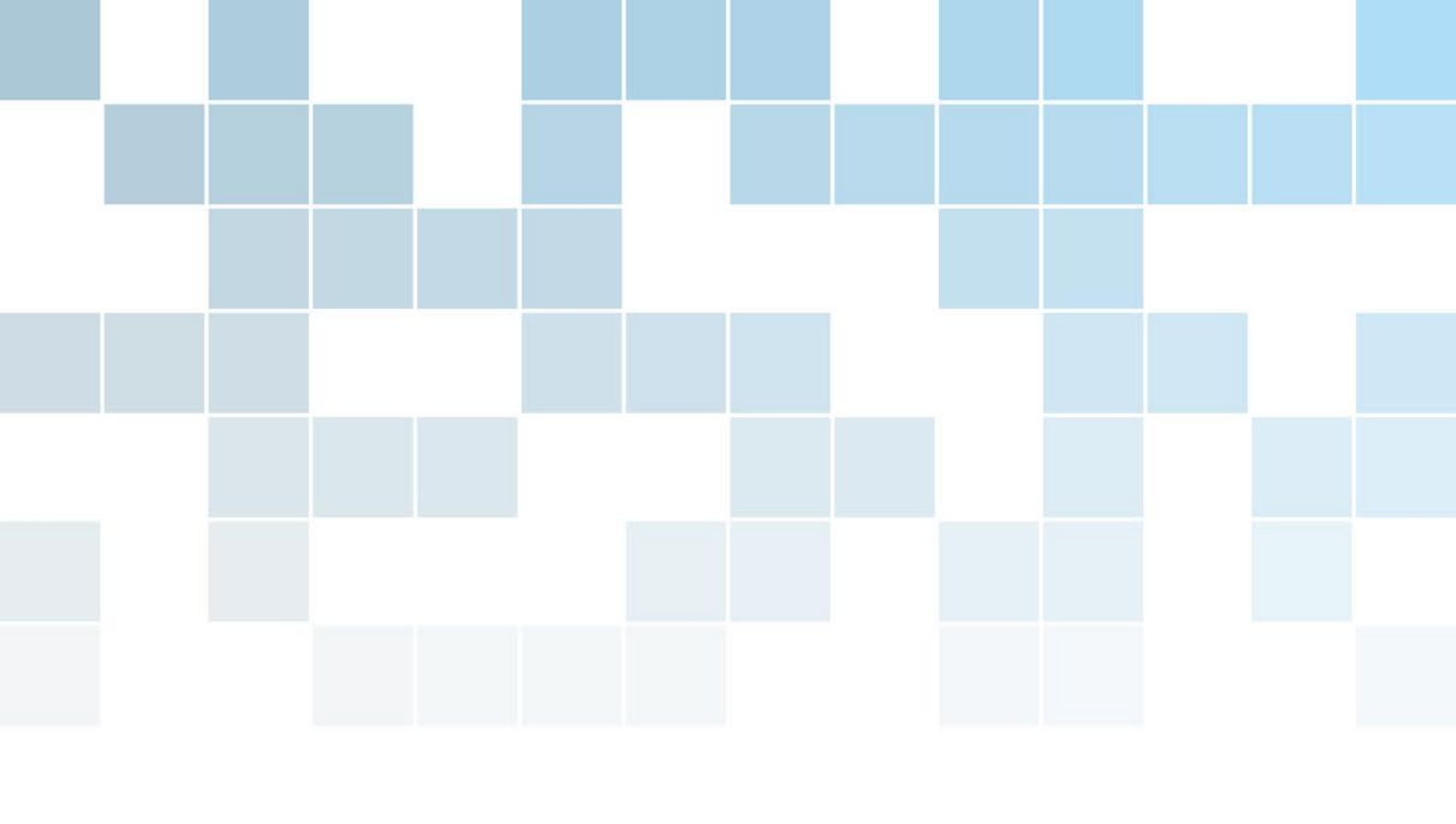
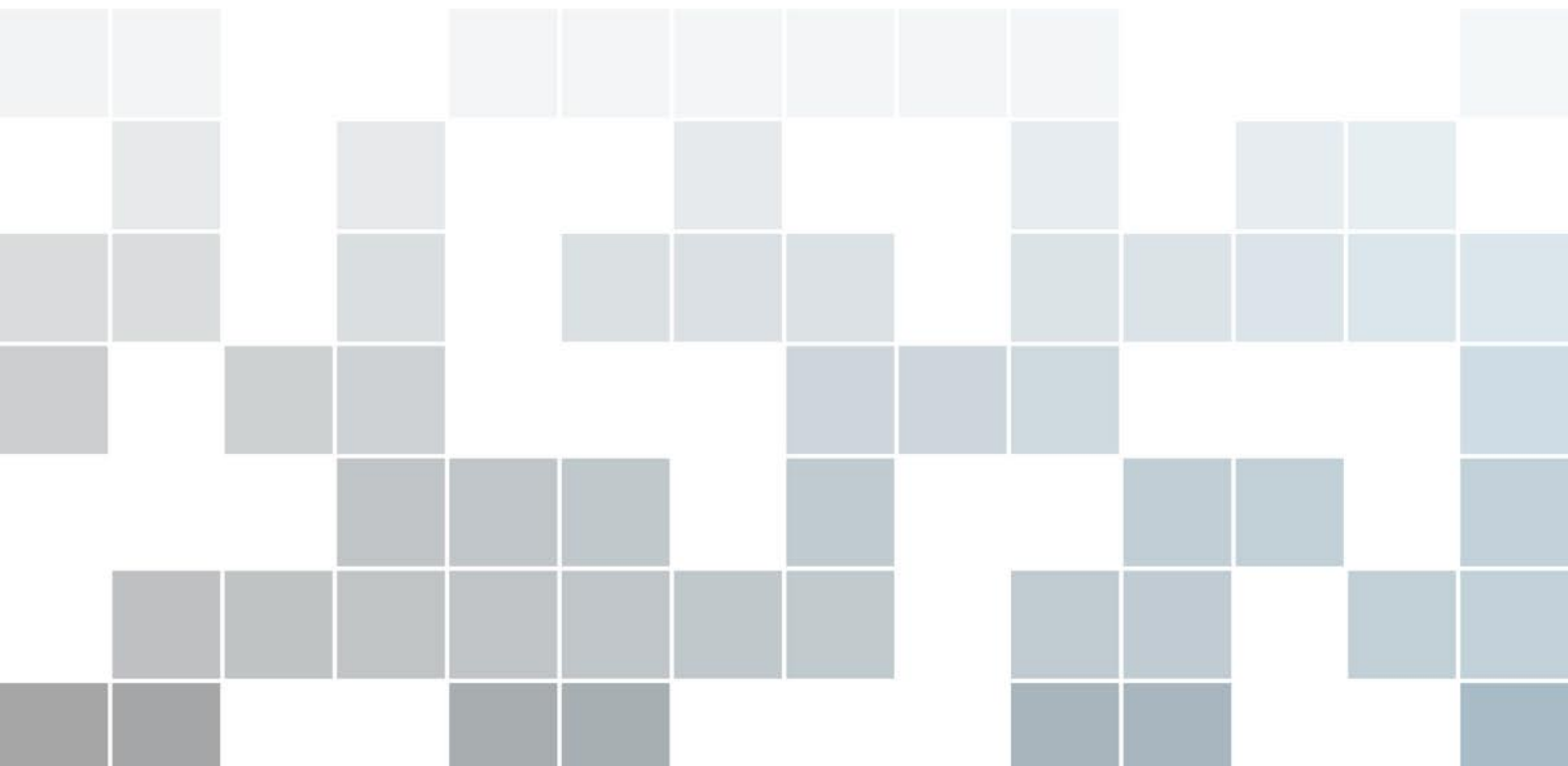




Nuestra Privacidad ha sido *Hackeada*

Aprende a protegerte

Fernando Méndez



Copyright © 2020 Fernando Méndez

[PUBLISHED]

`HTTPS://FERMDEZ.DDNS.NET`

Licensed under the Creative Commons Attribution-NonCommercial 4.0 Unported License (the “License”). You may not use this file except in compliance with the License. You may obtain a copy of the License at <https://creativecommons.org/licenses/by-nc/4.0/>. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Primera Edición, Marzo 2020

Índice general

I	Primera Parte: Empresas	
1	Introducción	7
2	OK Google	9
2.1	Mi cuenta de Google	11
2.1.1	Gestión de la privacidad	12
2.1.2	El equilibrio de la balanza	14
2.2	Android	15
3	Facebook, humanos, Facebook	17
3.1	Facebook	20
3.1.1	Mi cuenta de Facebook	20
3.2	Whatsapp	23
3.3	Instagram	24
II	Segunda Parte: Gobiernos	
4	NSA - National Spy Agency	27
4.1	Los programas de vigilancia de la NSA	29
4.1.1	PRISM	29
4.1.2	XKEYSCORE	29

4.1.3	TEMPORA	29
4.1.4	BULLRUN y EDGEHILL	30
4.1.5	QUANTUM y FOXACID	30
5	China && Huawei	31
6	La startup de la CIA	33
	Bibliografía	35
	Webs	35
	Artículos	37
	Índice alfabético	39



Primera Parte: Empresas

1	Introducción	7
2	OK Google	9
2.1	Mi cuenta de Google	
2.2	Android	
3	Facebook, humanos, Facebook	17
3.1	Facebook	
3.2	Whatsapp	
3.3	Instagram	

1. Introducción

A parte del hecho de que esté escribiendo este *libro*, nada de lo que ha pasado en los últimos años me sorprende. Construimos máquinas, enormes centros de procesamiento de datos, un ejercito entero no tripulado.

