Biblioteca INFOTEC

Ciudad de México, a 16 de junio de 2025

VISTO BUENO DE TRABAJO TERMINAL

Maestría en Derecho de las Tecnologías de la Información y Comunicación (MDTIC)

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación:

"Guía práctica para garantizar la protección de datos personales en el uso de aplicaciones móviles: caso Temu"

Desarrollado por el alumno: **César Constantino López García**, bajo la asesoría de la **Dra. María Beatriz Juárez Aguilar**, cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Dr. Juan Antonio Vega Garfias
Subgerente de Innovación Gubernamental

JAVG/jah

C.c.p. Mtra. Analy Mendoza Rosales. – Encargada de la Gerencia de Capital Humano. - Para su conocimiento.
César Constantino López García. – Alumno de la Maestría Derecho de las Tecnologías de la Información y Comunicación. – Para su conocimiento.

Transformación Digital

Agencia de Transformación Digital y Telecomunicaciones

INFOTEC

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

“Guía práctica para garantizar la protección de datos personales en el uso de aplicaciones móviles: caso Temu”

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de
MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

César Constantino López García

Asesora:

Dra. María Beatriz Juárez Aguilar

Ciudad de México, mayo de 2025

MDTIC
Maestría en Derecho de las Tecnologías de Información y Comunicación

INFOTEC
POSGRADOS

Agradecimientos

Quiero dedicar este espacio para expresar mi más profundo agradecimiento a las personas y las experiencias que han sido fundamentales en la culminación de esta tesina y en mi desarrollo personal y profesional.

En primer lugar, a mi familia, que en los momentos más desafiantes ha sido el motor que me impulsa a seguir adelante. Su acompañamiento, amor y apoyo incondicional, y la confianza en mí han sido la fortaleza para lograr la conclusión de este logro académico. A mi maestra de vida, mi madre, ejemplo de sabiduría, fortaleza, dedicación y amor, que me inculcó perseguir mis metas con esfuerzo y determinación.

A mis maestros, quienes han sido sabiduría y guía en este proceso académico. Gracias por su dedicación, por compartir su conocimiento, y por el desafío intelectual. No solo me enseñaron sobre derecho y ética, sino también sobre la importancia de la búsqueda constante del aprendizaje. Comprendí que no todos los abogados persiguen los mismos objetivos ni, mucho menos, comparten un perfil único.

Finalmente, a mi asesora, quien asumió el desafío más complejo dentro del ámbito de la asesoría y la docencia: la de ser guía. Le agradezco profundamente el respeto que mostró tanto hacia mis aciertos como hacia mis errores, evitando siempre correcciones impositivas o juicios personales, y proporcionándome en todo momento las herramientas necesarias para mi desarrollo conceptual. Valoro especialmente su capacidad para equilibrar los momentos de desánimo y ofrecer un estímulo positivo constante, aspectos que resultaron fundamentales para la conclusión de este trabajo, mi más sincero agradecimiento.

Tabla de contenido

Introducción 6
Objetivo general 9
Objetivos específicos 9
Alcances y Limitaciones 9
Resultados Esperados 10
Capítulo 1. Marco conceptual de las aplicaciones móviles y la privacidad en el entorno digital. 13
Las aplicaciones móviles 13
¿Qué son las Aplicaciones móviles? 13
Tipos de Aplicaciones 14
Características de las Aplicaciones 15
¿Las aplicaciones pueden transmitir virus? ¿Qué es un malware? 16
¿Qué son los términos y condiciones establecidos en las aplicaciones móviles? 17
Las Tecnologías de la Información y comunicación (TIC) y los entornos digitales. 18
¿Qué son los entornos digitales y cómo proteger la información personal en ellos? 19
Recomendaciones generales 20
La protección de la privacidad en las aplicaciones móviles 21
¿A cuáles datos pueden acceder las aplicaciones móviles? 21
¿Qué son los datos personales y su tratamiento? 22
¿Qué son los datos biométricos y su manejo? 24
¿Qué son los Derechos ARCO? 26
¿Qué es el consentimiento? 27
¿Qué es un aviso de privacidad? 27
Análisis de casos prácticos 28
Caso Temu 28
Caso TikTok 33
Caso Oxxo Smart Grab & Go 35
Comisión de Protección de Datos de Irlanda impuso infracción administrativa a TikTok por un importe total de 530 millones de euros. 40
Informe de la Comisión Federal de Comercio de los Estados Unidos (Federal Trade Commission *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*). 42

