caracterización y el planteamiento del Artículo 237 sobre Integración de Sistemas de Vigilancia, que señala: “La información, imágenes y datos de cualquier índole captados y/o almacenados por los sistemas de video o los medios tecnológicos que estén ubicados en el espacio público, o en lugares abiertos al público, serán considerados como públicos y de libre acceso (...).”

Las comunicaciones privadas que viajan a través del espectro electromagnético quedarían excluidas de la protección de la privacidad, pues serían consideradas públicas y de libre acceso.

⁷⁹ Dejusticia, Fundación Karisma y Privacy International. 2019. *The State of Privacy in Colombia*. <https://privacyinternational.org/state-privacy/58/state-privacy-colombia>. Pág. 7.

“El nuevo Código de Policía no parece tener en cuenta los complejos cambios tecnológicos que afectan la comunicación moderna. Por lo tanto, no está claro cómo se protege la privacidad de las comunicaciones digitales y de los espacios en línea, dadas las definiciones muy restrictivas de privacidad y espacio público incluidas en el Código.”⁸⁰



UNA LEGISLACIÓN PARA AMPLIAR Y CORREGIR

Si bien la legislación colombiana admite el derecho humano a la privacidad o intimidad y contiene un conjunto de normas que buscan la protección de datos personales y datos financieros, al igual que algunas disposiciones contra delitos informáticos y normas concernientes a actividades de inteligencia y contrainteligencia, la contratación, entrada y uso de tecnologías de la información, no tienen las restricciones necesarias para garantizar debidamente estos derechos.

En la actualidad y en medio de los escándalos, se conoció que existen dispositivos, aplicaciones, medios y formas de ataque a la información que atentan contra el derecho de intimidad sin que la legislación lo regule expresamente, como el fenómeno de la vigilancia masiva a través de sistemas como Hombre Invisible o SIGD.

Algunas organizaciones no gubernamentales nacionales e internacionales pugnan por la plena garantía del derecho a la privacidad. La era digital plantea grandes desafíos en este sentido y cada día aparecen nuevos elementos para su revisión. El análisis de nuestra legislación en esta materia es fundamental, pues constituye un nuevo campo de disputa en un país que, como sabemos, no se caracteriza por velar ni promover la defensa de los derechos humanos y al contrario, ha sido tradicionalmente el agente principal de su vulneración.

⁸⁰ Ibídem. Pág. 10.

CAPÍTULO 4



¿CÓMO PROTEGERNOS? UNA SEGURIDAD DIGITAL POSIBLE





*"No quiero vivir en una sociedad que hace este tipo de cosas.
No quiero vivir en un mundo donde se registra todo lo que hago y digo."*

EDWARD SNOWDEN

UNA CARTA COLOMBIANA AL RELATOR ESPECIAL SOBRE EL DERECHO A LA PRIVACIDAD

El 14 de marzo de 2016, la Fundación Karisma, Dejusticia, la Fundación para la Libertad de Prensa (FLIP) y la Comisión Colombiana de Juristas (CCJ) enviaron una carta al Relator Especial sobre el Derecho a la Privacidad, con el propósito de documentarlo para el ejercicio del mandato encomendado por el Consejo de Derechos Humanos. La misiva gira en torno a seis temas que en Colombia determinan la garantía y el respeto del derecho a la intimidad en la era digital.

- Legislación:** Las organizaciones señalan que la regulación colombiana sobre el tema es insuficiente o inapropiada, enunciando como ejemplo el monitoreo del espectro electromagnético que está permitido a las fuerzas policiales y de inteligencia sin control judicial. Igualmente, el hecho de que los proveedores de servicios de telecomunicaciones deben proporcionar toda la información requerida para investigaciones penales y conservar la información de cada usuario por 5 años para dichos efectos. En tercer lugar, que no hay controles efectivos a las actividades de inteligencia y contrainteligencia: la legislación colombiana no prevé controles y supervisión a estas actividades, la Comisión Legal de Seguimiento, conformada por 8 congresistas, aun no funciona. Como cuarto punto, la prohibición del envío de "mensajes en lenguaje cifrado o ininteligible", así como el hecho de que la Policía utiliza software de hackeo y que hay dos bases de datos de víctimas del conflicto armado que se sospecha que no están debidamente protegidas. Por último, la reserva de los



documentos de inteligencia es absoluta y los organismos que ejercen inteligencia no rinden cuentas.

2. **Comisión asesora de depuración de archivos de inteligencia:** “En Colombia existe un legado de abusos y uso ilegítimo de las actividades de inteligencia y contrainteligencia, que se hizo especialmente evidente durante la década del 2000. Una de las herramientas contempladas por la ley de inteligencia y contrainteligencia para garantizar que el almacenamiento de la información que reposa en las bases de datos de estos organismos no transgreda los fines y límites legales de este tipo de actividades, fue la creación de una Comisión Asesora para la Depuración de Datos y Archivos de Inteligencia y Contrainteligencia. Esta comisión está encargada de formular recomendaciones al Gobierno Nacional sobre los criterios de permanencia, retiro y destino de los mismos. Para ello, se le ha dado un periodo de trabajo de dos años, que vence en julio del presente año. Este proceso debería concluir con un plan estructural de depuración, dirigido a salvaguardar el derecho a la intimidad de las personas cuya información fue arbitraria o ilegalmente recaudada, y resolver las eventuales tensiones que surjan entre la seguridad nacional y el derecho a la intimidad, de un lado, y el derecho a la verdad, a la memoria y al acceso a la información pública, de otro. A este respecto, serían muy apreciados el conocimiento y las eventuales recomendaciones del Relator.”
3. **Aumento de capacidad para hacer vigilancia selectiva y masiva:** Las fuerzas de seguridad siguen adquiriendo equipos de interceptación que se usan de forma ilegal, en ocasiones contra personas defensoras de derechos humanos que han sido posteriormente desparecidas. El sistema de interceptación PUMA, que fue retenido por la Fiscalía por su uso ilegítimo, estaría siendo reactivado por la Policía. Los sistemas de interceptación y monitoreo PUMA y SIGD no tienen controles adecuados, pese a los escándalos recientes de interceptaciones ilegales.

4. **Hostigamientos a defensores y defensoras de derechos humanos y periodistas:** La carta plantea que Colombia reporta índices muy altos de agresiones contra estos ciudadanos y ciudadanas, amenazados frecuentemente por medios electrónicos, sin encontrar respuesta adecuada de las autoridades. Existen denuncias de que se presentan robos de información relacionada con la violación de derechos humanos. Continúan los hostigamientos contra periodistas y seguimientos, escuchas e interceptaciones ilegales por parte del Ejército, como la 'Operación Andrómeda', contra personajes vinculados al proceso de paz y su defensa.
5. **Cultura de protección a la intimidad en la era digital:** Las organizaciones plantean que se requiere comenzar en Colombia un proceso de alfabetización digital, para fomentar una cultura de la protección a la intimidad, pues la masificación del uso de la red ha multiplicado la miseria, el racismo, la xenofobia, la homofobia y demás formas de discriminación.
6. **Política pública de seguridad digital – COMPES:** Por último, el documento expone que en ese momento Colombia afrontaba un proceso de formulación de política pública de seguridad digital que, si bien tenía el compromiso del Gobierno con el respeto a los derechos humanos, apuntaba a su incumplimiento. El enfoque de esta política enfatiza en la seguridad bancaria y comercial y no en las injerencias arbitrarias o ilegales en la intimidad de las personas, especialmente las que son defensoras de derechos humanos, víctimas del conflicto armado, periodistas, de la oposición política y temas relacionados.



