

## 1984 - 2019...

*Johan López<sup>1</sup>*

### Resumen

A continuación, una breve explicación de la red, cómo su debido uso puede acarrear problemas y del software libre como una forma de soslayar esos inconvenientes.

En las pasadas elecciones presidenciales y de congreso se pudo notar la reducción de un fenómeno que, al menos desde finales del siglo XX e inicios del XXI se presentaba de manera constante en los comicios electorales, aquí me refiero, más que a la jocosidad y ridiculez en las campañas y sus candidatos, a la contaminación visual que inundaba las calles de nuestras ciudades, las paredes y muros de nuestros barrios, los postes de nuestras esquinas, y los pasacalles que de tanta sombra nos proveían.

Así, las campañas electorales optaron por bombardearnos con un sin fin de publicidad, sin importar que esta fuese a su favor o en contra de las demás candidaturas, siendo el común denominador para dichas acciones las plataformas digitales que a diario usamos para laborar, estudiar, (des)informarnos, comunicarnos, entretenernos, pero en su mayoría para perder el tiempo.

¿Es este un caso particular aislado o es posible asociarlo a una lectura más amplia de nuestra cotidianidad? Una breve mención y análisis acerca de la campaña politiquera nos permite desarrollar un concepto clave para el presente artículo, pues las comunicaciones desempeñan un papel fundamental en el desarrollo de nuestras actividades y en casi la totalidad de los casos no se tiene claro qué son, qué rol juegan ellas en nuestras vidas, ni la relación que poseen con el actual orden de las cosas. Y si tales actividades pueden ser empleadas a través de las nuevas tecnologías, es posible pasar de los meros casos específicos y llevarlos a una generalidad, afirmando que el continuo avance de las redes de comunicaciones tanto en el hardware como en el software han permitido que éstas logren penetrar en cada aspecto de nuestra existencia (o al menos la mayoría).

Sin embargo, no se deben entender las redes únicamente como la internet y/o las plataformas digitales, pues todo tipo de comunicación funciona en red, algunas con nodos o centros (como una atarraya) y otras más independientes, más lo que debemos apreciar en este punto es que cualquier método de conexión empleado es una red, por lo tanto, nuestros teléfonos fijos y

---

<sup>1</sup> Campesino, Mesero, Alfarero, Maquinista, Lustrabotas, Soldador, Tornero, Mecánico, Zapatero, Pescador, Minero, Electricista, Chofer, Sastre, Barbero, Panadero, Albañil, Barrendero, Pintor, Ventero... Una ama de casa... Una obrera, un obrero, ¡Un Proletario!

móviles también hacen parte de una, al igual que los televisores, radios, entre otros.

Hoy día son cada vez más las plataformas que existen y que exigen, ya sea por presión social, laboral y demás, la creación de un nuevo código ininteligible<sup>2</sup> para nosotros que se traducirá en una cuenta donde se almacenará toda la información que voluntariamente coercionados entregaremos a dichas plataformas, las cuales pueden también ser clasificadas como servicios en línea (Han, 2012), en red.

## **Migración**

En retrospectiva, tal es la enajenación, pues anteriormente y en diferentes ámbitos las relaciones eran mediadas por un limitante físico, y ahora se asientan en la virtualidad, tanto de manera individual como colectiva, en la creación de grupos con intereses comunes en los cuantiosos mundos virtuales que abundan en el espacio digital (Betty y Smith, 2002). Por lo tanto, en cuanto a redes virtuales es posible hablar del fuerte vínculo entre éstas y el brote de las ciudades digitales (Graham y Marvin, 2001). En otras palabras, se ha presentado una migración del espacio físico al digital. Además, con la sobreproducción de los artilugios necesarios para llevar a cabo el éxodo electrónico, es admisible la afirmación acerca de la masividad de éste fenómeno, no siendo el único factor influyente para esto, pues la constante creación de servicios en línea también permite acrecentar la situación antes mencionada.

Retomando entonces la idea anterior acerca del desplazamiento entre el espacio y el

ciberespacio, es factible mostrar la existencia de ciertas prácticas tanto en un lugar como en el otro. Una de esas prácticas que se ha llevado a cabo desde tiempos antiquísimos es el censo, herramienta que permite recopilar cierto tipo de información sobre los pobladores de una determinada región, por ejemplo, los censos de Israel posteriores a la esclavitud en Egipto consistían en registrar las tribus y clanes ya establecidos en lo que hoy es Palestina y el registro de la cantidad de hombres y sus edades en cada clan y cada tribu, con el objetivo de calcular cuántos hombres eran aptos para la guerra, la proporción de tierras que necesitaban y dónde se ubicaban éstas (Lyon, 1994). De igual manera, en tiempos más recientes los instrumentos de recopilación de la información no son tan diferentes puesto que, hasta el día de hoy seguimos siendo registrados en un censo estatal, además de otros medios como los son el catastro, la registraduría y más, pero lo aquí importante es entender que cualquier forma de registro por cualquier motivo es una forma de compendio de la información.

Ahora, si reflexionamos acerca de todos los servicios encontrados en red podemos advertir que las prácticas y registros que se llevaban en cuadernos y carpetas A-Z, hoy se disponen en discos duros conectados en línea, e importante también es reconocer que al cambiar la manera de almacenamiento de la información, es posible aglomerar cantidades exorbitantes de ella, pues hay una capacidad mayor de almacenamiento en contradicción con el espacio físico que éstos medios llegan a ocupar.

