Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Libro blanco para la deontología informática aplicada al empleo de redes sociales por empresas TIC

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Josep Rubio Gonzalez

Tutor: Juan Vicente Oltra Gutiérrez

2020-2021

Resumen

El uso de redes sociales desde las empresas, a modo de contacto directo con sus usuarios y la sociedad en general, conlleva una serie de problemas de carácter jurídico y ético. Los problemas jurídicos en ocasiones (p.e. en lo relativo a protección de datos) son referenciados desde las normas aludiendo a la necesidad de elaborar códigos tipo, pero los segundos no tienen un desarrollo establecido tan claro.

Con el presente TFG se pretende elaborar un libro blanco que sirva de cauce referencial para todo profesional que, desde una empresa TIC, deba afrontar el reto de abrir esa ventana cibernética al público que son las redes sociales.

Para ello, en primer lugar, referenciaremos con estructuras y ejemplos significativos algunos de los códigos tipo más relevantes en la profesión y, en segundo lugar y atendiendo a los aspectos éticos y deontológicos, procederemos a un estudio de los códigos éticos de las organizaciones del sector, destacando las convergencias y diferencias en el tratamiento de redes sociales, siendo complementado con aquellos elementos más destacados por la bibliografía de referencia en el área.

El documento resultante pretenderá ser en primer lugar útil, con una estructura similar a una norma técnica, siendo difundido mediante licencia CC BY-SA

Palabras clave: redes sociales, deontología, profesionalismo y libro blanco.

Abstract

The use of social networks from companies, as direct contact with their users and society in general, brings a number of legal and ethical problems. Legal problems are sometimes referred to in the rules (e.g. data protection) by referring to the need to develop model codes, but the latter do not have such a clear established development.

The aim of this TFG is to produce a white paper that will serve as a reference channel for all professionals who, from an ICT company, must face the challenge of opening this cyber window to the public that is social networks.

To this end, we will first reference with significant structures and examples some of the most relevant type codes in the profession and, secondly, taking into account ethical and ethical aspects, we will conduct a study of the ethical codes of the organizations of the sector, highlighting the convergences and differences in the treatment of social networks, being complemented with those elements most highlighted by the reference bibliography in the area.

The resulting document will first be useful, with a structure similar to a technical standard, being disseminated by CC BY-SA license.

Keywords: social media, deontology, professionalism and white book.

Agradecimientos

Gracias a mi tutor, Juan Vicente Oltra Gutiérrez, por su paciencia, apoyo constante y trabajo.

Índice general

Índice de figuras

1. Introducción

En los últimos años la protección de los datos personales se ha convertido en un tema de interés mundial, al conocerse las múltiples fugas de los datos por parte de empresas multinacionales como Facebook, Google o Yahoo![1] [1]. Con la intención de competir con la red social Facebook, Google creó Google+ pero nunca terminó de despegar. En esta plataforma nueva se produjo el fallo de seguridad, donde se expuso la información privada de 52,5 millones de usuarios. Los datos quedaron expuestos durante 6 días y fueron el nombre, el correo electrónico, empleo y edad. Aun así, la mayor fuga de datos la tiene Yahoo!, con 3.000 millones de cuentas hackeadas [2]. Este hecho se produjo en 2013, cuando un usuario llamado «Peace» trataba de vender los datos personales extraídos en la llamada Internet Profunda a finales de 2014.

Estos hechos provocaron que los usuarios se interesaran en como las empresas utilizaban sus datos y para qué. Se ha mejorado en seguridad por parte de los usuarios como de las empresas, aunque la preocupación trasladada por los expertos en seguridad informática continua. En el año 2020 habían más de 26.000 millones de dispositivos conectados a internet, un número que significa un gran desafío para la seguridad digital. Este número supone que cada segundo hay 11 nuevos usuarios en las redes sociales generando día tras día nueva información, que en la mayoría de las veces no tienen la protección necesaria para garantizar su seguridad [3]. El desconocimiento por parte de los usuarios en tareas de seguridad sigue muy presente pese a todos los avances en materia de protección de los datos personales.

El usuario medio es bastante confiado y no sospecha que le pueden estar sustrayendo los datos sin darse cuenta. El contenido del mensaje para atraer la atención puede variar desde informar de un problema en nuestra cuenta para que iniciemos sesión, contener algún archivo para ser descargado, algún enlace, incluso sorteos o comunicados falsos [4].

Como se ha podido observar este proyecto, fundamentalmente, ha sido implementado como guía para empresas como personas físicas, ya que presenta un claro enfoque para poder realizar un análisis de los peligros que tienen las redes sociales y que pasos hay que seguir para obtener la mayor seguridad, exponiendo en primer lugar la trascendencia de publicar nuestros datos personales

[1] Marcas registradas

en las redes sociales. Se explicará porque existe un interés elevado en obtener la información de los usuarios y las estrategias que las empresas utilizan para recabarla.

1.1. Motivación

La principal motivación para realizar este proyecto fue la idea de poder proporcionar una guía vital a los usuarios, ya que son el principal objetivo de las redes sociales y considero que son los más vulnerables a cualquier ataque informático. Me resulta muy importante que el usuario este informado sobre los peligros de las redes sociales, porque la tecnología avanza muy rápido, pero a los usuarios no se les proporciona una formación o guía que puedan utilizar para proteger sus datos personales.

Por otro lado, me resultó interesante poder profundizar en las estrategias que utilizan las empresas para recolectar los datos personales y su posterior tratamiento con fines lucrativos.

Otra motivación de realizar este proyecto es de carácter personal, proporcionar una guía para los usuarios y para las empresas con el fin de poder ofrecerles la información necesaria para que conozcan los peligros de las redes sociales, conozcan los riesgos de exponer sus datos personales y adquieran conocimientos para poder detectar los principales tipos de ataques informáticos y no caer en las trampas. De esta manera un usuario medio con una mínima información sobre los peligros de internet le podríamos evitar caer en estafas que conllevan la perdida de sus ahorros o la suplantación de identidad. Ya que no podemos detener la actividad de los piratas informáticos, sí que podemos ofrecer una defensa para los usuarios con poco conocimiento tecnológico.

1.2. Objetivos

Con este proyecto se pretende informar a los usuarios de internet, pero específicamente a los que utilizan las redes sociales del valor de sus datos personales y de la facilidad con la cual se sustraen sin que se den cuenta. Con el fin de lograr una protección mayor del usuario frente a las redes sociales, los objetivos que se presentan en este proyecto son los siguientes:

- Nombrar, explicar y desarrollar las principales herramientas de protección que tiene al alcance el usuario medio.

- Exponer las diferentes estrategias de recopilación de datos personales que se utilizan.

- Capacitar a un usuario medio para configurar su privacidad en las redes sociales.

1.3. Estructura de la memoria

A continuación, se incluirá como va a estructurarse la memoria de 7 capítulos, con una concisa explicación de cada uno de los puntos que va a tratar:

La introducción, motivación y estructura de la memoria corresponde al primer capítulo. En el segundo capítulo se encuentra el estado del arte, en el cual se explica la recopilación de todos los fallos de seguridad y que posibles soluciones podemos encontrar a nivel de usuario. El tercer capítulo corresponde a explicar que son los datos personales de las personas. El cuarto capítulo trata sobre la importancia y valor que les dan las empresas a los datos personales, se manifiesta el tratado posterior que tienen estos datos y como a partir de estos se extraen tendencias comerciales. El quinto capítulo consiste en elaborar una guía para el usuario medio, explicar cómo puede configurar la sección de privacidad en las redes sociales y que herramientas tiene para poder protegerse en internet y no poner en peligro sus datos personales. En el sexto capítulo se aclaran las estrategias más utilizadas para poder extraer los datos sin que los usuarios sean conscientes de lo que están haciendo. El séptimo capítulo se centra en las PYMES y las empresas emergentes, en que instrumentos tiene a su alcance para cuidar, preservar los datos de sus clientes. Finalmente, se indican las referencias bibliográficas a partir de las cuales se ha elaborado este proyecto. De esta manera, el lector podrá consultar con mayor profundidad la fuente de información si se desea.

2. Estado del arte

En este capítulo trataremos las principales redes sociales, los cambios en las leyes sobre la protección de los datos, las opciones que proporcionan las redes sociales a los usuarios para mantener su privacidad y si los usuarios son sabedores de estas herramientas.

Este análisis es fundamental para ver como la historia de la protección de los datos personales ha evolucionado, incrementando la posibilidad de obtener una

mayor privacidad al usuario y más control. De este modo, el usuario medio puede establecer unas pautas de protección personalizadas dependiendo en que red social este.

2.1. Historia y avances de la protección de datos personales

Partimos de la base de la Constitución española, España fue pionera en protección de datos y lo establece claramente en su artículo 18.1 «*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*» y 18.4 «*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*» [5].

No obstante, no fue hasta el año 1995 cuando salió la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de los datos personales de las personas físicas [6] que marcaba las pautas para que pudieran legislar los países de la Unión Europea en relación con el tema de protección de datos.

En España se sacó la ley en el año 1999, que es la LOPDCP 15/1999, de 13 de diciembre [7]. Esta Ley Orgánica junto con la Directiva de la Unión Europea del 1995 establece una serie de artículos muy importantes, uno de ellos los derechos a los que pueden acceder los ciudadanos. A continuación, se enumeran y se definen:

1. Acceso: Se tiene derecho de acceder a nuestros datos. Esa empresa que tiene nuestros datos guardados, podemos acceder a ellos. El derecho de acceso puede ser considerado repetitivo cuando se ejerza este derecho más de una vez en el plazo de 6 meses.

2. Rectificación: Evidentemente también la ley garantiza el derecho que tenemos a rectificar nuestros datos.

3. Cancelación: Por supuesto también la ley nos garantiza el derecho que tenemos a que nuestros datos sean cancelados. Una empresa que gestiona nuestros datos, nosotros podemos solicitar la cancelación de nuestros datos.

4. Oposición: En cuanto a la capacidad y el derecho que tenemos de oponernos a que nuestros datos sean tratados.

Sobre este último punto en esta ley de protección de datos, el consentimiento que teníamos que dar para que fueran tratados nuestros datos era tácito, es decir, si el usuario no respondía con una negativa en un plazo de 30 días, la empresa entendía que se podía tratar con sus datos. Este consentimiento cambiaría radicalmente en el 2018.

En el 2007, se aprueba el RDL 1720/2007, de 21 de diciembre [8] el reglamento de desarrollo de la citada anteriormente ley orgánica del 1999 pero no es hasta el año 2016 cuando se crea el Reglamento (UE) nº 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales [9]. Este reglamento afecta a aquellos territorios en los cuales, el responsable o el encargado del tratamiento de los datos recopilados estén establecidos en la Unión Europea. También cuando ninguno de estos dos esté instaurado en la Unión Europea, pero esas actividades si se realicen dentro de la Unión Europea y por lo tanto afecte a sus ciudadanos.

Este reglamento es de aplicación directa, hay que trasponerlo a la legislación española. Esa trasposición se ve efectiva con la actual LOPDGDD 3/2018, de 5 de diciembre [10] y trae uno nuevos derechos que definiremos ahora:

1. Supresión: Derecho a obtener la supresión de sus datos personales. Corresponde al antiguo derecho de cancelación.

2. Oposición: Oponerse al tratamiento de los datos personales. Este derecho no cambia.

3. Portabilidad: El derecho a recibir los datos personales relacionados con usted en un formato estructurado, leerlos mecánicamente y facilitarlos al responsable del tratamiento y transmitirlos a otro responsable del tratamiento. El derecho de portabilidad no se aplica a los tratamientos realizados en interés público o en el ejercicio del poder público, como el tratamiento realizado por cualquier organismo administrativo público (como sanidad).

4. Limitación: Por inexactitud, tratamiento ilícito, datos que no sean necesarios para la finalidad del tratamiento, o cuando se acredite el motivo legítimo de oposición al tratamiento, derecho a obtener restricciones de tratamiento de datos por parte del responsable del tratamiento.

El controlador de datos debe retener datos limitados y solo puede usar los datos con el consentimiento de las partes relevantes para reclamar o defender los derechos de otra persona física o jurídica, o para fines de interés público.

5. Acceso: El interesado tiene derecho a obtener confirmación por parte del responsable del tratamiento sobre si se están tratando o no sus datos personales y, en su caso, deberá facilitar información sobre él.

6. Rectificación: Obtener el derecho a corregir los datos personales incorrectos sobre usted. Teniendo en cuenta el propósito del proceso, las partes interesadas tienen derecho a completar o rectificar los datos personales incompletos, incluso a través de declaraciones adicionales.

En esta nueva ley, tiene como objetivo fortalecer la privacidad y las conexiones digitales de los trabajadores. Regular los derechos de privacidad y prohibir el uso de equipos de geolocalización y videovigilancia digital en el lugar de trabajo. Otro aspecto de esta nueva ley es dar a los ciudadanos un mayor control sobre su información privada en el mundo de los teléfonos inteligentes, las redes sociales, la banca online y las transferencias globales.

Gracias a este cambio en el 2018, muchas empresas se tuvieron que modificar internamente realizando cambios radicales para cumplir la nueva ley. Uno de los cambios más importantes es que ahora tenemos que dar nuestro consentimiento expreso, es decir, anteriormente era tácito y ahora nuestro consentimiento se tiene que llevar a cabo a través de la escritura, palabra hablada o signo inequívoco, disgregado.

Otro de los puntos más alicientes consiste en las competencias adquiridas por la Agencia Española de Protección de Datos. Esta agencia la trataremos en el siguiente punto, en el cual pretenderemos dar a conocer su historia, sus funciones y las áreas de actuación donde puede intervenir.

2.2. Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos es una entidad libre, con presupuesto propio y plena autonomía funcional. La AEPD se fundó en 1992 e inicio su actividad en 1994.

Desde 1994 su área de actuación se ha incrementado. Desde internet y redes sociales, reclamaciones de telecomunicaciones, publicidad no deseada, educación y menores, videovigilancia, innovación y tecnología hasta protección de datos y coronavirus.

Figura 2.1: Logo de la Asociación Española de Protección de Datos. Fuente: asesorias.

El cargo de presidente es elegido por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Sus directores han sido:

- D. Juan José Martín-Casallo López (1993 - 1998)
- D. Juan Manuel Fernández López (1998 - 2002)
- D. José Luis Piñar Mañas (2002 - 2007)
- D. Artemi Rallo Lombarte (2007 - 2011)
- D. José Luis Rodriguez Álvarez (2011 - 2015)
- Dña. Mar España Martí (2015 - actualidad)

2.2.1. Funciones y poderes de la AEPD

En el ámbito de las funciones, la AEPD tiene un total de 22 marcos donde puede actuar y en esta sección trataremos los que consideramos los más importantes y que más trascendencia pueden tener de cara al usuario medio. Ahora se enumeran las principales funciones [11]:

- Controlar la aplicación del Reglamento (UE) nº 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de

2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

- Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a personas menores de edad deberán ser objeto de especial atención.
- Asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.
- Promover la sensibilización de las personas responsables y encargadas del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento.
- Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros.
- Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento.
- Llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública.

Una vez expuestos las funciones más importantes, cabe recalcar que el resto de las funciones son muy trascendentes, pero en el presente documento hemos expuesto las que se cree que son de vital importancia para el conocimiento del usuario. Ahora se detallan los puntos más relevantes de los poderes que tiene esta agencia. Tiene

tres ámbitos en la parte de poderes, las cuales son investigación, correctivos y autorización y consultivos. En la parte de investigación podemos encontrar los siguientes:

- Ordenar a la persona responsable y al encargado del tratamiento y, en su caso, al representante de la persona responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones.
- Obtener de la persona responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones.
- Obtener el acceso a todos los locales de la persona responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión Europea o de los Estados miembros.

Siguiendo con los poderes, nos centramos en los correctivos que puede llegar a poner esta agencia:

- Sancionar a toda persona responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en la normativa de protección de datos.
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
- Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

Por último, vamos con la parte de autorización y consulta:

- Emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al

público, sobre cualquier asunto relacionado con la protección de los datos personales.

- Autorizar el tratamiento si el Derecho del Estado miembro requiere tal autorización previa.
- Asesorar a la persona responsable del tratamiento conforme al procedimiento de consulta previa.

2.3. Redes sociales

Hace unos años, la explosión de Internet produjo cambios en diferentes entornos civilizados, principalmente porque abrió nuevas formas de comunicación entre usuarios que no necesariamente necesitan estar en el mismo lugar. Por ejemplo, correo electrónico, página web o blogs. La comunicación interpersonal se ha vuelto cada vez más fuerte, suprimiendo muchas fronteras lingüísticas o culturales.

Debemos recordar que el nacimiento de Internet se remonta a 1947, cuando la Guerra Fría dio sus primeros pasos y enfrentó a ciudadanos de todo el mundo. Algunos occidentales y capitalistas (liderados por Estados Unidos), y algunos orientales y comunistas (liderados por la Unión Soviética).

Una verdadera lucha por el poder que inspiró muchos avances tecnológicos. Entre ellos, Estados Unidos creó la Agencia de Proyectos de Investigación Avanzada (APIA), que sentó las bases de la llamada Internet diez años después, porque su red APIANET permite a las organizaciones intercambiar información.

Por lo tanto, con el paso del tiempo, los usuarios de todo el mundo comenzaron a contactar por correo electrónico (el primer envío fue en el año 1971). Más adelante, en el año 1991, la red global informática y la World Wide Web (normalmente la llamamos "www") se hicieron públicas juntas y apareció Internet.

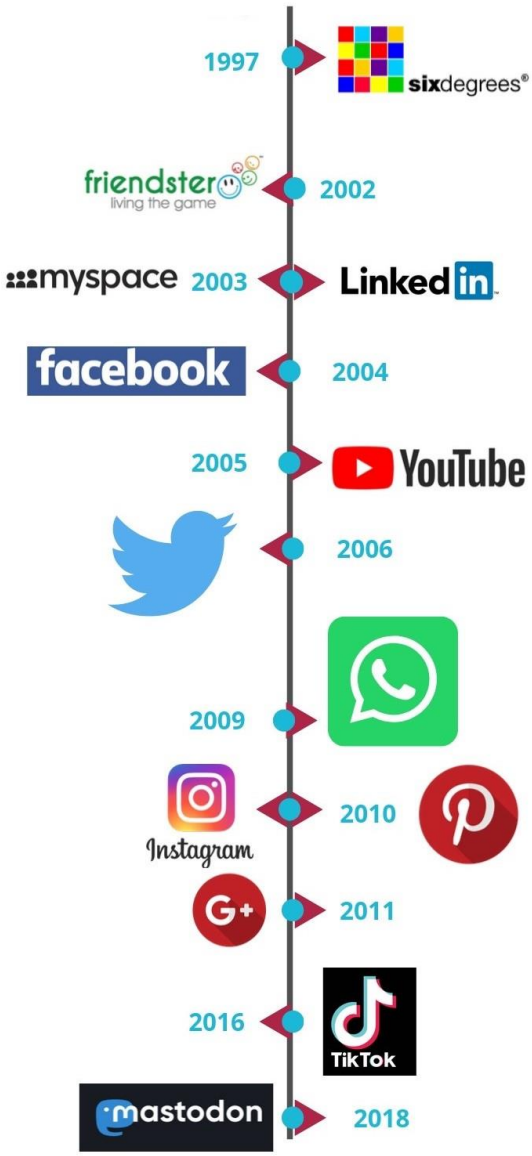

Figura 2.2: Año de creación de cada red social. Fuente: marketing4ecommerce.