Pero qué sucede cuando los *malos* roban las llaves, cuando todo aquello que construimos para informarnos, para mantenernos a salvo, se volvió contra nosotros.

Fue entonces cuando lo descubrimos, la privacidad no existe, o por lo menos, el concepto que hasta ahora teníamos de ella. Lo que hace unos años considerábamos nuestro y que, *de puertas para dentro quedaba en familia*, hoy podría conocerlo cualquiera.

Sin embargo, tengo una decepcionante noticia para la mayoría de vosotros, no importamos. No somos más que números o identificadores en una base de datos enorme. Este identificador asocia a nosotros atributos como nombre, edad, gustos, preferencias, tendencias de voto e incluso situación emocional en la que nos encontramos. Todos estos datos pueden variar y ser más o menos relevantes, dependiendo de aquello en concreto que, *el que esté al otro lado* quiera saber de nosotros.

Debemos tener claro que lo único que podemos considerar privado, es sólo aquello que pensamos, interiorizamos y jamás compartimos con nadie, ni de forma hablada ni de forma escrita. Son sólo nuestros pensamientos más profundos, nuestra privacidad a día de hoy. Teniendo ese concepto claro, podremos empezar a controlar lo que saben de nosotros.

Pues aunque no lo creamos, todo lo que las empresas, gobiernos y resto de personas del mundo saben o pueden saber sobre nosotros, lo decidimos nosotros, muchas veces sin saber los términos y condiciones que aceptamos al crear cualquier cuenta de usuario.

Las empresas no engañan a nadie, somos nosotros, con nuestro desconocimiento los que nos dejamos vulnerables. Aunque es cierto que, en algunas ocasiones, esos datos son extraídos por terceros de forma ilegal.

Y es que en el mundo hay más de 7.000 millones de seres humanos. Seguro que si una única persona controlase el suministro de agua de 2.500 millones de personas (más de un tercio de la población mundial), nos opondríamos. Sin embargo ¿alguno es consciente de que una sola persona controla la información de 2.500 millones de personas? Pues es cierto y lo mejor de todo es que no la ha comprado, no la ha robado, se la hemos cedido voluntariamente.

Es aquí donde entro yo, donde entra este libro. Pues con él, no pretendo generar una legión de personas paranoicas con un gorro de papel de plata en la cabeza que crean que los satélites les geo-localizan las 24 horas del día y controlan nuestra vida.

Con este libro quiero hacer que todo aquel que lo lea, sea consciente de los datos que cede en cada momento. Aunque, sí, también hablaremos más adelante de escándalos de empresas y gobiernos que han sobrepasado las leyes para beneficiarse a través de un uso indebido de los datos de los usuarios. Incluso gobiernos que han sobrepasado sus propias leyes civiles en nombre de la *libertad* y seguridad nacional.

Por último, como parte de esta introducción, he de decir que este no es un libro orientado a que pases largas horas leyendo una trama con un introducción, nudo y desenlace. Es más, no tienes ni por qué leer los capítulos en un orden concreto. Este libro está orientado a concienciar, a leerlo en una tarde, pero consultarlo cada vez que lo necesites, el resto de tu vida.

Por el hecho de ser paranoico, no significa que no te sigan.

2. OK Google

Comencemos por el comienzo. La pionera en esto de recopilar información de los usuarios, Google. Fueron de los primeros que empezaron a ganar dinero sin vendernos nada (por lo menos, no de forma directa), sólo y únicamente ofreciéndonos publicidad en base a nuestros gustos e intereses. O incluso, basándose en nuestro pasado para conocer nuestras tendencias futuras.

Es prácticamente imposible a día de hoy, estar fuera del *alcance* de Google. Si usas su buscador, si tienes un teléfono Android¹ o si tienes una cuenta de Gmail², Alphabet³ te conoce.

Supongo que nadie que esté leyendo este libro, habrá quedado exento de usar o haber usado, al menos uno de los servicios que acabo de mencionar.

Google no se libra de escándalos relacionados con el incumplimiento de políticas de privacidad.

Una demanda colectiva, impuesta en 2019, relaciona a Google y la Universidad de Chicago. A estos se les acusa de compartir de manera inapropiada con el gigante tecnológico los registros médicos confidenciales de miles de pacientes en Estados Unidos.

Según un reporte de The New York Times⁴, la institución médica y el gigante tecno-

¹Android es un sistema operativo móvil desarrollado por Google, basado en Kernel de Linux y otros software de código abierto.[2]

²Gmail es un servicio de correo electrónico gratuito proporcionado por la empresa estadounidense Google Inc.[3]

³Alphabet Inc. es una empresa multinacional estadounidense cuya principal filial es Google, que desarrolla productos y servicios relacionados con Internet, software, dispositivos electrónicos y otras tecnologías.[1]

⁴The New York Times es un periódico publicado en la ciudad de Nueva York, que se distribuye en los Estados Unidos.[4]

lógico hicieron una alianza en 2017 para compartir los registros de pacientes con el objetivo de mejorar el análisis predictivo de enfermedades con la ayuda de inteligencia artificial.

Frente a esta situación, un portavoz de Google dijo a The New York Times: *'Creemos que nuestra investigación sobre el cuidado de la salud podría ayudar a salvar vidas en el futuro, razón por la cual tomamos en serio la privacidad y seguimos todas las reglas y regulaciones relevantes en nuestro manejo de la salud'*.

El Centro Médico de la Universidad de Chicago es acusado de no notificar a sus pacientes ni obtener su consentimiento expreso, antes de entregar sus registros médicos confidenciales a Google 'para su propio beneficio comercial'.

Dividiremos este capítulo en secciones para que sea más amigable. Estas secciones serán, uno por uno, los principales servicios que la mayoría de nosotros usamos, pertenecientes a Google y cómo gestionarlos correctamente.

2.1 Mi cuenta de Google

En nuestra cuenta de Google se encuentra el epicentro gestor de la información que les cedemos. Desde aquí podemos gestionarlo todo y saber de qué información dispone Google sobre nosotros. Hay que admitir que de todas las empresas que basan su negocio en la información de sus usuarios, Alphabet es la que más accesible nos pone el control de todos estos datos.

Aunque a alguno le sorprenda, por defecto, a través de nuestra cuenta de Google y dependiendo de los dispositivos en los que hayamos iniciado sesión con ella, pueden tener acceso a la siguiente información:

- Historial de búsquedas.
- Historial de reproducciones de YouTube.
- Tiempo que pasamos navegando o en alguna aplicación.
- Localización en tiempo real.
- Aprendizaje de lugares que visitamos frecuentemente (casa, trabajo, universidad...)
- Si nos movemos del punto 'A' al punto 'B' andando o en qué medio de transporte (incluyendo velocidad, ruta y tiempo de recorrido).
- Gustos, intereses, estado de ánimo...

A continuación se muestra una imagen de un perfil generado por Google sobre un usuario, únicamente basándose en los datos que le permitimos recopilar, cuantos más datos, más preciso será el perfil. En este caso, el usuario cuida bien su privacidad, pues aunque no lo creamos, la información de este usuario es muy genérica y poco precisa.

Nos sorprende observar que, no sólo hay información sobre nuestro *sexo*, *edad* y *gustos*, también encontramos información como el ESTADO CIVIL, ESTADO PARENTAL E INCLUSO PROPIEDADES DE VIVIENDAS.