---

<sup>2</sup> El código fuente de un programa, éste establece cómo se estructura un programa informático, desde su funcionamiento hasta su apariencia (cualquiera que sea el programa).

## La Táctica «Pacífica»

La migración de un espacio a otro se ha dado no solo por las personas, ahora perfiles, sino también por servicios empresariales, personales y las herramientas necesarias para obtener registros e información, ya sea en una transacción cotidiana o de manera ilegal, teniendo presente que dicha data<sup>3</sup> puede emplearse para ejercer un control sobre la gente, tal y como sucedió con los Israelitas, pero también como en las pasadas elecciones presidenciales, donde las personas daban a conocer su posición «política» a partir de su interacción en la red, la cual se prestaba para censurar, desprestigiar o atentar contra quienes no seguían al «Pied Piper»<sup>4</sup> Colombiano.

En este sentido, nos referiremos a un método o herramienta de control social y territorial vital para la conservación del actual sistema político económico y de cómo éste puede valerse del auge de la red para continuar con su cometido de manera más sencilla e incluso más represiva, tomando así dos vertientes que examinaremos a continuación.

La primera vertiente obedece a la huida hacia los espacios virtuales por medio de la adquisición y el consumo de los materiales y servicios necesarios para hacerlo, aunque no en ese orden<sup>5</sup>. También la continua creación de plataformas digitales que permitan la

realización de nuestras actividades cotidianas detrás de una pantalla, es un aliciente para evitar la desconexión, así pues, tratamos de estar siempre en línea, en red, sintiéndonos «menos solos» pero sí, más aislados (Han, 2012). Y dicho aislamiento no es solo con nuestros congéneres, también lo es con la realidad concreta de nuestro territorio.

Pero, ¿por qué es ésta una forma de ejercer control territorial?, ¿por qué es una forma de ejercer poder? Porque se nos individualiza y de este modo pueden ocurrir dos cosas: a) aislarnos por completo convirtiéndonos en idiotas útiles para quienes ejercen el poder y su sistema económico; b) «movilizarse» a través de las plataformas digitales sin plantear acciones puntuales y reivindicativas por fuera de ellas, esto no es muy diferente a la actitud anterior ya que seguiríamos siendo idiotas útiles (pero «con sentido crítico») al no emprender acciones directas o mecanismos de presión donde se visibilicen los actores de un territorio determinado exigiendo sus derechos, y más importante aún, construyendo poder popular<sup>6</sup>.

Vemos entonces que llevar una «lucha» únicamente desde la red no ha de tener relevancia para quienes desean una transformación en la estructura social, porque sin importar que tan fuerte se pueda teclear las injusticias no finalizarán al son de

<sup>3</sup> Anglicismo que se usa en relación a los datos, información. La traducción al español es datos.

<sup>4</sup> El flautista de Hammelin, el cual a través de los años ha sido censurado para contarle a los niños y niñas, no obstante, en alemán e inglés sigue conservando la negatividad y crueldad que el personaje posee al asesinar al rededor de 120 niños y niñas de una región, ¿puede compararse con 10.000 casos de falsos positivos?

<sup>5</sup> En este punto se quiere dar a entender que es desemejante la adquisición de un dispositivo para el consumo fetichista en relación con la tecnología y la cotidianidad, y la adquisición del mismo debido a que los servicios y otros ámbitos de nuestra vida son solo accesibles por medio de la red, en otras palabras, tales situaciones pueden representarse como el dote voluntario de un bien de consumo y el dote obligatorio del mismo bien de consumo, pues como lo afirma (Chaparro, 2017) existe ahora en el modelo neoliberal la brecha digital, la cual genera un distanciamiento aún mayor entre pobres y ricos, ya que, el mundo y las distintas relaciones de poder se mueven digitalmente, quienes no puedan acceder a tal digitalización quedarán rezagados de las esferas a las que desean aspirar y de las que son partícipes.

<sup>6</sup> No obstante, académicos como Andres Merejo sostienen que gracias a acciones de éste tipo fue derrocado el dictador de Túnez Ben Ali (Merejo, 2017).

los algoritmos<sup>7</sup> que se utilizan, en este punto, quienes «luchan por redes» han sido coaccionados, se ha ejercido tal poder sobre ellos que se desconectan de su territorio, por ende, es factible comprender la migración al ciberespacio como un método de control social y territorial, al individualizar a una población específica a la que se puede dominar sin la necesidad del uso de la fuerza, pues basta una exigua expresión en la red para limpiar sus conciencias.

## **La Táctica Represiva**

La segunda vertiente recae sobre aquellas personas que buscan una transformación del orden establecido teniendo siempre presente que la ocupación y recuperación de los espacios físicos es vital para dicha transformación. Al comprender lo anterior entra a jugar un factor importante en el desarrollo de los cambios sociales, y es el discernimiento para entender que se entra en una pugna contra las fuerzas estatales por dichos espacios para dichas transformaciones, desencadenando de allí la posibilidad de correr riesgos de manera física. Ahora, es también factible correr tales riesgos en las redes y aquí me refiero a la gran posibilidad de llegar a ser un objetivo militar, dado que, la red se está militarizando. Tal y como lo afirman Fernández y Mancini:

Los contratistas principales de las agencias de inteligencia y fuerzas militares de decenas de países, son proveedores de estas tecnologías. Algunos de ellos son: VASTech, Gamma Corporation, Amesys, ZTE Corp, SS8, Hacking Team, Vupen, Phoenexia, Blue Coat,

y la lista continúa. En el 2012, los principales clientes fueron Libia, Egipto, Ucrania, Turquía, Sudáfrica, Hungría, China, Colombia, Brasil, Canadá, Estados Unidos, Reino Unido, España, Suiza, Rusia, Italia, India, Alemania, Francia, entre otros países. (p. 12).