REDUCIR LOS RIESGOS EN UN CAMPO MINADO

Hemos visto a lo largo de este trabajo que nuestra información está siendo atacada por varios flancos, por lo que debemos tomar medidas para no contribuir facilitar dichos ataques, en la medida de lo posible. Navegar en internet es un deleite y un hábito, al igual que tomar cotidiana y ansiosamente el teléfono móvil.

Sin embargo, hay varios clics que podemos evitar y que pueden hacer más seguro nuestro andar por la red y por nuestros propios computadores y dispositivos electrónicos. Así como la seguridad offline de un defensor y defensora de derechos humanos requiere protocolos de seguridad (evitar ciertos lugares, horarios y personas, junto a otras normas que deben convertirse en hábitos), la seguridad digital exige una actitud todavía más rigurosa, pues se trata de la información que puede hacernos realmente vulnerables.

Es imprescindible modificar nuestras costumbres de uso, tanto de los dispositivos como de nuestra forma de entrar y permanecer en la red. La seguridad digital no es solamente la seguridad de nuestra información, se trata de la seguridad personal. Es de suma importancia preservar los derechos a la privacidad, la libre expresión, la asociación, la investigación y el derecho mismo a la ida.

Partimos entonces de la idea de que el centro de la seguridad digital o la ciberseguridad es la protección de las personas y de los derechos humanos. En tal sentido, compartimos la definición de seguridad digital que desarrolla el grupo ‘Una internet libre y segura’ de la Freedom Online Coalition:

“La ciberseguridad es la preservación, a través de políticas, tecnología y educación de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente a fin de mejorar la seguridad de las personas tanto online como offline.”⁸¹

⁸¹ Sequera, M., Toledo, A. & Ucciferri, L. 2018. *Derechos Humanos y Seguridad Digital: Una Pareja Perfecta*. Diantres. https://www.academia.edu/36171255/Derechos_humanos_y_la_seguridad_digital. Pág. 6.

Por otro lado, dado que el marco jurídico de nuestro país está en deuda en lo que a protección a la privacidad se refiere y partiendo de la situación de violencia contra liderazgos sociales y políticos, cada persona defensora de derechos humanos tiene una responsabilidad concreta frente a su información personal, la de las comunidades y organizaciones con las que trabaja.

En este capítulo se expondrá, de la forma más didáctica y pedagógica posible una serie de recomendaciones básicas para incorporar paulatinamente en nuestra cotidianidad y convertirlas en prácticas de seguridad digital.

INFOGRAFÍA 6. Tipos de seguridad digital

HARDWARE O FÍSICA  A central computer monitor is connected by red arrows to various physical devices: a camera, a hard drive, a laptop, a desktop tower, a keyboard, a mouse, a printer, a scanner, a power strip, and a pair of shoes.	Se refiere a algunos recursos físicos que ayudan a garantizar la seguridad de nuestros dispositivos.
SOFTWARE O LÓGICA  Logos for Windows, Macintosh, and Linux operating systems.	Son programas que nos ayudan a mantener segura la información en nuestros dispositivos.
DE RED  Three blue user profile icons representing network users.	Es un nivel de seguridad avanzado que busca mantener la red de nuestra organización protegida ante posibles ataques. Se implementa tanto en hardware como en software.



INFOGRAFÍA 7.

Tipos de información

PÚBLICA  INTERNET	Es la información que se maneja públicamente y que además es de nuestro interés que se conozca.
PRIVADA O PERSONAL 	Es un tipo de información que, sin llegar a ser secreta, sí tiene reservas y no es de carácter público. Por ejemplo: nombres de familiares, estado de salud, cuentas bancarias, etc.
SECRETA O CONFIDENCIAL 	Es la información sensible que un número muy reducido de personas debe conocer, ya sea por razones éticas, de seguridad, organizacionales, políticas o de cualquier otro tipo.

Como recomendación principal, proponemos establecer los tipos de información que manejamos en las redes y en nuestros dispositivos para dar en cada caso el tratamiento requerido, priorizando la seguridad de la información, de nosotros mismos y de las personas con las que nos relacionamos en nuestros entornos personales, laborales, comunitarios y políticos.





RECOMENDACIONES PARA LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL Y DE LAS ORGANIZACIONES

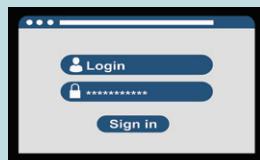
INFOGRAFÍA 8.

Tips y características de una contraseña segura

Cada uno de nuestros dispositivos (computadoras, tablets, teléfonos, memorias USB, discos duros extraíbles) deben contar con una contraseña, un pin o un patrón de desbloqueo, que impidan el acceso inmediato a nuestra información.

Aquí los elementos básicos de una contraseña relativamente segura:

Usar contraseñas robustas: Deben ser largas, entre más larga más segura. Debe contener caracteres, combinar mayúsculas y minúsculas. No incluir información personal para evitar que sea deducida fácilmente.



Usar contraseñas únicas: Cada dispositivo y cada acceso a un sitio de internet debe tener una contraseña diferente. No se debe usar la misma contraseña para varios dispositivos, ingresos a correos electrónicos o sesiones en sitios web o aplicaciones.

Mantener las contraseñas secretas: No se debe compartir la contraseña con otras personas, a menos que sea absolutamente necesario. Si se comparte una contraseña con un(a) amigo(a), familiar o colega, debe ser una contraseña temporal y luego debe ser cambiada cuando ya no se use más.

A menudo, hay alternativas para compartir una contraseña, como crear una cuenta separada para cada persona que necesite acceso. Mantener la contraseña secreta también significa prestar atención a quién puede estar leyendo sobre los hombres cuando la estemos escribiendo.



Usar un gestor de contraseñas: El que encontramos ampliamente recomendado es el KeePass, que existe para plataformas de Windows, Mac y Linux.



EJEMPLOS DE CONTRASEÑAS SEGURAS

- Luni74c0ns3n71d4c0L64d4d3lc13l0 (Lunita consentida colgada del cielo)
- ¿99lamazorcaestaqu3m4d4! (¿la mazorca está quemada!)



INFOGRAFÍA 9.

Medidas de protección para el teléfono móvil



Los llamados teléfonos inteligentes, ya sean Android, Windows o Apple (iOS), vulneran de forma permanente la seguridad de la información. No se trata solamente de los datos que tengamos alojados en ellos sino de que estamos obligados a proporcionar información personal para acceder a las aplicaciones que ofrecen las tiendas digitales: nombre, ubicación geográfica, correo electrónico y toda la información que hay en él, junto a otros requerimientos.

Dependiendo de nuestra necesidad podemos dar información cierta, falsa o medias verdades. Aun así, los teléfonos proporcionan, segundo a segundo, información de lo que hacemos y decimos: el micrófono está transmitiendo ininterrumpidamente, al igual que la cámara; todo lo que decimos y/o grabamos está siendo transmitido por nuestros teléfonos que están conectados de manera permanente a internet.