Resolución de la Segunda Sala de la Suprema Corte de Justicia de amparo en revisión sobre la recolección de datos de geolocalización. 43

Capítulo 2. Análisis de intervención, comparativos del Derecho a la Protección de Datos Personales e Inteligencia Artificial. 45

Metodología de intervención. 45

Análisis en protección de datos personales e inteligencia artificial 53

Principales instrumentos normativos internacionales 53

Análisis comparativo de las legislaciones sobre protección de datos personales: perspectivas desde Estados Unidos, China y la Unión Europea 58

Análisis comparativo de las regulaciones de Inteligencia Artificial (Estados Unidos, China y la Unión Europea) 65

El Derecho a la Protección de Datos Personales en México. 68

Capítulo 3. Cuestionario de Evaluación de Seguridad. 71

Cuestionario de seguridad extendido para descarga de aplicaciones móviles en dispositivos electrónicos. 71

¿Va a descargar la aplicación de fuentes oficiales? 72

¿Ha comprobado que el desarrollador de la aplicación sea TEMU, y coincida con el icono y las capturas de pantalla oficiales? 72

¿He leído las reseñas y comentarios de otros usuarios para tener una idea de la confiabilidad y experiencia de la aplicación? 73

¿He verificado la fecha de publicación de la aplicación y la frecuencia de actualizaciones? 73

¿He descargado la aplicación exclusivamente desde el sitio web oficial de TEMU? 74

¿Ha considerado usar la versión web en lugar de la aplicación? 74

¿Ha verificado qué el certificado de seguridad del sitio web sea válido y que la conexión sea “https”? 75

¿Mi dispositivo tiene un sistema operativo actualizado con las últimas correcciones de seguridad instaladas? 76

¿Tengo un antivirus de confianza instalado y actualizado en mi dispositivo? 77

¿Ha revisado los permisos que solicita la aplicación antes de aceptar la descarga? ¿Ha evitado consentir permisos no esenciales para el funcionamiento de la aplicación? 78

¿He concedido solo los permisos que son estrictamente necesarios para que la aplicación funcione correctamente? 79

¿Consultó la política de privacidad de la aplicación y comprende cómo se recopilan, utilizan y comparten sus datos personales? 80

Evaluación del Cuestionario: 82

Conclusiones Generales 84

Introducción

En la actualidad, la intersección entre el uso de la tecnología y la privacidad de las personas se ha convertido en un tema cada vez más complejo y desafiante en la sociedad contemporánea. A medida que la tecnología avanza y se integra en todos los aspectos de nuestras vidas, se manifiestan tanto sus beneficios como sus desventajas. Las innovaciones tecnológicas han aportado importantes ventajas, como la simplificación de tareas diarias, la mejora en la calidad de vida y el acceso instantáneo a una vasta cantidad de información y comunicación. Sin embargo, este progreso no está exento de retos significativos. Entre los más preocupantes se encuentran la brecha digital, que deja a ciertos sectores de la población sin acceso a las herramientas tecnológicas; el uso excesivo de dispositivos electrónicos y redes sociales, que puede afectar la salud mental y bienestar; el desempleo causado por la automatización, que transforma radicalmente el mercado laboral; y, sobre todo, la creciente pérdida de privacidad que enfrentamos en un mundo cada vez más interconectado.