Teniendo en cuenta que la invención de la red se debe en un principio al desarrollo militar, no es difícil comprender que su fin siempre ha sido el mismo, a pesar que en torno a ésta se hayan desarrollado otras dinámicas. Así pues, es fácil determinar cuándo nuestro territorio se encuentra militarizado, por el contrario, en la red podemos ignorarlo sin querer decir que no lo esté, pero ya no por soldados o al menos no de carne y hueso, sino por los dispositivos y el software necesario para satisfacer el mercado de monitoreo de contenido y tráfico de internet, trackeo por GPS<sup>8</sup>, monitoreo de comunicaciones móviles (llamadas), análisis semántico de contenido de comunicaciones, monitoreo de SMS<sup>9</sup> (mensajes de texto) y virus informáticos en dispositivos.

También, cabe recalcar la gran contradicción existente entre las herramientas análogas y las digitales, las técnicas pasadas y las nuevas, pues las primeras se reservaban para personas sospechosas ya estudiadas previamente y para las segundas no se es necesario ser sospechosa debido a que existe la capacidad de vigilarnos a cada una por igual, para posteriormente hacer filtros y vigilancia de manera más meticulosa, esto, gracias a la ubicuidad de la red (más que divina, material), dejando así obsoletos los viejos métodos de

---

<sup>7</sup> Son una sucesión de pasos que se emplean para la resolución de un problema. Todos los programas informáticos son creados con base en ellos.

<sup>8</sup> Rastreo de dispositivos por medio del GPS (Sistema de Posicionamiento Global en español), no solamente para móviles o celulares, sino que se usa para cualquier equipo que tenga un GPS, ejemplo, un vehículo.

<sup>9</sup> Aunque éstos ya no son tan utilizados se siguen teniendo en cuenta para la vigilancia y el monitoreo.

espionaje. Aquí cabe recalcar que la capacidad a los que nos referimos es: i) La cantidad de información que se puede almacenar sobre una persona; ii) El tiempo en el que se le puede someter a vigilancia.

Resumiendo de manera escueta, «Todo durante todo el tiempo». Es decir, en la red será registrado y guardado todo lo que se consume<sup>10</sup> durante todo el tiempo que los perfiles/personas permanezcan activos.

En consecuencia, los actuales métodos de vigilancia asociados a las herramientas digitales permiten un nivel de privacidad casi nulo preocupante para toda la población, sin embargo, lo es mucho más para las organizaciones sociales y sus integrantes, y algunas otras personas con un distorsionado sentido de la justicia, debido a qué, por sus

convicciones y acciones políticas se tiende a ejercer sobre ellos el uso y abuso de la fuerza, sea ésta Estatal y/o paraestatal. Por lo tanto, valiéndose de las redes el Gran Hermano es omnipresente, todo lo registra, todo lo escucha, todo lo observa y quién no osa someterse al partido único la policía del pensamiento lo subyuga, apresando, torturando y doblegando hasta que deshechos y derrotados aceptemos la verdad impuesta<sup>11</sup>.

Pasando ahora de George Orwell a nuestro presente (de 1984 a 2019), no es complicado hallar las prácticas que se advertían anteriormente, manifestadas también por Edward Snowden<sup>12</sup> en los aproximadamente 1,7 millones de documentos de máxima inteligencia (Top secret) extraídos de las organizaciones de inteligencia del gobierno de EE.UU. En síntesis fueron expuestas redes



Hombre aterrado por la tecnología de vigilancia. En *Acuerdo contra la vigilancia en internet*, por L. Sturniolo, 2003, Buenos Aires, Los Andes, Tomado de: <https://losandes.com.ar/article/acuerdo-contra-vigilancia-internet-729444>

<sup>10</sup> Consumir no equivale únicamente a comprar un bien o un servicio, consumir también compete a la información que descargamos, el cine que vemos, los sitios que visitamos, etc.

<sup>11</sup> Breve referencia a la distópica novela de George Orwell, 1984.

<sup>12</sup> Antiguo consultor tecnológico y experto en seguridad informática de la NSA (Agencia de seguridad Nacional, en español) y de la CIA (Agencia Central de Inteligencia, en español), de las cuales reveló diversos métodos de investigación y vigilancia masiva, incluyendo jefes de Estado. Cabe aclarar que Snowden no ha sido el primero en revelar información de tal magnitud, sin embargo, gracias a la era digital, si ha sido a quien más atención se le ha prestado. Algunos de ellos son: John Marks, asociado en el Centro de Estudios para la Seguridad Nacional y fue asistente del director de la Oficina de Inteligencia e Investigación del Departamento de Estado; Robert Borosage, exdirector del Centro de Estudios para la Seguridad Nacional; Herbert Scoville, exdirector ejecutivo para la Investigación en la CIA y exdirector asistente de Ciencia y Tecnología para la Agencia de Control de Armas y Desarma; Morton Halperin, Asistente Ejecutivo del Secretario de la Defensa; William Colby,

de espionaje a niveles gubernamentales<sup>13</sup>, además de programas, servicios informáticos y empresas que colaboraban con la inteligencia dando acceso completo a sus respectivos servidores, algunos de ellos son: Angry birds, iOS, Android, Outlook, Microsoft, Google, Apple, Facebook, Yahoo, AOL, entre otros<sup>14</sup>. Los documentos filtrados pueden encontrarse en wikileaks<sup>15</sup>.