El teléfono móvil es el dispositivo que más información suministra sobre nosotros. En 2009, Malte Spitz solicitó a la compañía Deutsche Telekom que le entregara toda la información que tuviera sobre él.

Inicialmente, la compañía se negó; luego de algunas demandas legales, DTAG entregó un registro de tan sólo 6 meses de datos en un archivo de Excel, con 35.830 líneas de información. Con esta información, Spitz ex-

hibió en 2011 un mapa en el cual podemos ver toda la información que el usuario género en esos 6 meses⁸²: con quién habla y por cuánto tiempo, cuándo duerme, cuándo come, dónde está, entre otros datos.⁸³

A continuación, unas recomendaciones mínimas para proteger y protegerse del celular:

Establecer con claridad la información que debe estar permanentemente en el teléfono; lo demás debe ser almacenado en computadoras, discos duros o nubes; si es posible, de manera encriptada.

Usar contraseñas robustas o pins. Una contraseña distinta para cada dispositivo. No es conveniente usar la huella digital o el desbloqueo facial, estas herramientas no son muy seguras.

Decidir bien qué se sincroniza con la nube. Si se borra una foto o algún archivo, puede que ya esté respaldado en la nube.

Configurar el teléfono para que no muestre detalles de las notificaciones en la pantalla.

Usar las aplicaciones estrictamente necesarias y aquellas de las que se conozca su procedencia.

Tener cuidado con los permisos que las aplicaciones solicitan. En términos generales, son contactos, mensajes, galería de fotos y videos, ubicación y algunos otros específicos.

No guardar información confidencial o sensible por mucho tiempo en el celular.

De ser posible, mantener cifrada la información en el dispositivo.

No llevar teléfono móvil si participa en alguna reunión confidencial. Este sigue transmitiendo información a través del GPS, el micrófono y la cámara, aunque esté apagado.

Llevar o no llevar el celular personal a las marchas o jornadas de movilización es el dilema. En caso de portarlo, se debe ser consciente de que estará siendo monitoreado/a por programas que toman y guardan información que puede ser usada en contra posteriormente. Durante 5 años puede utilizarse dicha

⁸² <https://www.zeit.de/datenschutz/malte-spitz-data-retention>

⁸³ Fundación Karisma. 8 de mayo de 2019. *Malte Spitz, una experiencia tangible de la retención de datos*. <https://web.karisma.org.co/malte-spitz-una-experiencia-tangible-de-la-retencion-de-datos/>



información con validez para cualquier proceso jurídico; para tareas de inteligencia del Estado no tiene vencimiento.

Tener un teléfono para manejar información pública. Este dispositivo sí debería portarse en marchas, plantones y otras jornadas de protesta, ya que puede servir para grabar atropellos y excesos de la fuerza pública. Las transmisiones en vivo son una herramienta bastante útil porque, aunque el teléfono sea arrebatado, esta información ya está en la red.

No permitir que la Policía revise el celular. No es legal, solamente está autorizada a solicitarlo para revisar y verificar que no esté reportado como robado, en cuyo caso, las autoridades deben pedir que se digite *#06# para visualizar el IMEI⁸⁴.

No es permitido revisar su contenido, a menos que tengan una orden judicial (Artículo 159 de la Ley 1801 de 2016; Artículo 269A del Código Penal). En caso de que la Fuerza Pública tome el teléfono sin una orden judicial, se debe registrar el número de placa del funcionario y presentar una denuncia.

Evitar revelar la contraseña si confiscan el celular.

Colocar un autoadhesivo a la cámara para que sólo pueda fotografiar y grabar las imágenes que el usuario desee. Esto es válido también para computadores y tabletas. Organizaciones como Colnodo ofrecen kits de seguridad digital⁸⁵, en los que se incluye bloqueador del micrófono.

Utilizar aplicaciones que permitan eliminar los mensajes automáticamente.

Una sugerencia de Snowden que se puede usar en casos extremos es quitarle al teléfono el micrófono y la cámara, de tal manera que ninguno de los dos pueda grabar ni enviar ningún tipo de información.

El GPS sigue transmitiendo nuestra ubicación. No es útil el modo avión, ni apagarlo, ni quitarle la pila.

⁸⁴ International Mobile Equipment Identity (IMEI), es un identificador único que tiene cada teléfono móvil.

⁸⁵ <https://escueladeseguridadaddigital.co/esd-lanza-la-segunda-version-del-kit-de-seguridad-digital-conocela/>



INFOGRAFÍA 10.

Cuadro comparativo entre las aplicaciones de mensajería instantánea

WhatsApp	Telegram	Signal
		
Número de teléfono móvil	Número de teléfono móvil	Número de teléfono móvil
Número de tus contactos (los que usan WhatsApp y los que no)	Nombre de perfil, foto y descripción	
Nombre de perfil, foto y mensaje de estado	Correo electrónico (para utilizar la verificación de dos pasos y la recuperación de la cuenta)	
Correo electrónico (para utilizar la verificación de dos pasos y la recuperación de la cuenta)	Número de tus contactos (los que usan Telegram y los que no)	
Grupos a los que te uniste y listas de difusión en las que estas asociado	Ubicación mediante el GPS (al utilizar las funciones de compartir ubicación)	
Ubicación aproximada (a través de la IP y el número de teléfono)		
Ubicación mediante el GPS (al utilizar las funciones de compartir ubicación)		
Información sobre el dispositivo y la conexión: modelo, sistema operativo, navegador, idioma, zona horaria, dirección IP e información de la red móvil (potencia de la señal y proveedor)		
Actividad: cómo y cuándo utilizas el servicio (incluido cuando interactuas con una empresa) y el tiempo, la frecuencia y la duración de tus actividades e interacciones. Archivos de registro, informes de diagnósticos, error y rendimiento		



Funcionalidad	WhatsApp	Telegram	Signal
Cifrado extremo a extremo	Mensajes si. Metadatos no	Solo en chats secretos	Si incluso metadatos
Eliminar mensajes	Si	Si	Si
Mensajes temporales (Autodestrucción)	Si. Después de 7 días	Si. En 1 o 7 días en chats normales. A partir de 1 segundo en chats secretos	Si
Backup	Si. Sin cifrar en Google Drive	Si. En nube propia	Solo local
Verificación en dos pasos	PIN opcional	PIN opcional	PIN de bloqueo por defecto
Bloqueo de aplicación	Si, por huella	Si, PIN y huella	Si, bloqueo Android
Bloqueo de capturas de pantalla	No	Solo en chats secretos	Si
Enmascarar IP en videollamadas	No	Si	Si
Remitente confidencial	No	Parcial	Si
Notificaciones sin contenido	No	Si	Si

Fuente: <https://www.welivesecurity.com/la-es/2021/05/27/privacidad-diferencias-entre-whatsapp-telegram-signal/>



INFOGRAFÍA 11.

Formas de blindaje y medidas de protección para computadores, tablets y dispositivos de almacenamiento portables

En la vida cotidiana, un defensor y una defensora de derechos humanos manejan información en el computador de la oficina y en el equipo personal (portátil o de escritorio), además de usar memorias USB y algunas veces discos externos.

