A. Riesgos

Las principales redes sociales (Facebook, Twitter, TikTok, Snapchat, Instagram, LinkedIn, etc.) le permiten registrarse en sus servicios de forma gratuita para intercambiar mensajes y archivos multimedia con amigos o contactos. A cambio, estas redes recopilan su información y sus datos personales, y los revenden. Nuestra privacidad y datos personales son el combustible de estas empresas. Permiten crear perfiles publicitarios extremadamente precisos.

Una red social como Facebook permite que sus clientes le conozcan a usted en profundidad. No subestime sus capacidades técnicas. Algunos investigadores han demostrado que una red como Facebook es capaz de entender casi a la perfección la personalidad y los rasgos psicológicos de sus usuarios a partir de unos pocos *likes*[1], información «usable» con fines comerciales y políticos. Hoy, esta información puede resultar inofensiva en su caso, pero mañana, en otras circunstancias, podría ser legítimo cuestionarse sobre el uso que se hace de estos datos personales e íntimos.

Entre las muchas técnicas de *tracking* (a las que volveremos en un capítulo próximo), las redes sociales pueden, por ejemplo, depositar un píxel de seguimiento en su navegador. Este píxel es una imagen invisible, integrada en un correo electrónico o una página web, que seguirá su navegación fuera de la red social para permitir al comerciante recopilar información sobre usted, con objeto de tomarle como objetivo y comprender mejor su comportamiento[2].

Pero las redes sociales tienen muchas otras formas de seguirle durante toda su navegación. También le rastrean cuando usa un servicio de autenticación única (SSO) ofrecido por la red social en otro sitio. Volveremos a esto más específicamente en el capítulo Seguridad en los pagos, contraseñas, autenticación de dos factores (A2F). Nos referimos a las opciones de inicio de sesión disponibles ahora en muchos sitios a partir del formulario **Iniciar sesión con Google, Apple o Facebook**. Su interés radica en iniciar sesión con la misma cuenta en todos sus sitios. Las redes sociales aún pueden rastrearle a través de los botones *Me gusta* o *Compartir* que se muestran en los sitios. Simplemente, examinan sus hábitos e intereses en su plataforma.

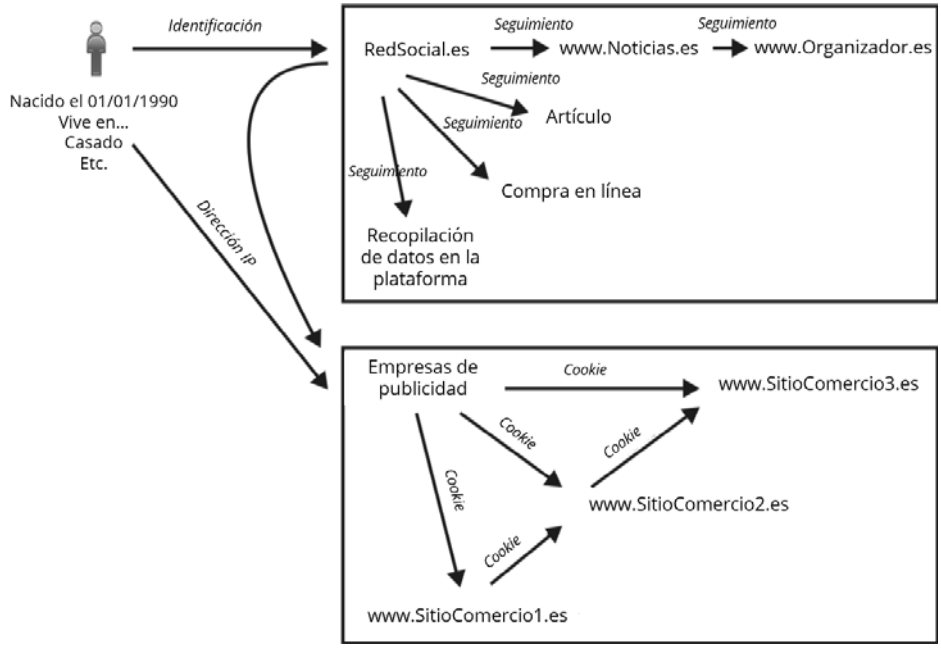
Algunas cifras permiten comprender la magnitud del enorme interés económico en este campo para las *Big Tech*. En lo que respecta a Google, el 81 %[3] de su cifra de negocio en 2021 provino de los ingresos publicitarios; en el caso de Facebook, fue superior al 97 %[4] en 2022.

Y si no está registrado en estas redes, no crea que está a salvo; puede que tenga un perfil fantasma. Facebook ha reconocido que, aunque una persona no esté registrada en su red social, podría tener un perfil fantasma a través de información recopilada por personas cercanas que pueden dar acceso a la red social a sus contactos[5].