Todo esto (aunque queda faltando mucho) a nivel de la geopolítica, de la cual dejaremos hasta aquí para enfocarnos en casos concretos de la acción policiva/militar gestada en nuestro territorio a partir de intervenciones en la red:

a) A mediados del 2013 se dio a conocer el caso de «las cinco anarquistas de Barcelona», quienes fueron detenidas y acusadas de asociación terrorista, únicamente por divulgar sus ideas libertarias a través de las redes sociales. Llamaban a la rebelión por medio de sus perfiles de Facebook, tanto individual, como colectivamente. A pesar de que eran solo ideas (pues no llevaban una acción en

curso) fueron capturadas como método de prevención, aunque sobre su arresto se especula que se llevó a cabo como táctica para disuadir a otros grupos.

b) El 9 de Junio de 2011 en España detienen a tres supuestos miembros de Anonymous<sup>16</sup> por ataques informáticos a diferentes entidades privadas como BBVA, Sony PlayStation, Bankia, etc, y también a los gobiernos de Chile, Colombia, Nueva Zelanda, Libia, Egipto, Argelia, entre otros.

c) A los reporteros de la W radio se les interceptaron los equipos donde llevaban a cabo la investigación del famoso caso de «La comunidad del anillo», una red de prostitución que se gestaba al interior de la Policía Nacional y en la cual se encontraba involucrado el antiguo general de la institución Rodolfo Palomino.

d) En el año 2002 los Grupos de Acción Unificada por la Libertad Personal (GAULA) interceptaron más de dos mil líneas telefónicas de manera ilegal, los afectados

---

exdirector ejecutivo de Planes de la CIA; Víctor Marchetti, exoficial de personal directivo de la CIA. (Borosage y Marks, 1976).

<sup>13</sup> Una de ellas conocida como Five Eyes (cinco ojos) compuesta por los gobiernos de Australia, Canadá, EEUU, Nueva Zelanda e Inglaterra (actualmente), creada desde finales de la 2da guerra mundial. Es considerada como la alianza de espionaje más completa a nivel mundial, no obstante, no puede negarse que existen muchas más aunque no a niveles tan colosales.

<sup>14</sup> Se emplean algunos de los servicios, programas y empresas reconocidos y usados en nuestra cotidianidad para dar a entender la magnitud del problema (a pesar de que en últimas instancias se ignoren). Y aunque éstos programas, servicios y más, representan una grave violación a nuestra privacidad no son los más poderosos, aquí nos encontramos con software clandestino como PRISM, XkeyScore, ECHELON, MUSCULAR, TEMPORA, y otros.

<sup>15</sup> Es una organización sin ánimo de lucro dedicada a la publicación de material en inteligencia gubernamental y contenido sensible de carácter público, la publicación se hace por medio de su sitio web y los documentos son filtrados por los mismos miembros de las entidades de espionaje y en ocasiones por reporteros. Toda la información filtrada y editada puede encontrarse en <https://wikileaks.org>. Además, con el retroceso de las políticas y las prácticas reaccionarias del actual presidente Ecuatoriano Lenin Moreno se permite la captura de Julian Assange (uno de los fundadores y portavoz de la organización), y como rechazo a tal acto Wikileaks habilitó un enlace en el cual se puede encontrar información aún no editada: <https://file.wikileaks.org/file>.

<sup>16</sup> Organización de «Hackers» a nivel mundial que no poseen una directriz vertical, por lo que diversas capturas de sus integrantes no evitan que ésta siga operando. Asimismo, no tienen una dirección en cuanto a las acciones que llevan a cabo, pues cada operación se organiza, se planea y se ejecuta por los involucrados directamente, generando diversos flancos de una misma lucha. Para aclarar, el término hacker es usado por los medios de comunicación para estigmatizar a aquellos que emplean un uso distinto de las redes, pues éste puede llegar a tener otros fines distintos al simple consumo.

fueron la Asociación de Familiares de Detenidos y Desaparecidos (ASFADDES), en el transcurso de dichas interceptaciones desaparecieron dos de sus integrantes.

e) En el año 2014 la unidad del ejército Colombiano «Andrómeda»<sup>17</sup> fue denunciada por espiar durante casi un año al equipo negociador de la Habana, encargado de entablar el diálogo entre el gobierno y la guerrilla Farc-EP. El espionaje se llevó a cabo por militares activos y «hackers» civiles. De acuerdo con las múltiples entrevistas, a los militares involucrados Andromeda realizaba control, pero su principal objetivo no eran los negociadores de la Habana, sino distintas ONG's de derechos humanos.

f) Según [privacyinternational.org](http://privacyinternational.org):

Los grupos especiales de inteligencia estratégica del DAS sometieron a vigilancia selectiva a alrededor de 600 figuras públicas, entre las que había parlamentarios, periodistas, activistas y abogados de derechos humanos y jueces. Según los archivos recuperados en el curso de una investigación de la Fiscalía, el DAS interceptó llamadas telefónicas, tráfico de mensajes de correo electrónico y listas de contactos nacionales e internacionales y utilizó esta información para compilar perfiles psicológicos de los afectados y someter a vigilancia tanto a ellos como a sus familias, incluidos niños. (2015)

Entre los afectados encontramos personalidades interceptadas como Hollman Morris, Gustavo Petro, Piedad Cordoba, Ivan Cepeda y Claudia Duque, abogada y periodista del CAJAR (Colectivo de Abogados Javier Alvear Restrepo) quien sobrevivió a múltiples atentados e intentos de secuestro.

g) En el año 2011 las interceptaciones de llamadas telefónicas y mensajes de texto permitieron la localización del líder de las FARC-EP Alfonso Cano, quien murió posteriormente en un ataque militar, caso similar al de Jorge Briceño, miembro del Secretariado del mismo grupo insurgente. Tales intervenciones en las telecomunicaciones se gestaron a partir del proyecto Esperanza<sup>18</sup> formalizado en el año 2005, Convenio Interadministrativo 038 de 2005.