El uso de aplicaciones móviles se ha vuelto una parte fundamental de nuestra vida cotidiana, las herramientas digitales son esenciales no solo para comunicarnos, sino también para trabajar, estudiar o simplemente disfrutar del entretenimiento. No obstante, a pesar de su conveniencia y funcionalidad, el uso de estas aplicaciones conlleva riesgos significativos en cuanto a la exposición de la privacidad y la protección de los datos personales, en un entorno donde cada clic puede ser rastreado y cada interacción puede ser analizada, es crucial que los usuarios comprendan las implicaciones de sus decisiones digitales.

La creciente popularidad de las aplicaciones móviles, especialmente aquellas enfocadas en el comercio electrónico, han generado una serie de preocupaciones relacionadas con la privacidad y seguridad de los datos personales de los usuarios. La falta de conocimiento sobre las prácticas de recopilación y uso de datos por parte de estas aplicaciones, así como la complejidad de los ajustes de privacidad, exponen a los usuarios a riesgos significativos, lo que permite que se generen perfiles precisos y predictivos de los usuarios, lo que plantea grandes preocupaciones sobre la privacidad y seguridad de la información de las personas.

En el contexto de las Tecnologías de la Información y la Comunicación, un riesgo, se refiere a cualquier amenaza o vulnerabilidad se convierta en desastre, y comprometa la integridad y confidencialidad de la información personal, afectando la seguridad y privacidad de los usuarios. En el caso de las apps móviles de comercio electrónico, su creciente popularidad y uso masivo han generado un riesgo importante, ya que recopilan y procesan gran cantidad de datos personales sin que los usuarios comprendan claramente cómo se utilizan esos datos.

Este riesgo se agrava porque la complejidad de los ajustes de privacidad y la falta de información clara exponen a los usuarios a que se generen perfiles precisos y predictivos, lo que puede resultar en violaciones a su intimidad, robo de información, fraudes o usos indebidos de sus datos personales. Y en ocasiones las mismas aplicaciones pueden sufrir de fallas técnicas en su constitución que también puede derivar en incidentes de robo o perdida de información.

Un cuestionario de seguridad es un acompañamiento ideal para combatir este riesgo porque permite:

- *Determinar el nivel de conocimiento y prácticas del usuario* respecto a la privacidad y seguridad en la descarga y uso de aplicaciones móviles.
- *Guiar al usuario a través de preguntas clave* que le hagan reflexionar sobre los permisos que concede, la configuración de privacidad y los riesgos asociados.
- *Identificar áreas de vulnerabilidad personal* y ofrecer recomendaciones personalizadas para mejorar la protección de sus datos personales.
- *Fomentar la conciencia y cultura de seguridad*, facilitando que el usuario tome decisiones informadas y responsables al interactuar con aplicaciones móviles.

De esta forma, el cuestionario actúa como una herramienta educativa y preventiva que ayuda a reducir la exposición a riesgos derivados del desconocimiento o de malas prácticas, fortaleciendo la protección de la privacidad en el entorno digital.

¿Es posible que el acompañamiento de una guía práctica para la descarga segura de aplicaciones móviles pueda mejorar la consciencia y la cultura de las personas en la protección de datos personales y así reducir los

riesgos de que les sea violentado el derecho a la privacidad en el entorno digital?

La hipótesis de investigación sugiere que la creación y difusión de una guía práctica específica en el uso de aplicaciones móviles, como el caso de Temu, puede contribuir a desarrollar la conciencia en el cuidado de la privacidad en la sociedad, progresivamente evolucionar la cultura de la protección de datos personales y garantizar el respeto de los derechos fundamentales de las personas en el entorno digital, si bien la guía se enfoca en el caso Temu, su amplitud y el desarrollo de la misma permite que sea aplicada de forma general en otros casos de descarga de aplicaciones móviles, ya que su estructura está conformada con base en la constitución y los factores estratégicos de una aplicación móvil.

El problema central radica en el desconocimiento y la ausencia de materiales que informen a los usuarios de los riesgos que acompañan las descarga de aplicaciones móviles, surge la necesidad de proporcionar a los usuarios una herramienta práctica y accesible que les permita evaluar de manera objetiva los riesgos de los usuarios respecto a la privacidad y seguridad de sus datos en este tipo de plataformas en la descarga e instalación de aplicaciones como Temu.