2.3.1. SixDegrees

A pesar de todos estos avances, todavía no existían aplicaciones, herramientas o elementos que permitan a los usuarios socializar entre ellos. Esta situación cambió en 1997, cuando Andrew Weinreich creó SixDegrees, que puede considerarse la primera red social del mundo. Una red que podía ubicar a otros miembros de la red y crear una lista de amigos, y la red se basaba en la teoría de los seis grados de separación, que establece que se puede establecer contacto con cualquier otra persona del mundo en tan solo 6 pasos.

La primera red social finalizo su actividad en diciembre de 2000. Aunque ha habido diferentes intentos por copiar su estilo e incluso sitios con el mismo nombre desde que cesara su actividad. En sus tres años de vida, esta red social tuvo un total de tres millones de usuarios [12].

Figura 2.3: Logo la red social SixDegrees. Fuente: Wikipedia.

2.3.2. MySpace, Friendster y LinkedIn

Como decíamos, SixDegrees desapareció en el año 2000, pero solo tomó unos meses para que los afortunados usuarios digitales comenzaran a disfrutar de nuevas redes sociales, como Friendster, que fue creada en 2002 para los amantes de los videojuegos. MySpace y LinkedIn aparecieron en 2003 y se consideran redes más profesionales y orientadas a los negocios. Las viejas redes sociales desaparecieron, aunque no todas.

Jonathan Abrams y Ross MacKinnon crearon Friendster para conocer chicas, es decir, una red social de citas registrando 3 millones de usuarios en sus primeros 3 meses. Tras pasar de dueños varias veces, en el 2015 la compañía anunciaba que se tomaba un descanso, nunca volvió.

Continuando con MySpace, Tom Anderson, Jon Hart y Chris DeWolfe se encargaron de crear esta red social. Siguió los mismos pasos que Friendster y en 2011 el dueño de la compañía anunciaba una nueva estrategia y definía su red social como un sitio de «entretenimiento social» [13].

Figura 2.4: Perfil de un usuario en la red social MySpace. Fuente: MySpace.

Reid Hoffman, Konstantin Guericke, Allen Blue, Jean-Luc Vaillant y Eric Ly fundaron LinkedIn. En particular, LinkedIn tuvo un impacto inmediato en el mundo empresarial, ya que en 2008 sus usuarios registrados habían superado los 25 millones y se había expandido a 150 empresas de diferentes industrias. Hoy cuenta con más de 600 millones de usuarios registrados.

Esta red social centrada en el ámbito profesional es la única hoy en día que sigue siendo popular comparada con las dos redes analizadas anteriormente.

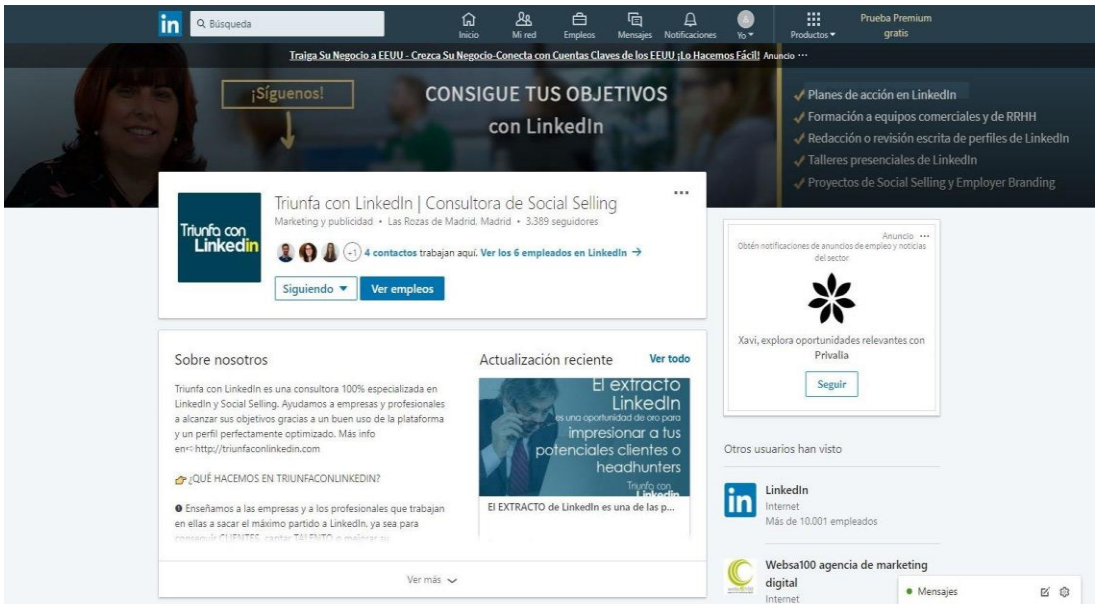

Figura 2.5: Perfil de una empresa en LinkedIn. Fuente: LinkedIn.

2.3.3. Facebook

Y, como no, en 2004, un joven estudiante universitario de la Universidad de Harvard creó la red social más importante del mundo actual: Facebook. El nombre del joven estudiante es Mark Zuckerberg. La historia de Zuckerberg y la de cómo creó Facebook es fascinante: Zuckerberg era un niño prodigio, programaba a los 10 años y a los 12 ya creo su primera empresa. En el 2004 creó un portal llamado Facemash, cuyo propósito no es más que conectar las opiniones de los estudiantes de Harvard entre sí y tener una visión sobre quién es la persona más atractiva y menos atractiva de la universidad, algo que llega a la misma oficina general que provoca que echen al estudiante de la universidad.

Sin embargo, su habilidad informática es tan claramente visible en esa aplicación que poco tardo en evolucionar y crecer a lo que es hoy en día. Una red social con más de 2.500 millones de usuarios activos mensuales [14].

Figura 2.6: Perfil de un usuario de Facebook. Fuente: facebook.

2.3.4. Youtube

Apenas un año después, en 2005, surgió una nueva revolución, y hoy sigue siendo una de las redes sociales más importantes: YouTube. Una red creada por Chad Hurley, Steve Chen y Jawn Karim en San Bruno, California.

El nacimiento de YouTube surge de las dificultades que encontraron tres jóvenes al compartir una serie de videos con sus amigos cuando asistieron a una fiesta en San Francisco.

El bombardeo de esta red provocó que usuarios de todo el mundo subieran rápidamente varios videos a la red, lo que perdió levemente su intención original. Pero a pesar de esto, cuando los usuarios comenzaron a colocar enlaces de YouTube en sus páginas de MySpace, el tráfico se disparó aún más. Hoy, la red tiene aproximadamente 2 mil millones de usuarios activos mensuales [15].

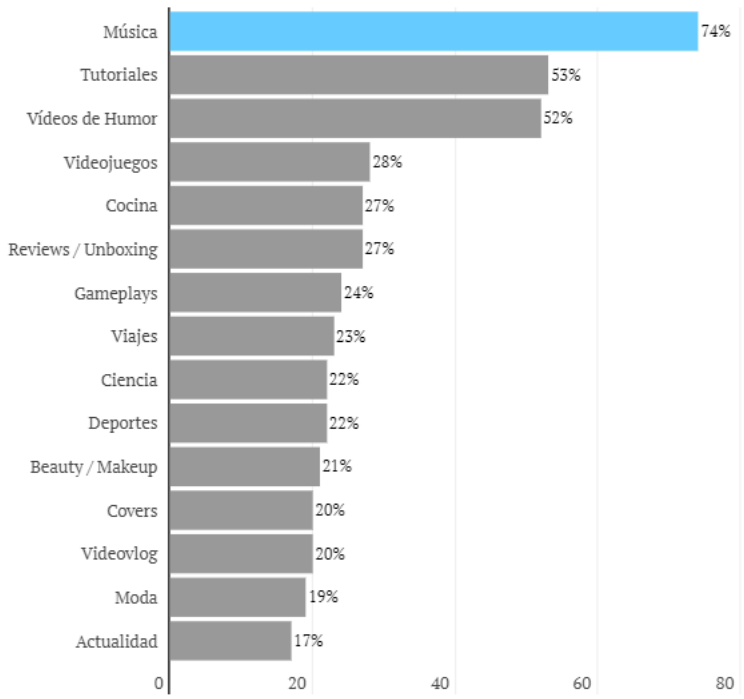

Figura 2.7: Temáticas favoritas en Youtube. Fuente: industriamusical.

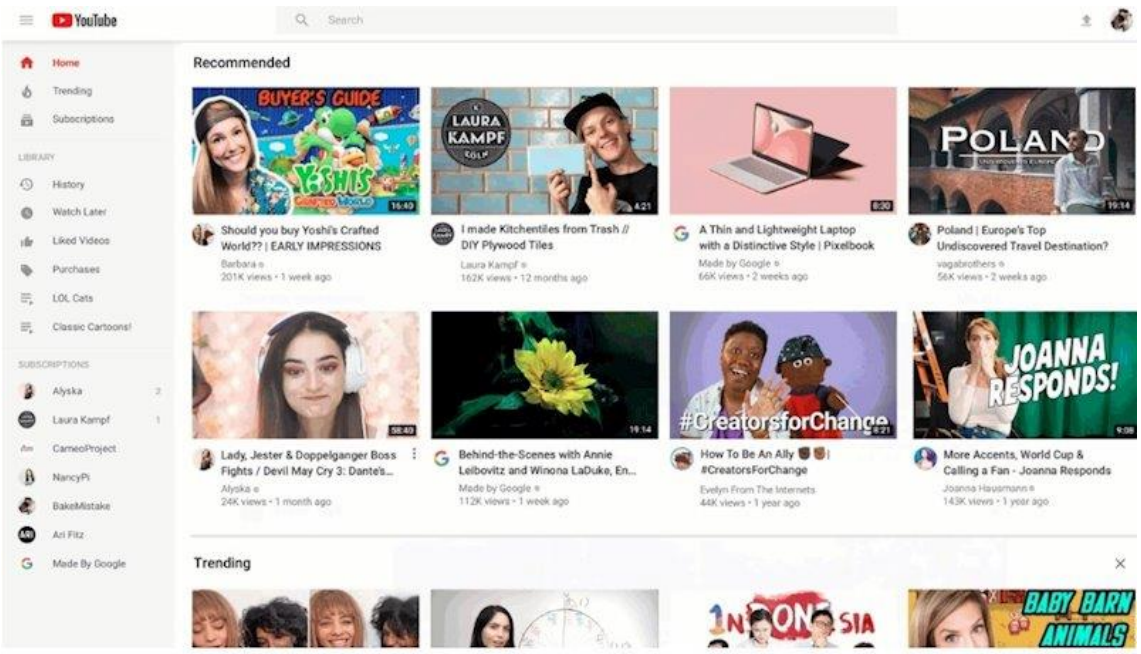

Figura 2.8: Página principal de Youtube. Fuente: youtube.

2.3.5. Twitter

En 2006, la red social de microblogging Twitter (originalmente llamada *twttr*) nació de las manos de Jack Dorsey, Noah Glass, Biz Stone y Evan Williams en San Francisco, y luego evolucionó hasta su nombre actual.

Hoy en día, la influencia de esta red es tan grande que incluso medios como la televisión, la radio y los medios digitales de noticias utilizan todo el espacio para hablar de tweets, tendencias o mencionar específicamente el impacto en determinadas noticias de actualidad. Y es que, a pesar de que tiene extrañas carencias, lo cierto es que mucha gente atribuye su éxito a su sencillez de uso.

Tiene el mismo uso que en su origen: la cantidad de caracteres que permite a sus usuarios comunicarse entre sí es limitada, en concreto 140 caracteres. Hoy, la red tiene aproximadamente 340 millones de usuarios activos mensuales [16].

Figura 2.10: Perfil de la cuenta oficial de Twitter. Fuente: twitter.

2.3.6. WhatsApp

Hoy en día, podemos considerarla como la aplicación de mensajería instantánea más famosa, que fue creada en 2009 por el ucraniano Jan Koum.

Originalmente fue creado como una especie de agenda inteligente, por lo que está vinculado a la lista de contactos de nuestro terminal móvil, lo que permite a los usuarios ver qué están haciendo todos en cualquier momento, para saber si puedo iniciar una conversación con él.

Hoy, tiene más de 2 mil millones de usuarios, ubicándose en la cima de aplicaciones como Facebook Messenger o Telegram. En 2014, el fundador de Facebook, Mark Zuckerberg (Mark Zuckerberg), lo compró por no más de 19.000 millones de dólares.

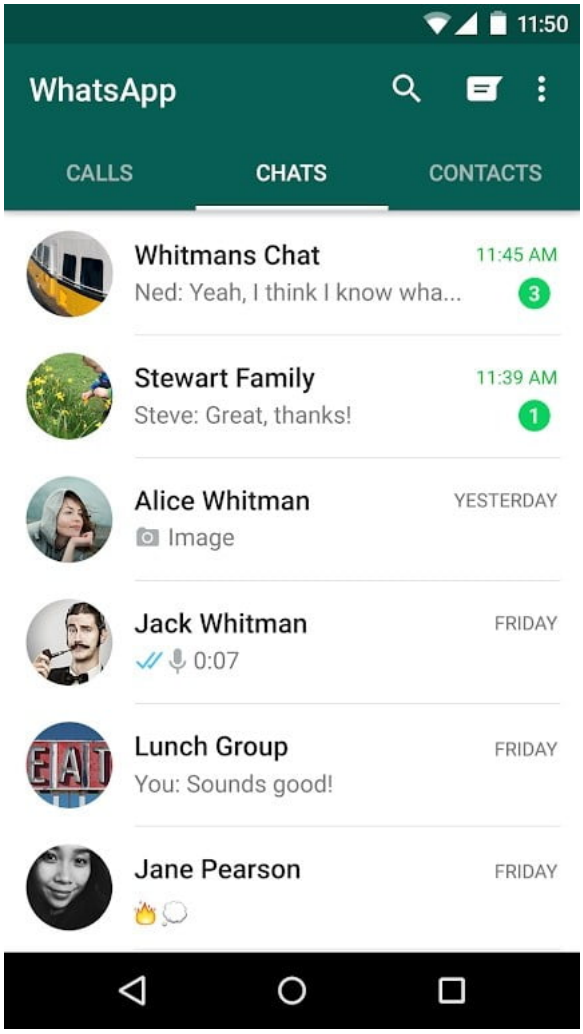

Figura 2.11: Conversaciones de un usuario de WhatsApp. Fuente: zapptales.

2.3.7. Instagram

En 2010, Instagram ingresó al mercado y rápidamente se posicionó como la mejor red social para la fotografía, logrando mayor éxito que otras opciones como Flickr.

Instagram fue fundado por Kevin Systrom y Mike Krieger, y su singularidad (que todavía existe hoy) es que procesa sus imágenes y fotos de manera cuadrada para conmemorar las cámaras Kodak Instamatic y Polaroid, contrastando con la relación de aspecto más vertical con la que hoy en día cuentan la mayoría de las cámaras de los móviles.

Además, en enero de 2011, fue una red pionera en promover hashtags junto con Twitter, con el propósito de facilitar a los usuarios el descubrimiento de fotos compartidas por otros usuarios sobre el mismo tema o lugar, y que no podían llegar a verse de otra forma.

Instagram alcanzó una gran popularidad en los primeros meses de su nacimiento. En abril de 2012 (solo dos años después) alcanzó más de 100 millones de usuarios activos, y en 2014 llegó a más de 300. Hoy en día sigue creciendo -unos mil millones de usuarios activos- sobre todo porque es una red social enfocada a una nueva generación de redes sociales, ya que está mostrando a nuestros contactos 24/7 lo que estamos haciendo. Las fotos se colocan en nuestro feed o nuestra historia (este formato se define como que el contenido público desaparece después de 24 horas, donde Snapchat es el pionero, y al cabo de un tiempo llega a Instagram y Facebook).

Para ser precisos, esta nueva herramienta (publicar tu propia historia) es la clave del destino de Snapchat, ya que era la red social de más rápido crecimiento en el mundo en ese momento. Posteriormente, Instagram copio la idea de las historias, dejando de lado a Snapchat.

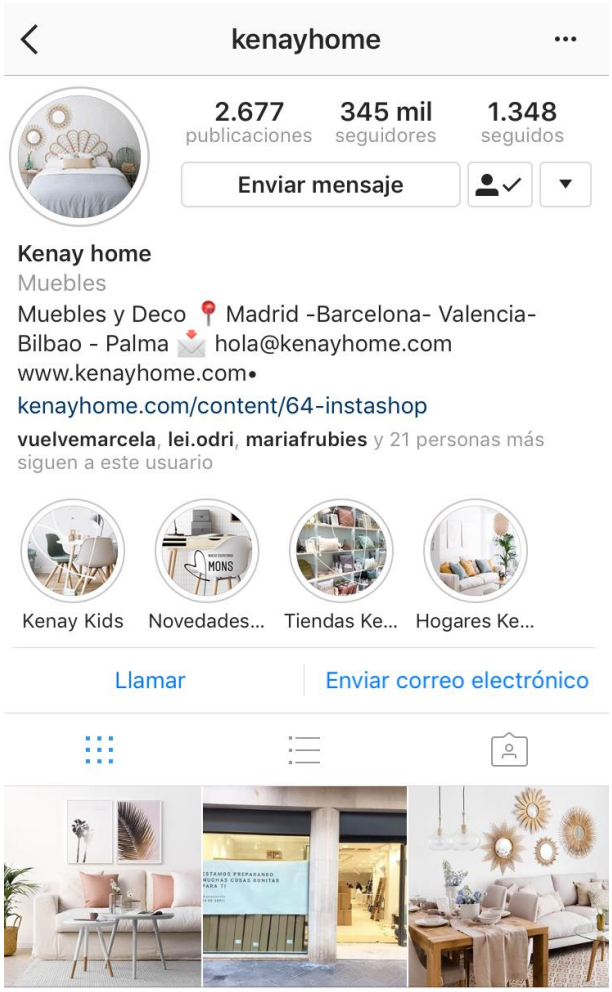

Figura 2.12: Perfil de un usuario empresarial en Instagram. Fuente: Instagram.