Vamos a enumerar recomendaciones básicas para mantener la seguridad digital de la información contenida en el computador, la tableta y los dispositivos portables de almacenamiento:

Determinar los niveles de información que se tiene en los equipos: confidencial, privada y pública. Proceder luego a establecer lugares concretos de almacenamiento: ya sea en discos externos, en el disco del computador o en unidades virtuales.

Respaldar la información de los dispositivos regularmente, basándose en un protocolo que indique qué, cuándo, dónde y con qué frecuencia. Este hábito permite tener resguardada la información en caso de sustracción, manipulación u otros ataques y a la vez, permite trabajar en computadores y tablets con mayor rendimiento.

Observar los dispositivos donde se conectan memorias USB y discos duros portables. Si la información en ellos es lo suficientemente sensible, debería estar cifrada y con protección tanto de copiado como de escritura. Así, cuando se conecten a un computador, este no podrá: a) copiar en ellos ningún tipo de virus ni de información, a menos que se le permita explícitamente y b) hacer copias de los archivos que se encuentran en ellos, a menos que sea autorizado de manera explícita. Algunos de estos dispositivos ya vienen con una protección desde el momento mismo de su adquisición.

Cifrar todos los dispositivos (teléfonos celulares, memorias, discos duros, computadores y tablets). Así, en caso de que se pierdan o sean robados, no se podrá acceder fácilmente a la información personal o de la organización.

En lo posible, usar el sistema operativo Linux.

Actualizar con regularidad el sistema operativo del computador y la tableta.

Utilizar bloqueo de pantalla.

Utilizar contraseña en todos los dispositivos.



Utilizar una contraseña de BIOS⁸⁶, si el sistema operativo es Windows.

Utilizar un software conocido y/o de procedencia confiable, así como no saturar los dispositivos con software innecesario.

Instalar y actualizar un antivirus en todos los dispositivos.

Desfragmentar discos duros regularmente.

Tabla 1. Algunas recomendaciones generales para el manejo de la información según los computadores usados.

Programas	Personal	De uso compartido	Público/Cybers
Contraseña 	Debe tener contraseña segura.	Tener usuario propio y contraseña segura.	Usar memorias USB con programas portables.
Cifrado 	De ser posible debemos tener el disco duro y todo su contenido cifrado.	Puedes tener carpetas cifradas y/o ocultas para mantener tu información segura, cifrar la información.	Cifrar la información en la memoria USB.
Sistema operativo 	El sistema operativo más seguro es Linux, debes revisar cuál de sus versiones se acomoda más.		
Navegador 	Se recomienda usar Firefox que es de código abierto Tor, el navegador más seguro.	se recomienda usar Tor o Firefox y navegar en modo oculto. Se puede correr el navegador desde una memoria USB.	Memoria USB con tor y navegar en modo oculto.

Nota: En términos generales sugerimos emplear programas *Open source* (código libre), aunque todos no son gratuitos, ya que conllevan demasiado trabajo diseñarlas y programarlas si son sin costo alguno para el usuario (aunque esperan apoyo con algo de dinero), y el código de programación ha sido realizado de manera abierta y colaborativa. Debemos recordar que estos programas en su versión portátil se encuentran fundamentalmente para SO de Windows.

⁸⁶ “BIOS es la abreviatura de Binary Input Output System y es un software que reside en un chip instalado en la tarjeta principal del computador, que realiza su tarea apenas presionamos el botón de encendido del equipo. También es el primer programa que se ejecuta al encender el PC.” (*¿Qué es la Bios?*, sf).

 SISTEMAS OPERATIVOS

Un sistema operativo es el software o conjunto de programas informáticos que gestiona los recursos y herramientas de la máquina física. Hay por lo menos 80 sistemas operativos, entre los que se encuentran Windows, Mac OS, Unix, Solaris, FreeBSD, OpenBSD, Debian y GNU/Linux.

Windows es el sistema operativo menos seguro y a la vez el más usado; le siguen Mac y Linux.



Tabla 2. Seguridad de los Sistemas Operativos.

Tabla 2. Seguridad de los Sistemas Operativos.		
Windows	Mac	Linux
<p>El menos seguro de los Sistemas operativos, con varios huecos de seguridad. Implementa parches para subsanar sus debilidades.</p> 	<p>Número Sin ser el mejor, es más seguro que Windows, existe el mito de que no hay virus para Mac. teléfono móvil</p> 	<p>Sistema operativo de código abierto, es el más seguro de estos tres, tiene como debilidad que los programas son tan amigables como en las plataformas anteriores. Pero, definitivamente es el más seguro.</p> 



PROGRAMAS PORTÁTILES

Existe una serie de programas portátiles para todas las plataformas y/o sistemas operativos. Se recomienda usar aplicaciones portátiles para las computadoras que tienen Windows y son de uso compartido o públicas. Se puede tener una serie de aplicaciones (Word, Firefox, descompresores, etc.) que se ejecuten desde una memoria USB para no dejar huella en los archivos temporales de Windows.



BORRADO SEGURO

No sólo debemos preocuparnos por la información que queremos guardar de ojos ajenos en lugares seguros sino también por aquella información que queremos eliminar. En términos generales, no es posible borrar información de nuestros dispositivos, por lo que se sobrescribe encima de dicha información para transformarla.

Un archivo está compuesto de paquetes de bits. Un bit es un cero (0) o un uno (1). Un byte es un paquete de 8 bits, compuestos de ceros y unos:⁸⁷

⁸⁷ Según un informe de Fox News sobre los avances de almacenamiento en el 2013, se sabe que la NSA creó un Data Center en Utah con capacidad de entre 1 ZettaByte (1 billón de TeraBytes) y 1 YoyaByte (mil billones de Terabytes). Estos discos pueden almacenar hasta nueve veces la cantidad de información que circula en internet en un año.

<https://www.businessinsider.com/pictures-of-the-nsas-utah-data-center-2013-6/>

Tabla 3. Composición de un archivo.

1 byte =

0	1	1	1	0	0	1	0
---	---	---	---	---	---	---	---

 Código Binario

1 kilobyte son 1024 bytes (1 Kb)
 1 megabyte son 1024 kilobytes (1 Mb)
 1 gigabyte son 1024 megabytes (1 Gb)
 1 terabyte son 1024 gigabytes (1 Tb)

Y así hasta los ahora conocidos *Pentabits*, *Yottabits* y *Zettabits*.

Elaboración propia

Para hacernos una idea de cómo es un archivo, aquí una ilustración de éste como un grupo de paquetes que contempla tres secciones:

Tabla 4. Estructura de un archivo.



Elaboración propia

Los paquetes del archivo en el disco duro (Hard Disk) están copiados de manera aleatoria, no secuencial.

Es así como el encabezado le indica al lector del disco cuántos paquetes son y cuál es el orden en que debe leerlos. La cola indica que es el último de los paquetes. Cuando borramos un archivo este realmente no se borra; simplemente el programa está indicándole al sistema operativo que puede usar ese espacio en caso de ser necesario, lo que significa que el archivo en cuestión sigue ahí y que si se diera la situación en que el sistema operativo reescribiera sobre ese espacio, aun así quedarían partes del archivo en otros lados.



Se recomienda entonces que, así como se deben usar programas de criptografía para mantener segura la información sensible, se deben usar programas de borrado seguro. Estos reescriben sobre el espacio específico en donde se encuentran todas las partes del archivo original. Sin embargo, los expertos indican que es posible recuperar, si no toda la información, sí parte de ella.