Figura 2.1: Ejemplo de un perfil de usuario creado por la información obtenida por Google

2.1.1 Gestión de la privacidad

Haremos un receso en este punto, pues muchos os estaréis preguntando en este mismo instante cómo gestionar la información de la cuenta de Google.

Los pasos son muy sencillos:

1. Accedemos o *google.com* con la sesión iniciada en la cuenta de usuario que queremos gestionar. Y entramos en *Gestionar tu cuenta de Google*.

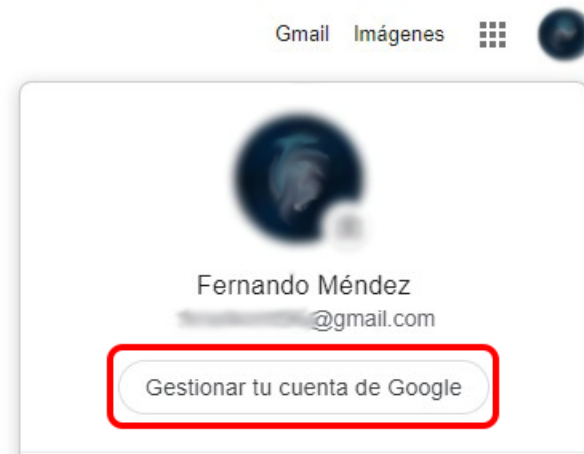


Figura 2.2: Panel del perfil

2. Nos redirigirá a nuestro *Panel de control de la cuenta*. Aquí observaremos todos los ajustes que podemos modificar, sólo hay que curiosear un poco para ver todo lo que podemos personalizar.

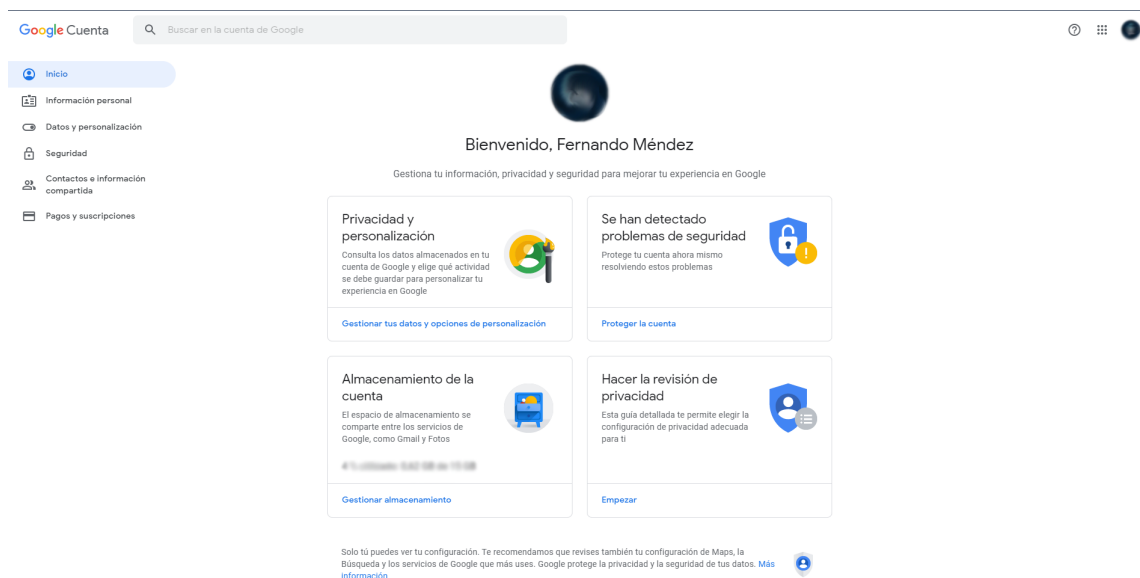


Figura 2.3: Panel de control de la cuenta de Google

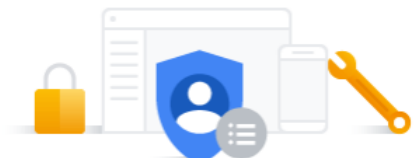
3. Si accedemos por ejemplo al panel de *Datos y personalización*, podremos detener todos los historiales de registros que Google controla.

Datos y personalización

Tus datos, actividad y preferencias para que los servicios de Google te resulten más útiles

Hacer la revisión de privacidad

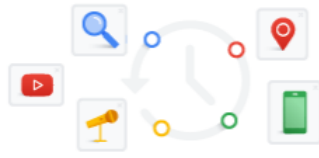
Esta guía detallada te permite elegir la configuración de privacidad adecuada para ti



[Empezar](#)

Controles de la actividad de tu cuenta

Guarda tu actividad si quieres disfrutar de una experiencia más personalizada en Google. Puedes activar o pausar estos ajustes cuando quieras.



 Actividad en la Web y en Aplicaciones	 Detenido	>
 Historial de ubicaciones	 Detenido	>
 Historial de YouTube	 Detenido	>

[Gestionar los controles de la actividad de tu cuenta](#)

Figura 2.4: Controles de la actividad de tu cuenta

2.1.2 El equilibrio de la balanza

Está claro que limitar el uso que hacen las empresas de nosotros es muy importante, sin embargo, es su modelo de negocio y, aunque los servicios sean gratuitos, nadie regala nada.

Debemos tener en cuenta que aumentar nuestra privacidad disminuye de forma proporcional la cantidad de ventajas y servicios que podemos usar.

Por ejemplo, si desactivamos el historial de búsquedas de YouTube, Google dejará de saber con exactitud cuáles son nuestros gustos musicales. Sin embargo, si veo un vídeo que me gusta y no lo almaceno en una lista de reproducción o lo guardo de alguna forma, luego no podré encontrarlo si no recuerdo cuál era el título. Lo mismo pasaría con el historial de ubicaciones.

Hay que buscar el equilibrio entre los servicios que deseamos usar en nuestro día a día y lo que saben de nosotros. No debemos dar más datos de los necesarios, pero siendo realistas, no vamos a dejar de usar *Google Maps* cuando volvemos a casa después de una larga noche de fiesta y sin saber siquiera dónde estamos.

Es por ello que si nos ponemos a desactivar como locos y sin leer servicios de Google, podremos observar que tenemos una experiencia de usuario peor a la que solíamos tener con anterioridad.

Si lo que de verdad queremos es que no sepan nada de nosotros, la solución es no crear una cuenta de usuario o borrar las que tenemos e irnos a vivir a una cueva en medio del bosque sin contacto alguno con la civilización.

Obviamente esto es una exageración y una locura que nadie va a hacer, así que, no te preocupes ni te pongas paranoico, pues como contábamos en la introducción de este mismo libro, el concepto de privacidad ha cambiado por completo y tenemos que aprender a adaptarnos a estos nuevos conceptos. Al fin y al cabo, es el objetivo de este libro.

Con ello tampoco quiero que veáis a las empresas como ladrones de datos sin escrúpulos. Su objetivo, es ganar dinero, para ello ofrecen servicios que los usuarios podemos querer o no, pero si los queremos tenemos que pagar el precio. No hay que confundir que los servicios sean gratuitos económicamente con el hecho de que no nos cueste nada.

Nadie da nada gratis y eso se deja claro en todos los términos y condiciones de los contratos que aceptamos al crear una cuenta de usuario en cualquier web, red social o comercio.

2.2 Android

Este es el Sistema Operativo móvil⁵ por excelencia. A día de hoy, más del 80 % de los *smartphones* o *tablets* usan Android. El resto, usa mayoritariamente iOS⁶. Y, aunque vayamos a hablar de Android, pues es propiedad de Google, la mayoría de lo que se cuenta en esta sección se puede extrapolar a iOS y Apple.

Teniendo en cuenta que lo que nos acompaña a lo largo del todo el día, desde que nos levantamos hasta que nos acostamos, es el teléfono, no es exagerado decir que estos dispositivos nos conocen mejor que nuestras propias madres, pues es así. Están a la escucha, pueden grabar todo lo que decimos y hacemos, recopilan toda la información posible sobre nuestros hábitos, conversaciones, consultas en la web. Se comunican con otros dispositivos cercanos para saber con quién estamos en cada instante de tiempo.

En resumen, si hay algo que nos define mejor que nada, es nuestro teléfono móvil.