La presente investigación se justifica por las siguientes razones:

Brecha de conocimiento: Existe una evidente brecha entre la popularidad de estas aplicaciones y el conocimiento de los usuarios sobre las implicaciones de su uso en términos de privacidad y seguridad.

Riesgos para la privacidad: La recopilación masiva de datos personales representa un riesgo significativo para los usuarios, ya que la información puede ser utilizada para fines comerciales, de marketing o incluso para fines delictivos.

Complejidad de las configuraciones de privacidad: Los ajustes de privacidad de las aplicaciones móviles suelen ser complejos y difíciles de entender para el usuario promedio, lo que dificulta la protección de sus datos.

Falta de herramientas formales de evaluación: No existen herramientas estandarizadas y accesibles que permitan a los usuarios evaluar de manera rápida y sencilla los riesgos asociados con la descarga de una aplicación.

Objetivo general

El objetivo general es desarrollar una guía informativa y de acompañamiento que genere cuestionamientos y proporcione directrices claras para asegurar la protección de datos personales de los usuarios en la utilización de aplicaciones móviles, centrándose en el caso específico de la aplicación Temu.

Objetivos específicos

- Diseñar una guía práctica de acompañamiento a las personas para la descarga segura tomando como base la aplicación Temu y así para comprender otras aplicaciones móviles.
- Enriquecer y familiarizar a los usuarios con los conceptos básicos relacionados con la tecnología de aplicaciones móviles y el entorno digital.
- Generar consciencia e informar a los usuarios sobre el derecho de protección de datos personales y los riesgos al otorgar el consentimiento sin análisis de la información.
- Generar una cultura de protección del derecho a la privacidad y la protección de datos personales.

Alcances y Limitaciones

- Alcances: la guía fue diseñada para ser clara y accesible para el usuario promedio, ofreciendo recomendaciones prácticas y directrices fundamentadas en la normativa vigente, así como en el análisis de los factores clave presentes en las mejores prácticas internacionales.
- Limitaciones: la intervención no garantiza una protección total e integral de los datos personales, dado que existen factores externos y políticas internas de las aplicaciones que escapan al control del usuario. Sin embargo, el objetivo

es proporcionar las mejores herramientas posibles y el acompañamiento para promover el mayor cuidado y resguardo de la privacidad.

Resultados Esperados

- Aumento en el nivel de conocimiento y conciencia de los usuarios respecto a la protección de sus datos personales.
- Disminución de los riesgos relacionados con la descarga y uso de aplicaciones móviles.
- Contribución significativa al fortalecimiento de una cultura de privacidad y protección de datos en el entorno digital.

Esta propuesta de intervención y análisis está concebida para ofrecer una solución integral, práctica y replicable, que atienda de manera efectiva las necesidades actuales de los usuarios en materia de privacidad y protección de datos personales en aplicaciones móviles.

En el primer capítulo, se abordará el marco conceptual de las aplicaciones móviles en profundidad, los diversos tipos de aplicaciones, sistemas más utilizados y sus características principales. Se analizará específicamente la aplicación Temu, poniendo a comparación la aplicación china TikTok y la aplicación mexicana Oxxo Smart Grab and Go. Se expone la clasificación de los diferentes tipos de datos personales y en qué consisten los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) que asisten a los ciudadanos en el manejo de su información personal. Además, se abordará el concepto de entornos digitales y su relevancia en la protección del derecho a la privacidad, destacando cómo estos espacios virtuales pueden ser tanto seguros como vulnerables. Lo que nos dará el contexto para comprender los conceptos relacionados con las aplicaciones móviles y la seguridad en el entorno digital.