Si se quiere recuperar un archivo, existen programas de fácil acceso y manejo. Uno de esos programas es Recuva, que nos permite recuperar información que ha sido eliminada y es de gran ayuda, aunque no se compare con los potentes recuperadores que tienen programadores, tanto privados como estatales.



PROGRAMAS DE BORRADO RELATIVAMENTE SEGURO

Si el objetivo es no dejar el más mínimo rastro de la información, se recomienda un martillo, teniendo en cuenta que, si el disco es Hard Disk, el cual funciona como un disco de acetato, un martillazo puede ser efectivo. Pero si es un disco sólido o SD, dado que almacena la información en chips distribuidos, la destrucción debe ser total y absoluta para que no queden partes con información. De seguro se necesitan unos cuantos martillazos.

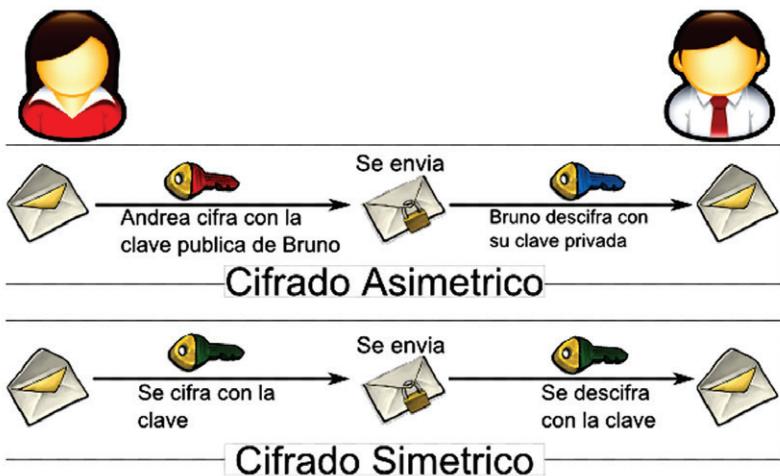
De cualquier forma, es mejor encriptar la unidad sólida antes de empezar su uso. Se expuso arriba que el borrado seguro consiste en la reubicación de las diferentes partes del archivo y la sobreescritura en ellas con ceros y unos de manera aleatoria. Algunos programas lo hacen 3 veces y otros hasta 50 veces, generando menor posibilidad de recuperación. Por supuesto que entre más veces se reescribe, más lento será el proceso de borrado.

A continuación, algunos programas. También se pueden visitar las páginas oficiales de los fabricantes de discos duros, allí también se ofrecen programas propios para este tipo de borrado.

Tabla 5. Programas de borrado seguro según SO.

Windows	Macintosh	Linux
Cleaner: Este programa además de borrar archivos temporales (en Windows hay muchos), realiza también una limpieza de cookies. Él te permite realizar borrado normal (rápido) y borrado seguro (con 35 pasadas). (Guzmán, 2017)	El mismo sistema operativo tiene una herramienta que permite este proceso, luego de borrar la información y de limpiar la basura.	BleachBit: de las pocas herramientas de borrado seguro en Linux con interfaz gráfica.
File Shredder: este programa realiza borrados con hasta 50 pasadas	En herramientas de disco pedimos borrar el espacio libre, este proceso puede hacerse en tres niveles dependiendo de lo seguro que deseas el borrado y de la disponibilidad de tiempo.	Wipe: Este es un programa de borrado seguro que funciona desde la consola. KillDisk: aplicación nativa para Linux, permite borrar varios discos a la vez, soporta tamaños máximos de 4 TB, (Yubal, 2017).

Elaboración propia





CIFRADO O ENcriptación

Es un método de codificación de la información que será almacenada o transferida. “Consiste en aplicar un patrón matemático a un conjunto de datos y cifrarlo de forma que parezca incomprensible para aquellos que no conozcan el método de descifrarlo o la clave.”⁸⁸

Tabla 6. El Cifrado.

Pros	Contras
Mantiene la información “segura”. Es difícil acceder a la infomración sin la clave que la protege.	Relentiza el sistema, este tarda más en iniciar y algunos procedimientos los hace más lentamente.
Elaboración propia	

Existen dos técnicas para proteger nuestra información: la criptografía y la esteganografía, técnicas tan antiguas como la humanidad.



CRIPTOGRAFÍA

La criptografía sirve para cifrar nuestra información. Aunque otras personas puedan verla, su contenido no es comprensible; se requiere una clave para acceder a la información. Hay dos formas de criptografía:

- Simétrica o convencional:** Consiste en que cada una de las partes involucradas en el mensaje debe conocer la contraseña.
- Asimétrica o no convencional:** A diferencia de la anterior, aquí cada persona involucrada posee un único par de claves: una pública y otra privada. Quien encripta lo hace usando la clave pública del destinatario, pero para leer se usa la clave privada que sólo conoce quien recibe el mensaje.

⁸⁸ Vitaliev, D. 2009. *Seguridad y privacidad digital para los defensores de derechos humanos*. Front Line. Pág. 34.

En EE. UU. al igual que en Colombia, está considerado como vulneración de la seguridad nacional toda información que el Estado no esté en capacidad de leer, argumentando que la información, si bien es privada, aquel puede acceder a ella con una orden judicial. Es así como el PGP⁸⁹, que en su momento fue uno de los mejores programas de criptografía y no se contaba con las herramientas necesarias para leerlo, fue prohibido, dando hasta seis meses de cárcel por su uso.

Se creó una versión internacional (PGPi) que era legal ya que contenía una ‘backdoor’⁹⁰ que permitía a las agencias de seguridad acceder a la información en caso de ser necesario. Es útil si quien nos amenaza no es el Estado.

Ahora bien, si realmente queremos proteger nuestra información, nos corresponde usar verdaderos programas de encriptación o cifrado. Hay que estar al tanto de la evolución de estos programas, ya que van surgiendo algunos que ofrecen mejoras y otros que van perdiendo su capacidad criptográfica y se vuelven vulnerables a medida que se desarrollan otras herramientas.

- ❑ **GnuPG o GPG (GNU Privacy Guard):** Esta herramienta está disponible para varias plataformas, incluyendo Mac OS a través de GPG Suite. Aunque por defecto funciona desde línea de comandos, en su página oficial se encuentran programas con entorno gráfico para usarla. Es una alternativa libre y gratuita.
- ❑ **TrueCrypt:** Es una aplicación de código abierto que, además de cifrar la información que se requiera, permite crear volúmenes cifrados o cifrar particiones enteras del disco duro, empleando diferentes algoritmos como AES, Serpent y Twofish, así como la combinación de varios de ellos.
- ❑ **VeraCrypt:** Aplicación derivada de Truecrypt y mejorada. Se pueden cifrar los archivos, los discos duros con todo su contenido, una unidad virtual creada en la computadora para almacenar allí en concreto lo que queremos mantener cifrado y también una memoria USB y otros dispositivos extraíbles.

⁸⁹ Pretty Good Privacy.

⁹⁰ Puerta trasera: se denomina así a la configuración que tienen algunos programas que permiten a terceros acceder a información del usuario sin que este se dé cuenta.