Que a nadie le sorprenda, pero cuando encendemos por primera vez nuestro nuevo y flamante smartphone y aceptamos sin leer todos esos términos y condiciones, por el simple hecho de tener muchísimas ganas de comenzar a usarlo, estamos cometiendo un gravísimo error. Por defecto, cedemos a Google (o Apple en caso de los iPhones), el derecho a grabar en cualquier momento del día nuestras conversaciones, tener acceso a la cámara del dispositivo y recopilar toda la información guardada en el teléfono.

Es curioso e incluso divertido que además, en el caso de Android, desde nuestra cuenta de Google, podemos acceder a algunos de los fragmentos de estas grabaciones de audio.

El pasado mes de Noviembre de 2019, una brecha de seguridad permitió que, durante cinco días, decenas de miles de personas descargaran grabaciones desde la nube a las que, en teoría, no debían tener acceso. Google se disculpó tras haber permitido, por equivocación, que completos desconocidos accedieran a vídeos de los usuarios.

Y aunque Google insiste en que pone especial cuidado en proteger nuestra información, al mismo tiempo sigue vigilando nuestros movimientos, incluso cuando dice que no es así. Una reciente investigación realizada por Associated Press⁷ descubrió que, muchos de los servicios de Google para Android y Apple almacenan los datos de ubicación de los usuarios incluso cuando estos habían desactivado esa opción en la configuración de privacidad.

Alphabet además, compra información de aplicaciones externas y luego la cruza con otros datos que tiene de cada usuario. Todo esto permite la creación de perfiles de comportamiento que luego son vendidos a los anunciantes, con grandes beneficios para Google (Alphabet).

⁵Un sistema operativo móvil o SO móvil es un conjunto de programas de bajo nivel que permite la abstracción de las peculiaridades del hardware específico del teléfono móvil y provee servicios a las aplicaciones móviles, que se ejecutan sobre él.[5]

⁶iOS es un sistema operativo móvil de la multinacional Apple Inc. Originalmente desarrollado para el iPhone, después se ha usado en dispositivos como el iPod touch y el iPad. [6]

⁷The Associated Press o AP es una agencia de noticias de Estados Unidos.[7]

Con datos reales en la mano, podemos afirmar que, si tienes un teléfono Android, le envías 12 megabytes (MB) de información personal al día a Google, mientras que el iPhone le envía unos 6 MB.

Enfrentarse al duopolio Google/Apple no es fácil, incluso empresas tan poderosas como Microsoft⁸ lo intentaron con Windows Phone⁹ y fracasaron. Es tan poderosa la influencia que ejercen los teléfonos inteligentes sobre nuestras vidas, que muchos usuarios prefieren hacer *la vista gorda* a la recopilación de información que realizan los gigantes tecnológicos. A esto se le suma una enorme falta de conciencia respecto a este tema, algo que intentamos poner fin con este libro.

Cerca de dos tercios de los encuestados en Estados Unidos no sabía que Google compra información a aplicaciones externas. Más de la mitad, no se había dado cuenta de que sus cuentas de Google estaban vinculadas con sus búsquedas en la web.

La actitud ante esto, sin embargo, está cambiando. Las numerosas violaciones de datos están impulsando a que los usuarios empiecen a estar, cada vez, más concienciados.

⁸Microsoft Corporation es una compañía tecnológica multinacional con sede en Redmond, Washington, EE.UU.[8]

⁹Windows Phone (abreviado WP) es un sistema operativo móvil, desarrollado por Microsoft como sucesor de Windows Mobile.[9]

3. Facebook, humanos, Facebook

Muchos pensaréis en Facebook como la red social¹ y ya está. Muchos os equivocaréis. Facebook Inc. es la empresa más importante del mundo en lo que a redes sociales se refiere.

Facebook Inc. controla redes tan importantes como Whastapp, Instagram, Messenger y, cómo no, el propio Facebook.

Con todas estas compras y adquisiciones, Facebook se ha hecho a lo largo de los años con la mayor base de datos de la historia sobre miles de millones de usuarios. Siendo esto, en la era de la información en la que vivimos, el tesoro más importante del que disponen y que muchas otras empresas querrían tener.

Cuando aceptamos los términos y condiciones de cualquier red social perteneciente a Facebook, aceptamos el tratamiento directo de nuestros datos por la propia empresa y **el tratamiento de forma anónima por terceros**, a las que Facebook puede vender estos datos. Empresas de confianza y con buenas intenciones que quieran usar esta enorme base de datos de Facebook (o una parte), para hacer estudios, predicciones o vender productos.

A pesar de estos términos y condiciones, **Facebook sobrepasó sus propios límites y en 2018 incumplió sus propias normas, con el escándalo de Cambridge Analytica.**

El escándalo de datos de Facebook-Cambridge Analytica fue un gran escándalo político a principios de 2018, cuando se reveló que Cambridge Analytica había recopilado los datos personales de millones de perfiles de Facebook de personas sin su consentimiento y los utilizó con fines publicitarios políticos.

Se ha descrito como un momento decisivo en la comprensión pública de la privacidad en

¹Una red social es una estructura social compuesta por un conjunto de usuarios que están relacionados de acuerdo a algún criterio.[10]

internet y precipitó una caída masiva en el precio de las acciones de Facebook y propició una regulación más estricta del uso de datos personales por parte de las empresas tecnológicas.

En un principio se especuló mucho con el número de usuarios afectado por esta recopilación ilegal de datos. Facebook más tarde confirmó que en realidad, se habían visto comprometidos datos sobre hasta 87 millones de usuarios, de los cuales, 70.6 millones de esas personas eran de Estados Unidos.

Hubo muchas especulaciones sobre una equivalencia entre el uso de datos por Cambridge Analytica y la campaña de Barack Obama² de 2012, que, según Investor's Business Daily³, *'alentó a los simpatizantes a descargar una aplicación de Obama en 2012 que, cuando se activaba, permitía que dicha aplicación recopilase datos de Facebook tanto sobre los usuarios como sobre sus amigos'*.

Lo que está claro es que los datos obtenidos se usaron principalmente para **marketing dirigido a los votantes intencionalmente incomodados**.

El director ejecutivo de Facebook, Mark Zuckerberg, primero se disculpó por el escándalo con Cambridge Analytica en la CNN⁴, llamándolo un *'problema'*, un *'error'* y una *'violación de la confianza, en efecto'*, les recordó su derecho de acceso a los datos personales. Otros directivos de Facebook argumentaron en contra de llamarlo una *'violación de datos'*, argumentando que aquellos que realizaron el cuestionario, consintieron ceder su información personal.

Zuckerberg se comprometió a hacer cambios y reformas en la política de privacidad de Facebook para evitar violaciones similares en un futuro.

El 25 de marzo de 2018, Zuckerberg publicó una carta personal en varios periódicos disculpándose en nombre de Facebook.

Otras empresas como Amazon⁵ dijo que cesaron a Cambridge Analytica de usar sus servicios web, cuando se enteraron de que su servicio estaba recopilando información personal.

A principios de julio de 2018, la Oficina del Comisionado de Información del Reino Unido anunció que tenía la intención de multar a Facebook 500.000 libras esterlinas (663.000 dólares) por el escándalo de los datos, siendo esta la multa máxima permitida en el momento de la infracción, diciendo que Facebook *'contravenía la ley al no salvaguardar la información de las personas'*.

²Barack Hussein Obama es un político estadounidense que ejerció como el 44 presidente de los Estados Unidos de América desde el 20 de enero de 2009 hasta el 20 de enero de 2017.[11]

³Investor's Business Daily es un periódico y sitio web estadounidense que cubre el mercado de valores, los negocios internacionales, las finanzas y la economía.[12]

⁴CNN o Cable News Network es un canal de televisión por suscripción estadounidense.[13]

⁵Amazon, Inc. es una compañía estadounidense de comercio electrónico y servicios de computación en la nube a todos los niveles.[14]

En marzo de 2019, una demanda judicial del Fiscal General del Distrito de Columbia de los Estados Unidos alegó que Facebook sabía de las *'prácticas de recopilación de datos inadecuadas'* de Cambridge Analytica meses antes de que se informaran públicamente por primera vez en diciembre de 2015.

En julio de 2019, la Comisión Federal de Comercio votó a favor de aprobar multar a Facebook alrededor de 5.000 millones de dólares para resolver finalmente la investigación del escándalo.