2.3.8. Tik-Tok

Además, en enero de 2011, fue una red pionera en promover hashtags junto con Twitter, con el propósito de facilitar a los usuarios el descubrimiento de fotos compartidas por otros usuarios sobre el mismo tema o lugar, y que no podían llegar a verse de otra forma.

Por su parte, Tik-Tok (también conocida como Dou Yin en China), que apareció a finales de 2016, es una red social que tiene un gran atractivo entre los adolescentes de hoy. Tik-Tok es una red social adquirida por Musically en 2018.

Se puede comparar con el uso mixto de Vine y Snapchat, a través de ella se pueden crear y compartir videos muy cortos, que van desde 15 segundos hasta un máximo de un minuto. Los videos que los usuarios jóvenes pueden hacer casi cualquier cosa. Se pueden editar utilizando las poderosas herramientas proporcionadas por la aplicación.

Desde luego, existen muchas más redes sociales que no se han llegado a analizar y exponer. En este apartado se han desarrollado las redes más famosas en España.

Otras regiones del mundo cuentan con sus propias aplicaciones: China tiene QZone, Baidu, Tieba y Sina Weibo. Rusia, por ejemplo, contiene Odnoklassniki y Vkontakte que suman cientos de millones de usuarios en redes que son auténticas desconocidas para nosotros [17].

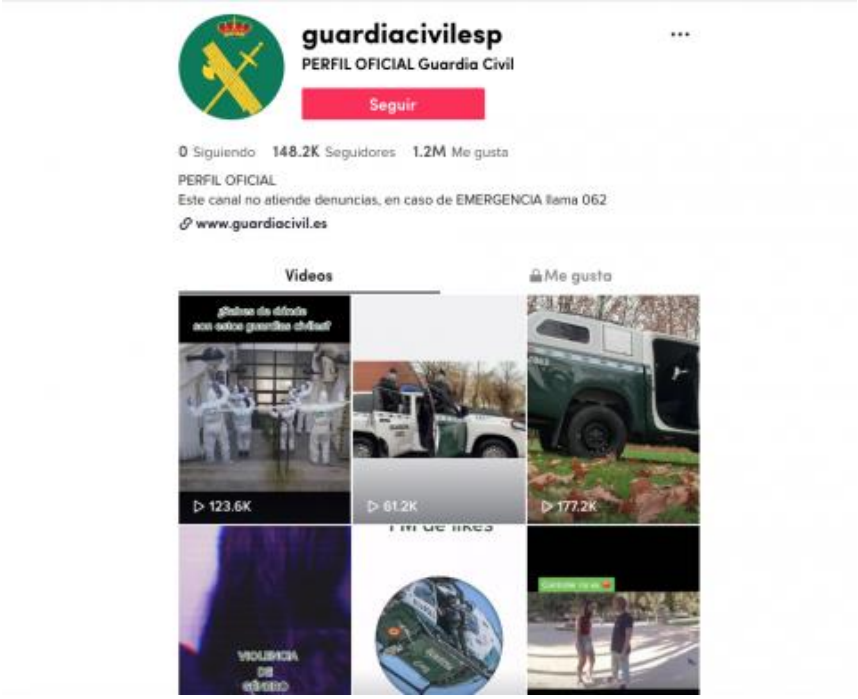

Figura 2.11: Perfil de la guardia civil en Tik-Tok. Fuente: tik-tok.

3. ¿Qué son nuestros datos personales?

En este capítulo trataremos de explicar que nuestros datos personales, es decir, datos que nos identifican frente a un sistema, así como definir y detallar los diferentes tipos que existen. Incluiremos informes sobre los diferentes tipos de datos personales y también los que más se han sustraído de las redes sociales con ataques informáticos.

Según el RGPD, los datos personales son:

> […] toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. (p.33)

Los datos personales que han sido anonimizados, encriptados o presentados bajo un seudónimo, pero que pueden usarse para volver a identificar a una persona, aún pertenecen a los datos personales y están dentro del alcance del RGPD.

Los datos personales que han sido anonimizados, de modo que la persona no pueda ser identificada o ya no lo sea, dejarán de ser considerados datos personales. Para que los datos se consideren realmente anónimos, el anonimato de esa persona debe ser irreversible.

En 2016, la AEPD publicó una guía para agilizar los procedimientos de anonimización de datos personales. Con ello, se pretende minimizar los riesgos que puede sufrir una persona a que se reidentifique, aunque se mantiene la exactitud de estos, es decir, se quiere evitar la identificación de las personas, pero también se debe asegurar que al tratar después con estos datos no sean diferentes a los reales.

En este transcurso de anonimizar los datos, se debe de tener en cuenta que se rompe el encadenado para identificar a las personas, tanto directa como indirecta. De forma indirecta se entiende por aquella que juntando edad, sexo, padecimiento de una enfermedad y fecha de nacimiento se puede llegar a identificar a una persona.

La AEPD señala una seria de principios de anonimización, los cuales vamos a detallar a continuación:

1. Principio proactivo: La protección de la privacidad es el objetivo principal de la anonimización y su gestión debe ser activa en lugar de pasiva. Dado que se han reparado las lagunas en el proceso de anonimización

o el daño a partes relacionadas, no se puede garantizar la privacidad a posteriori, por lo que es necesario asegurar que no exista una posible cadena de reidentificación de partes relacionadas en los datos anonimizados.

2. Principio de privacidad por defecto: El primer requisito conceptual del diseño de un sistema de información es asegurar la confidencialidad de las partes relacionadas. Por lo tanto, considerando la granularidad o el nivel final de detalle que deben tener los datos anónimos, la privacidad debe protegerse desde el principio.

3. Principio de privacidad objetiva: Como resultado de la Evaluación de Impacto en la Protección de Datos, habrá un umbral de riesgo reidentificado o un índice de riesgo residual. El índice de riesgo será asumido por el personal responsable de la documentación y procesamiento como un riesgo aceptable, y será tenido en cuenta en el diseño del proceso de anonimización.

4. Principio de plena funcionalidad: Desde el inicio del diseño del sistema de información, se considerará la utilidad última de los datos anónimos, y se garantizarán los datos no anónimos en la medida de lo posible sin distorsión. De esta forma se garantizará la utilidad de los datos anónimos. En algunos casos, para garantizar la privacidad de las personas, puede ser necesario utilizar distorsiones geográficas, como personas con enfermedades extremadamente raras.

5. Principio de privacidad en el ciclo de vida de la información: Las medidas para garantizar la privacidad de las partes interesadas se aplican a todo el ciclo de vida de la información, comenzando con información no anónima.

6. Principio de información y formación: Una de las claves para garantizar la privacidad de las partes relacionadas es brindar capacitación e información a las personas involucradas en el proceso de anonimización y el uso de información anónima. Durante el ciclo de vida de la información, todas las personas que tengan acceso a datos anónimos o no anónimos recibirán la formación adecuada y comprenderán sus obligaciones.

Por último, la AEPD apunta que en el proceso de anonimizar los datos no puede asegurar al 100% que en un futuro no se pueda reidentificar a las personas, por lo que se debe tener en cuenta estas garantías jurídicas:

1. Un acuerdo de confidencialidad que involucra a los siguientes participantes: Responsable de documentos; Responsable del proceso de anonimización; Responsable del tratamiento de datos anónimos; Personas con acceso a información anónima.

2. Obtener el juramento de que el destinatario de la información permanecerá en el anonimato, y queda obligado a notificar al responsable del documento en caso de cualquier duda sobre la reidentificación.

3. Auditar el uso de información anónima por parte del responsable del archivos y responsable del tratamiento anónimo de datos.

4. La garantía se incluirá en el contrato firmado entre el responsable del documento y el destinatario de la información anónima [18].

Independientemente de la tecnología utilizada para procesar los datos personales, RGPD protegerá los datos personales, es "tecnológicamente neutral" y apto para el procesamiento automático y manual, siempre que los datos estén organizados de acuerdo con estándares predeterminados (como el orden alfabético). Además, no importa cómo se almacenen los datos; en un sistema informático, mediante videovigilancia o en papel; en todos estos casos, los datos personales están sujetos a requisitos.

3.1. Datos de identificación

Podemos considerar como datos de identificación el nombre, los apellidos, el estado civil, la firma autógrafa y electrónica, el lugar y fecha de nacimiento, la nacionalidad, la fotografía y la edad.

Estos son los datos más comunes que ponemos en las redes sociales y, por lo tanto, los que más riesgo puedes sufrir de ser filtrados o robados. Así fue en 2018 cuando Facebook sufrió el primer gran hackeo de su historia, asumido y publicado por la compañía, aunque tardaron 3 días en avisar a sus usuarios de tal ataque.

En total 50 millones de cuentas se vieron comprometidas, ya que los piratas informáticos aprovecharon la utilidad de «*ver cómo*» -que autoriza al usuario de una cuenta observar el estado que tiene su perfil a ojos de una tercera persona- para hacerse con el poder de las cuentas de terceros [19].

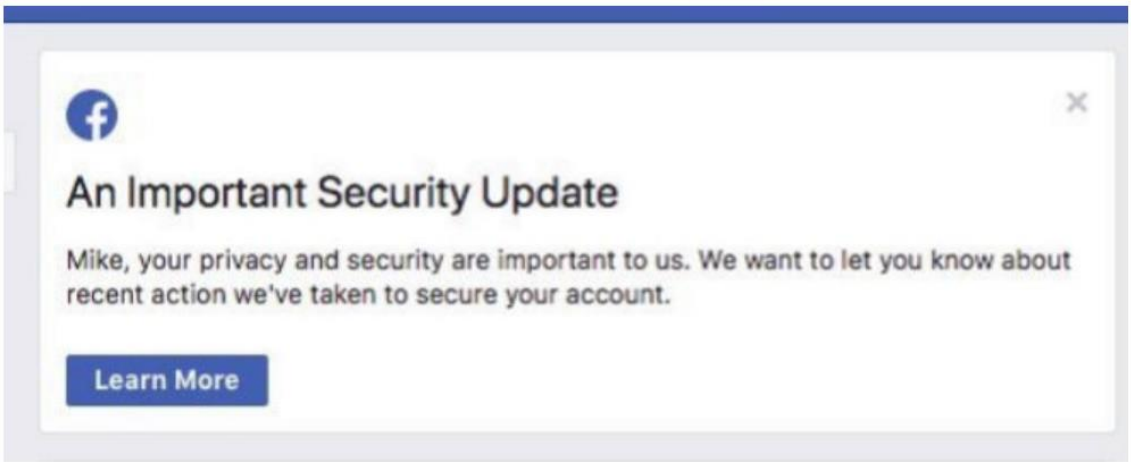

Figura 3.1: Notificación que recibieron los usuarios de Facebook afectas por el ataque. Fuente: elmundo.

En 2014, el almacenamiento en la nube de Apple sufrió varios ataques y de manera constante. El caso más viral ocurrió cuando salieron a la luz fotografías comprometidas de más de cien famosos después de sufrir un ataque en iCloud. Los responsables del ataque robaron estas fotografías y posteriormente las colgaron en un portal llamado 4chan, donde se dedican a subir todo tipo de contenido extraído por parte de los hackers y posteriormente se vieron por todo internet.

Según Apple, el ataque vino por dos causas: la primera fue por una vulnerabilidad en la función de «*Buscar mi iPhone*» por la cual se podría haber conseguido una entrada a las cuentas de los damnificados.

La segunda fue a través del sistema de almacenamiento en la nube que tiene Apple, debido a un ataque de fuerza bruta que consistía en mecanizar la prueba de contraseñas frágiles hasta dar con la que necesitaban para acceder al sistema, esto lo consiguieron gracias a un script en el lenguaje Python disponible en GitHub.

Apple negó rotundamente que se tratara de un fallo de seguridad en iCloud afirmando que ciertas cuentas de famosos fueron comprometidas debido a un ataque muy específico sobre contraseñas, nombres de usuario y preguntas de seguridad. Acusó de utilizar contraseñas fáciles de descifrar y hasta el día de hoy sigue negando que tuviera un fallo de seguridad [20].

3.2. Datos de contacto y patrimoniales

En este apartado consideramos datos de contacto el domicilio, el correo electrónico y el teléfono (ya sea fijo o móvil) entre otros datos. Mencionamos los más importante y destacados ya que son los más buscados por los responsables de los ataques informáticos.

Por datos patrimoniales entendemos propiedades, bienes muebles e inmuebles, historial crediticio, ingresos, cuentas bancarias, seguros, números de tarjeta de crédito y número de la seguridad social entre otros.

En 2018 la compañía de hoteles Marriott sufrió uno de los mayores robos de datos y se convirtió en uno de los casos más conocidos mundialmente. En total se expuso la información personal de 500 millones de personas. Los datos de contacto y patrimoniales son los más buscados por los hackers por lo que en este apartado, daremos algunos consejos para ayudarte a resguardarte contra su uso indebido en caso de que hayan podido quedar expuestos.

La cadena de hoteles afirmó que el incidente de seguridad de datos empezó 4 años antes, es decir, en el año 2018. 4 años en los que la información de cada cliente que realizaba una reserva en su hotel podía quedar comprometida. Tenemos que añadir que la cadena cuenta con más de 6500 establecimientos repartidos por 120 países y con más de 1,1 millones de habitaciones.

Este hecho fue debido a que su base de datos de reservas quedó expuesta a través de un masivo hackeo. No quedó ahí el percance ya que, en 2020, la compañía volvió a sufrir otro ataque dejando expuesta la información de más de 5 millones de personas. Este ataque, tuvo similitudes con el sufrido en 2018 [21].

A continuación, vamos a redactar una serie de puntos para realizar en caso de que haya podido quedar expuesta nuestra información privada:

- Revisaremos los informes de nuestros pedidos de cuentas online, es decir, cada cuenta que se tenga en un sitio web que posibilite la opción de comprar cualquier artículo, debe ser revisada buscando cualquier encargo no reconocido.

- Revisaremos minuciosamente los extractos de nuestra cuenta de las tarjetas del banco. Nos fijaremos en cada transacción por si se reconoce algún cargo fraudulento o no realizado.

- Colocaremos alertas antifraude en nuestras tarjetas de crédito. Este tipo de alertas sirven para advertirnos que podríamos ser víctima del robo de nuestra identidad y por lo tanto se debería verificar la identidad de cualquiera que intente tomar nuestra tarjeta con nuestro nombre. Las alertas antifraude son gratis y tiene una duración de un año.

- Consideraremos colocar una herramienta de congelamiento de crédito gratis en nuestras cuentas bancarias. Con este tipo de instrumento es más difícil que una persona abra una cuenta bancaria nueva con nuestro nombre. Esta función no impedirá que un delincuente realice cargos a nuestras cuentas existentes.

En el año 2013, uno de los mayores robos en cuanto a números de tarjetas de crédito lo sufrió la compañía Target, una cadena de grandes almacenes que resulta ser la sexta empresa de comercio minorista más grande de Estados Unidos. Target tardó aproximadamente 3 semanas en admitir el gran hackeo que había sufrido de 40 millones de números de tarjetas de crédito. Informó a través de un correo electrónico a sus clientes y a raíz de esta información, los bancos más importantes y con más volumen del país decidieron limitar la cantidad de dinero en efectivo que podían sacar sus clientes en los cajeros automáticos, así como la cantidad que podían pagar con las tarjetas.

El asunto fue tan grave que llegó al senado de Estados Unidos. En concreto los ladrones robaron los nombres de los clientes, fechas de caducidad de las tarjetas de crédito o débito, números de las tarjetas de crédito o débito, así como el código de seguridad CVV- el valor de verificación de tarjeta que consta de 3 dígitos- situado en la parte trasera de la tarjeta.

Con este tipo de información sustraída, los hackers pueden replicar tarjetas. Sin embargo, los números PIN los números de la Seguridad Social y los registros de los trabajadores no quedaron comprometidos.

Esta brecha de seguridad se produjo debido a que los ladrones tuvieron un camino fácil para encontrar los datos de los puntos de venta, es decir, cualquiera podría acceder a los terminales, en los cuales se han podido pasar tarjetas de crédito o datos recogidos por el sistema de tarjetas de crédito [22].

Otro acontecimiento parecido ocurrió en el 2018, cuando dos marcas de lujo como son Saks Fifth Avenue y Lord & Taylor, sufrieron un ataque cibernético en el cual los ladrones tuvieron acceso a más de 5 millones de números de tarjetas de crédito y débito.

La grave situación no sabemos cuándo tardaron en percatarse, pero si por quien fue descubierta. La empresa de seguridad cibernética Gemini Advisory advirtió de la venta de los números de las tarjetas en la «*dark web*».

Gemini apuntaba a un grupo de hackers llamado «*Fin7 Syndicate*», ya que estos fueron quienes publicaron el anuncio de la venta de más de 5 millones de números de tarjetas de crédito y débito robadas.

Una vez solucionado el problema se trataba de averiguar cómo pudieron acceder a dicha información. Muchos expertos en seguridad informática expusieron la posibilidad de que los hackers obtuvieran la información a partir de los puntos de venta, es decir, por donde se hayan pasado las tarjetas. Es la misma situación que el caso anterior, por esto se han modernizado los sistemas en los puntos de venta [23].

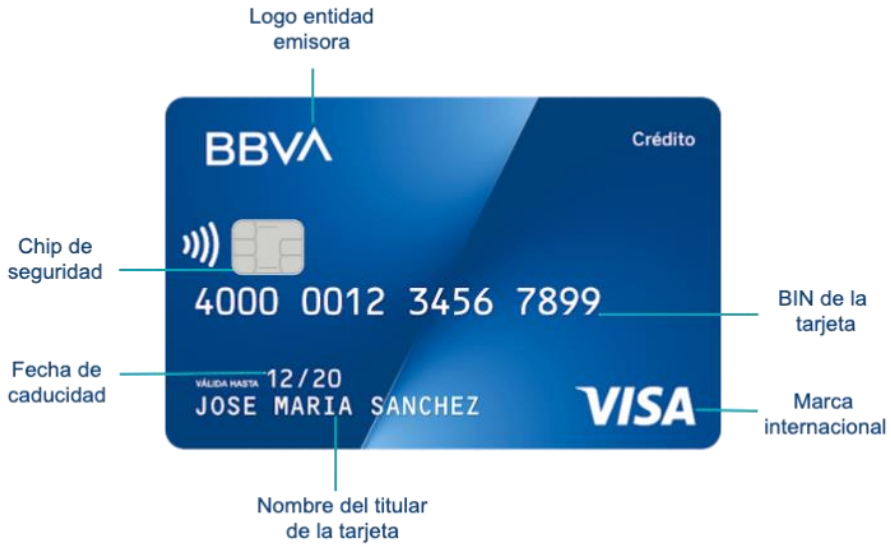

Figura 3.2: Imagen de la parte delantera de una tarjeta de crédito. Fuente: bbva.