6

ESTEGANOGRÁFÍA

Del griego *steganos* (cubierto u oculto) y *graphos* (escritura). Es una técnica que sirve para ocultar la información entre elementos. Esta herramienta, al igual que la criptografía, es tan antigua como la necesidad de trasmisir información de manera segura. Existen varios tipos y formas de usar esta técnica.

Las personas esclavizadas usaban los peinados como información cifrada para conocer caminos de escape (mapas).

Hoy en día podemos usar nuestro ingenio para usar esta técnica, pero además existen algunos programas que nos permiten ocultar la información a transmitir en otros archivos, que pueden ser de texto, audio, imagen o video.

Tabla 7. Cifrar computadores, tabletas y celulares según Sistema Operativo.

Windows	Linux	Macintosh/iOS	Android
<p>Se deben usar programas adicionales para lograr esta función, tales como:</p> <ul style="list-style-type: none"> * BitLocker * Drive * Encryption 	<p>Linux, es un sistema operativo que contiene toda la información cifrada.</p> <p>Esta se descifra cuando se ingresa usuario y contraseña y vuelve a cifrarse en cuanto salimos de nuestro usuario.</p>	<p>Puede o no cifrar la información: ofrece esta posibilidad, y se es libre de usarla o no, puede hacerse desde el panel de seguridad con "FileVault".</p> <p>En iPhone el teléfono se cifra al colocarle una contraseña.</p> <p>Para iOS se puede utilizar la opción Find my iPhone.</p>	<p>A pesar de ser un Sistema Operativo de Google para celulares, es considerado uno de los más seguros, tiene la posibilidad de cifrar tanto el celular como la tarjeta Sd.</p> <p>Ir a Ajustes > Seguridad > Cifrar teléfono.</p>

Nota: Debemos tener en claro que este tipo de cifrado sólo sirve contra delincuentes comunes o del policía de a pie, en caso de querer ocultar la información de ojos más perspicaces es bueno usar mecanismos de encriptación más seguros, además de no cargar la información sensible en la computadora sino en dispositivos externos que estén bien resguardados.

Elaboración propia
Fuente: <https://seguridaddigital.org/>



— INFOGRAFÍA 12.

Navegación segura en internet y uso consciente de aplicaciones



Navegadores

El sistema operativo Windows trae instalado por defecto el navegador Internet Explorer, que además de ser de calidad regular no ofrece ninguna seguridad.

Hay una serie de programas que pueden hacer nuestra navegación en internet un poco más segura e incluso más agradable y ligera:

Mozilla Firefox: El modo privado de este navegador evita que el historial de búsqueda y sitios visitados queden en la memoria y borra las contraseñas usadas. Sin embargo, no hace anónima nuestra navegación a los ojos del ISP ni de las páginas en las que navegamos.



Existen numerosas extensiones que pueden mejorar los aspectos de seguridad en él.



Opera: Es un buen navegador para computadores de poca potencia; en su modo privado incorpora la posibilidad de navegar en una VPN.

Epic: Desarrollado a partir del código fuente de Chromium, está centrado en la privacidad, permaneciendo siempre en modo privado. Bloquea rastreadores y Cookies. Al salir elimina el historial y toda la información. Muestra un indicador de los rastreadores bloqueados. No genera sugerencias en las búsquedas al no enviar ningún tipo de datos.



Tor: Navegador basado en Firefox que no permite rastreo, ya que esconde la dirección IP. No permite que se sepa qué se está visitando; si alguien está mirando, solamente puede saber que se está usando Tor y las cookies se borran automáticamente una vez que se sale del navegador. Este programa puede usarse tanto en su versión portátil como instalándolo en el computador personal.

Este navegador sirve también para navegar en la Deep Web, su seguridad está comprobada hasta ahora. Las ocasiones en que ha sido vulnerada ha sido por mal uso, al instalársele un plugin que permite a la NSA establecer su propia codificación en la computadora que lo aloja. Tiene como desventaja que la conexión es más lenta que con otros navegadores, ya que funciona en logia de 'encebollado' (codifica por lo menos tres veces la conexión a internet).

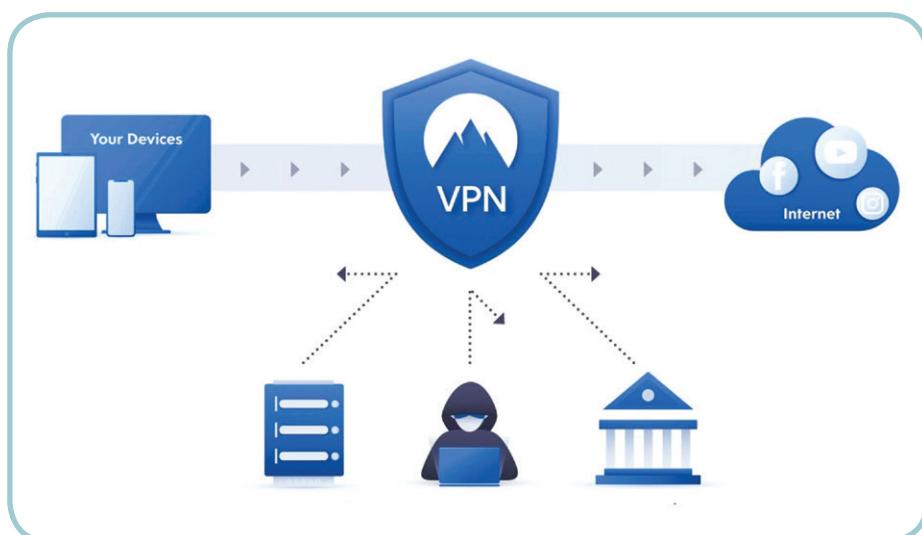
Indistintamente del navegador que se use, es importante usar el protocolo HTTPS en lugar del HTTP.



RED PRIVADA VIRTUAL (VIRTUAL PRIVATE NETWORK), VPN

La red privada virtual es una aplicación que nos permite conectarnos mediante cualquier navegador y no dejar rastro de quiénes somos; los sitios que visitamos no tendrán acceso a nuestra dirección IP y, sobre todo, no podrán ver lo que estamos haciendo. No es totalmente anónimo, pues la empresa que nos provee el servicio de internet tendrá la información de lo que estamos haciendo.

VPN funciona tanto en celulares como en computadoras. Puede descargarse como extensión para algunos navegadores como Firefox o como aplicación que se activa al conectarnos a la red.



BÚSQUEDAS SIN GOOGLE

Como ya vimos, Google y su batería de productos almacenan una gran cantidad de información a partir de nuestra actividad en internet. Para quienes no queremos aportar a esa jugosa fortuna, existe el buscador duckduckgo.com, que hace la búsqueda en



DuckDuckGo

diferentes bases de datos indexadas y no guarda información sobre nosotros.

Si bien, este buscador también muestra anuncios en pantalla, estos no son personalizados dado que no genera perfiles de usuarios. Empezó como un rival de Google, enfocado en la protección de la privacidad y seguridad de quienes buscan.

REDES SOCIALES SIN FACEBOOK

Existen redes sociales basadas en software libre, donde la importancia radica en el usuario y la usuaria, por lo que es impensable que obtendrán dinero vendiendo datos y/o preferencias.