Durante su testimonio ante el Congreso el 10 de abril de 2018, Mark Zuckerberg dijo que fue su error personal y que no hizo lo suficiente para evitar que Facebook fuera utilizado para causar daño. *'Eso va por las noticias falsas, la interferencia extranjera en las elecciones y el discurso de odio'*. Durante el testimonio, Mark Zuckerberg se disculpó públicamente por la violación de datos privados: *'Fue mi error, y lo siento. Yo empecé Facebook, lo dirijo y soy responsable de lo que sucede aquí'*.

Posteriormente **se le pidió a Cambridge Analytica que eliminara todos los datos recopilados. Más tarde fue descubierto por The Guardian⁶ y The New York Times que los datos no habían sido eliminados.**

Según The Associated Press, una empresa dirigida por ex-directivos de Cambridge Analytica, *Data Propria*, ha estado trabajando para conseguir la reelección del presidente Donald Trump en 2020.

A día de hoy, **Facebook no para de intentar mejorar su imagen**, modificando sus políticas de privacidad para proteger al usuario y notificando de todas las formas que tenemos de decidir qué datos compartimos sobre nosotros en sus redes sociales.



Figura 3.1: Ejemplo de iniciativas por parte del equipo de Facebook para recuperar la confianza de los usuarios.

⁶The Guardian es un diario británico.[15]

3.1 Facebook

Ahora sí, hablamos de **Facebook como red social, no como empresa**.

Se considera la red social por excelencia y, aunque no fue la primera, sí que fue la que más ha triunfado, marcando un antes y un después en esto de conectar a las personas a través de internet.

A día de hoy, **Facebook cuenta con alrededor de 2.320 millones de usuarios** registrados por todo el mundo.

Esta red social muestra un perfil muy *idealizado* del usuario, pero no como Instagram, donde la gente quiere mostrar simplemente su mejor imagen, si no que, en Facebook, quieres mostrar tus mejores aptitudes en el día a día, de la forma más real posible.

Vacaciones familiares perfectas y parajes visitados a través de fotos hechas con una cámara profesional (pero claro, sin contar todo lo que se ha podido discutir por el camino). Lo feliz y contento que estás con tu nuevo trabajo soñado (pero claro, sin contar todo lo que has sufrido para llegar hasta allí o todas las horas extras que vas a tener que hacer). Así es Facebook y así es como Facebook quiere que sea.

Esto no sólo permite a Facebook conocer cómo es el usuario, si no, además, cómo le gustaría ser. Aprovechando para mostrarle anuncios de eventos, grupos y productos que podrían ayudarle a conseguir ese objetivo de ser la persona a la que dirige su vida.

A esto se le suma la idea que tuvo la empresa de Mark Zuckerberg de añadir en la red social un *Market*, donde poder comprar y vender productos a otros usuarios.

3.1.1 Mi cuenta de Facebook

Facebook nos permite desde la propia página web o aplicación ver y configurar todos los datos de los que disponen sobre nosotros.

A continuación enumeraremos cómo ver esta información.

1. Lo primero que debemos hacer es acceder a la **configuración de nuestra cuenta**.



Figura 3.2: Panel de configuración

2. En la sección **tu información en Facebook** podremos ver, dividido en sub-secciones, qué podemos administrar sobre nuestros datos. Destacamos aquí apartados como **descargar tu información y actividad fuera de Facebook**.



Figura 3.3: Tu información en Facebook

3. Si entramos en **actividad fuera de Facebook**, averiguaremos qué empresas comparten información con Facebook sobre nosotros y una breve explicación de cómo y por qué disponen de dicha información.



Figura 3.4: Empresas que comparten con Facebook tu información

4. Por último y más interesante, destacamos el hecho de que puedes solicitar **descargar tu información** a Facebook y en unos pocos minutos, te ofrecerán un archivo completo con fotos, publicaciones, chats, intereses y todo lo que sepan acerca de ti.

Descargar tu información

Puedes descargar una copia de tu información de Facebook cuando quieras. Puedes descargarla en su totalidad o seleccionar solo los tipos de datos e intervalos de fechas que te interesen. Tienes la opción de recibir esta información en formato HTML, que permite una lectura sencilla, o en formato JSON, que facilita la importación mediante otro servicio.

La descarga de tu información es un proceso protegido con contraseña al que solo tú tendrás acceso. Una vez generada, la copia estará disponible para su descarga durante unos días.

Si quieres consultar tu información sin descargarla, puedes acceder a tu información cuando quieras.

Solicitar copia Copias disponibles

Intervalo de fechas: Todos mis datos Formato: HTML Calidad del contenido multimedia: Alta **Crear archivo**

Tu información Desmarcar todo

- Publicaciones**
Publicaciones que has compartido en Facebook, publicaciones que has ocultado de tu biografía y encuestas que has creado ✓
- Fotos y vídeos**
Fotos y vídeos que has subido y compartido ✓
- Comentarios**
Comentarios que has realizado en tus publicaciones, en las de otras personas o en los grupos a los que perteneces ✓
- Me gusta y reacciones**
Publicaciones, comentarios y páginas que has indicado que te gustan o a los que has reaccionado ✓
- Amigos**
Personas con las que estás conectado en Facebook ✓
- Historias**
Fotos y vídeos que has compartido en tu historia ✓
- Cuentas que sigues y seguidores**
Personas, organizaciones o empresas cuyo contenido has decidido ver, y personas que te siguen ✓

Figura 3.5: Descargar toda la información que Facebook tiene sobre ti.

3.2 Whatsapp

Efectivamente, la red social número uno de mensajería es propiedad del gigante Facebook Inc. Si esto le ha pillado por sorpresa a alguno, necesitaba este libro más de lo que creía, pues es sus infinitos intentos por mejorar su imagen, Facebook no para de poner en todas sus Redes Sociales (que no son el propio Facebook), la frase *"From Facebook"*.

A día de hoy, la empresa de Mark Zuckerberg, pierde dinero con Whatsapp (puede que en un futuro cambie), sin embargo, esto sigue sin ser un problema para que Facebook pagara nada más y nada menos que **21.800 millones de dólares por Whatsapp** en el año 2014.

¿Cuál es la razón de que, a pesar de que no tienen beneficios directos, desembolsaran esta inmensa cantidad de dinero por Whatsapp?

La respuesta es sencilla, sus usuarios y la información que pueden obtener de ellos a través de sus conversaciones. Pues **cada día se intercambian en Whatsapp más de 60.000 millones de mensajes** y que cuenta casi **2.000 millones de usuarios** (datos del año 2019). Una barbaridad que además, sirvió como excusa para la migración de todos estos datos a los servidores de Facebook. Centralizando así toda la información.

Consideramos que Whatsapp es una red social privada, pues las conversaciones son directas entre personas, las cuales conoces, o por lo menos, tienes su número de teléfono. Y además, están correctamente cifradas (hay que admitir que interceptar un mensaje entre dos usuarios de Whatsapp por un tercero, es complicado).

Sin embargo, planteémoslo de la siguiente forma. Cuando tú envías un mensaje a otro usuario, dicho mensaje se almacena en tu teléfono, en el teléfono del receptor y en los servidores de Facebook (además de en Google Drive⁷ o iCloud⁸, dependiendo de si tenemos un Android o un iPhone y si, al menos uno de los dos, tiene activadas las copias de seguridad en la nube). Acabamos de meter en un simple mensaje entre dos personas a 5 nodos (emisor, receptor, Facebook, Google y/o Apple).

Ahora bien, dependiendo de los términos y condiciones que hayamos aceptado para cada uno de los servicios, cada una de las empresas que han intervenido en el envío y recepción de este mensaje (y eso que no estamos teniendo en cuenta para nada a las compañías de telecomunicaciones), pueden analizar y utilizar la información de estos mensajes, para mejorar los conocimientos que tienen a cerca de estos usuarios y, por lo menos en caso de Facebook, mejorar la publicidad que va dirigida a ellos.

Por ejemplo, si yo empiezo a hablar con mi madre de que mi teléfono está fallando y me tengo que comprar uno nuevo en las próximas semanas, probablemente, me comiencen a salir anuncios de smartphones en Facebook o Instagram. ¿Casualidad? Ya sabemos que no.

Es por todo esto que Whatsapp es una Red Social por la que Facebook puede permitirse perder dinero, pues **supone una fuente de información muy personal** de los usuarios, algo que no conseguirían a través de, por ejemplo Instagram, de la cual hablaremos a continuación.