La historia reciente de estas redes ha demostrado que tienen poco respeto por los datos de sus usuarios. Incluso podemos cuestionar la gestión interna de nuestros datos por parte de estas empresas, ya que, no hace mucho, varios empleados de compañías como Google, Amazon y Snapchat fueron condenados por la explotación de datos personales de los usuarios[6-8]. Estos empleados pudieron acceder a los datos de los usuarios aparentemente sin demasiada dificultad.

Nunca comparta su número de teléfono con una red social. Si una red social solicita su número de teléfono como parte de la autenticación de dos factores, tenga en cuenta que es preferible utilizar una técnica alternativa de doble autenticación (consulte el capítulo Seguridad en los pagos, contraseñas, autenticación de dos factores (A2F)). Evite dar su número de teléfono, ya que la red social puede usarlo para publicidad dirigida. Del mismo modo, no acepte compartir sus contactos con una aplicación de red social, ya que luego podría enviar publicidad dirigida utilizando sus contactos[9,10].

Facebook y Twitter, por ejemplo, han usado los números de teléfono de sus usuarios, recopilados en el marco de la activación de la autenticación de dos factores, para realizar publicidad dirigida. De esta manera, incluso aunque nunca haya proporcionado su número a una de estas plataformas, es posible que puedan conocerle a usted porque uno de sus contactos haya transmitido su número de teléfono y contactos, incluido el suyo, a la red social.



En el caso presentado, Máximo está mezclando las esferas personal y profesional. La red social le propone a sus compañeros como potenciales contactos porque ha creado su perfil personal con su dirección de correo electrónico del trabajo o porque ha indicado el nombre de su empresa. Además, da información en tiempo real sobre su vida. Esta información puede ser fácilmente explotada por piratas informáticos que buscan llegar a Máximo o su empresa. Para lograrlo, deben conocer su vida, sus hábitos y sus datos de contacto profesional. Máximo les está facilitando enormemente la tarea.

Pregúntese: ¿es necesario que todos sus contactos tengan acceso a cierta información que le concierne? ¿Es necesario que su colega, jefe o secretaria tenga acceso a sus fotos familiares o de ocio?

El hecho de mostrar a personas o elementos de su vida puede revelar mucha información sobre sus hábitos, lo que piensa, lee, mira... en definitiva, quién es usted. Hoy puede que no sea un problema, pero ¿quién sabe mañana? ¿Ha publicado una foto de su fantástica casa? Un reclutador podría considerar que probablemente sea usted demasiado ambicioso en cuanto a expectativas salariales. Si en el comentario de una publicación confiesa en tono de la broma que no habla bien inglés, un reclutador podría quedarse con esta información, que va en contra de usted.

El Estado también muestra interés en nuestros datos. La administración tributaria, por ejemplo, practica la minería de datos para encontrar correlaciones entre varias piezas de información. Por decirlo claramente, las autoridades fiscales pueden recopilar y utilizar los datos personales que usted ha publicado abiertamente en las redes sociales y otros sitios clasificados para detectar posibles fraudes. En Francia, por ejemplo, las autoridades fiscales están trabajando con Google y Capgemini para detectar «elementos con implicaciones fiscales», es decir: piscinas, pérgolas, cobertizos de jardín, extensiones que no han sido declaradas[11].

Desde el punto de vista de la seguridad, las redes sociales son una gran oportunidad para individuos o grupos que buscan hacerle daño. Esto se denomina *doxing* o *doxxing*, es decir, divulgación de datos personales con la intención de perjudicar. Es una amenaza cada vez más popular que está proliferando principalmente gracias a las redes sociales. También es importante llamar la atención sobre el desarrollo de técnicas OSINT (*Open Source Intelligence*) o ROSO (*Open Source Intelligence*). Este concepto agrupa un conjunto de técnicas y herramientas que tienen como objetivo encontrar la mayor cantidad de datos sobre una persona, una organización o un hecho a través de datos «abiertos», accesibles a todo el mundo, de forma legal y utilizando técnicas y herramientas relativamente accesibles. Si bien la disciplina del OSINT no es de por sí maliciosa, puede permitir que los posibles atacantes o acosadores se dirijan de manera más efectiva a su víctima. He aquí una razón más para controlar mejor nuestros rastros digitales.

Desde el punto de vista de su seguridad, la información publicada en las redes sociales es una fuente de datos importante y estratégica para un potencial atacante. Si muestra fotos de sus vacaciones, significa que no está en casa. Le pueden robar. La policía recomienda no proporcionar detalles en las redes sociales sobre sus vacaciones[12], incluidas las fechas de partida y regreso. Esta información podría utilizarse en su contra. ¿Ha publicado una foto de su última y magnífica compra? ¿Y si un ladrón lo ha visto y decide robársela? Del mismo modo, en el ámbito de la empresa, una foto tomada en las oficinas puede revelar muchos detalles sobre su entorno de trabajo, proyectos actuales, una contraseña escrita en un post-it, etc.