El segundo capítulo presenta un análisis detallado de la metodología empleada en la intervención, incluyendo su justificación y el planteamiento claro del objetivo general, seguido por los objetivos específicos que guían el desarrollo del estudio. Además, se profundiza en el análisis sobre la protección de los datos personales, tanto en México como a nivel global, explorando los antecedentes normativos y las prácticas vigentes en distintas regiones. De manera complementaria,

se realiza una comparativa exhaustiva entre las naciones que lideran la innovación en el campo de la inteligencia artificial, destacando cómo cada nación aborda los retos y las oportunidades en materia de privacidad y seguridad de la información. Este enfoque permite comprender no solo el contexto local, sino también las tendencias internacionales que influyen en la regulación y protección de los datos personales.

Finalmente, en el último capítulo se presenta un cuestionario de seguridad cuidadosamente diseñado para guiar a los usuarios en la realización de una descarga segura de aplicaciones móviles. A través del acompañamiento paso a paso en la descarga de la aplicación Temu, el usuario podrá comprender y aprender no solo el proceso específico de esta app, sino también aplicar este conocimiento para cualquier otra aplicación móvil. Este cuestionario funciona como una herramienta práctica y didáctica para identificar y evaluar los riesgos potenciales asociados tanto a la descarga como al uso de aplicaciones móviles. Asimismo, se hace hincapié en la importancia de adoptar prácticas responsables y seguras al interactuar con tecnologías digitales, promoviendo una cultura de protección y prevención frente a las vulnerabilidades y amenazas a la información personal en el entorno digital actual y así fortalecer al usuario con conocimientos que contribuyan a minimizar riesgos y robustecer la seguridad en el uso cotidiano de aplicaciones móviles.

Concluyentemente, esta tesina busca contribuir significativamente a la generación de conciencia sobre la importancia vital de adoptar una cultura sólida en torno a la protección de los datos personales. Al promover el uso responsable y seguro de las aplicaciones móviles, aspirando a garantizar no solo la privacidad individual sino también un entorno digital más seguro para todos.

Capítulo 1

Marco conceptual de las aplicaciones móviles y la privacidad en el entorno digital.

Capítulo 1. Marco conceptual de las aplicaciones móviles y la privacidad en el entorno digital.

En el primer capítulo se analiza el marco conceptual de las aplicaciones móviles, sus principales tipos y sistemas operativos. Se compara la aplicación Temu con TikTok y Oxxo Smart Grab and Go, haciendo hincapié que debido a la gran cantidad de información generada sobre la red social TikTok y las similitudes que presenta con la aplicación del caso permite realizar comparativos claves, y la aplicación mexicana es material de nuevo que ha se fue generando con la investigación, gestado con información limitada que ha hecho pública la cadena comercial, con la intención de abrir brecha y llenar campos vacíos, siendo un tema no analizado a profundidad.

Además, se clasifican los tipos de datos personales y se explican los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) para la gestión de información personal. Finalmente, se aborda la importancia de los entornos digitales en la protección de la privacidad, resaltando oportunidades y riesgos para la seguridad de los datos. Este capítulo ofrece el contexto básico para comprender la relación entre aplicaciones móviles y seguridad digital.

Las aplicaciones móviles

¿Qué son las Aplicaciones móviles?

El concepto de aplicación móvil, comúnmente conocida como app, es un software diseñado específicamente para ser ejecutado en dispositivos móviles, como smartphones y tabletas[1]. Estas aplicaciones permiten a los usuarios realizar diversas tareas, desde la comunicación y el entretenimiento hasta la gestión de actividades diarias. A diferencia de los sitios web, las aplicaciones móviles están optimizadas para aprovechar las características únicas de los dispositivos móviles como: la cámara, el GPS y los sensores táctiles, lo que les permite ofrecer una experiencia de usuario más interactiva y personalizada.

[1] Universidad Nacional Autónoma de México, “Tienda de Apps UNAM”, *Dirección General de Cómputo y de Tecnologías de la Información y la Comunicación*, Universidad Nacional Autónoma de México, México, 2023, *https://sistemas.tic.unam.mx/wp-content/uploads/2023/09/20230804_DSSI_CSC_DTE_Aplicaciones_Moviles.pdf*

Para su óptimo funcionamiento utilizan los recursos del dispositivo en el que se ejecutan y pueden requerir una conexión a Internet para desempeñarse adecuadamente, esto significa, que hacen enlace con la red.