⁷Google Drive es un servicio de alojamiento de archivos que fue introducido por la empresa estadounidense Google.[16]

⁸iCloud es un sistema de almacenamiento nube o cloud computing de Apple Inc.[17]

3.3 Instagram

Facebook compró Instagram en 2012 por 1.000 millones de dólares, lo que cualquiera podría pensar que, **con sus más de 1.000 millones de usuarios** es una ganga a día de hoy, y lo es (¡menos de un dólar por usuario!).

Instagram proporciona a Facebook una gran cantidad de ingresos por anuncios dirigidos a los usuarios de los cuales tiene toda la información que ha recopilado a través de Facebook/Messenger, Whastapp y la propia Instagram.

Cada dos historias de Instagram, aparece un anuncio específico para los intereses del usuario, cada 3 ó 4 publicaciones, lo mismo. Existen, además, cuentas específicamente creadas para vender productos. Y a todo ello se le suma la ventaja de que desde toda la aplicación, se pueden poner enlaces de venta directos.

Instagram es una red social íntegramente audio-visual (a pesar de que los mensajes directos también existen, pero no es lo que más le interesa a Facebook).

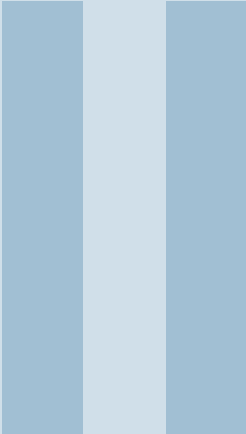
De Instagram se pueden analizar la reacciones de los usuarios a los diferentes tipos de publicaciones, fotografías y vídeos. Y es que en los términos y condiciones de la aplicación y, si le cedemos permisos para acceder al micrófono y la cámara, Facebook puede analizar nuestras expresiones faciales al momento de estar usando Instragram, de tal forma que es capaz de saber si una foto nos gusta o nos desagrada sin necesidad de que le demos *like* o lo expresemos a través de un comentario escrito.

Además, si a esto le sumamos la posibilidad de estar hablando con algún amigo, pueden analizar lo que hablamos al respecto de la publicación que estamos viendo y *sugerirnos* nuevas publicaciones similares en un futuro cercano.

A más de uno le habrá pasado estar hablando con amigos de un tema y que a las horas, Instagram comience a bombardearnos con anuncios sobre ese tema, hasta que encuentre otro tema que nos interese en ese momento y cambie.

Todo esto lo hace en base a la información que ha captado a través de todas las aplicaciones de Facebook, pero a diferencia del resto, la publicidad que nos muestran en Instagram es de algo que queremos o hemos hablado impulsivamente recientemente y no algo que podamos querer a largo plazo.

¿Será por cómo es el perfil del típico usuario que navega por Instagram o simplemente por tener un estilo diferente al resto de redes sociales en las que se muestra publicidad?



Segunda Parte: Gobiernos

4	NSA - National Spy Agency	27
4.1	Los programas de vigilancia de la NSA	
5	China && Huawei	31
6	La startup de la CIA	33
	Bibliografía	35
	Webs	
	Artículos	
	Índice alfabético	39

4. NSA - National Spy Agency

En 2013, las filtraciones de Edward Snowden ¹ mostraron cómo la Agencia Nacional de Seguridad (NSA), estaba explotando el dominio de los Estados Unidos en los servicios de Internet y las comunicaciones, para espiar a los ciudadanos del mundo.[24]

A pesar del robo de documentos secretos de Snowden y las revelaciones que ello supuso, su decisión de solicitar asilo en Rusia, hizo que los estadounidenses tuvieran opiniones enfrentadas con respecto a él.

Unos lo veían como un héroe, mientras que otros, como un traidor.

Internet había hecho mucho más difícil proteger la privacidad de los ciudadanos estadounidenses, mientras dejaba el resto de los datos del mundo desprotegidos.

Las declaraciones oficiales de que el gobierno de los Estados Unidos no espiaba a los estadounidenses, no tranquilizaron a un público que sabía que la NSA tenía enormes bancos de datos de sus propios ciudadanos y de los de muchos otros países.

La decisión de Snowden de divulgar información clasificada sobre los programas de vigilancia masiva de la NSA, tuvo importantes consecuencias para los negocios estadounidenses.

Los competidores extranjeros argumentaron que no se podía confiar en las empresas estadounidenses para almacenar datos personales. Pues, o bien estaban ayudando a la NSA, recopilando información para ellos, o bien eran vulnerables a sus programas de vigilancia. En cualquier caso, el constante argumento del gobierno estadounidense de que *la intención era proteger a las personas*, no estaba ayudando.

¹Edward Joseph Snowden es un consultor tecnológico estadounidense, informante, antiguo empleado de la Agencia Central de Inteligencia y de la Agencia de Seguridad Nacional.[18]

Las estimaciones iniciales de las pérdidas para las empresas tecnológicas de EEUU, del *efecto Snowden*, oscilaron entre 35 mil millones y 180 mil millones de dólares. Los gigantes de Silicon Valley ² exigieron reformas en las leyes de privacidad y el control que ejercía la NSA sobre las empresas estadounidenses.

En 2015, el Tribunal Europeo de Justicia anuló un acuerdo vital que permitía a las empresas transferir datos personales a los Estados Unidos, alegando temores de vigilancia del gobierno estadounidense. Para 2016, funcionarios de Estados Unidos y de la Unión Europea habían negociado un nuevo acuerdo sobre datos personales, el *seguro de privacidad de Estados Unidos y la UE*.

Acorralado, por hacer como presidente lo que criticó como candidato, Barack Obama defendió los programas de vigilancia masiva y aseguró que no se escuchaban las conversaciones de los ciudadanos y que sólo afectaba mínimamente a la privacidad de algunos, un precio que, según él, valía la pena pagar para mantener a la nación a salvo del terrorismo.

No se puede tener, un 100% de seguridad y un 100% de privacidad. Hay que hacer concesiones y estas pequeñas concesiones nos ayudan a prevenir ataques terroristas.

Al margen del debate sobre la eficacia real para la seguridad de un Estado que pueda tener esta recolección masiva de datos, el impacto en los derechos de los ciudadanos es múltiple, no sólo por la vulneración de la privacidad, sino por las consecuencias en otras libertades como las de expresión o asociación. El 28 de septiembre, el New York Times detallaba cómo se estarían realizando perfiles sociales cruzando estos datos con otros que sí son públicos, lo que abre la puerta a seguimientos selectivos en función de tendencias, gustos o afinidades.

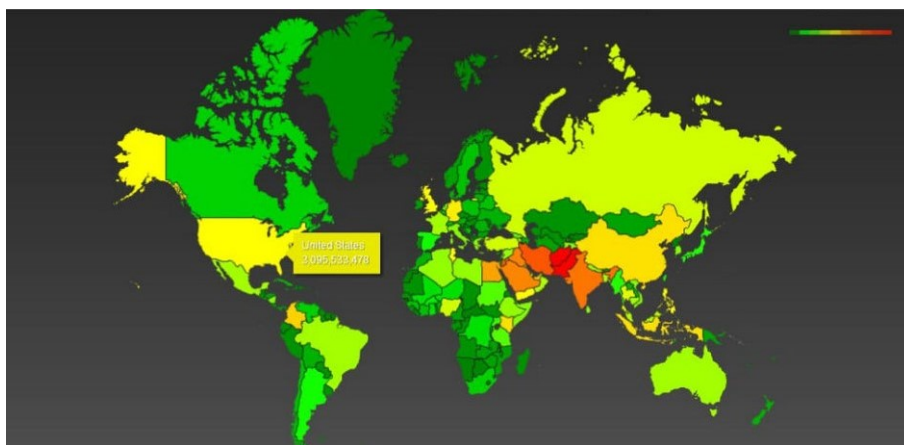


Figura 4.1: Mapa global de calor sobre la recopilación de datos de la NSA. El esquema de color varía de verde (menos sujetos vigilados) a amarillo y naranja a rojo (mayor número de sujetos vigilados).

²Silicon Valley, en el área de la bahía de San Francisco de California, es la sede de muchas compañías emergentes y globales de tecnología. Apple, Facebook y Google se encuentran entre las más destacadas.[19]

4.1 Los programas de vigilancia de la NSA

4.1.1 PRISM

Operativo desde 2007, **permitía la vigilancia masiva de ciudadanos de la UE mediante un acceso directo a los servidores centrales de empresas estadounidenses líderes en internet**, como Google, Microsoft, Facebook, Yahoo, o Apple. La cantidad y modalidad de los datos aportados variaba según la compañía.