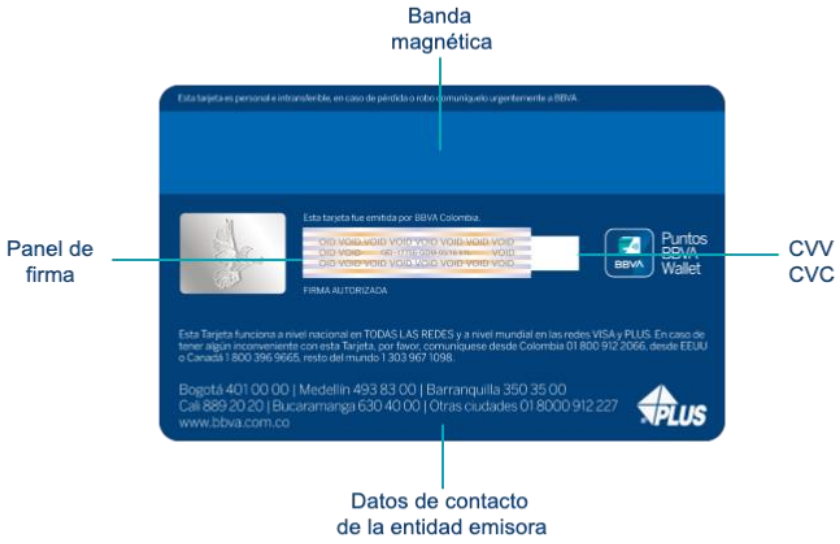

Figura 3.3: Imagen de la parte trasera de una tarjeta de crédito. Fuente: bbva.

3.3. Datos médicos

La valoración, la preservación, el cuidado, el mejoramiento y la recuperación sobre el estado físico o mental y la información genética pertenece al apartado de datos médicos. Existen muchos más, pero hemos seleccionado aquellos que consideramos lo más importantes.

El primer gran hackeo que se hizo público fue en el año 2015, cuando la empresa farmacéutica Comunity Health System, que tiene 206 hospitales por todo Estados Unidos reportó que unos hackers habían accedido a sus ordenadores robaron 4,5 millones de datos de pacientes.

Los ladrones tuvieron acceso a los números de la seguridad social, nombres, direcciones físicas, números de teléfonos, fechas de cumpleaños y todo su historial médico. Recordamos que en un historial médico contiene la información, datos y valoraciones de cualquier tipo sobre la situación y evolución de un paciente a lo largo del proceso asistencial.

El problema fue de tal magnitud que cualquiera que hubiera pasado por alguno de estos centros en los últimos 5 años se vio afectada. Como objetivo principal de los ladrones, el robo les permitía abrir cuentas bancarias, solicitar préstamos y adquirir tarjetas de crédito. Una empresa externa contratada por Community Health System determinó que los hackers actuaron desde China con un programa maligno de alta calidad para lanzar los ataques.

Los piratas informáticos también robaron datos clínicos de los pacientes como los historiales médicos y las operaciones clínicas. El FBI investigó el caso llegando a presentar cargos contra altos mandos del ejército chino por su presunto papel en las operaciones prolongadas de ciberespionaje contra empresas estadounidenses [24].

Hoy en día los datos médicos se están convirtiendo en un valor al alza. Más todavía cuando a finales de 2019 y principios del 2020 se descubrió un nuevo virus, SARS-CoV-2. Presuntamente de origen artificial, es decir, salido de un laboratorio. En concreto, de uno situado en la ciudad de Wuhan, donde se encuentra un laboratorio que trabaja con coronavirus.

A partir de entonces se empezaba una guerra, la guerra por descubrir la primera vacuna, una lucha invisible que se llevaría a cabo con sabotajes, espías y robo de datos.

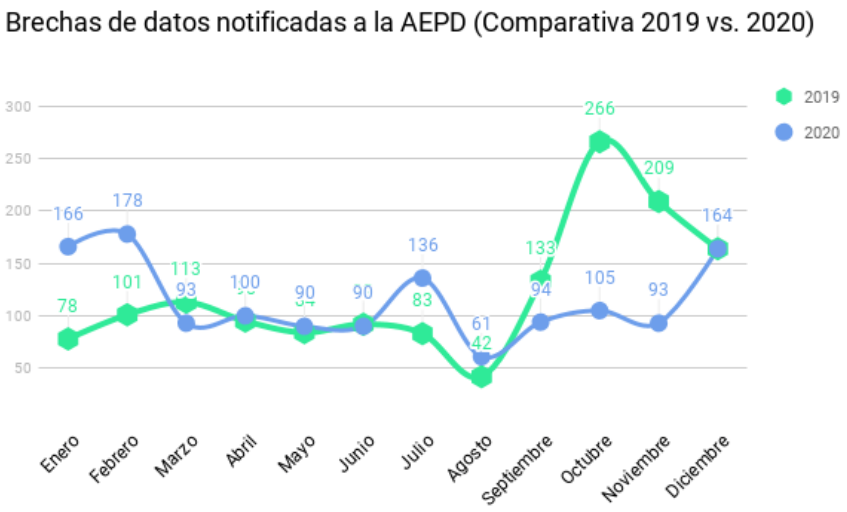

Figura 3.4: Comparativa de hackeos entre 2019 y 2020 notificados a la AEPD. Fuente: bitlifemedia.

La pregunta que se plantea es clara. ¿Alguien está en contra de desarrollar la vacuna? Esta pregunta tiene muchos matices y tenemos que contextualizarla. Las organizaciones ciberdelincuentes están interesadas en sabotear su distribución o desarrollo, obtener información delicada sobre la vacuna, robar datos sanitarios de los ciudadanos, extorsionar a quienes la producen o aprovechar la avalancha informativa para estafar a la gente.

Las principales farmacéuticas se han blindado contra el escape de informaciones y no se ha revelado ningún ataque contra ellas. Estamos hablando de Pfizer, Moderna, AstraZeneca y Janssen que estuvieron a la cabeza del desarrollo de la vacuna.

Pero se pudo descubrir que la Universidad de Oxford y AstraZeneca sí que recibieron un ataque por parte de un grupo norcoreano llamado Lazarus, un grupo mundialmente conocido. Hubo varias acusaciones entre Rusia, Estados Unidos, Canadá, China y Reino Unido en las cuales se acusaban de intentar torpedear las plantas de desarrollo de la vacuna, intentar atrasar la producción para sacar ellos la primera vacuna.

En España no nos hemos librado de los ciberataques, el Centro Nacional de Inteligencia (CNI) manifestó en el mes de septiembre que piratas informáticos chinos habían logrado conseguir información relacionada con la vacuna que se estaba preparando por los científicos españoles. Conscientes de ello, la cúpula del poder español puso en marcha un plan de vigilancia que iba a ser coordinado por el Consejo Nacional de Ciberseguridad. Este dispositivo estaba alerta ante las posibles amenazas, robos de informaciones, intrusiones o espionajes [25].

Figura 3.5: Producción en cadena de la vacuna. Fuente: diariomedico.

La primera vacuna aprobada en Europa por la Agencia Europea del Medicamento (EMA) es la desarrollada por BionTech y Pfizer, cuenta con un 95 por ciento de eficacia. Aunque esta fue la primera vacuna aprobada en Europa, la primera vacuna registrada contra el supuesto nuevo virus chino fue Rusia, que registró la vacuna Sputnik V en agosto del 2020.

La desconfianza en la Unión Europea era evidente hasta tal punto que hoy en día sigue sin estar aprobada, aunque según el presidente ruso, Vladimir Putin, afirmaba que todos los voluntarios que recibieron la vacuna desarrollaron anticuerpos [26].

3.4. Datos laborales y académicos

Como datos laborales podemos encontrar el cargo que se ocupa, el domicilio de trabajo, correo electrónico, teléfono de trabajo, fecha de ingreso y salida del empleo y salario entre otros.

Por otro lado, como datos académicos vemos que la trayectoria académica, títulos, cedula profesional, certificados y reconocimientos entre otros son los principales datos que podemos agregar a este punto.

En 2018, Estados Unidos anunciaba sanciones contra 9 individuos iraníes, así como a la consultora estratega MABNA, con origen iraní, por robar más de 31 terabytes de información académica de universidades estadounidenses con el fin de ser empleada para obtener beneficio financiero y así aumentar el presupuesto del Ejército iraní.

Para poder obtener una idea de lo que se puede almacenar en 31 terabyte, vamos a nombrar algunos ejemplos. 7.750.000 millones de fotos elaboradas con una cámara de 12 megapíxeles, 7.750 películas o 15.500 horas de vídeo en HD o 201,5 millones de páginas de documentos, almacenados regularmente como archivos de Office, PDF y presentaciones. En papel, equivaldría a 1.300 estanterías llenas de papel.

Con este ataque consiguieron extraer información de más de 100.000 profesores y más de 8.000 alumnos. Estos delincuentes y la entidad MABNA no es la primera vez que organizan ataques de este calibre. Intentaron extraer información de más de 144 universidades estadounidenses y otras 176 universidades alrededor del mundo desde el 2013 [27].

En el curso 2019-20 y 2020-21 en el cual se ha impuesto la docencia híbrida, es decir, combinar las clases virtuales con las clases presenciales los centros docentes, así como sus alumnos están más expuestos al robo de datos académicos.

Vamos a dar unas pautas de seguridad para que puedan seguir cualquier miembro de un centro docente:

- Es mejor ser consciente de los riesgos que pueden traer los ciberdelincuentes por el uso fraudulento de nombres de dominio o entidades universitarias (como instituciones legítimas y confiables de los usuarios). Por lo tanto, es necesario verificar cualquier comunicación de correo electrónico sospechosa con fuentes oficiales.

- Se tiene en cuenta posibles errores ortográficos y gramaticales en el mensaje, ya que esto puede indicar que son fraudulentos.

- Se deben tomar precauciones extremas cuando reciba un correo electrónico solicitando credenciales de inicio de sesión o una advertencia de que el servicio o la cuenta se suspenderán si no se hace clic en el enlace.

- Se utilizan las contraseñas correctamente para que la integridad como método de autenticación seguro no se vea comprometida. Esto significa utilizar una contraseña única para cada sitio que el usuario desee visitar, hacerlo lo más seguro posible y cambiarlo con frecuencia.

- Al ingresar al sitio web y otras plataformas universitarias, se debe ingresar directamente la dirección del sitio en su navegador para mejorar la seguridad.

3.5. Otros

Los datos expuestos anteriormente no son los únicos datos personales que posee una persona. Hemos seleccionado los que consideramos más relevantes para realizar el análisis, pero podemos encontrar otros datos. Con el paso del tiempo poseemos más datos personales en los cuales debemos de tener en cuenta con quien los compartimos o a quien le damos acceso para que los puedan ver. A continuación, expondremos el resto de los datos personales que tiene una persona:

- Datos sobre características físicas: Color de piel, color del iris o del cabello; señas particulares o cicatrices, estatura, peso complexión y tipo de sangre.

- Datos biométricos: forma del iris, huella dactilar, forma de la palma de la mano, patrones de la voz u otras características únicas.

- Datos ideológicos: Posturas ideológicas, religiosas, filosóficas o morales. Posturas políticas o de afiliación sindical.

- Datos sobre vida sexual: Comportamiento, preferencias, prácticas o hábitos sexuales.

- Datos sobre origen étnico: Pertenencia a una etnia o región con condiciones e identidades sociales, culturales y económicas. Costumbres, tradiciones o creencias.

4. ¿Por qué tienen tanto valor e importancia nuestros datos para las empresas?

A lo largo de los años y con la evolución de la tecnología tenemos más datos personales, lo cual conlleva más riesgos y por eso tenemos que estar bien informados sobre todas las posibles incursiones en nuestra vida privada.

En este punto trataremos los temas más incómodos para las empresas responsables de guardar nuestros datos personales, desde que empresas son las que más venden nuestros datos a terceros hasta cuales son las que más tienen información sobre el usuario. También analizaremos como a través de los datos

personales, se pueden incentivar ciertas conductas de consumo e incluso predecir hábitos.

4.1. Historial de las principales transacciones con datos personales

Con el desarrollo de Internet, las ventas de nuestros datos se han vuelto cada vez más importantes. Hoy, la empresa quiere recopilar todos los datos posibles de los usuarios de forma precisa. Por lo tanto, será más fácil personalizar los servicios que brindan de acuerdo con los intereses exactos de los consumidores, aumentando así su volumen de ventas.

En otras palabras, lo que pretende hacer es personalizar los anuncios que se proporcionan de forma extrema. La información recopilada se puede ver a partir de cookies, enlaces que compartimos en redes sociales o publicaciones que hacemos, y en la mayoría de los casos les agregamos nuestra ubicación.

Figura 4.1: Estadística de las empresas que más información toman de los usuarios. Fuente: statista.

En esta figura podemos observar cómo las dos primeras plataformas, son propiedad de Mark Zuckerberg, el cual, acumula numerosas multas por filtrar, vender o dejar desprotegidos los datos de sus usuarios. La multa más

importante que ha tenido que asumir la compañía americana es de 5.000 millones de dólares. Esta multa fue impuesta en el 2019, a la cual acompañaba una serie de medidas para mejorar la política de protección de datos de sus usuarios. Las nuevas medidas de protección se aplicaron además de Facebook, a Instagram, Messenger y WhatsApp.

La multa surge a raíz de la reincidencia de Facebook por permitir que la compañía Cambridge Analytica tomara datos de 87 millones de usuarios usados para las elecciones estadounidenses del año 2016. Los usuarios afectados no fueron informados y posiblemente ni siquiera identificados por parte de Mark Zuckerberg [28].

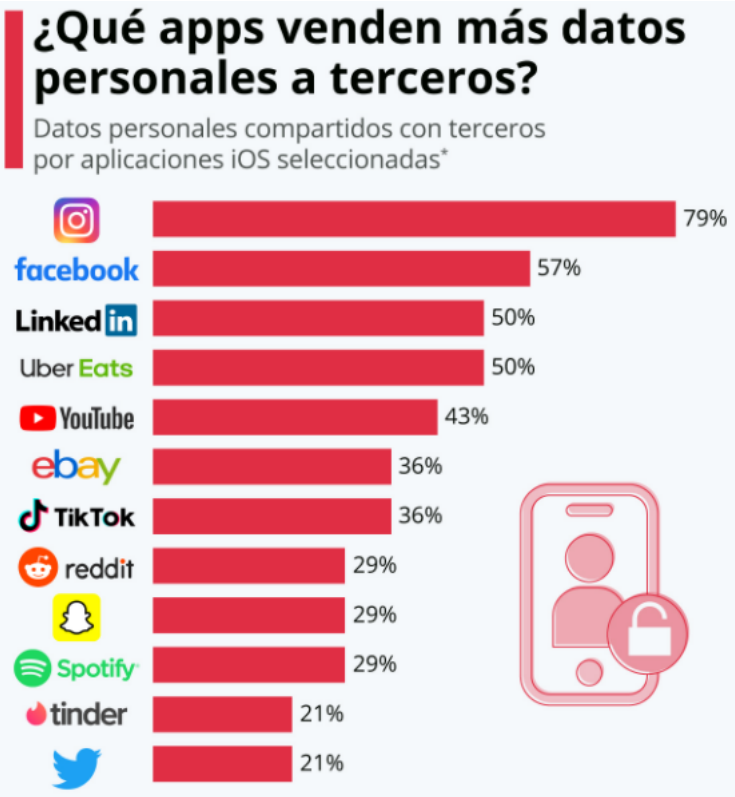

Figura 4.2: Estadística de las compañías que más datos venden de sus usuarios. Fuente: statista.

El año 2019 fue un año terrible para el fundador de Facebook. Hubo filtraciones que impactaron en 1,5 mil millones de cuentas, más de la mitad del total. Por lo tanto, podemos deducir que aquello usuarios que usaran esta red social, tuvieron un 50% de posibilidades de haberse visto afectado en mayor o menor medida por esta filtración [29].

Si ya hemos podido apreciar que Instagram y Facebook eran las que más datos recopilaban de sus usuarios, no defraudan en esta gráfica y son los que más datos venden a terceros.

4.2. Análisis de la cotización al alza de los datos personales

Los datos personales son el nuevo petróleo. Las personas que no siguen las reglas roban la información personal de los usuarios y la venden en el mercado negro, son tesoros más suculentos que son más fáciles de obtener. En España no existen muchos tipos de actividades indebidas, pero algunas empresas proceden de países como Países Bajos, Israel o India.

Estas personas traen robots a la red y recopilan todas las cosas públicas. Por ejemplo, si dices en Twitter que te gusta el nuevo modelo de esta marca de ropa y tienes una cuenta de correo electrónico asociada a tu perfil, pueden buscar automáticamente estos datos y enviarle un anuncio de la nueva colección de ropa.

Estos bots suelen enviar una gran cantidad de invitaciones en Facebook o LinkedIn para acceder a información que los usuarios comparten solo con sus contactos. En Twitter, Instagram y Tik-tok se tiene más facilidad ya que los perfiles pueden verse desde cualquier cuenta. Conservan los datos y los venden a empresas interesadas en enviar publicidad a un determinado tipo de perfil.

Existen muchas empresas que se dedican a realizar estas actividades. Guardan los datos y posteriormente los venden a empresas publicitarias que quieren enviar ciertos anuncios a un perfil específico.

El precio que se tiene que pagar por esta información varía mucho, desde los pocos céntimos con información escasa, hasta decenas de euros con informes detallados. A gusto del consumidor [30].

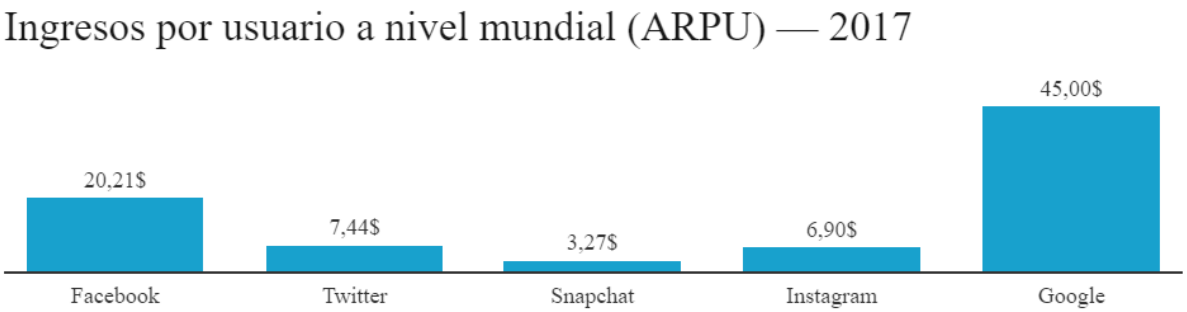

Figura 4.3: Ingresos en dólares de las principales redes sociales por usuario a nivel mundial en 2017. Fuente: businessinsider.