Aquí algunos ejemplos que invitamos a explorar:

Diáspora: Es la alternativa libre a Facebook. El código de esta red social es libre, al alcance de cualquiera interesado en él. Diáspora se basa en “tres filosofías claves”:

- 1) Descentralización: no aloja la información privada en únicos servidores centralizados.
- 2) Libertad: no obliga al uso de una identidad real.
- 3) Privacidad: el usuario es dueño de sus datos, fotos, audios, videos y comentarios, de todo.

Elgg: Es una plataforma de red social de software libre y permite la publicación de blogs o wikis, así como compartir archivos, entre otras funciones.

Identica.ca: Es una alternativa a Twitter, una plataforma cabalmente abierta y libre, sin restricciones. Permite además vincularse con Twitter, para que en caso de publicar un mensaje en una de las dos redes, aparezca en ambas de forma automática.

Mastodon: Es otra opción para salir de Twitter, que distribuye a los usuarios en comunidades autónomas: instancias, que se comunican entre sí. Un fediverso (federación-universo). En esta red basada en software libre, no hay publicidad ni datos personales expuestos para la venta. Se establecen unos códigos en cada comunidad, que moderan los con-



tenidos, restringiendo el machismo, la homofobia, el racismo y diversas formas de discriminación.

Kune: Es una plataforma descentralizada para red social, que permite crear un espacio grupal online con libertad y control de la privacidad, donde hay un chat, la posibilidad de creación de documentos, un correo electrónico, un espacio multimedia para compartir, fotos, videos y audios, entre otras funciones.

CORREO ELECTRÓNICO SIN GMAIL

Gmail es una de las herramientas de correo electrónico más inseguras en cuanto a información se refiere. Sin embargo, hay algunas alternativas como extensiones que cifran los correos electrónicos de este aplicativo de Google. Lo ideal es tener nuestras cuentas de correo en servidores que provean el servicio y aseguren en sus políticas que los mensajes son cifrados de extremo a extremo (de emisor a receptor).

También que la información almacenada en su servidor está completamente cifrada, de tal manera que la misma empresa no puede acceder a estos datos. Los servidores en cuestión **sólo** funcionan para enviar correos y no proporcionan ninguna otra utilidad distinta a la seguridad en esta actividad. No piden datos personales para crear la cuenta, solamente el usuario y la contraseña.

Dos servicios de correo que recomendamos como alternativa a Gmail, por ofrecer correo cifrado de extremo a extremo, son:



Tutanota: Servicio de correo electrónico cifrado PtoP. El correo electrónico va cifrado durante todo el recorrido y sólo pueden leerlo el emisor y el destinatario. Ambos deben ser usuarios de esta plataforma. En caso de que el correo vaya dirigido a un servidor externo, pide una clave para que el receptor pueda ver el correo. Tutanota asegura que no guardan la IP desde la que te conectas.

Protonmail: Al igual que la anterior opción, el correo va cifrado desde el emisor hasta el receptor. Este servicio fue creado por un grupo de científicos del CERN (Conseil Européen pour la Recherche Nucléaire; en español, Consejo Europeo para la Investigación Nuclear) a partir de las revelaciones de Edward Snowden.



CLIENTES DE CORREO ELECTRÓNICO

Estos programas permiten descargar el correo al computador o a una unidad externa sin dejar información en la nube:

K-9 Mail: Es un cliente de correo electrónico libre y de código abierto (u open source) independiente para Android. Está bajo la licencia Apache 2.0. El programa está promocionado como un reemplazo más funcional para las aplicaciones incluidas en la mayoría de los terminales.



Thunderbird: Programa multiplataforma de Mozilla, de código abierto, que permite revisar el correo de manera remota y descargar la información. Se pueden manejar varios correos a la vez.



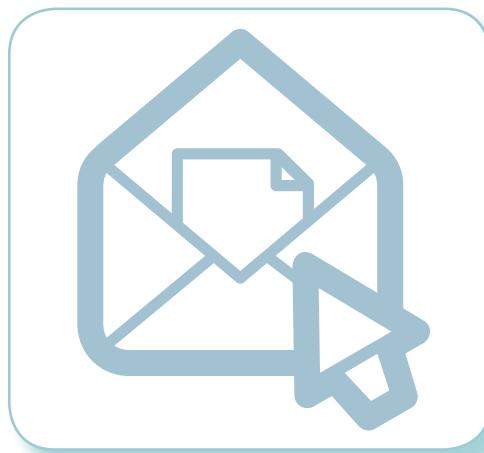


En caso de necesitar enviar alguna información sin que quede registro del remitente, se puede usar alguno de los siguientes servicios. Hay que tener presente no hacerlo desde donde se conecta habitualmente, ya que quedará registro de la IP y de la MAC-address.

Extensiones (correo y Firefox)⁹¹

Estos son pequeños programas que se pueden instalar en Firefox, que permiten personalizar y mejorar el desempeño de esta herramienta:

- HoxxVpn:** Extensión que configura una Red Privada Virtual (VPN) para poder navegar de forma anónima.
- Privacy Badger:** Bloqueador que inhibe el seguimiento por parte de las páginas web que se visitan.
- FlowCrypt:** Extensión para enviar correos encriptados desde Gmail.
- Enigmail:** Una extensión para buscadores Thunderbird y Seamonkey que permite cifrar mensajes de correo electrónico, usando el estándar OpenPGP. Se integra muy bien en estos gestores de correo y permite crear claves distintas por cada cuenta de usuario, entre otras opciones.



⁹¹ Se puede encontrar una serie de extensiones para mejorar su seguridad en: <https://www.eff.org/>



CONCLUSIONES

El desarrollo de las tecnologías de la comunicación y la información (en particular, el internet) reflejan el desenvolvimiento de las relaciones sociales, políticas y económicas que se tejen en el mundo *offline*, regido preponderantemente por la lógica neoliberal: un mundo en donde todo se ha mercantilizado y, por tanto, está plagado de profundas desigualdades, injusticias sociales y deterioro ambiental.

Es así como la génesis de la red de redes, si bien surge de un proceso descentralizado y colaborativo de construcción del conocimiento, deviene en un proceso de privatización de las plataformas, cuyo modelo de negocio convierte la cultura participativa en una de la conectividad, donde las interacciones y los datos generados a partir de la vida de las usuarias y usuarios se convirtieron en mercancías. La vida privada es la nueva materia prima para transformarse en valor y la misma vida humana es la fuerza de trabajo que genera dichos datos.

Con el valor agregado de esta nueva mercancía, los comerciantes aumentan sus ventas, el electorado elige a quien lo opriime, los imperios concentran los recursos naturales y los gobiernos despóticos eliminan a quienes se les oponen. En este tipo de explotación no sólo no hay ninguna remuneración, sino que la misma se produce en contravía del ejercicio de derechos fundamentales, como el derecho a la información, a la privacidad o intimidad y a la libre opinión, por mencionar los más cercanos al entorno digital.

Como reflejo de esa realidad offline, el internet se convierte en un terreno en disputa, donde existe una constante tensión entre el ser relacional de la humanidad, que busca participación, diálogo, información y conocimiento, y el libre mercado, que quiere sacar ganancias de cualquier actividad humana, por vital que sea.