El Proyecto Esperanza ha sido gran protagonista en el espectáculo de las interceptaciones mediáticas alcanzando su máximo esplendor en el régimen de Álvaro Uribe, no obstante, lo más importante no es que un déspota lo usara, pues el siguiente también habría de hacerlo, lo realmente relevante es la relación existente entre un proyecto gubernamental y la empresa privada, vale decir que Esperanza requiere de la colaboración del proveedor de servicios para su funcionamiento.

## La Teoría y La Praxis

Hasta aquí se divisa un paisaje desolador, no solo por lo citado anteriormente, sino también por lo encontrado en el ámbito académico para la transformación del uso de las redes, pues existe una gran cantidad de artículos y libros que retratan la distópica realidad con respecto a nuestra privacidad (y por ende a nuestro cuidado) basándose solamente en la cuestión teórica en cuanto al problema sin proponer una posible solución, tal y como: (Han, 2012), (Molina, 2001), (Chaparro, 2017), (Graham y Marvin, 2001), (Betty y Smith, 2002), (Lyon, 1994),

<sup>17</sup> Unidad del ejército nacional creada únicamente para la interceptación de información.

<sup>18</sup> Este proyecto es o mejor dicho actúa como un conjunto de interceptación de comunicaciones manteniendo una estrecha relación entre la Fiscalía, la Policía y el DAS (cuando aún existía).

(Hermelin, 2017), (Merejo, 2017). Esto puede radicar en la «incapacidad» (más bien pereza, incluso indiferencia) de comprender, asumir y trabajar en la interdisciplinariedad comprometiéndose a plantear un panorama distinto o también puede ser un miedo recurrente a perder la comodidad que ofrece la academia, puesto que, implementar una alternativa va en contra de los intereses de ésta y del régimen que la manipula.

Caso contrario al del matemático Theodore Kaczynski<sup>19</sup> quien da cuenta y teoriza acerca del problema, no únicamente como una cuestión de privacidad, sino también como parte del modelo de producción capitalista, indicando que la tecnología ha llevado a recrudecer las contradicciones entre las clases sociales, además de fortalecer al sistema mismo a costa de nuestra libertad individual y autonomía como personas y como pueblos. Kaczynski propone, primero, que el sistema de producción vigente debe cambiar y que este cambio no puede ser con meras reformas, es necesaria entonces una revolución, y segundo, que la tecnología y el modelo de producción tendrán que desaparecer al unísono, dado que desde la revolución industrial se ha visto un acelerado progreso en todas las formas de represión que logra ejercer el sistema de producción,

dicho de otra forma, el sistema capitalista se beneficia en múltiples ámbitos al mantener la tecnología y su desarrollo oblicuo a él.

En consecuencia, como propuesta inicial a la transformación del uso de las redes encontramos a Kaczynski manifestando su aniquilamiento, refiriéndose a aquellas redes que dependen y reproducen el actual modelo económico, pues las que no se someten a dicho modelo se encuentran al alcance de las comunidades y pueden llegar a ser de carácter autónomo para las mismas.

Ahora, una segunda propuesta nace desde el ideal de «la toma de las redes» con miras a un uso y desarrollo por fuera de la lógica bajo las cuales fueron construidas, dicha propuesta se ha venido manifestando desde la década de 1980 con el surgimiento del movimiento del Software Libre<sup>20</sup>, el cual consiste en promover la lucha contra la privatización del conocimiento y la seguridad en la red, ésta última interpretándose como seguridad en cuanto a nuestra integridad física, la cual comienza a ganar fuerza por parte de las comunidades más alejadas a los movimientos relacionados con las redes y la informática, debido a la persecución realizada a Aaron Swartz<sup>21</sup> por parte del Instituto Tecnológico de Massachusetts (MIT), FBI y El

---

<sup>19</sup> Matemático nacido en EEUU, nombrado como Unabomber por los medios de comunicación. Escribió *La Sociedad Industrial y su futuro*, publicado en el Washington Post, mejor conocido como *Manifiesto Unabomber* el cual relaciona de manera negativa nuestra sociedad y el desarrollo tecnológico, por lo que es considerado como un neoludita. Fue capturado por enviar cartas y paquetes bombas a las instituciones que componen la sociedad industrial. En prisión continuó escribiendo, con el agravante de que la mayoría de sus ensayos son censurados y no expuestos al público.

<sup>20</sup> Es un movimiento social que tiene el objetivo de obtener y garantizar las libertades que permiten a los usuarios de programas informáticos ejecutarlos, estudiarlos, cambiarlos y redistribuir copias del mismo con o sin cambios, sobre la base de las tradiciones y filosofías de la cultura hacker (puede resumirse como libre acceso a la información) y el mundo académico de los años 70's (y académico debido a que el término hacker existe desde mucho antes del primer ordenador; es decir, no tiene que ver solamente con la informática).