Por último, las redes sociales tienen un impacto psicológico real en los usuarios, especialmente en los más jóvenes[13], y sobre todo en los adolescentes: relación con el cuerpo, acoso, depresión, privación de sueño, etc. En este ámbito, los problemas que plantean estas redes son numerosos, como demuestran la denunciante Frances Haugen[14] y los últimos estudios[15].

1. Noticias y ejemplos

- *En la primera mitad de 2021, Facebook sufrió dos ataques masivos con violación de datos*[16].
- *En agosto de 2021, las autoridades surcoreanas multaron a Facebook con casi 4,7 millones de euros por recopilar datos de reconocimiento facial de 200 000 usuarios sin su consentimiento*[17].
- *El programa de mensajería de Facebook, Messenger, finalmente ha implementado el cifrado de extremo a extremo de los mensajes de audio y vídeo*[18]*, pero es una opción que debe activarse.*
- *En junio de 2021, la red social TikTok introdujo la recopilación de datos biométricos (impresiones faciales y de voz) de sus usuarios*[19].
- *Gracias a la explotación de los datos abiertos, se ha podido rastrear el jet del famoso CEO de Tesla, Elon Musk. Cada vez que su avión entraba en un aeropuerto, se creaban datos abiertos yaccesibles. Un usuario de Twitter lo aprovechó para crear una cuenta en la que seguía losmovimientos del famoso CEO, Algo que molestó a Musk. Sin embargo, esto es legal: ¡los datos recopilados son públicos! Debemos ser conscientes de que las cuentas de redes sociales también producen datos procesables que son accesibles para cualquier persona con habilidades básicas*[20].

B. Consejos

1. Para todos

- Sea discreto con su información personal. Elija apodos, fotos no relacionadas con su identidad real, una fecha de nacimiento falsa, intereses falsos, etc.
- En Internet, facilite su número de teléfono lo menos posible. Si no lo ve claro, pero necesita proporcionarlo para continuar su proceso en línea, use un número temporal.
- Utilice un correo electrónico específico o un alias para sus redes sociales.
- Configure la privacidad de cada red social (puede consultar los talleres prácticos al final de este libro).
- Deniegue el acceso a sus contactos. Haga que sus contactos sean visibles solo para usted. Su lista de contactos es una fuente importante de información. Dependiendo de su red de relaciones, se puede deducir mucha información sobre usted.
- Limite el uso de los chats (conversaciones instantáneas) en las redes sociales, elimine regularmente el historial de sus hilos.
- Al igual que con los correos electrónicos, se recomienda utilizar múltiples perfiles, dependiendo de su uso personal o comercial.
- Preste atención a la activación de la opción de reconocimiento facial[21], ya que puede ser extremadamente intrusiva[22]. Evite publicar una foto de perfil.
- Dependiendo de la red social, puede dar a sus contactos más o menos visibilidad en sus publicaciones. Organice sus contactos según la proximidad personal.
- Utilice las redes sociales en un navegador separado, dedicado a este propósito, no relacionado con sus compras en línea ni otros hábitos de navegación.
- Las aplicaciones oficiales de redes sociales son muy permisivas: permiten que la red social acceda a sus datos, como su ubicación precisa, su calendario, contactos, cámara, etc. Para evitarlo, configure los permisos que otorga a cada una de ellas.
- Las aplicaciones de redes sociales requieren muchas autorizaciones. Estas aplicaciones pueden ser muy intrusivas, especialmente si las deja conectadas en segundo plano. Después de cada uso, desconéctelas para que dejen de ejecutarse en segundo plano.

- Prefiera consultar sus redes sociales a través del navegador; así las aislará del resto de su teléfono inteligente. O bien instale un *front-end*, es decir, una aplicación desarrollada independientemente que le permita consultar sus redes sociales sin otorgarles todos los permisos. Estas aplicaciones a menudo ofrecen ventajas considerables en comparación con las aplicaciones oficiales (sin publicidad, uso ilimitado, interfaz más ergonómica, opciones adicionales, etc.). Sin embargo, tenga en cuenta que estas soluciones pueden evolucionar o incluso desaparecer dependiendo de las comunidades que las gestionen o de los límites impuestos a estos mismos desarrolladores.

Invidious[23], Newpipe[24], Skytube[25], YouTube Vanced[26] (YouTube), Fritter[27], Nitter[28] (Twitter), Frost[29] (Facebook) etc.