Es así como la red sigue posibilitando la construcción comunal del conocimiento y potencia procesos de organización, surgiendo expresiones colectivas que se han manifestado en las calles y plazas, desplazando la intermediación de los grandes monopolios de la información para convocarse, intercambiar opiniones, generar material pedagógico, posturas y visiones de la situación de cada país.

Todos los movimientos reseñados en el segundo capítulo, más allá de los resultados y de las demandas que los configuraron, constituyen, en tanto luchas, enormes avances en cuanto a la democracia, pues evidencian formas posibles y novedosas de discusión pública, fuera de los ámbitos institucionales. En estas expresiones organizativas las redes *online* y *offline* se retroalimentan, derrumbando dos mitos liberales: 1) Que las mayorías no tienen tiempo ni interés de inmiscuirse en asuntos públicos y 2) que las personas son seres esencialmente individuales que sólo persiguen su interés personal.

En esta perspectiva, la red tiene el potencial de ser el ala *online* del ámbito de lo público, del *Ágora*, donde se pueden desplegar las libertades y los intereses individuales. Es un espacio de trabajo colectivo y voluntario que, si bien es apropiado por el capital, tiene expresiones en todo el mundo de lucha contra la privatización de los productos construidos socialmente. Es una forma de resistir y una experiencia fundamental de coexistencia comunal.

Internet tiene alternativas de producción libre, colectiva, descentralizada, respetuosa del derecho a la privacidad, a la información veraz, al diálogo y la interacción como fines en sí mismos, que deben ser abordados por las personas defensoras de derechos humanos. Esas alternativas merecen ser potenciadas, impulsadas en nuestras agendas y liderazgos, al igual que la adecuación de la legislación relativa al derecho a la información, la intimidad, y la rendición de cuentas.

El mismo mundo respetuoso de los derechos, la participación, la vida y la paz que reclamamos como personas defensoras, debemos ampliarlo al ámbito *online* gracias al cual evadimos la censura, la indiferencia de los grandes medios y el pensamiento unidireccional y unidimensional.

La disciplina en nuestros hábitos comunicacionales debe desarrollarse como parte de nuestras luchas. Por otra parte, con estas tecnologías también es posible vigilar a la clase política, grabar y difundir el uso desmedido de la fuerza policial, hacer seguimiento a las acciones de funcionarios/as públicos/as, entre otras posibilidades.

Una de las grandes conclusiones sería que es el capitalismo -y no la tecnología- el que pone precio a la subyugación y a la impotencia. El capitalismo

y su panóptico no son la tecnología en sí misma; son una lógica que impregna la tecnología y la pone a su servicio. El capitalismo de la vigilancia es una forma de mercado que resulta inimaginable fuera del medio ambiente digital, pero que no es lo mismo que «lo digital».

Así mismo, no es la tecnología, ni las plataformas tecnológicas y su industria las que deben dictar los valores y pautas de la sociedad para la cual diseñan sus productos, sino que son estas quienes deben adecuarse a los principios éticos, acordes con las necesidades de la humanidad.

Los capitalistas de la vigilancia ya no dependen de las personas como consumidoras. El eje de la oferta y la demanda cambia, orientándose hacia un público-cliente formado por empresas y negociantes deseosos de prever el comportamiento de las poblaciones, los grupos y los individuos⁹².

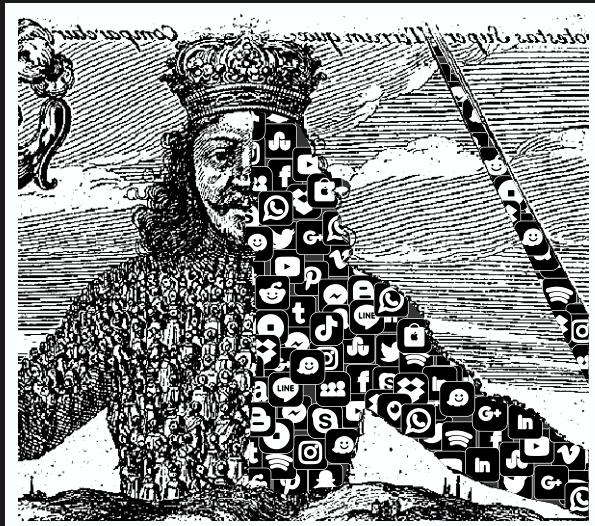
La comunidad de los derechos humanos debe estar alerta a los cambios que están surgiendo en materia de nuevos delitos cibernéticos y nuevos derechos fundamentales o neuroderechos⁹³ que deben ser incluidos dentro de la legislación nacional e internacional, antes que las grandes plataformas desplacen, como está pasando, a los Estados y su poder de interceder ante los avances de la inteligencia artificial y la Big Data.

En el caso colombiano, el papel de la justicia y de la Fiscalía General de la Nación en particular, es bastante preocupante por dos razones fundamentales: i) no son las plataformas digitales las llamadas a ejercer justicia (ciberjusticia) en los casos de mensajes de odio y discriminación por parte de figuras públicas, puesto que ellas son intermediarias y su negocio en la red es aprobado por los gobiernos y ii) cuando la Fiscalía decide adelantar investigaciones producidas en el entorno digital, lo hace con el objetivo político de perseguir a la oposición y a todos aquellos que considere enemigo público para la perpetuación de la derecha en el poder.

Por lo anteriormente dicho y como se planteó a lo largo de este texto, el entorno digital en toda su amplitud es un terreno que merece nuestra atención y formación especializada, que demanda de parte de las organizaciones sociales y de derechos humanos habilitar espacios para la discusión y construcción de propuestas para limitar el poder de las plataformas tecnológicas y su uso por parte de los grandes emporios económicos y las agencias estatales de inteligencia.

⁹² Zuboff, Sh. 2018. *La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder*. Ediciones Paidós. Pág. 662.

⁹³ <https://www.investigacionyciencia.es/revistas/mente-y-cerebro/resiliencia-741/nesecitamos-neuroderechos-universales-16560>



LOS DATOS: EL QUINTO PODER: es un documento de análisis realizado por el Programa Somos Defensores, sobre los avances de las tecnologías de la información en la cuarta revolución industrial (4Ri) y como estos están cambiando de manera acelerada el acceso y control de la información en el planeta. Por ello hemos denominado este trabajo Los datos, El Quinto Poder, para destacar que son el petróleo del siglo XXI, su poder incommensurable y disruptivo promete reescribir la historia de la humanidad.

Dichas tecnologías de la 4Ri están siendo implementadas en Colombia por el gobierno nacional, y algunas de ellas como el internet de las cosas (IoT) y la inteligencia artificial hacen parte de la imperceptible intromisión en la vida cotidiana(computación ubicua). Son avances que pese a sus bondades, le han permitido a algunas democracias y regímenes autoritarios sofisticar la persecución contra la oposición y las personas defensoras de derechos humanos y sus organizaciones.

El Programa Somos Defensores con este documento pretende contribuir con algunos insumos en provocar el debate a partir de unos elementos básicos respecto de la necesidad de repensar la protección de los datos ante el inminente avance de las tecnologías y, cómo empezar a construir estrategias de defensa en este nuevo campo de disputa.



**PROGRAMA
SOMOS DEFENSORES**

PROGRAMA NO GUBERNAMENTAL DE PROTECCIÓN A
DEFENSORES DE DERECHOS HUMANOS