<sup>21</sup> Fue un programador autodidacta que desdeñaba de lo infructífero de la academia para el desarrollo del intelecto humano. Se involucró en el desarrollo de diversos programas y servicios que incluso hasta hoy se continúan utilizando (fundador de openlibra.com, fuentes web RSS, marcadores Reedit, entre otros), sin embargo, el trabajo más sobresaliente está sustentado en su política acerca del poder de la información y llevar la información a las masas populares, ergo...

Departamento de Justicia<sup>22</sup>, que lo hostigaban por liberar en la red de forma gratuita algunas de las bases de datos académicas más importantes y robustas, entre ellas JSTOR<sup>23</sup>; cabe mencionar que el asedio a Swartz por las entidades antes mencionadas desembocaron en su muerte.

Así, en los pensamientos y las acciones de una persona (pero que no ha sido la única) se refleja todo un movimiento que busca la libertad de conocimiento y de información con el fin de dar autonomía a las comunidades, trabajando conjuntamente con ellas para alcanzar el objetivo antes planteado, Bluetooth, Copyleft<sup>24</sup>, GCC<sup>25</sup>, GNU... son algunos de los ejemplos y/o adelantos que se han hecho en pro de una sociedad libre.

Observamos entonces dos propuestas que parten de distintos puntos pero con propósitos comunes. Ya sea desde los Manifiestos hechos en una máquina de escribir o los códigos escritos en editores de texto plano<sup>26</sup>, vemos una sincronía entre la destrucción total de las herramientas que cohíben al ser humano de Kaczynski y la creación de otras que promueven la libertad de las personas (Software libre). Siendo una, prosecución de la otra en el camino por la construcción de una sociedad más justa, teniendo siempre presente la articulación con otros procesos y otras luchas.

## Todo lo sólido se desvanece en el aire

Aquí, para entender la afirmación y desarrollar la idea acerca de «la toma de las redes» debemos comprender que si bien éstas requieren de un medio físico o material para funcionar, sólo serían chatarra con un bonito diseño sin el software que manipule la información que viaja por sus diversas estructuras, y tal software nos ofrece una dicotomía, permitiendo que las redes puedan tomarse para otras actividades distintas a las de reprimir, restringir, prohibir, privatizar, vigilar y demás.

¿Y cómo que el Software? Recordemos que este elemento es la parte no tangible de la informática, pero si ahondamos un poco en el tema, podemos denotar que la informática va mucho más allá de los ordenadores y que, tautológicamente los dispositivos digitales tienen un software integrado que permite la interacción entre una máquina y una persona, así, un reloj digital, una máquina expendedora de dulces o de café, un teléfono fijo e incluso un horno microondas tienen un software instalado (sistema operativo) y cada uno es completamente diferente de los demás, ya sea por la función a ejecutar o por la industria que lo desarrolla.

Profundizando un poco más, aseveramos que existen dos tipos de software conocidos por la imposición y censura del mercado pero

<sup>22</sup> Es el equivalente a la Fiscalía General de la Nación aquí en Colombia.

<sup>23</sup> Journal STORage, almacén de publicaciones periódicas. Es una base de datos de publicaciones académicas.

<sup>24</sup> Basado en los derechos de autor (copyright) pero se presenta una enorme diferencia entre ellos, pues los izquierdos de autor (copyleft) prohíben prohibir; de los izquierdos de autor se desprende lo que hoy conocemos como Creative Commons, una licencia que no amarra los derechos de los trabajos académicos, obras artísticas y demás, a una empresa de determinada industria.

<sup>25</sup> Es un compilador. Un programa que tiene la capacidad de traducir el código de un lenguaje de programación al lenguaje máquina, permitiendo su ejecución e interacción con el usuario. Al usarlo, condiciona a que todo lo que pase por él, sea libre.

<sup>26</sup> Son editores de texto que no permiten seleccionar un formato para su contenido, es decir, no se puede cambiar la fuente ni su tamaño, si es cursiva o en negrita, ejemplo de éstos son el «bloc de notas», pero hay más y mejores: Nano, Latex, sublimeText, Vi, Vim, Emacs, entre otros.

desconocidos desde su carácter ideológico y político. Es probable que aquí se piense en microsoft (windows) y GNU/Linux (mal llamado linux)<sup>27</sup>, pero esta no es la dirección correcta, puesto que, los tipos de software no son los S.O. (sistemas operativos) en sí, sino cada uno de los programas que lo componen, es decir, el S.O. es un conjunto de programas que permiten su funcionamiento. Ahora, cada programa posee una licencia que denota el carácter antes mencionado.

Así, las licencias son de dos clases: a) Las licencias que normalmente exigen un pago por el uso del programa en relación (no siendo un requisito) y la aceptación de otras cláusulas (esos textos extensísimos que salen antes de usar cualquier programa, los cuales nunca leemos y nos limitamos a buscar rápidamente el botón de «acepto») y que generalmente tienen incluida una cláusula que les da permiso de examinar y almacenar nuestra información<sup>28</sup>. Esta licencia se asocia a los programas que no permiten ni siquiera compartirse, a menos que sea de manera ilegal o pirata (y aunque ilegal, legítima en el sendero hacia una soberanía tecnológica<sup>29</sup>), éste tipo de licencia es conocida como software privativo o propietario y no permite que el usuario controle el programa, sino que el programa restringe casi completamente al usuario.

b) La otra es la Licencia Pública General (GPL<sup>30</sup>) la cual consta de cuatro libertades irreductibles para considerarse como GPL:

o: La libertad de usar el programa, con cualquier propósito (uso).

1 : La libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a las propias necesidades (estudio).