- La Fundación Mozilla ha desarrollado dos interesantes extensiones para aislar sus actividades dentro del mismo navegador Firefox y evitar, así, que todas sus actividades sean rastreadas durante su navegación.

Facebook Container[30] para aislar la actividad de Facebook del resto de su navegación y Firefox Multi-Account Containers[31] para aislar todas sus actividades entre sí.

2. Para usuarios avanzados

- Existen redes sociales descentralizadas que respetan los datos de los usuarios; una de las más conocidas es Mastodon, una red social descentralizada y de código abierto que se asemeja a Twitter.

Mastodon[32], Diaspora[33], Mobilizon[34] (organización de eventos y gestión de grupos), etc.

- Elimine su historial de redes sociales regularmente (consulte el capítulo sobre el taller de Facebook).
- En lugar de utilizar la mensajería de las redes sociales, elija su aplicación de mensajería instantánea diaria (consulte el capítulo Mensajería instantánea y metadatos).

C. Referencias

[1] https://www.presentacionespublicas.com/los-me-gusta-en-facebook-y-los-rasgos-de-personalidad/

[2] https://www.inboundcycle.com/blog-de-inbound-marketing/facebook-pixel-que-es-como-configurar

[3] https://www.puromarketing.com/14/34808/hay-vacas-flacas-google-publicidad-ingresos-anuncios-alcanza-resultados-record

[4] https://es.statista.com/estadisticas/525573/facebook-ingresos-mundiales-trimestrales-por-segmento/

[5] https://www.latercera.com/mouse/facebook-perfiles-fantasma/

[6] https://www.genbeta.com/seguridad/google-ha-despedido-a-80-empleados-tres-anos-hacer-uso-indebido-datos-clientes-usuarios-motherboard

[7] https://www.20minutos.es/tecnologia/ciberseguridad/trabajadores-de-amazon-pudieron-tener-acceso-a-datos-personales-de-clientes-del-ecommerce-entre-2015-y-2018-4899407/

[8] https://www.europapress.es/portaltic/ciberseguridad/noticia-empleados-snapchat-utilizaban-herramienta-interna-podian-espiar-usuarios-motherboard-20190524160458.html

[9] https://www.eff.org/deeplinks/2018/09/you-gave-facebook-your-number-security-they-used-it-ads

[10] https://www.eff.org/deeplinks/2019/10/twitter-uninentionally-uses-your-2fa-number-targeted-advertising

[11] https://www.genbeta.com/actualidad/esta-ia-google-ayuda-a-recaudar-impuestos-detectando-piscinas-no-declaradas-francia-lleva-20-000-ano

[12] https://www.europapress.es/nacional/noticia-policia-pide-prudencia-anunciar-vacaciones-redes-sociales-medida-prevenir-robos-domicilios-20220630130205.html

[13] https://faros.hsjdbcn.org/es/articulo/riesgos-redes-sociales-salud-mental-adolescentes

[14] https://www.lavanguardia.com/tecnologia/20211005/7769784/frances-haugen-filtradora-archivos-facebook-toxicidad-desinformacion-pmv.html

[15] https://www.lavozdegalicia.es/noticia/sociedad/2021/09/16/instagram-oculta-provoca-baja-autoestima-tres-chicas/0003_202109G16P45991.htm

[16] https://www.xataka.com/seguridad/robo-masivo-datos-facebook-datos-personales-533-millones-usuarios-se-filtran-online.html

[17] https://www.businessinsider.es/facebook-multada-46-millones-euros-corea-sur-921921

[18] https://www.enter.co/chips-bits/apps-software/el-cifrado-de-extremo-a-extremo-llega-a-facebook-messenger/

[19] https://hipertextual.com/2021/06/peligros-compartir-datos-biometricos-con-tiktok

[20] https://hipertextual.com/2022/02/elon-musk-quiso-pagar-a-un-joven-de-19-anos-para-cerrar-un-bot-de-twitter-pero-este-le-vacilo

[21] https://www.genbeta.com/redes-sociales-y-comunidades/reconocimiento-facial-de-facebook-que-es-como-funciona-y-como-puede-desactivarse

[22] https://www.genbeta.com/actualidad/esta-app-utilizada-policia-eeuu-canada-cuenta-millones-fotos-obtenidas-redes-sociales-para-poder-identificarte

[23] https://github.com/iv-org/invidious

[24] https://newpipe.net/

[25] https://skytube-app.com/

[26] https://vancedapp.com/

[27] https://fritter.cc/

[28] https://nitter.net/

[29] https://allanwang.github.io/Frost-for-Facebook/

[30] https://www.mozilla.org/es-ES/firefox/facebookcontainer/

[31] https://addons.mozilla.org/es/firefox/addon/multi-account-containers/

[32] https://mastodon.social/about

[33] https://diasp.eu/

[34] https://mobilizon.org/es/