El lanzamiento en 1997 del celular Nokia 6110[2], se le reconoce como el surgimiento de las aplicaciones móviles al incluir el juego *Snake*, demostrando el potencial de los dispositivos móviles como plataformas de entretenimiento. Sin embargo, fue con la introducción del iPhone en 2007[3] y la posterior creación de la App Store que se desencadenó una verdadera revolución. La democratización del desarrollo de aplicaciones y la creciente capacidad de los dispositivos móviles transformaron radicalmente la forma en que interactuamos con la tecnología.

Inicialmente, las aplicaciones se concebían como herramientas básicas de productividad, pero rápidamente evolucionaron hacia un amplio espectro de funcionalidades, desde el entretenimiento hasta la organización de la vida cotidiana. La proliferación de teléfonos inteligentes y el desarrollo de sistemas operativos móviles como Android aceleraron esta tendencia, dando lugar a un ecosistema de aplicaciones cada vez más diverso y sofisticado.

En la actualidad, las aplicaciones móviles han permeado todos los aspectos de la vida moderna, convirtiéndose en una herramienta indispensable para la comunicación, el consumo de contenidos y la realización de diversas tareas. La creciente integración de inteligencia artificial en las aplicaciones sugiere que su impacto continuará expandiéndose en los próximos años, aunque podemos apreciar avances significativos, resulta imposible prever con certeza los alcances exactos que tendrán.

Tipos de Aplicaciones

La variedad de aplicaciones móviles modernas abarca desde experiencias de entretenimiento sofisticadas hasta soluciones empresariales especializadas, pasando

[2] Mobile Phone Museum, “Nokia 6110”, *Phone detail, https://www.mobilephonemuseum.com/phone-detail/nokia-6110*

[3] Apple inc., “Apple Reinvents the Phone with iPhone”, *Apple UK and Ireland Public Relations*, United Kingdom, 09 de enero de 2007, *https://www.apple.com/uk/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/*

por herramientas educativas innovadoras y sistemas de gestión personal. En el ámbito del entretenimiento: encontramos juegos interactivos que funcionan con realidad aumentada, aplicaciones multimedia con streaming de alta calidad, y plataformas de redes sociales que facilitan la conexión instantánea con comunidades globales.

Un aspecto particularmente relevante de las aplicaciones móviles contemporáneas es su capacidad de adaptarse a diferentes situaciones de uso. Por un lado, existen aplicaciones que operan exclusivamente en línea, manteniendo una conexión constante con servidores remotos para proporcionar servicios actualizados y sincronizados, como las plataformas de comercio electrónico, que permiten transacciones seguras en tiempo real, y las aplicaciones educativas que acceden a recursos didácticos dinámicos y bases de conocimiento actualizadas constantemente.

Por otro lado, las aplicaciones offline han demostrado ser valiosas, permitiendo una funcionalidad autónoma incluso sin conexión a Internet, siendo especialmente útiles en situaciones donde la cobertura de red es limitada o inexistente, en situaciones como viajes o en zonas remotas. La capacidad de funcionar de manera independiente ha llevado al desarrollo de aplicaciones versátiles que alternan entre modos online y offline según las necesidades y circunstancias de los usuarios.

Con el avance de tecnologías emergentes como el aprendizaje automático o *deep learning* y la inteligencia artificial, las aplicaciones están adquiriendo capacidades cada vez más sofisticadas para realizar necesidades específicas, adaptarse a patrones de comportamiento individuales y ofrecer experiencias personalizadas.

Características de las Aplicaciones

Las aplicaciones móviles o apps, se han convertido en herramientas esenciales en la vida cotidiana, gracias a una serie de características que las hacen sumamente atractivas y funcionales:

- **Fáciles de usar:** Su diseño intuitivo las hace de uso simple, incluso para aquellos usuarios que no tienen experiencia previa en el manejo de este tipo de tecnologías.