Según un documento filtrado, en el que la propia NSA explicaba su funcionamiento, era capaz de obtener historial de búsquedas, contenido de correos electrónicos, transferencia de archivos, chats, fotografías, videoconferencias o registros de conexiones.

Esta recogida masiva e indiscriminada de información se realizaba bajo la supuesta cobertura legal de la **Ley Patriótica** (Patriot Act), aprobada por el Congreso estadounidense tras los ataques del 11 de septiembre de 2001, y, sobre todo, de la Ley de vigilancia de extranjeros o **FISA** (Foreign Intelligence Surveillance Act), una norma de 1978 enmendada en numerosas ocasiones (la última vez en 2008). Esta ley establece un tribunal secreto (FISA Court), que es el que autoriza las operaciones de rastreo emprendidas por la NSA.

4.1.2 XKEYSCORE

Se trataba de un programa dedicado a la búsqueda y análisis del contenido y los metadatos de nuestras comunicaciones online.

Tenía la capacidad de acceder, sin ningún tipo de autorización previa, a prácticamente cualquier actividad del usuario típico de internet, según destacaba el documento filtrado, orientadas a la formación de los analistas.

El propósito de XKEYSCORE, según explicaba *The Guardian*, era *permitir a los analistas buscar tanto en los metadatos como en el contenido de los correos electrónicos y otras actividades de internet*, como búsquedas, conversaciones en redes sociales o el historial de navegación. Y todo ello de una forma tan sencilla, como rellenar en el sistema un formulario que **no exigía justificar la búsqueda**.

Las búsquedas se podían efectuar a partir del nombre, el número de teléfono, la dirección IP, palabras clave, el idioma o el tipo de navegador utilizado.

4.1.3 TEMPORA

Programa de la agencia de inteligencia británica, para el acceso a redes informáticas y telefónicas, y a datos de localización, así como a algunos sistemas. Fue destapado por *The Guardian* el 21 de julio de 2014. **La inteligencia británica tiene acceso a la red de cables que transportan llamadas telefónicas y el tráfico de internet de todo el mundo**, y, con este programa, comenzó a procesar grandes flujos de información personal sensible que compartía con su socio estadounidense, la Agencia Nacional de Seguridad (NSA). Este programa de vigilancia, almacenaba grandes volúmenes de datos procedentes de cables de fibra óptica hasta 30 días para que pudiera ser filtrada y analizada.

4.1.4 BULLRUN y EDGEHILL

Programa conjunto de la NSA y la inteligencia británica, para eludir sistema de cifrado online. Podían vulnerar sistemas de encriptado y protocolos seguros ampliamente utilizados, como *HTTPS*³.

Este programa habría eludido o agrietado gran parte de la codificación que salvaguarda los **sistemas bancarios y el comercio global**, que protege datos sensibles de tal calibre como **secretos comerciales o registros médicos**.

4.1.5 QUANTUM y FOXACID

Programas de ataques selectivos contra usuarios de TOR⁴, según mostraban los documentos filtrados sobre su funcionamiento publicados el 4 de octubre. El modo en que operaban se basaban no tanto en atacar a la propia red *TOR* como a los sistemas de los usuarios que accedían a ella.

Los ataques de la NSA se hacían de forma individual y explotando vulnerabilidades en sus navegadores Firefox, y no la aplicación *TOR* directamente.

Tras identificar un usuario de TOR, la NSA utilizaba su red de servidores secretos de internet para redirigir los usuarios a otro conjunto de servidores secretos de internet, con el nombre en clave *FOXACID*, para infectar el ordenador del usuario. Para ejecutar este ataque, la NSA se servía de unos servidores secretos de alta velocidad denominados *QUANTUM*.

³El Protocolo seguro de transferencia de hipertexto (HTTPS) es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.[20]

⁴Tor son las siglas de The Onion Router. Es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela su identidad, es decir, su dirección IP (anonimato a nivel de red) y que, además, mantiene la integridad y el secreto de la información que viaja por ella. Por este motivo se dice que esta tecnología pertenece a la llamada darknet o red oscura que no se debe confundir con la deep web o web profunda.[21]

5. China & Huawei

Hace 32 años Huawei no existía. Hoy es un gigante mundial que domina el mercado de las infraestructuras de telecomunicaciones y es la segunda mayor empresa del mercado de la telefonía móvil, solo superada por Samsung y por delante de Apple. Pero la detección de un chip en los teléfonos de la marca Huawei, que no entraba dentro de las especificaciones de ningún terminal y del cuál, la empresa no quiere detallar su finalidad exacta, supuso, de nuevo, la eterna duda de si China espía, ya no sólo a sus ciudadanos, sino a cualquier habitante del planeta.

Pero no sólo eso, China podría estar usando su poder como fábrica mundial de componentes electrónicos para espiar a cualquier ciudadano. Un teléfono móvil de cualquier marca, sea americana, europea o surcoreana, cuenta con una mayoría de componentes de origen chino.

Y no sólo los teléfonos, los datos son transmitidos a través de una infraestructura que, está plagada de componentes chinos y sobre los que China tiene control, la información de internet, se almacena en servidores que pueden estar en cualquier punto del planeta, pero entre sus placas y chips hay presencia componentes fabricados e incluso diseñados en China.

Este supuesto espionaje no está demostrado con pruebas fehacientes. Lo más cercano es una investigación publicada en el año 2018, que afirmaba que hackers chinos (ceranos al Gobierno) habrían logrado infiltrar pequeños chips en decenas de miles de placas base para servidores de la firma *Super Micro Computer* con las que habrían podido espiar a más de 30 multinacionales como Amazon o Apple. Las empresas afectadas lo negaron, y no han salido a la luz las supuestas placas *hackeadas*.

Sin embargo, Estados Unidos se tomó muy en serio la amenaza. En el 2012, Huawei y ZTE (otra empresa china de telecomunicaciones) fueron objeto de una investigación para

determinar si podían resultar un peligro para la seguridad del país. El informe del Congreso de EEUU determinó que *Huawei no cooperó por completo con la investigación y no estuvo dispuesta a explicar su relación con el Gobierno chino o con el Partido Comunista Chino, mientras que, existen pruebas creíbles de que no cumple con las leyes de EEUU.*

Huawei, líder mundial en redes de telecomunicaciones, se enfrenta a un intenso y continuo examen por su relación con el gobierno de China y a las acusaciones lideradas por Estados Unidos y el presidente Donald Trump¹, de que sus dispositivos podrían ser utilizados para espiar por Pekín.

Aunque la empresa ha negado en repetidas ocasiones esta afirmación, otros países como Australia o Nueva Zelanda restringieron el acceso de Huawei a sus mercados. Y Estados Unidos sigue presionando a Europa para que no utilice tecnología de origen chino en el despliegue del 5G².

A día de hoy, Huawei tampoco puede usar tecnología estadounidense en sus dispositivos, debido al veto impuesto por Trump. Esto supone que, por ejemplo, los teléfonos de la marca no pueden acceder a los servicios de Google y por tanto, no disponen de sus aplicaciones (aunque es cierto, que estos, siguen incluyendo la parte que es de uso abierto del sistema operativo Android).

Otras como Intel, Qualcomm y Broadcom han ordenado no hacer tratos con la compañía china hasta *nuevo aviso*.

Sin embargo, aunque Huawei haya sido la más afectada por el foco de sospechas hacia sus productos y tecnologías, no olvidemos que otras empresas chinas, como Xiaomi, tienen una gran presencia en mercados tan importantes como el europeo. Si resulta que las presiones del gobierno Chino a Huawei, para recopilar datos e información, son ciertas, seguramente el resto de empresas del país estén sometidas a esta misma *política*.

¹Donald John Trump es el 45 presidente de los Estados Unidos desde el 20 de enero de 2017.[22]

²En telecomunicaciones, 5G son las siglas utilizadas para referirse a la quinta generación de tecnologías de telefonía móvil. Es la sucesora de la tecnología 4G.[23]

6. La startup de la CIA

Durante más de medio siglo, los gobiernos de todo el mundo confiaron en una sola empresa para mantener en secreto las comunicaciones de sus espías, soldados y diplomáticos.[25]

Crypto AG fue una empresa suiza especializada en comunicaciones y seguridad de la información. Fue propiedad secreta de la Agencia Central de Inteligencia de Estados Unidos (CIA) y del Servicio Federal de Inteligencia de Alemania Occidental (BND) desde 1970 hasta alrededor de 1993, con la CIA continuando como única propietaria hasta alrededor de 2018.