2: la libertad de distribuir copias del programa, con lo cual se puede ayudar a otros usuarios (distribución).

3: la libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie (mejora).

Los programas que posean esta licencia son reconocidos como Software Libre. Entonces, retomando dos elementos anteriores como lo son el movimiento del Software Libre y el Software Libre ya como programa y recalando la coexistencia de su esfuerzo aunado, es notoria la manifestación de realidades inmateriales para la protección de la información y el anonimato en las redes, o sea, el Software Libre nos brinda herramientas y métodos para nuestra seguridad en distintos ámbitos de la informática, los cuales pueden enumerarse de la siguiente forma:

---

<sup>27</sup> Linux es el Kernel (núcleo) que permite la interacción del hardware y software, de ese modo GNU/Linux (Software/Núcleo), por ende, cuando nombramos únicamente Linux, nos estamos refiriendo solo al núcleo y dejamos de lado todo el movimiento social que caracteriza al software libre.

<sup>28</sup> Licencias de uso como las de las plataformas digitales, google, facebook, youtube y demás, indican en sus contratos que la información que por sus servidores circule podrá ser usada como mejor le convenga a la empresa. En el caso de los programas, la mayoría suministran la información, pues tienen la capacidad de enviarla a sus servidores, por ejemplo: los archivos con extensión pdf que son abiertos con Acrobat Reader son enviados a una base de datos (servidores) de Adobe y si leemos los informes filtrados por Wikileaks y Snowden se encontrará la colaboración entre la empresa y las agencias de inteligencia.

<sup>29</sup> Concepto asociado al desarrollo tecnológico en términos de autonomía para la creación y el uso de las herramientas requeridas (Hardware & Software) para satisfacer las necesidades de una nación (algo similar a la soberanía alimentaria).

<sup>30</sup> Es una licencia de derechos de autor usada ampliamente en el ámbito del Software Libre y el movimiento de código abierto (este movimiento solo comparte el concepto de compartir el código fuente de los programas, ignorando completamente la parte política y filosófica), está basada en el principio de prohibido prohibir y es la sucesión del Copyleft.

- Iniciando por el S.O. existe una gran variedad de distribuciones GNU/Linux<sup>31</sup>.
- La red TOR<sup>32</sup>, VPN (Virtual Private Network), Proxys<sup>33</sup>.
- Encriptación de la red, encriptación de correos<sup>34</sup>.
- Cifrado de archivos, cifrado de carpetas.
- Cifrado de particiones de discos duros, cifrado completo de discos.
- Creación de particiones virtuales y su cifrado, creación de discos duros virtuales y su cifrado.
- Clonaciones de los seriales del hardware.
- Implementación de un S.O. no instalado en disco duro<sup>35</sup>.

Hasta aquí puede parecer que hemos olvidado otros aparatos que cumplen la función de conectarnos, sin embargo, al no requerir de un sesudo análisis para explicar y entender que tanto las tabletas electrónicas (tablets), como los dispositivos

móviles (celulares) son los aparatos más inseguros, debido a que sostienen una relación de dependencia extrema con los servicios de Google (no funciona sin ello), se ha dejado para el final (aquí también caben microsoft y apple con sus respectivos aplicaciones y pseudoservicios).

Los usuarios de celulares y/o tablets (que es casi todo el mundo) están obligados a tener un correo de gmail para activar la cuenta de la tienda de Google, para permitir que las aplicaciones funcionen correctamente, de modo que, el problema aquí es quien obliga a las personas a usar sus servicios, por ende, la alternativa a ofrecer es cambiar el S.O. de éstos dispositivos, cortando el problema de raíz. Tales alternativas son los S.O. Openmoko<sup>36</sup>, Replicant<sup>37</sup>, LineageOS<sup>38</sup>. Ahora, para una solución menos radical podemos mencionar la tienda de aplicaciones (repositorio) F-Droid<sup>39</sup>, ésta puede funcionar en cualquier S.O. de celulares/tabletas y no requiere de un registro previo o posterior a su uso, además de que no solicita los permisos requeridos para la manipulación del dispositivo (si la intención no es controlar, no los necesita).

<sup>31</sup> Las cuales podemos encontrar en <https://distrowatch.com>.

<sup>32</sup> Conocemos TOR como un navegador, un programa, sin embargo, no es del todo cierto pues TOR es una red completa de servidores que permiten el anonimato en la red.

<sup>33</sup> Todas las herramientas descritas son protocolos para pasar desapercibido en la red.

<sup>34</sup> Bitmessage, S/MIME, TLS, PGP, GPG... Las diferencias entre los protocolos son las maneras como se encripta, se almacena y viaja la información.

<sup>35</sup> Esto se conoce como una Memoria Viva y consiste en usar un S.O. desde una USB, CD/DVD, FDD (Flash Disk Drive) sin la necesidad de usar el disco duro del Pc en mención. Esto permite ocultar cualquier registro de cualquier actividad realizada en dicho equipo. Ahora bien, son tantos los protocolos, programas, redes y formas de protegernos de manera virtual que resulta insólito que no se conozcan o se pongan en práctica, asimismo, al ser un mercado tan ingente no es posible enfocarse en todas.