- **Interfaz táctil:** aprovechan al máximo las capacidades táctiles de los dispositivos móviles, ofreciendo una experiencia de usuario interactiva y fluida.

- **Acceso a la información:** uno de los mayores atractivos de las apps es su capacidad para brindar acceso rápido y sencillo a una gran cantidad de información y servicios, en muchos casos incluso sin necesidad de conexión a internet, especialmente valiosa en situaciones donde la conectividad es limitada o inexistente.

- **Personalización:** las apps se pueden personalizar para adaptarse a las necesidades y preferencias de cada usuario, lo que permite crear experiencias únicas y a medida. Esta capacidad de personalización contribuye a aumentar la satisfacción del usuario y fomenta el uso continuo de la aplicación.

¿Las aplicaciones pueden transmitir virus? ¿Qué es un malware?

No hay que olvidar que las aplicaciones son programas que se instalan en los dispositivos, por tanto, tienen capacidad para albergar virus, es por lo que se recomienda la descarga de las apps en tiendas oficiales como App Store, BlackBerry World o Google Play Store ya que son las más confiables en el mercado, al ser las más rigurosas en cumplir con las medidas de seguridad en los programas[4].

El software malicioso, o malware, es cualquier código de software o programa informático, incluidos ransomware, troyanos y spyware, escrito intencionalmente para dañar los sistemas informáticos o a sus usuarios[5], La evolución constante de las tecnologías de la información ha propiciado una proliferación de nuevos tipos de malware, adaptados a las vulnerabilidades emergentes y a las nuevas plataformas digitales.

[4] Softcorp, “Definición y cómo funcionan las aplicaciones móviles”, Venezuela, 2010, *https://servisoftcorp.com/definicion-y-como-funcionan-las-aplicaciones-moviles/*
[5] IBM, “¿Qué es el malware?”, *International Business Machines*, México, 14 de abril de 2022, *https://www.ibm.com/mx-es/think/topics/malware*

¿Qué son los términos y condiciones establecidos en las aplicaciones móviles?

Los términos y condiciones de las aplicaciones móviles son acuerdos legales que regulan la relación entre el usuario y el proveedor de la aplicación, suelen incluir información sobre el uso de la aplicación, la recopilación y tratamiento de datos personales, las responsabilidades de ambas partes, las limitaciones de responsabilidad, entre otros aspectos relevantes para el uso adecuado de la app, en todos los casos, deben estar redactados de forma clara, precisa y comprensible, y deben ser aceptados por los usuarios antes de hacer uso de la aplicación.

En el contexto de las aplicaciones móviles, los términos y condiciones son fundamentales para establecer las reglas de uso, proteger los derechos de los usuarios y los desarrolladores, y garantizar una interacción segura y transparente entre ambas partes.

Existen plataformas que muestran los términos de uso de una forma breve y con un lenguaje comprensible, que permite que el usuario tenga la posibilidad de realizar una lectura rápida y comprenda fácilmente las implicaciones del consentimiento, como lo es el gigante del comercio electrónico Amazon. Pero, por desagracia, existen compañías que expresan los términos de uso con un lenguaje legal técnico y una mala traducción al español, que genera ciertas confusiones, y se respaldan exponiendo que la información en el idioma inglés es las versión más adecuada, además, de presentar contenidos en extremo extensos para la lectura rápida, lo que imposibilita al usuario de conocer lo que está consintiendo al aceptar, lo que muestra que oportunidades de mejora en la regulación de dichas términos de uso, como sucede en el caso de Temu.

Es importante tomarse el tiempo de leer los términos y condiciones, para comprender que al realizar el clic en el recuadro de aceptar, omitimos leer detalles como:

- Desconocimiento de la relación comercial: al desconocer las especificaciones legales que se establecen en estos acuerdo legales, en ocasiones, renunciamos a la posibilidad de reclamación por productos.