Un buen sistema de privacidad de los usuarios haría que los ingresos de las compañías descendiesen drásticamente, ya que el uso de estas redes es gratuito.

En esta gráfica podemos observar como Google lidera el ranking con más del doble de la siguiente que es Facebook. Tenemos que puntualizar que los datos corresponden a 2017. En las siguientes gráficas observaremos como sube el valor y coge relevancia e importancia a la hora de elaborar campañas publicitarias con la creación de las cookies para personalizar anuncios.

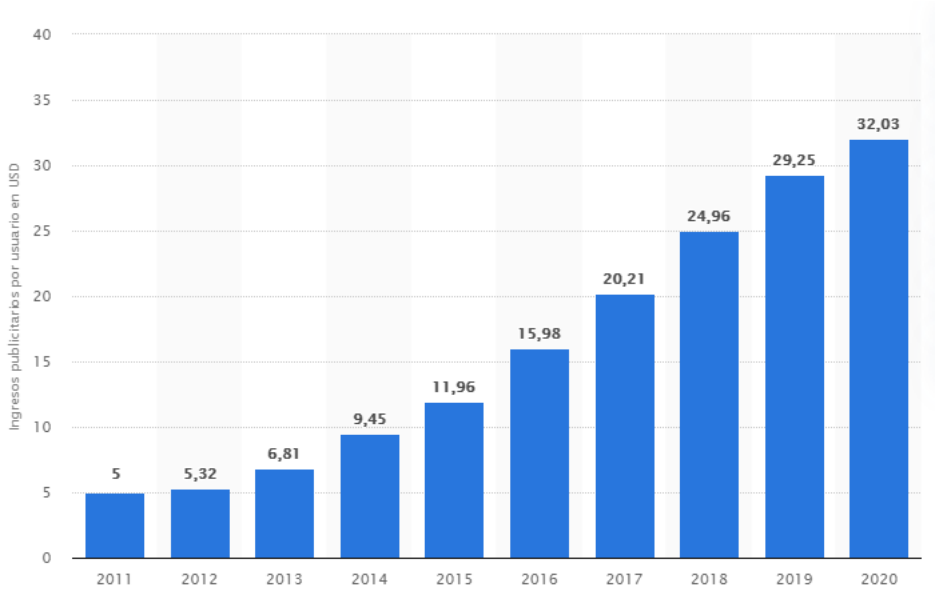

Figura 4.4: Ingresos medio por usuario (ARPU) de Facebook a nivel mundial entre 2011 y 2020. Fuente: statista.

Hemos elegido la compañía Facebook por los continuos fallos de seguridad en la contención de los datos de sus usuarios. A medida que pasan los años, los ingresos medios por usuario suben, es decir, el precio y valor de los datos sigue subiendo y nuestra previsión es que sigan subiendo.

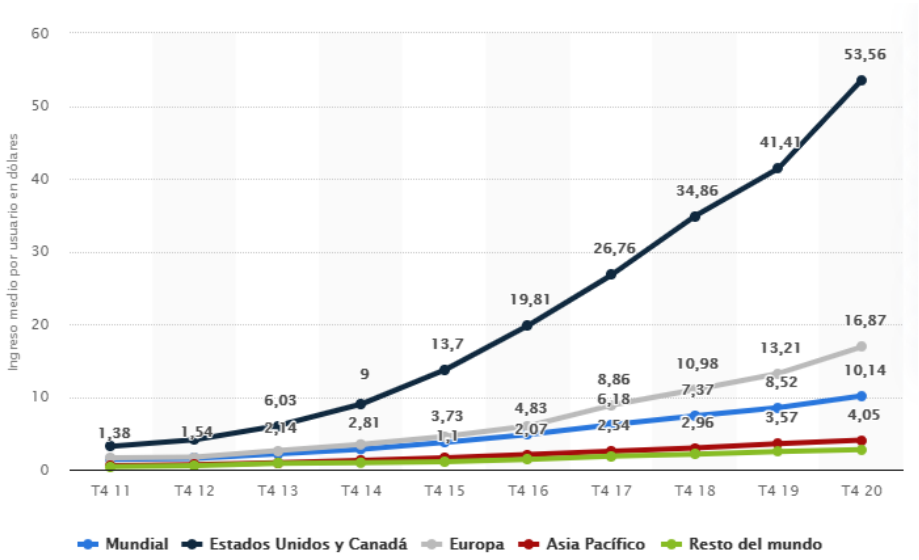

Figura 4.5: Ingreso medio por usuario (ARPU) de Facebook entre 2011 y 2020, por área geográfica. Fuente: statista.

Como podemos observar en la gráfica, los usuarios por los cuales más se pagan son los norteamericanos, seguidos por los europeos a una considerable distancia. La media mundial se sitúa en 10,14 dólares por usuario, incrementándose en 2 dólares aproximadamente respecto al año anterior.

La tendencia que vemos es clara, sigue ascendiendo y no tiene techo. Pensamos que aplicando la lógica seguirá ascendiendo, ya que cada vez poseemos más artilugios tecnológicos que nos mejoran la vida, pero a la vez registran más datos.

5. Como podemos proteger nuestros datos personales

En este punto trataremos las principales funciones que nos brindan las redes sociales para configurar nuestra protección. Nos centramos en la aplicación WhatsApp, ya que cada día millones de personas utilizan WhatsApp para comunicarse con los demás.

Esta es la red social líder en mensajería instantánea usada en todo el mundo para mantener conversaciones privadas en las que se intercambia información personal y de todo tipo, por lo tanto, para todos los usuarios es primordial conocer las funciones de privacidad y seguridad de esta plataforma.

5.1. Privacidad y seguridad en WhatsApp

Este punto se puede tomar como guía para un usuario que quiera configurar la protección y la seguridad. A continuación, se detallará una serie de pasos a seguir para tener una buena seguridad y privacidad:

5.1.1. Solicitar informe sobre nuestra cuenta

Lo primero que hay que saber es que en cualquier momento podemos solicitar a WhatsApp un informe sobre nuestra cuenta que recibiremos a los 3 días de solicitarla y de este modo comprobaremos si esta se encuentra plenamente protegida.

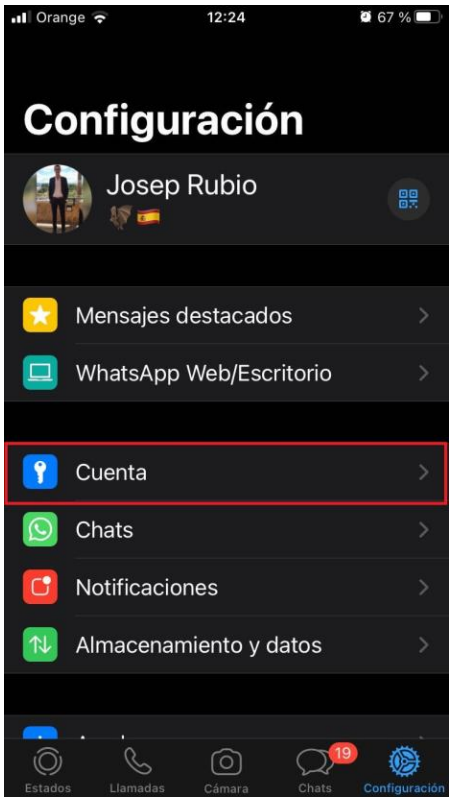

Figura 5.1: Primer paso para solicitar el informe sobre el estado de nuestra cuenta. Fuente: elaboración propia.

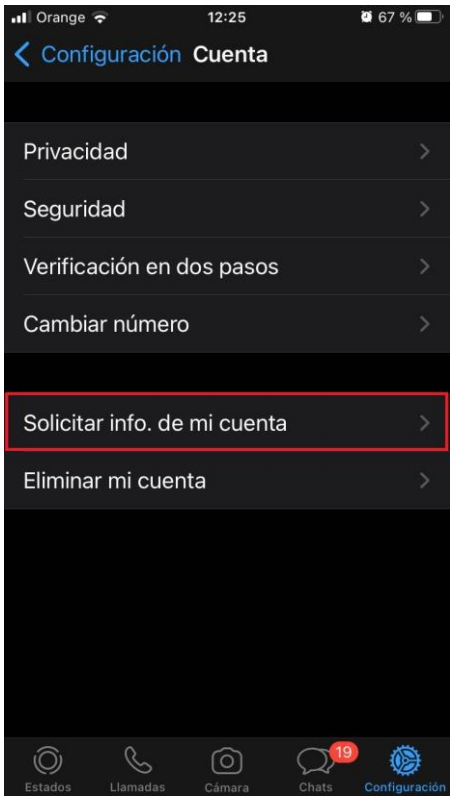

Figura 5.2: Segundo paso para solicitar el informe sobre el estado de nuestra cuenta. Fuente: elaboración propia.

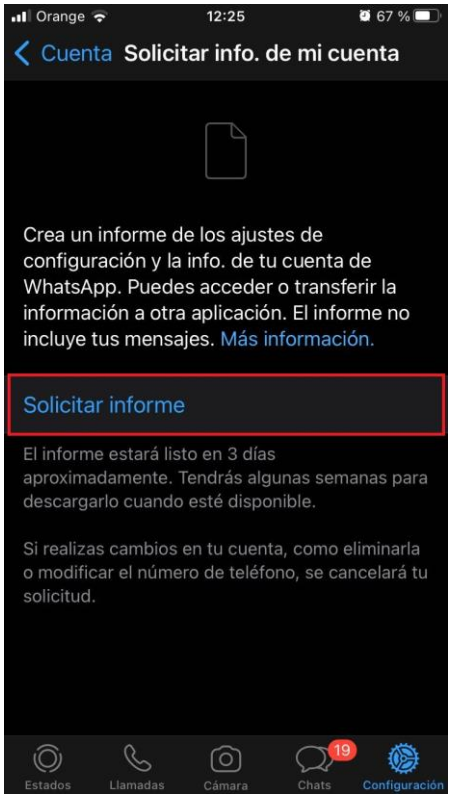

Figura 5.3: Tercer paso para solicitar el informe sobre el estado de nuestra cuenta. Fuente: elaboración propia.

5.1.2. Verificación en dos pasos

Es conveniente saber que podemos realizar la verificación en dos pasos para aumentar la seguridad en nuestra cuenta. Al activarla, cualquier intento de verificación de tu número de teléfono en WhatsApp debe ir acompañado de un pin de 6 dígitos que puedes establecer al accionar dicha función.

Esto lo haremos en configuración, después en cuenta, seguidamente clicaremos en verificación en dos pasos y activar. Este pin también nos protegerá evitando el robo de la cuenta y deberemos introducirlo si tenemos que recuperar la cuenta o cambiamos de dispositivo.

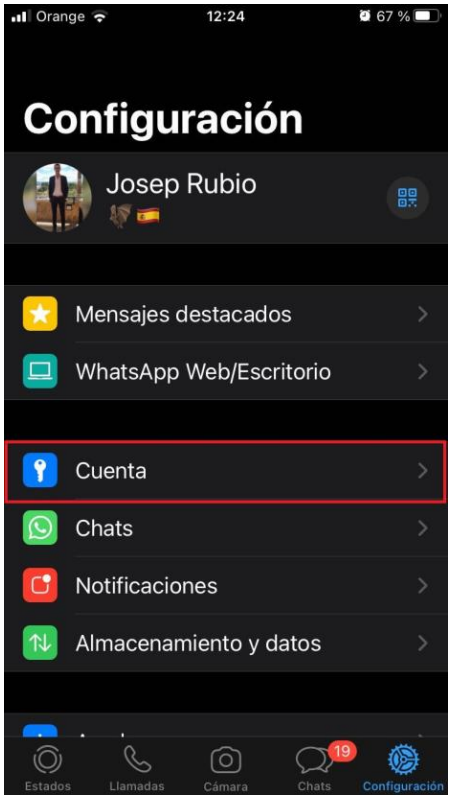

Figura 5.4: Primer paso para activar la verificación en dos pasos. Fuente: elaboración propia.

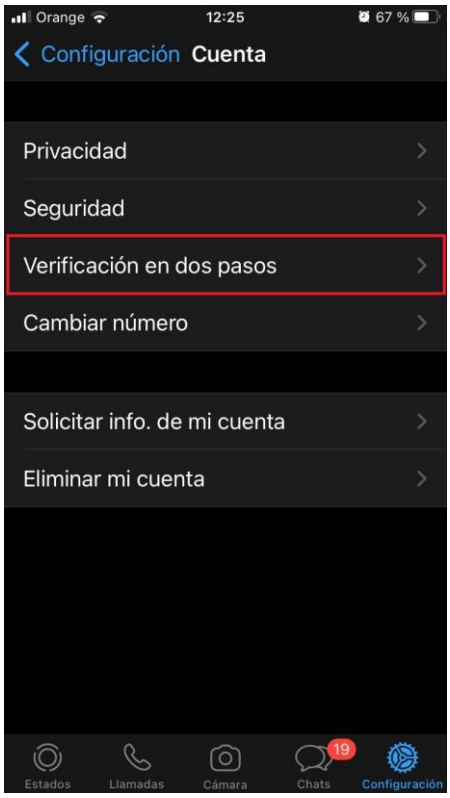

Figura 5.5: Segundo paso para activar la verificación en dos pasos. Fuente: elaboración propia.

Figura 5.6: Tercer paso para activar la verificación en dos pasos. Fuente: elaboración propia.

5.1.3. Cambiar ajustes de privacidad por defecto

Recordamos que los ajustes de privacidad de WhatsApp vienen por defecto al descargar la aplicación. Esto puede llegar a perjudicar nuestra privacidad si queremos que solo nuestros contactos vean nuestra foto de perfil, nuestra información o nuestro estado.

Tendremos que entrar en el apartado de privacidad de WhatsApp y escoger la opción mis contactos, también podremos seleccionar que nadie pueda ver esto, ya que la aplicación tiene esa opción.

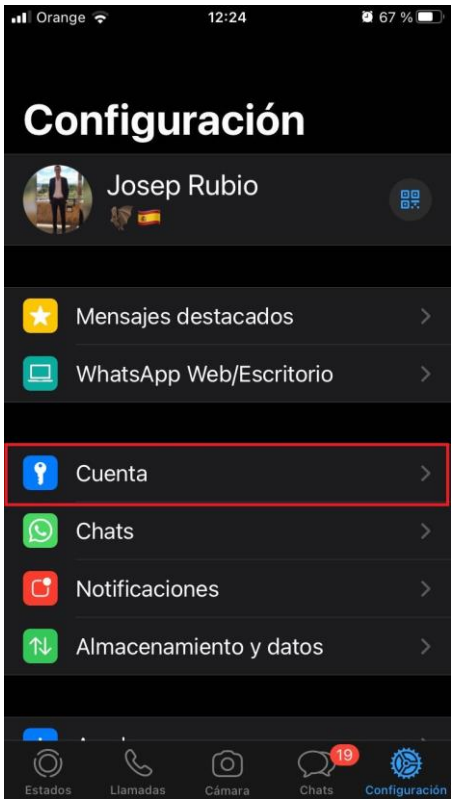

Figura 5.7: Primer paso para cambiar los ajustes de privacidad. Fuente: elaboración propia.

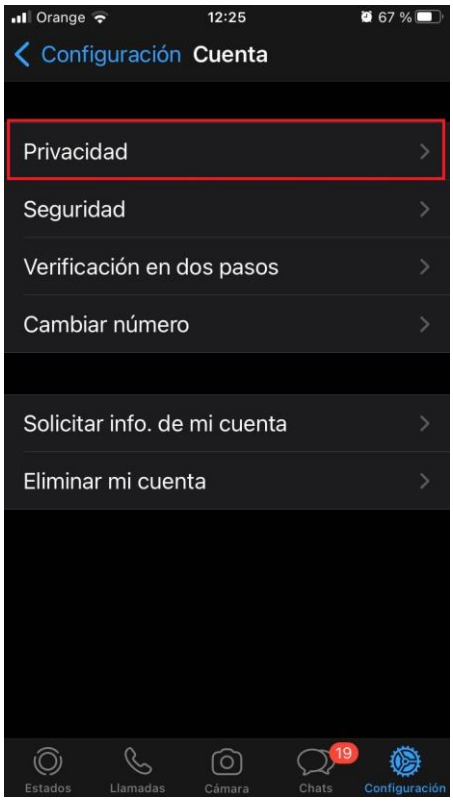

Figura 5.8: Segundo paso para cambiar los ajustes de privacidad. Fuente: elaboración propia.

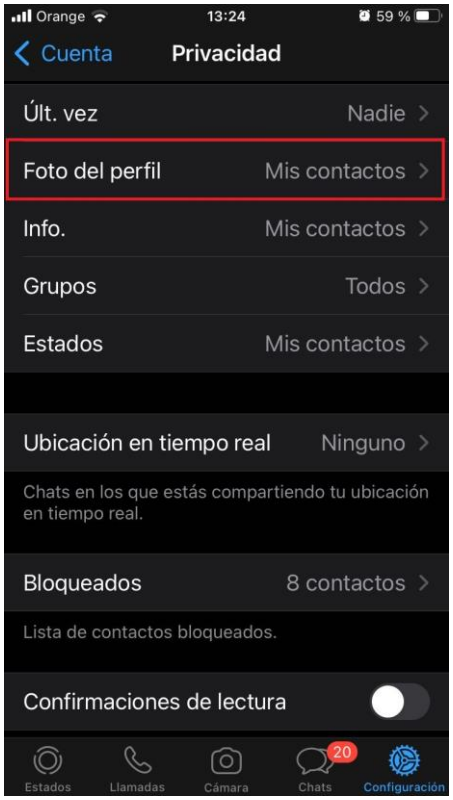

Figura 5.9: Tercer paso para cambiar los ajustes de privacidad. Fuente: elaboración propia.