Con sede en Steinhausen, la compañía era un fabricante de máquinas y una amplia variedad de dispositivos de cifrado.

Esta compañía, vendía productos, con una *puerta trasera* accesible para la CIA. La firma suiza vendió sus productos a más de 120 países hasta bien entrado el siglo XXI. Entre sus clientes se encontraban Irán, juntas militares de América Latina, rivales nucleares como India y Pakistán, e incluso el Vaticano.

Esta operación, conocida primero por el nombre en clave *Thesaurus* y más tarde *Rubicon*, se encuentra entre las más audaces en la historia del espionaje.

Ninguna empresa que contrató los servicios de Crypto AG, fue consciente en ningún momento de que la CIA estaba detrás de todo ello.

Fue el golpe de inteligencia del siglo, se detallaba en el informe de la CIA.

Los gobiernos extranjeros estaban pagando un buen dinero a los Estados Unidos y Alemania Occidental por el privilegio de que sus comunicaciones más secretas fueran leídas por al menos dos (y posiblemente hasta cinco o seis) países extranjeros.

A partir de 1970, la CIA y su agencia hermana, la NSA, controlaban casi todos los aspectos de las operaciones de criptografía en la empresa, presidiendo con sus socios alemanes las decisiones de contratación, diseñando su tecnología, saboteando sus algoritmos y dirigiendo sus objetivos de ventas.

Ahora, los espías de EE.UU. y Alemania Occidental sólo tenían que sentarse a escuchar.

Monitorizaron a los *mulás* de Irán durante la crisis de los rehenes de 1979, realizaron informes de inteligencia sobre el ejército argentino para Gran Bretaña durante la Guerra de las Malvinas, rastrearon las campañas de asesinato de dictadores sudamericanos y grabaron a funcionarios libios felicitándose por el bombardeo de 1986 de una discoteca de Berlín.

El programa tuvo sus limitaciones. Los principales adversarios de Estados Unidos, incluyendo la Unión Soviética y China, nunca fueron clientes de Crypto AG. Sus sospechas infundadas de los lazos de la compañía con Occidente, les protegieron de la exposición, aunque la historia de la CIA sugiere que los espías estadounidenses aprendieron mucho, al monitorizar las interacciones de otros países con Moscú y Beijing.

La agencia de espionaje alemana, el BND, consideró que el riesgo de exposición era demasiado grande y dejó la operación a principios de la década de 1990. Pero la CIA compró la participación de los alemanes y simplemente siguió adelante, hasta 2018, cuando la agencia vendió los activos de la compañía, según antiguos y actuales funcionarios de la agencia.

La importancia de la compañía en el mercado global de la seguridad, había disminuido para entonces, debido a la propagación de la tecnología de cifrado en línea.

Los productos de Crypto AG todavía están en uso en más de una docena de países de todo el mundo, y su letrero naranja y blanco todavía se cierne sobre el antiguo edificio de la sede central de la compañía cerca de Zug, Suiza. Pero la compañía fue desmembrada en 2018 y liquidada por accionistas cuyas identidades han sido permanentemente protegidas por las leyes bizantinas de Liechtenstein.

Bibliografía

Webs

- [Wik20b] Wikipedia. *Alphabet*. Palo Alto, California, Enero de 2020. URL: https://es.wikipedia.org/wiki/Alphabet_Inc. (véase página 9).
- [Wik20d] Wikipedia. *Android*. Palo Alto, California, Enero de 2020. URL: <https://es.wikipedia.org/wiki/Android> (véase página 9).
- [Wik20i] Wikipedia. *Gmail*. Palo Alto, California, Enero de 2020. URL: <https://es.wikipedia.org/wiki/Gmail> (véase página 9).
- [Wik20u] Wikipedia. *The New York Times*. 620 Eighth Avenue, Nueva York, feb. de 2020. URL: https://es.wikipedia.org/wiki/The_New_York_Times (véase página 9).
- [Wik20r] Wikipedia. *SO móvil*. Feb. de 2020. URL: https://es.wikipedia.org/wiki/Sistema_operativo_m%C3%B3vil (véase página 15).
- [Wik20m] Wikipedia. *iOS*. Palo Alto, California, feb. de 2020. URL: <https://es.wikipedia.org/wiki/IOS> (véase página 15).
- [Wik20s] Wikipedia. *The Associated Press*. Nueva York, EEUU, feb. de 2020. URL: https://es.wikipedia.org/wiki/Associated_Press (véase página 15).
- [Wik20n] Wikipedia. *Microsoft*. Redmond, Washington, mar. de 2020. URL: <https://es.wikipedia.org/wiki/Microsoft> (véase página 16).

- [Wik20w] Wikipedia. *Windows Phone*. Redmond, Washington, mar. de 2020. URL: https://es.wikipedia.org/wiki/Windows_Phone (véase página 16).
- [Wik20p] Wikipedia. *RRSS*. Feb. de 2020. URL: https://es.wikipedia.org/wiki/Red_social (véase página 17).
- [Wik20e] Wikipedia. *Barack Obama*. Hawái, EEUU, feb. de 2020. URL: https://es.wikipedia.org/wiki/Barack_Obama (véase página 18).
- [Wik20l] Wikipedia. *Investor's Business Daily*. Los Ángeles, California, mar. de 2020. URL: https://en.wikipedia.org/wiki/Investor's_Business_Daily (véase página 18).
- [Wik20f] Wikipedia. *CNN*. Atlanta, Georgia, feb. de 2020. URL: es.wikipedia.org/wiki/CNN (véase página 18).
- [Wik20c] Wikipedia. *Amazon*. Seattle, Washington, feb. de 2020. URL: <https://es.wikipedia.org/wiki/Amazon> (véase página 18).
- [Wik20t] Wikipedia. *The Guardian*. Londres, Reino Unido, feb. de 2020. URL: https://es.wikipedia.org/wiki/The_Guardian (véase página 19).
- [Wik20j] Wikipedia. *Google Drive*. Palo Alto, California, feb. de 2020. URL: https://es.wikipedia.org/wiki/Google_Drive (véase página 23).
- [Wik20k] Wikipedia. *iCloud*. Palo Alto, California, feb. de 2020. URL: <https://es.wikipedia.org/wiki/ICloud> (véase página 23).
- [Wik20h] Wikipedia. *Edward Snowden*. Carolina del Norte, EEUU, feb. de 2020. URL: https://es.wikipedia.org/wiki/Edward_Snowden (véase página 27).
- [Wik20q] Wikipedia. *Silicon Valley*. San Francisco, California, feb. de 2020. URL: https://es.wikipedia.org/wiki/Silicon_Valley (véase página 28).
- [Wik20o] Wikipedia. *Protocolo HTTPS*. Feb. de 2020. URL: https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto (véase página 30).
- [Wik20v] Wikipedia. *Tor*. Feb. de 2020. URL: [https://es.wikipedia.org/wiki/Tor_\(red_de_anonimato\)](https://es.wikipedia.org/wiki/Tor_(red_de_anonimato)) (véase página 30).
- [Wik20g] Wikipedia. *Donald Trump*. Nueva York, EEUU, feb. de 2020. URL: https://es.wikipedia.org/wiki/Donald_Trump (véase página 32).
- [Wik20a] Wikipedia. *5G*. Feb. de 2020. URL: <https://en.wikipedia.org/wiki/5G> (véase página 32).

Artículos

- [Zab17] Nerea Zaballa. *La vigilancia masiva de la NSA*. Barcelona, España, sep. de 2017. URL: <https://forbes.es/empresas/31995/la-vigilancia-masiva-la-nsa/> (véase página 27).
- [Mil20] Greg Miller. *The intelligence coup of the century*. Washington, EEUU, feb. de 2020. URL: <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/> (véase página 33).

Índice alfabético

A

Android 15

B

BULLRUN y EDGEHILL 30

C

China y Huawei 31

CIA 33

E

El equilibrio de la balanza 14

F

Facebook 20

Facebook, humanos, Facebook 17

G

Gestión de la privacidad 12

Google 9

I

Instagram 24

Introducción 7

M

Mi cuenta de Facebook 20

Mi cuenta de Google 11

N

NSA - National Spy Agency 27

P

PRISM 29

Programas de vigilancia de la NSA 29

Q

QUANTUM y FOXACID 30

T

TEMPORA 29

W

Whatsapp 23

X

XKEYSCORE 29

*Dedicado a todos aquellos que me habéis ayudado a llegar hasta aquí.
Vosotros sabéis quiénes sois.*