<sup>36</sup> Es un proyecto el cual creó el primer S.O. libre para móviles a nivel mundial. Cabe recalcar que puede reprogramarse como el usuario desee y no depende de los servicios de terceros. [https://wiki.openmoko.org/wiki/Main\\_Page/es](https://wiki.openmoko.org/wiki/Main_Page/es)

<sup>37</sup> Es un S.O. basado en Android. Replicant ha reemplazado todos los drivers y programas de privativos de Android por código abierto, además deja de usar los servicios de terceros. <https://replicant.us>

<sup>38</sup> Similar a Replicant, pero permite elegir entre usar los servicios de terceros o no. <https://lineageos.org>

<sup>39</sup> Repositorio para Android, alberga únicamente aplicaciones de software libre y código abierto. <https://f-droid.org>

A manera de conclusión podemos decir que el Software Libre nos ha proporcionado una gran cantidad de herramientas para desarrollar una actividad en particular, diseño, contabilidad, simuladores y demás, pero, para efectos de este artículo las herramientas que se recomiendan son aquellas en las que podemos refugiarnos, salvaguardarnos, eso sí, con el fin de continuar trabajando por una sociedad más equitativa. Sabemos pues, que el Software Libre no es el fin, pero puede ser la manera de materializar las ideas de aquellos tantos que se han pensado una forma de organización más humanitaria.

**Nota:** Sabemos bien que durante este intento de artículo se han insinuado métodos y herramientas que no se desarrollan, una explicación racional para ello es la complejidad que acarrea el desarrollo teórico en conjunción de diversos manuales o tutoriales para el manejo de los elementos expuestos, sin embargo, dejaremos un compendio de enlaces para acceder al material de interés, desde navegación anónima, hasta cifrado de archivos y otros. Y como la seguridad trasciende los S.O. habrá tutoriales para windows y GNU/Linux.

## Manuales

<https://openlibra.com/es/book/manual-basico-de-seguridad-informatica-para-activistas>

<https://openlibra.com/es/book/defiende-tu-pc-guia-de-seguridad-para-ordenadores-personales>

<https://openlibra.com/es/book/circumvention-tools-evadiendo-la-censura-en-internet>

<http://cryptoperiodismo.org/leer>

## Bibliografía y Cibergrafía

Batty, M., & Smith, A. (2002). *Virtuality and cities. Definitions, geographies, design*. En P. Fisher & D. Unwin (Eds.), *Virtual geography* (pp. 270-291). London: Taylor & Francis.

Graham, S., & Marvin, S. (2001). *Telecommunications and the city. Electronic spaces, urban places*. Londres: Routledge.

Borosage, R. and Marks, J. (1976). *Los archivos de la C.I.A.*. 1st ed. Mexico D.F.: Diana S.A.

Chaparro, J. (2017). *Un mundo digital: territorio, segregación y control social a inicios del siglo XXI*. 1st ed. Bogotá: Universidad Nacional de Colombia, Sede Bogotá, Facultad de Ciencias humanas.

Han, B. (2012). *La sociedad de la transparencia*. 1st ed. España: Herder, pp.69, 93.

Hermelin, D. (2017). *Una mirada crítica al estudio de las relaciones entre desastres, medios, saberes, poder y sociedad*. Trilogía Ciencia Tecnología Sociedad, 9(17).

Merejo, A. (2017). *La globalización del ciber mundo*. Trilogía Ciencia Tecnología Sociedad, 9(17).

Molina, J. (2001). *El análisis de las redes sociales. Una introducción*. 1st ed. Barcelona: Bellaterra, S.L.

Lyon, D (1994). *El ojo electrónico. El auge de la sociedad de vigilancia*. (Eds.), Alianza Editorial (pp. 41-45). Madrid.

Privacyinternational.org. (2015). *Un estado en la sombra: vigilancia y orden público en Colombia*. [online] Available at: [https://privacyinternational.org/sites/default/files/2017-12/ShadowState\\_Espanol.pdf](https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf) [Accessed 23 Jan. 2019].

El Tiempo (2019). [online] Available at: <https://www.eltiempo.com/archivo/documento/CMS-5436047> [Accessed 10 Jan. 2019].

Mancini, P. and Fernández, N. (n.d.). *Cryptoperiodismo*. [online] Cryptoperiodismo.org. Available at: <http://cryptoperiodismo.org/leer/> [Accessed 26 Feb. 2019].

El diario (2019). [online] Available at: [https://www.eldiario.es/catalunya/anarquistas-Barcelona-libertad-prision-preventiva\\_o\\_177082324.html](https://www.eldiario.es/catalunya/anarquistas-Barcelona-libertad-prision-preventiva_o_177082324.html) [Accessed 20 May 2019].

---

RT (2019). [online] Available at: <https://actualidad.rt.com/actualidad/view/28336-Detienen-a-tres-hackers-de-red-Anonymous-en-Espa%C3%B1a> [Accessed 30 Jan. 2019].

Semana (2019). [online] Available at: <https://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3> [Accessed 25 May 2019].

Semana (2019). [online] Available at: <https://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3> [Accessed 21 Nov. 2018].

Washington Post (2019). [online] Available at: <https://www.washingtonpost.com/wp-srv/national/longterm/unabomber/manifesto.text.htm?nedirect=on> [Accessed 30 May 2019].

Gnu.org. (n.d.). Overview of the GNU system. [online] Available at: <https://www.gnu.org/gnu/gnu-history.html> [Accessed 23 Mar. 2019].

Fsf.org. (n.d.). Free Software Foundation. [online] Available at: <https://www.fsf.org/> [Accessed 11 May 2019].

Silveira, S. (2013). Aaron Swartz y las luchas por la libertad del conocimiento. Conectas, [online] (28). Available at: <https://sur.conectas.org/es/aaron-swartz-y-las-luchas-por-la-libertad-del-conocimiento/> [Accessed 30 May 2019].