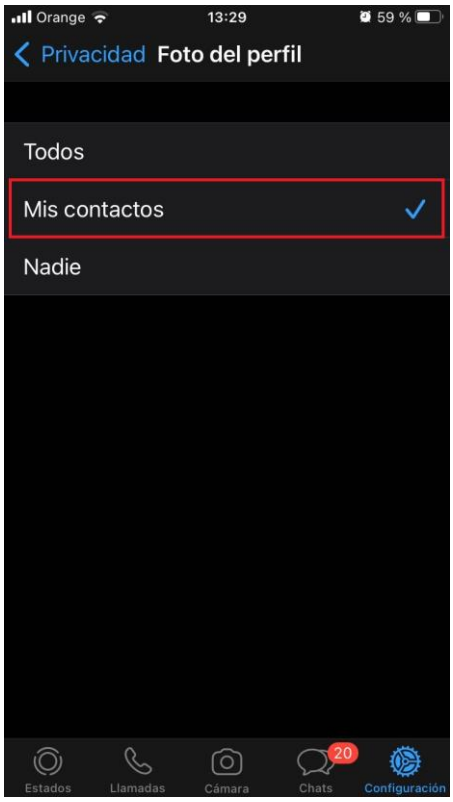

Figura 5.10: Cuarto paso para cambiar los ajustes de privacidad. Fuente: elaboración propia.

También podremos cambiar la opción para que solo nuestros contactos vean nuestra información o estado. En la sección de privacidad, justo bajo de foto del perfil, tenemos info y estados. Seleccionamos la opción de mis contactos.

5.1.4. Inhabilitar la hora de nuestra última conexión

Para salvaguardar nuestra privacidad, también podremos inhabilitar la información sobre la hora de nuestra última conexión dentro de los ajustes de privacidad. Así como la confirmación de lectura de nuestros mensajes, desactivando las confirmaciones de lectura en nuestro menú de privacidad.

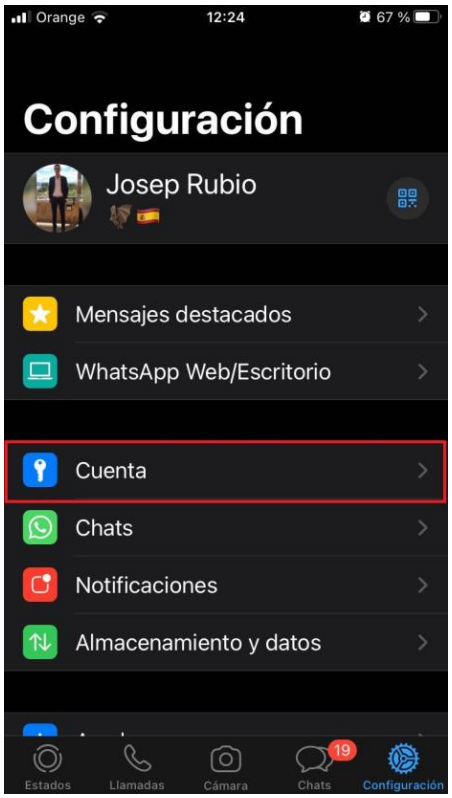

Figura 5.11: Primer paso para inhabilitar la hora de nuestra última conexión. Fuente: elaboración propia.

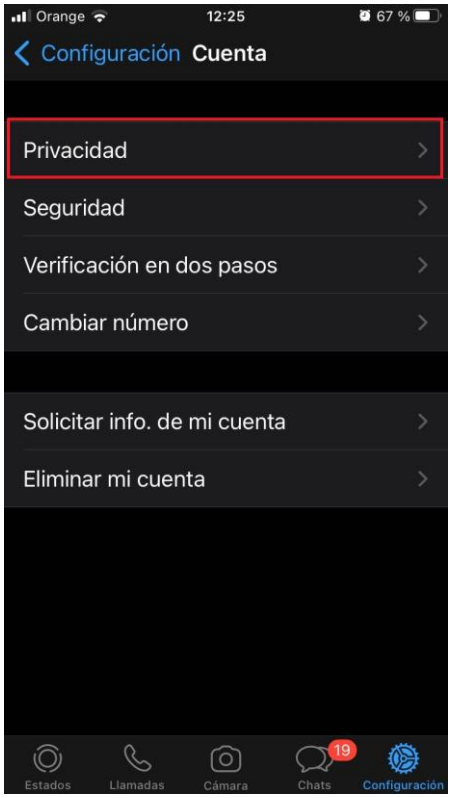

Figura 5.12: Segundo paso para inhabilitar la hora de nuestra última conexión. Fuente: elaboración propia.

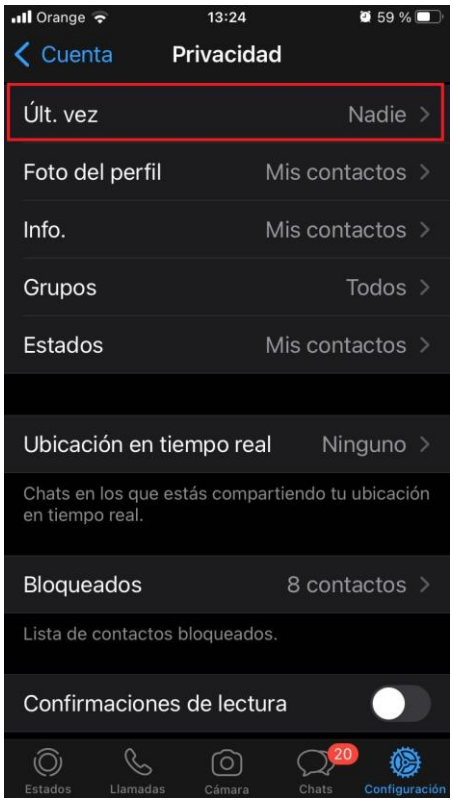

Figura 5.13: Tercer paso para inhabilitar la hora de nuestra última conexión. Fuente: elaboración propia.

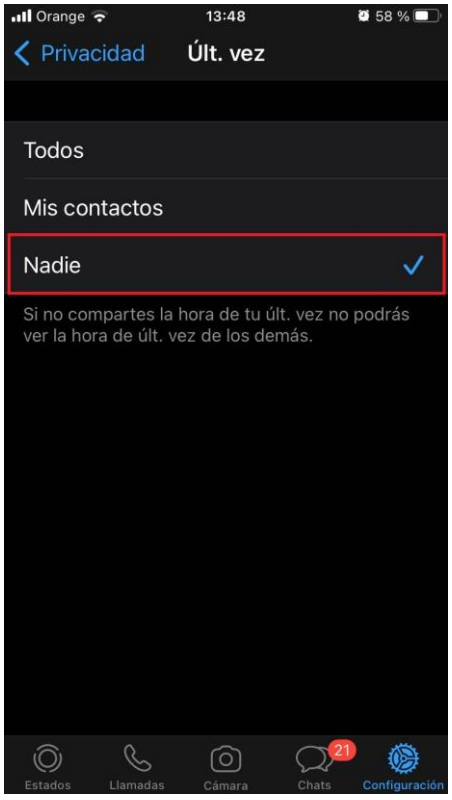

Figura 5.14: Cuarto paso para inhabilitar la hora de nuestra última conexión. Fuente: elaboración propia.

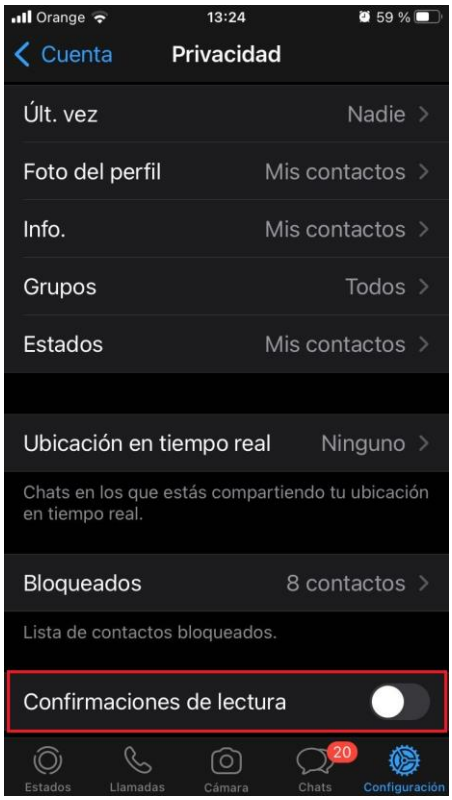

Figura 5.15: Inhabilitar la confirmación de lectura. Fuente: elaboración propia.

5.1.5. Compartir tu ubicación

En cuanto a la opción de compartir tu ubicación, recordamos que solo es recomendable hacerlo con tus contactos de confianza para que nadie conozca una información que tú deseas mantener en privado.

Tenemos dos opciones a la hora de compartir ubicación. Una en la cual la posición que mandamos es fija, es decir, si nos movemos no se ve reflejado en la ubicación que mandamos al chat.

De otra manera, podemos enviar nuestra ubicación en tiempo real, la cual se moverá en la ubicación que hayamos compartido en el chat y se sabrá en todo momento donde estamos por un periodo de máximo 24 horas.

Si utilizamos Google maps para compartir nuestra ubicación, debemos estar atentos ya que no para de compartirla hasta que nosotros entremos y lo paremos.

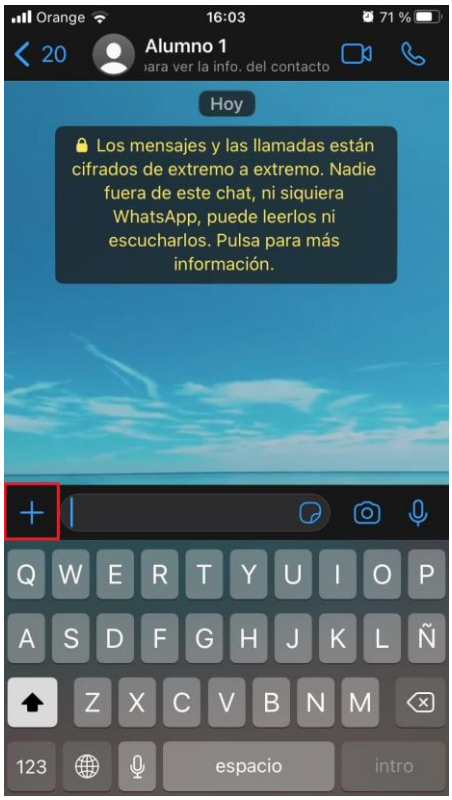

Figura 5.16: Primer paso para compartir ubicación con un usuario. Fuente: elaboración propia.

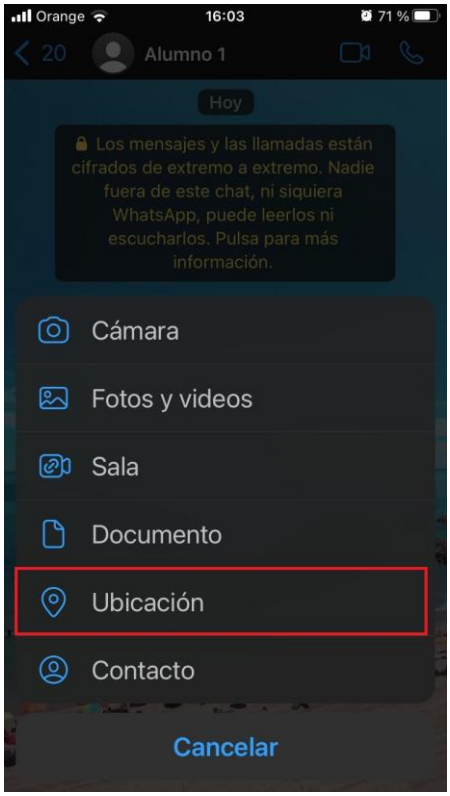

Figura 5.17: Segundo paso para compartir ubicación con un usuario. Fuente: elaboración propia.

Figura 5.18: Tercer paso para compartir ubicación con un usuario. Fuente: elaboración propia.

5.1.6. Grupos

Es bastante habitual que nuestros contactos nos añadan a grupos en WhatsApp. Se pueden definir quién puede meternos en grupos a través de la opción grupos, en los ajustes de privacidad.

Ahí podemos escoger entre todos, mis contactos e incluso podemos seleccionar los contactos específicos que podrán añadirnos en grupos.

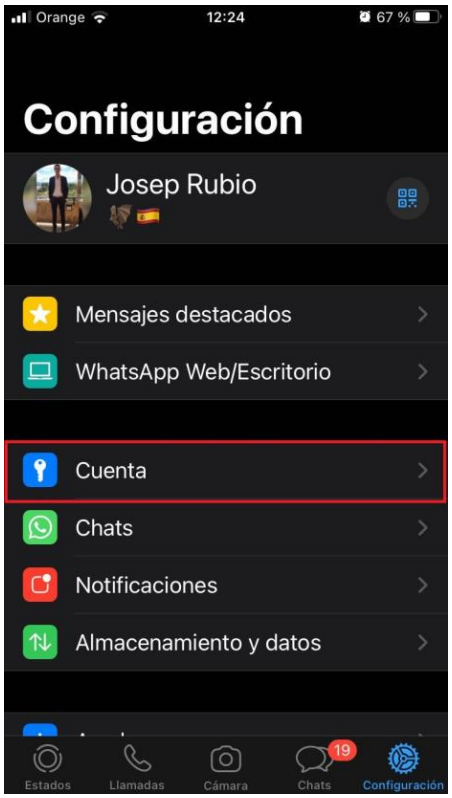

Figura 5.19: Primer paso para gestionar la herramienta de grupos. Fuente: elaboración propia.

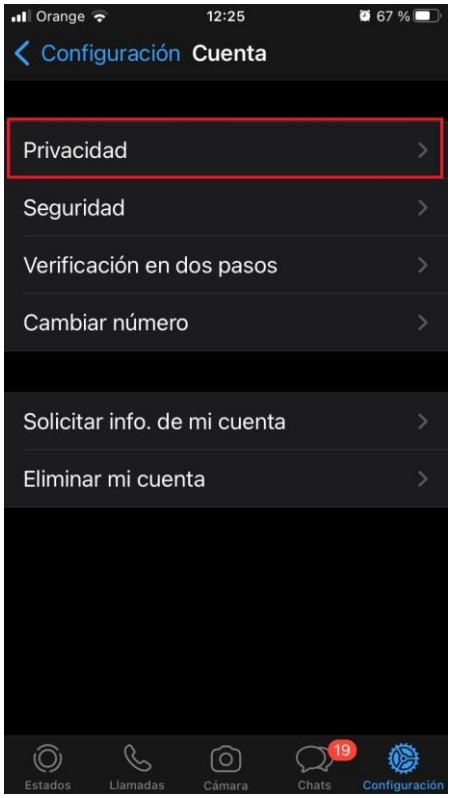

Figura 5.20: Segundo paso para gestionar la herramienta de grupos. Fuente: elaboración propia.

Figura 5.21: Tercer paso para gestionar la herramienta de grupos. Fuente: elaboración propia.

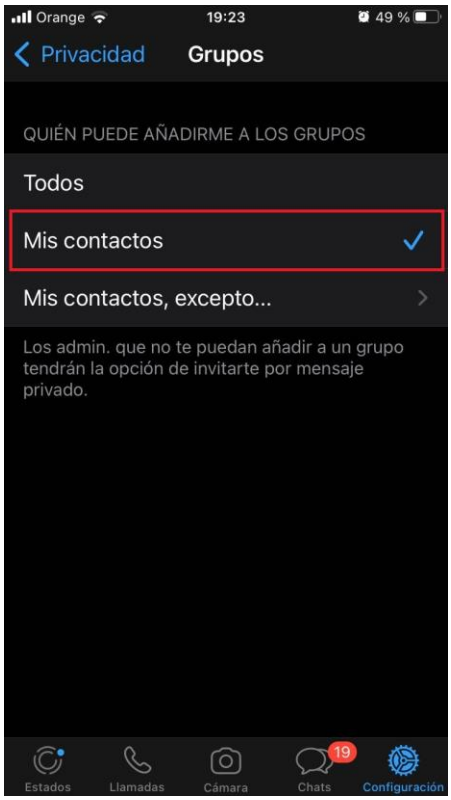

Figura 5.22: Cuarto paso para gestionar la herramienta de grupos. Fuente: elaboración propia.

5.1.7. Reportar un número desconocido o bloquear un número

En alguna ocasión podemos recibir un mensaje de alguien desconocido. Es posible que esto nos genere desconfianza por eso WhatsApp presta la opción de reportar este número directamente desde el chat, tocando el nombre del contacto y clicando sobre reportar contacto. Esta opción también se puede realizar en los grupos en los que haya contactos desconocidos.

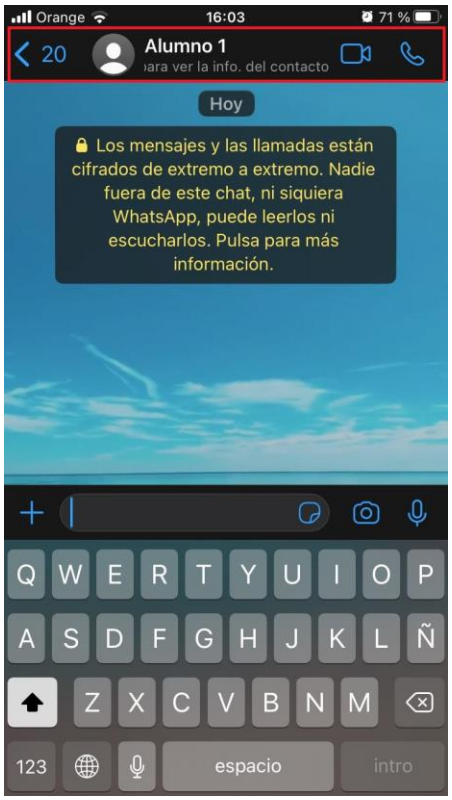

Figura 5.23: Primer paso para reportar un número desconocido. Fuente: elaboración propia.

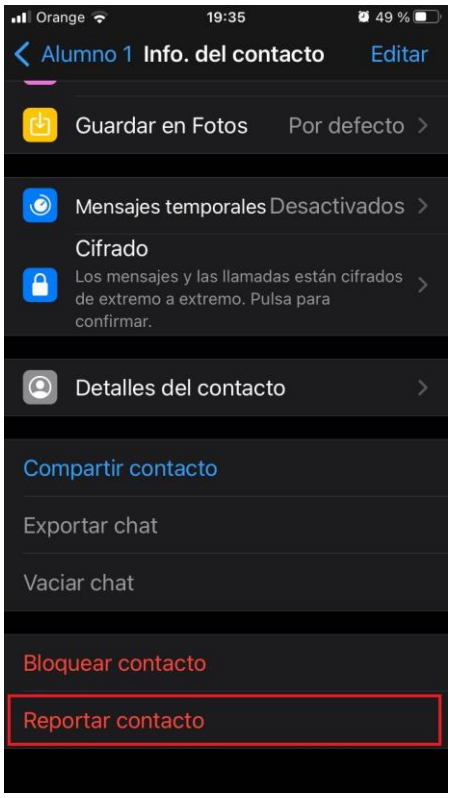

Figura 5.24: Segundo paso para reportar un número desconocido. Fuente: elaboración propia.

Si directamente queremos bloquear un contacto o un número desconocido la aplicación presenta varias maneras. Desde el propio menú de privacidad, entrando en contactos bloqueados y añadiendo el nuevo contacto bloqueado.

También podemos abrir el chat del contacto y pulsando su nombre elegiremos bloquear ese contacto. Activando esta opción no recibirás mensajes, llamadas o actualizaciones de estado de dicho contacto y a su vez éste no podrá ver tu información, cambio de estado, de foto del perfil o la última vez que has estado en línea.

Telegram funciona a través de usuarios, con lo que nuestro número de teléfono no se ve expuesto. Esta es una gran ventaja ya que nuestro número nos aseguramos de que no lo tenga personas que no queremos. También permite restringir las llamadas que puedas recibir a través de la aplicación. Esta función, WhatsApp aun no la ha sacado.

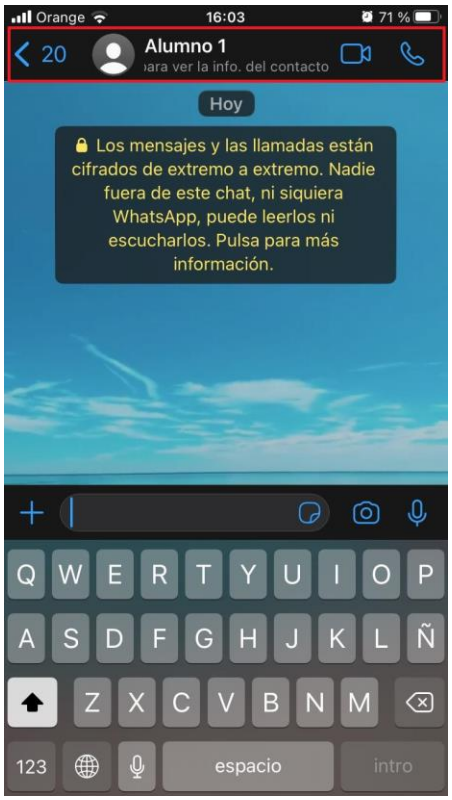

Figura 5.25: Primer paso para bloquear un número desconocido. Fuente: elaboración propia.

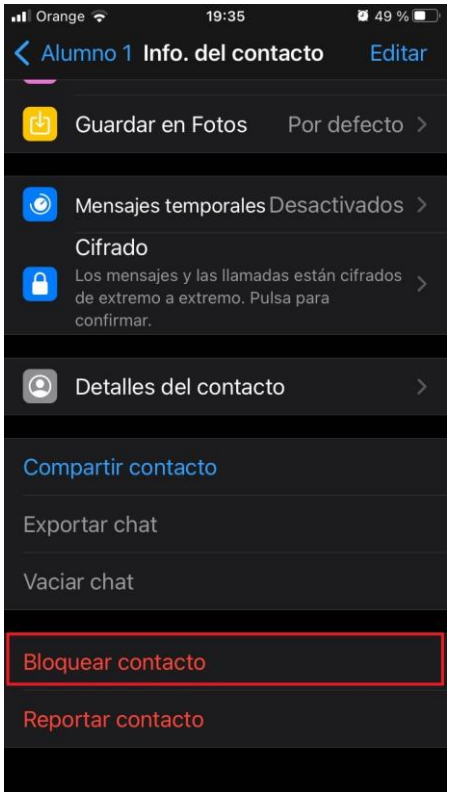

Figura 5.26: Segundo paso para bloquear un número desconocido. Fuente: elaboración propia.

5.1.8. Chats cifrados de extremo a extremo

WhatsApp presenta los chats cifrados de extremo a extremo, que tienen su propio código de seguridad y que protegen tanto las llamadas como los mensajes que se envíen en ese chat. Dicho código de seguridad se puede ver como en formato QR como código de 60 dígitos.

Para confirmar que dicho chat está protegido ábrelo, toca el nombre del contacto y después clica en cifrado para ver el código QR o el numérico. Al escanear el código QR aparecerá un tic verde que confirmará la seguridad del chat.

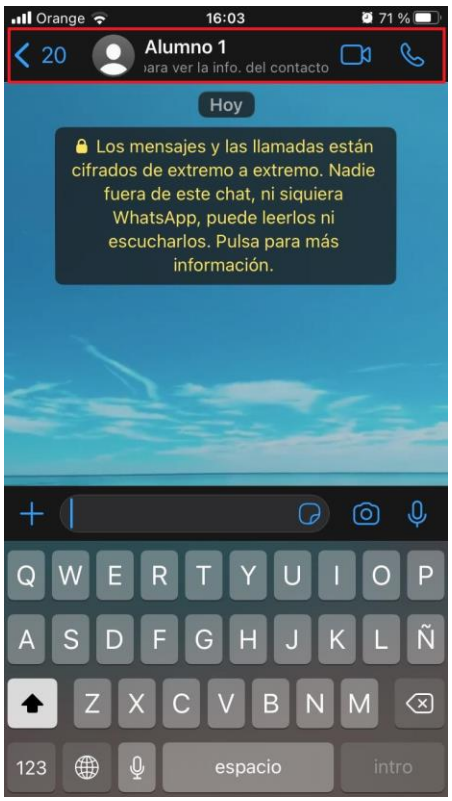

Figura 5.27: Primer paso para comprobar el cifrado. Fuente: elaboración propia.

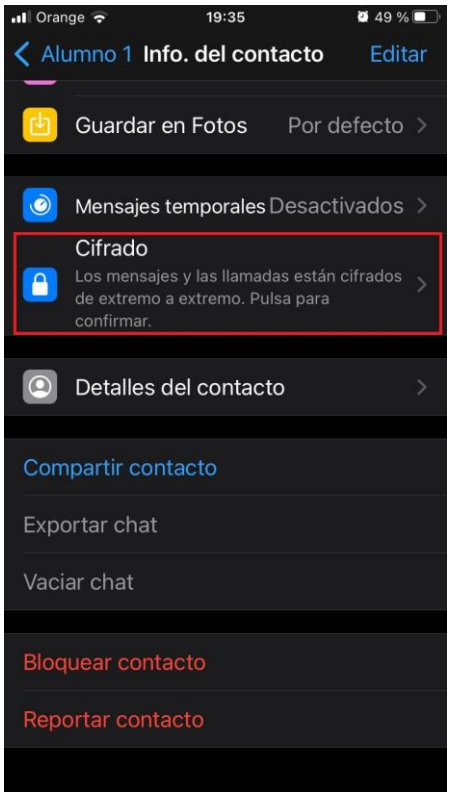

Figura 5.28: Segundo paso para comprobar el cifrado. Fuente: elaboración propia.

Figura 5.29: Tercero paso para comprobar el cifrado. Fuente: elaboración propia.

5.1.9. WhatsApp Web

Al utilizar el WhatsApp web, el usuario debe recordar siempre cerrar la sesión cuando haya terminado de usarlo. En el ordenador también puedes comprobar si te has dejado alguna sesión abierta.

Para comprobarlo desde el móvil, clicamos en WhatsApp web y vemos que sesiones tenemos abiertas. Para cerrar una sesión, clicamos sobre ella y pulsamos cerrar.

En esta comparativa con Telegram, WhatsApp sale ganando ya que, para iniciar sesión desde un ordenador, tenemos que escanear un código QR que nos muestra el móvil. Por lo contrario, si usamos Telegram, con el nombre de usuario y un código podemos establecer la conexión.

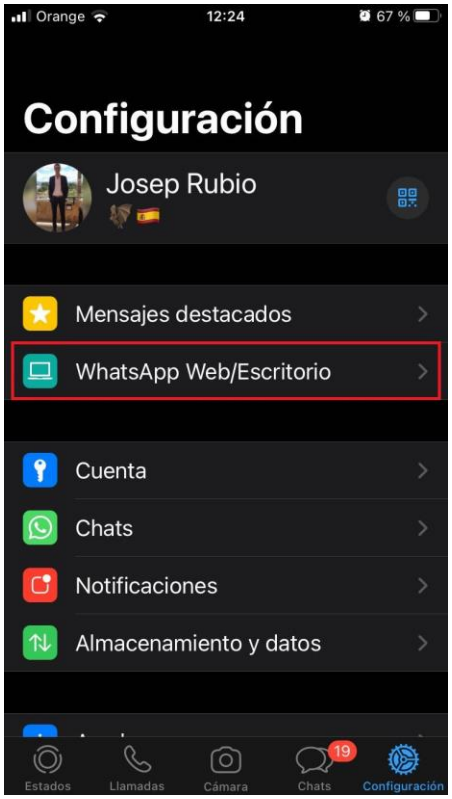

Figura 5.30: Primer paso para cerrar sesión. Fuente: elaboración propia.

Figura 5.31: Segundo paso para cerrar sesión. Fuente: elaboración propia.

Figura 5.32: Tercero paso para cerrar sesión. Fuente: elaboración propia.

5.1.10. Notificaciones

Si queremos evitar que cualquiera pueda leer nuestros mensajes en las notificaciones que aparecen en la pantalla del teléfono, entra en configuración, notificaciones, previsualización en iPhone para poder beneficiarte de toda la privacidad que necesites.

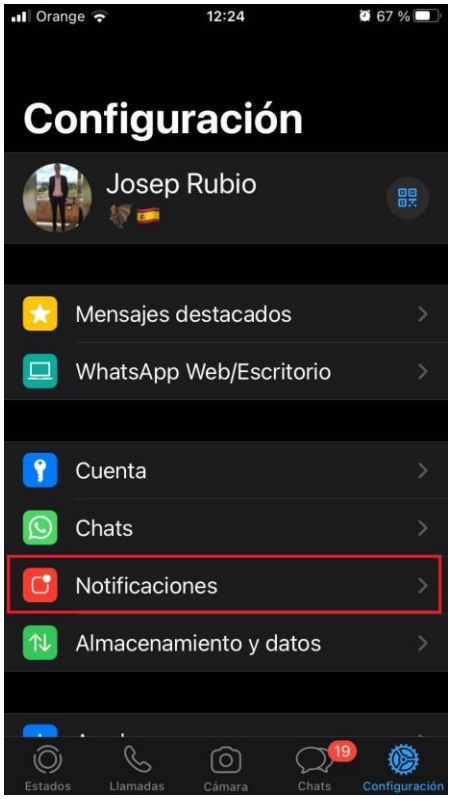

Figura 5.33: Primer paso para ocultar la visualización de las notificaciones. Fuente: elaboración propia.

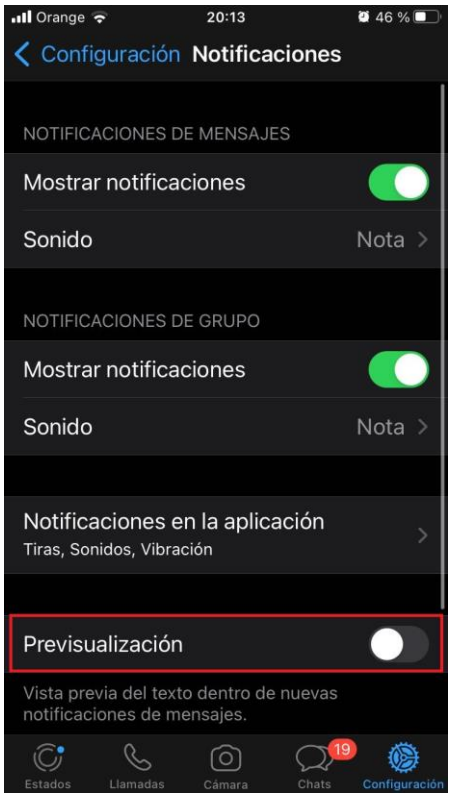

Figura 5.34: Segundo paso para ocultar la visualización de las notificaciones. Fuente: elaboración propia.

5.1.11. Eliminar mensajes ya enviados

WhatsApp nos brinda la posibilidad de eliminar mensajes enviados. Para ello tenemos que entrar en el chat con el mensaje que deseamos eliminar ya sea personal o de grupo.

Presionamos sobre el mensaje o sobre los mensajes, clicamos sobre eliminar y elegimos si los eliminamos solo para nosotros en eliminar para mí o para el resto de los usuarios en eliminar para todos.

En el caso de Telegram, antes de enviar los mensajes podemos elegir el tiempo que van a permanecer en el chat. De esta manera, una vez enviados y transcurrido el tiempo que hemos seleccionado, el mensaje se eliminará tanto para nosotros como para nuestro contacto que estamos manteniendo una conversación.

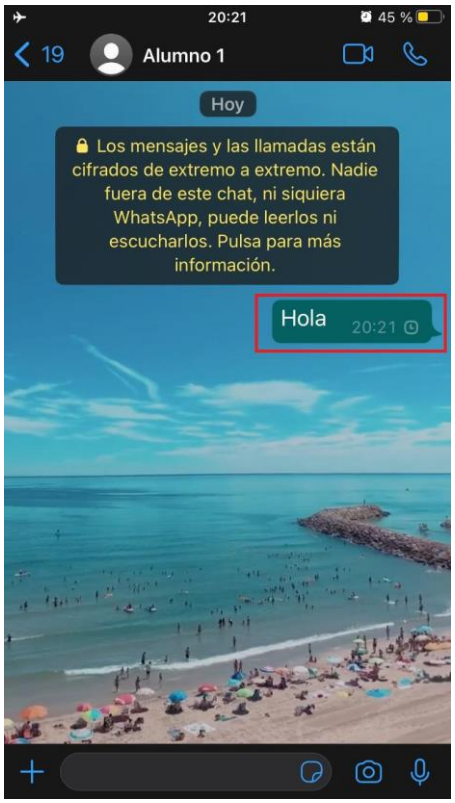

Figura 5.35: Primer paso para eliminar mensajes enviados. Fuente: elaboración propia.

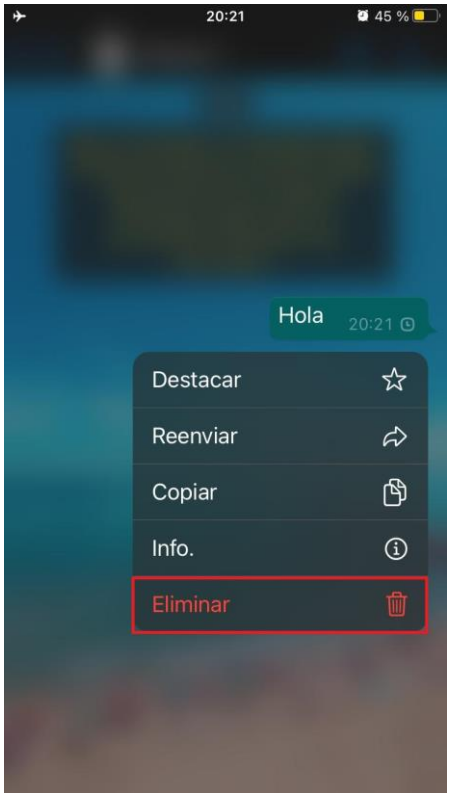

Figura 5.36: Segundo paso para eliminar mensajes enviados. Fuente: elaboración propia.

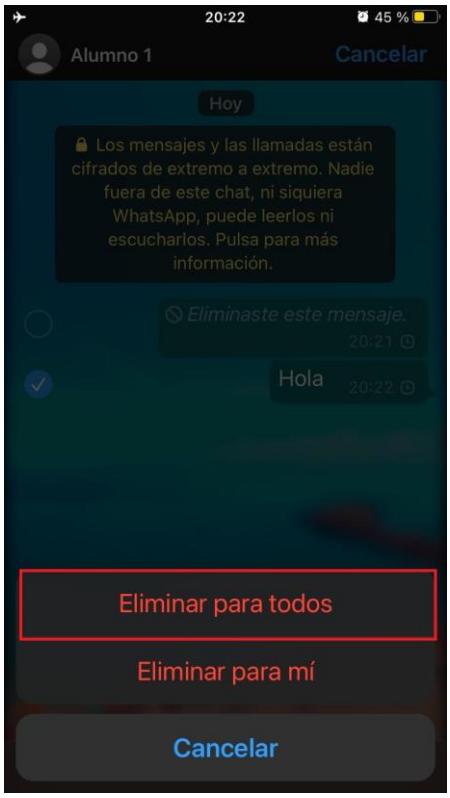

Figura 5.37: Tercer paso para eliminar mensajes enviados. Fuente: elaboración propia.

5.1.12. Contactar con los gestores de WhatsApp

WhatsApp pone a nuestra disposición la opción de contacto con sus gestores dentro de la aplicación, por si queremos reportar alguna acción o vulneración de la seguridad.

Solo tenemos que entrar en ajustes, ayuda y contáctanos y de esta manera podremos enviarles la información detallada para que puedan ayudarnos a resolver cualquier problema que tengamos.

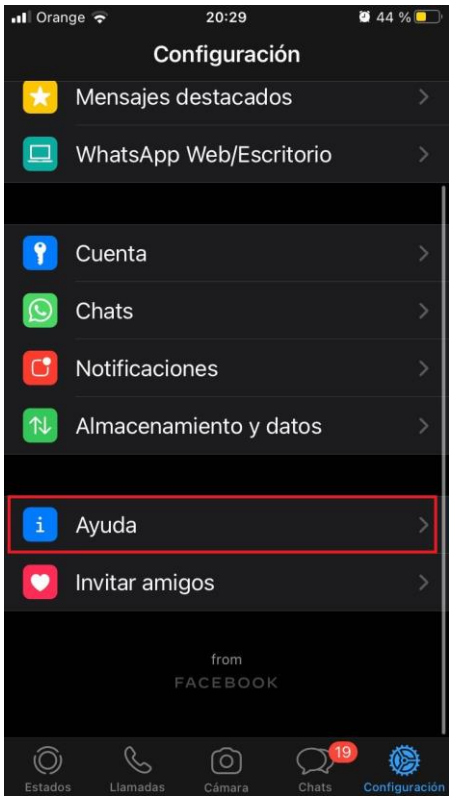

Figura 5.38: Primer paso para contactar con los gestores de WhatsApp. Fuente: elaboración propia.

Figura 5.39: Primer paso para contactar con los gestores de WhatsApp. Fuente: elaboración propia.

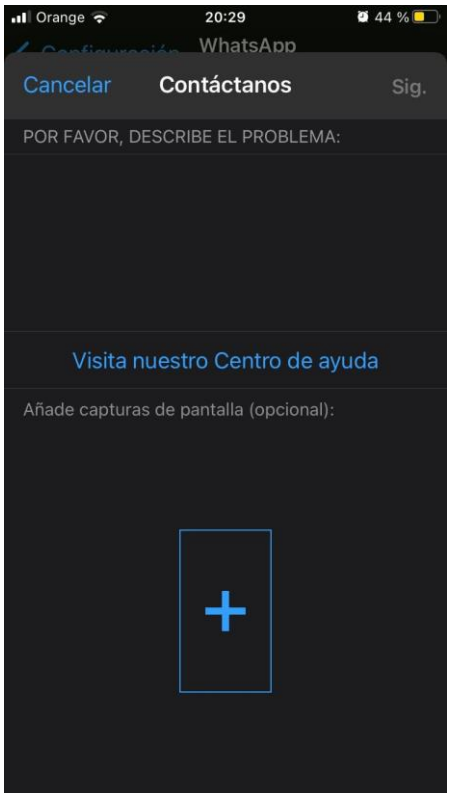

Figura 5.40: Primer paso para contactar con los gestores de WhatsApp. Fuente: elaboración propia.

6. Herramientas de las empresas para obtener nuestros datos personales en redes sociales

En este apartado trataremos de explicar cómo y de qué manera consiguen tener los permisos para recopilar nuestros datos con interminables políticas de privacidad que tenemos que aceptar, para de esta manera, poder interactuar con la aplicación que estemos usando.

Si no aceptamos la política de privacidad, no podemos usar la aplicación que queramos. De este punto trataremos a continuación, como una vez aceptada la política de privacidad la empresa está cubierta.

6.1. He leído y acepto…

Uno de los principales peligros de la privacidad de los datos de los usuarios radica en la forma en que interactúan con Internet. Porque las empresas que se comprometen a recopilar y procesar información personal de manera legal intentan mantener una buena ética y moral para no tratar esos datos y actuar dentro del marco regulatorio vigente, pero si esta persona no lee lo que acepta, correrá riesgo de que la empresa pase los datos a otras empresas con una finalidad muy diferente.

La mayoría de las políticas de privacidad de las redes sociales contienen más letras que la Constitución española. A este volumen de políticas, tenemos que añadir que Boris Johnson tenía intención de elaborar su propia ley sobre la protección de datos personales, algo que no convencía a la Unión Europea. Aun así, se ha llegado a un acuerdo y la Unión Europea declara que la protección de datos en el Reino Unido es equivalente a la que tenemos en la actualidad en suelo europeo. Lo que supone que la información puede circular libremente entre Reino Unido y la Unión Europea.

La decisión de adaptación que se toma hoy es una de conformidad con el Reglamento General de Protección de Datos y la otra en la Directiva de Protección de Datos en Materia Penal. Por primera vez, se incluye la denominada “cláusula de extinción” por si surgen futuros desacuerdos entre Bruselas y Londres.

La cláusula limita el plazo de vigencia de la resolución a un máximo de cuatro años, transcurridos los cuales la resolución solo podrá actualizarse si la comisión considera que Reino Unido sigue garantizando un nivel adecuado de protección de datos. Además, durante su mandato, Bruselas asegura la posibilidad de intervención en cualquier momento de acuerdo con el desarrollo de la legislación británica [31].

El problema actual es el desconocimiento. Las personas se registran en muchos sitios web, pero no saben lo que hacen, y algunas empresas recopilan y utilizan estos datos. Las personas están de acuerdo sin saberlo, y luego se sorprenderán si su información personal se comercializa, lo cual es legal el 90% de las veces.

Otro problema son los datos que los usuarios publican voluntariamente en Internet. Legalmente, de acuerdo con las políticas de cada red social, esta información pertenece a las plataformas que las publican, y solo puede ser utilizada con el consentimiento de estas plataformas y de los propios usuarios. Sin embargo, si alguien puede acceder a los datos, cualquiera puede usarlos, incluso si es ilegal.

Cuando permitimos que las aplicaciones móviles accedan a nuestras fotos o contactos telefónicos, ponemos en riesgo los datos del tercero sin notificarlo y sin su consentimiento. Incluso si etiquetamos a una persona en una

red social, también estamos promoviendo su identificación para que pueda ser identificada en todos los videos o fotos donde aparece, incluso si no usa la red social.

Los datos son cada vez más valiosos, por lo que las personas están cada vez más interesadas en recopilar la mayor cantidad de datos posible. Para ello se utilizan procedimientos y mecanismos ajenos a la ley y desconocidos para el usuario.

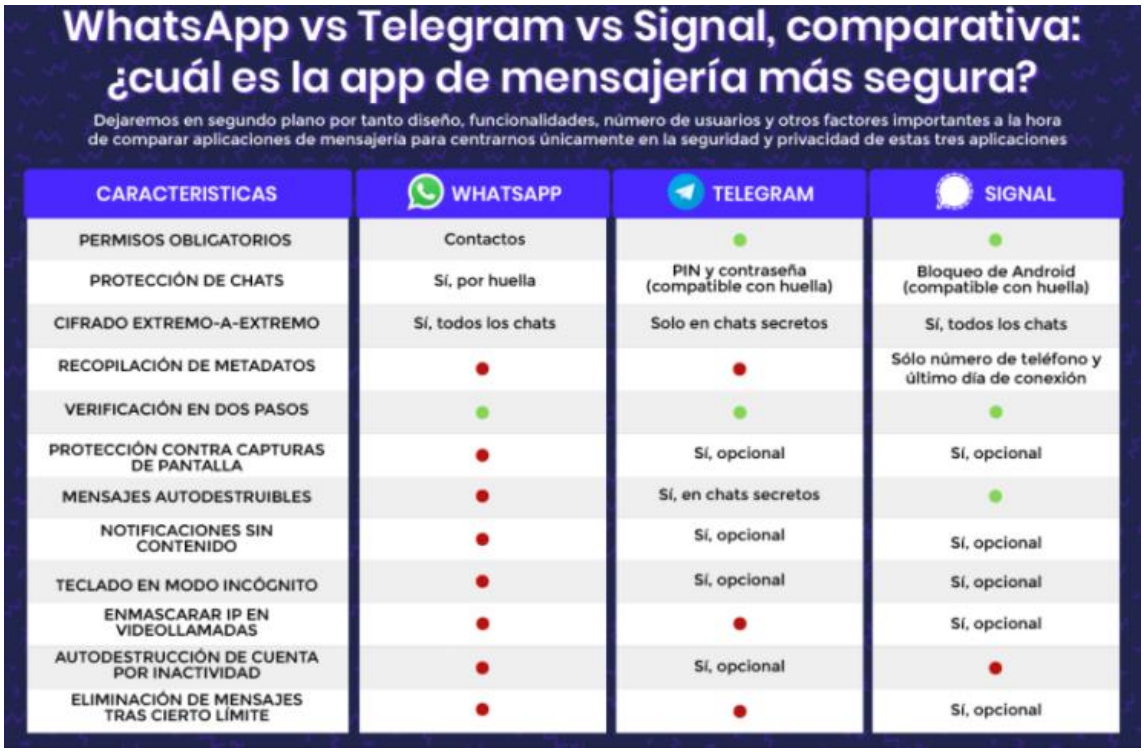

Figura 6.1: Comparativa de las principales aplicaciones de mensajería instantánea. Fuente: infografía.

7. Conclusiones

El origen de este proyecto surgió de la necesidad de aportar una guía al usuario medio para poder defenderse de internet y poder obtener un nivel de seguridad básico para mantener sus datos personales a salvo. Repasando todas las fugas de datos personales y como su valor ha ido creciendo a un ritmo vertiginoso que, sigue sin parar de ascender.

Durante la realización de este proyecto, hemos podido observar como las grandes empresas de las redes sociales, utilizan nuestros datos con fines

lucrativos. El usuario se queda indefenso ante la avalancha de paginas que tienen las políticas de privacidad, en las cuales aceptan sin leerse.

Es por esto, con este trabajo, queremos orientar y ofrecer una mínima seguridad al usuario medio. Poniendo en su conocimiento los antecedentes de los datos personales, las maniobras de las grandes empresas que trabajan con miles de datos y las asociaciones que intentan con menor o mayor acierto defender la privacidad del usuario medio.

Aunque, nuestra intención es que cualquiera que tenga dudas sobre su seguridad en la red, pueda echar mano de este trabajo y arrojar luz sobre las habilidades para proteger los datos.

A niveles personales, este proyecto ha supuesto un reto mayúsculo ya que había que realizar una guía para los usuarios medios, resaltando la importancia de tener una buena seguridad exponiendo los principales robos o filtraciones de datos personales y sus consecuencias. Este reto se ha conseguido y se tiene una guía bastante completa para empezar a tener competencias de seguridad, sabiendo los riesgos que existen en internet.

La perspectiva de futuro de este trabajo es poder realizar una guía de seguridad para cada red social, en la cual, a través de estas guías se mantenga los datos protegidos y no se publique un dato innecesario. Seguir en la formación de los usuarios a través de cursos, en los cuales se podrán ir aumentando progresivamente las habilidades para reforzar la seguridad y detectar si se es objetivo de bulos o intentos de robo. La intención siempre es brindar la máxima protección al usuario, pero debido al tiempo y recursos limitados no se ha podido llegar más lejos.

No obstante, se ánima a cualquiera que desee compartir sus recursos para realizar estos puntos anteriormente dichos y de esta manera que el usuario medio tenga siempre un documento que consultar en caso de duda o formación.

8. Bibliografía

[1] MARTÍNEZ, Álvaro, 2018. Las mayores fugas de datos de la historia. En: *Abc* [en línea]. Disponible en: https://www.abc.es/tecnologia/redes/abci-mayores-fugas-datos-historia-201812120256_noticia.html?ref=https:%2F%2Fwww.google.com%2F [consulta: 12 diciembre 2020].

[2] SÁNCHEZ, Jose María, 2017. El robo de datos, la puntilla que le faltaba a Yahoo. En: *Abc* [en línea]. Disponible en: https://www.abc.es/tecnologia/redes/abci-robo-datos-puntilla-faltaba-yahoo-201609260232_noticia.html#ns_campaign=mod-

sugeridos&ns_mchannel=relacionados&ns_source=el-robo-de-datos-la-puntilla-que-le-faltaba-a-la-debil-yahoo&ns_linkname=noticia.video.tecnologia&ns_fee=pos-2 [consulta: 12 diciembre 2020].

[3] VARGAS, Connie, 2019. Tendencias en seguridad informática para el 2019. En: *Trycore* [en línea]. Disponible en: https://trycore.co/tendencias-tecnologicas/tendencias-seguridad-informatica-2019/ [consulta: 15 diciembre 2020].

[4] Ataques comunes en redes sociales y cómo. En *Testdevelocidad* [en línea]. Disponible en: https://www.testdevelocidad.es/2020/07/21/ataques-comunes-redes-sociales-consejos/#:~:text=Phishing%20por%20redes%20sociales,pasar%20por%20una%20organizaci%C3%B3n%20leg%C3%ADtima. [consulta: 16 diciembre 2020].

[5] Constitución española (BOE núm. 311, de 29 de diciembre de 1978). Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con [consulta: 28 diciembre 2020].

[6] Derogada. Unión Europea, Directiva (UE) 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea L 281, de 23 de noviembre de 1995, pp. 0031 – 0050. Disponible en: http://data.europa.eu/eli/dir/1995/46/oj [consulta: 30 diciembre 2020].

[7] Derogada. España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 14 de diciembre de 1999, núm. 298, pp. 43088 – 43099. Disponible en: https://www.boe.es/eli/es/lo/1999/12/13/15/con [consulta: 5 enero 2021].

[8] España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de datos de carácter personal. Boletín Oficial del Estado, 19 de enero de 2008, núm. 17, pp. 4103 – 4136. Disponible en: https://www.boe.es/eli/es/rd/2007/12/21/1720/con [consulta: 7 enero 2021].

[9] Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016, pp. 1 – 88. Disponible en: http://data.europa.eu/eli/reg/2016/679/oj [consulta: 8 enero 2021].

[10] España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018, núm. 294, pp. 119788 – 119857. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3 [consulta: 10 enero 2021].

[11] Agencia Española de Protección de Datos. Disponible en: https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/funcion-y-poderes [consulta: 14 enero 2021].

[12] Six Degrees: cómo fue y quien creó la primera red social de internet, inspirada por la teoría de los «seis grados». En: *bbc* [consulta: 14 enero 2021]. Disponible en: https://www.bbc.com/mundo/noticias-48558989#:~:text=La%20red%20social%20SixDegrees%20original,a%20p%C3%A1ginas%20web%20de%20an%C3%A1lisis.

[13] Las redes sociales que quisieron frustrar a Facebook. En: *expansión* [consulta: 15 enero 2021]. Disponible en: https://expansion.mx/tecnologia/2019/08/22/las-redes-sociales-que-quisieron-frustrar-a-facebook#:~:text=Friendster%20(2002%2D2015)&text=Un%20grupo%20de%20capitalistas%20de,p%C3%A1ginas%20simplemente%20no%20se%20cargaron.

[14] Estadísticas de redes sociales 2021: Usuarios de Facebook, Instagram, Youtube, LinkedIn, Twitter, Tik-Tok y otros. En: *juancmejia* [consulta: 18 enero 2021]. Disponible en: https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/

[15] Analizando el perfil de los usuarios de Youtube. En: *reasonwhy* [consulta: 20 enero 2021]. Disponible en: https://www.reasonwhy.es/actualidad/estudio-usuarios-youtube-webedia-2019

[16] CUADRADO, Natalia, 2019. Este es el perfil del tuitero español. En: *cronicaglobal* [en línea]. Disponible en: https://cronicaglobal.elespanol.com/vida/perfil-tuitero-espanol-usuarios-twitter_228696_102.html [consulta: 25 enero 2021].

[17] Estadísticas de Tik-Tok. En: *cocktailmarketing* [en línea]. [consulta: 25 enero 2021]. Disponible en: https://cocktailmarketing.com.mx/estadisticas-de-tiktok/

[18] FERNÁNDEZ, Carlos, 2016. La AEPD publica una guía para facilitar los procedimientos de anonimización de datos personales. En: *noticiasjuridicas* [en línea]. Disponible en: https://noticias.juridicas.com/actualidad/noticias/11421-la-aepd-publicado-una-guia-para-facilitar-los-procedimientos-de-anonimizacion-de-datos-personales/ [consulta: 20 febrero 2021]

[19] OLLERO, Daniel, 2018. Facebook sufre el primer gran hackeo de su historia y deja expuestas más de 50 millones de cuentas. En: *elmundo* [en línea]. Disponible en: https://www.elmundo.es/tecnologia/2018/09/29/5bae76a9e2704e25778b45d9.html [consulta: 23 febrero 2021]

[20] Apple detecta un fallo de seguridad que afecta a todos sus dispositivos. En *lavozdegalicia* [en línea]. Disponible en: https://www.lavozdegalicia.es/noticia/tecnologia/2014/02/25/apple-detecta-fallo-seguridad-afecta-dispositivos/00031393317438883100137.htm [consulta: 1 marzo 2021].

[21] La crisis de Marriott reafirma el problema de ciberseguridad de los hoteles. En *tecnohotelnews* [en línea]. Disponible en: https://tecnohotelnews.com/2018/12/04/marriott-hoteles-ciberseguridad/ [consulta: 2 marzo 2021].

[22] Hackers roban los datos de 40 millones de tarjetas de crédito. En *cnnespañol* [en línea]. Disponible en: https://cnnespanol.cnn.com/2013/12/22/hackers-roban-los-datos-de-40-millones-de-tarjetas-de-credito/ [consulta: 4 marzo 2021].

[23] PEÑA, Milenka, 2018. Hackers roban datos de 5 millones de tarjetas de crédito de tiendas de lujo. En *digitaltrends* [en línea]. Disponible en: https://es.digitaltrends.com/negocios/hackers-roban-tarjetas-tiendas-lujo/ [consulta: 5 marzo 2021].

[24] Hackers roban datos de 4,5 millones de usuarios de la salud en USA. En *hn* [en línea]. Disponible en: https://www.hn.cl/blog/hackers-roban-datos-de-4-5-millones-de-usuarios-de-la-salud-en-usa/ [consulta: 6 marzo 2021].

[25] G. PASCUAL, Manuel, 2021. Sabotajes, espías y robos de datos: la guerra invisible por la vacuna de la covid que se libra en el ciberespacio. En *elpais* [en línea]. Disponible en: https://elpais.com/tecnologia/2021-03-23/sabotajes-espias-y-robo-de-datos-la-guerra-invisible-por-la-vacuna-de-la-covid-que-se-libra-en-el-ciberespacio.html [consulta: 6 marzo 2021].

[26] SEBASTIÁN, Nieves, 2020. Rusia anuncia el registro de la primera vacuna contra la covid-19. En *gacetamedica* [en línea]. Disponible en: https://gacetamedica.com/investigacion/rusia-anuncia-el-registro-de-la-primera-vacuna-contra-la-covid-19/ [consulta: 6 marzo 2021].

[27] EE. UU. acusa a 9 iraníes y a una entidad de un gigantesco robo de datos académicos. En *publico* [en línea]. Disponible en: https://www.publico.es/internacional/eeuu-acusa-9-iranies-y-entidad-gigantesco-robo-datos-academicos.html [consulta: 8 marzo 2021].

[28] POZZI, Sandro, 2019. Facebook pagará en EE. UU. una multa de 5.000 millones y deberá mejorar sus sistemas de protección. En *elpais* [en línea]. Disponible en: https://elpais.com/economia/2019/07/24/actualidad/1563983967_275285.html [consulta: 10 marzo 2021].

[29] MILLÁN, Víctor, 2021. Si tenías una cuenta de Facebook en 2019, tienes n 50% de posibilidades de que tus datos se hayan filtrado. En *hipertextual* [en línea]. Disponible en: https://hipertextual.com/2021/04/facebook-privacidad-datos-filtraciones [consulta: 10 marzo 2021].

[30] RODRÍGUEZ, Pablo, 2020. Hay empresas que tiene extensos informes con tus datos personales recopilados en Internet y los venden por más de cien euros. En *xataka* [en línea]. Disponible en: https://www.xataka.com/privacidad/hay-empresas-que-tiene-extensos-informes-tus-datos-personales-recopilados-internet-venden-cien-euros [consulta: 15 marzo 2021].

[31] Bruselas declara equivalente la protección de datos en UE y Reino Unido. En *swissinfo* [en línea]. Disponible en: https://www.swissinfo.ch/spa/ue-r--unido_bruselas-declara-equivalente-la-protecci%C3%B3n-de-datos-en-ue-y-reino-unido/46742636 [consulta: 20 marzo 2021].