- Disposiciones legales de arbitraje: las plataformas se protegen estableciendo sus domicilios legales y fiscales fuera del país donde realizamos la interacción con la aplicación, lo que los exime de responsabilidades y controversias en el servicio, por ejemplo, la aplicación Temu establece que cualquier tipo de controversia se regirá por las leyes del estado de Nueva York, específicamente la Ley Federal de Arbitraje, y en caso de no encontrar solución, y buscar un proceso judicial se tendrá que llevar forzosamente por un tribunal en Singapur con un representante legal de la aplicación China.

En conclusión, el aviso de privacidad se enfoca en la proteger e informar del usuario de sus derechos y obligaciones, mientras que los términos y condiciones se enfocan en el uso de la aplicación, como recomendaciones de uso adecuado, y que en caso contrario genera responsabilidades vinculantes.

La presente información busca generar una reflexión positiva, que si bien el ajetreo de las actividades diarias complica la dedicación con total concentración en interacciones con la tecnología, es de suma importancia concientizarnos al momento de realizar descargas móviles y prácticamente en todas las interacciones en la red que requieran de consentimiento para el acceso a su información, recuerde que los datos son personales, cuídelos.

Las Tecnologías de la Información y comunicación (TIC) y los entornos digitales.

Las tecnologías de la información y la comunicación, usualmente abreviadas como TIC, se definen por la Organización de las Naciones Unidas como:

> *"un conjunto diverso de herramientas y recursos tecnológicos utilizados para transmitir, almacenar, crear, compartir o intercambiar información. Estas herramientas y recursos tecnológicos incluyen computadoras, Internet (sitios web, blogs y correos electrónicos), tecnologías de transmisión en vivo (radio, televisión y webcasting), tecnologías de transmisión grabada (podcasting, reproductores de audio y video, y dispositivos de almacenamiento) y telefonía*

(fija o móvil). , satélite, visio/video-conferencia, etc.).[6]”

Las TIC abarcan una amplia gama de tecnologías, desde computadoras, teléfonos móviles, internet, redes sociales, software de productividad, hasta sistemas de almacenamiento en la nube, entre otros. Su objetivo principal es facilitar la creación, acceso, intercambio y procesamiento de información de manera rápida, eficiente y segura.

Estas tecnologías tienen un impacto significativo en la sociedad, la economía, la educación, la salud y prácticamente en todos los aspectos de la vida moderna, permitiendo la conexión global y la comunicación instantánea entre personas, empresas e instituciones en cualquier parte del mundo.

¿Qué son los entornos digitales y cómo proteger la información personal en ellos?

Los entornos digitales se refieren a los espacios en línea donde llevamos a cabo las interacciones, actividades y transacciones a través de dispositivos electrónicos como computadoras, tabletas, teléfonos inteligentes, etc.[7]

Estos entornos pueden ser por ejemplo:

Redes Sociales: plataformas en línea donde las personas pueden conectarse, compartir información, comunicarse y participar en diversas actividades sociales, por ejemplo: Facebook, Twitter, Instagram, LinkedIn, etc.

Comercio Electrónico: sitios web y aplicaciones que permiten la compra y venta de bienes y servicios en línea, por ejemplo: Temu, Amazon, eBay, Alibaba, etc.

---

[6] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, “Medición de las tecnologías de la información y la comunicación (TIC) en educación: manual del usuario”, *IIEP Learning Portal*, Canadá, 2009, *https://learningportal.iiep.unesco.org/en/glossary/information-and-communication-technologies-ict*

[7] Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, “¿Qué entendemos por entorno digital?”, *Construyendo ciudadanía en entornos digitales. Punto de partida*, Uruguay, capítulo 3, 2025, *https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/ publicaciones/construyendo-ciudadania-entornos-digitales-punto-partida/construyendo-4#*

Educación en línea: plataformas y sistemas que imparten cursos, tutoriales y recursos educativos a través de Internet, por ejemplo: Coursera, edX, Moodle, etc.

Aplicaciones de Trabajo Colaborativo: son herramientas en línea que facilitan la colaboración y la comunicación en entornos laborales, permitiendo a equipos trabajar juntos de manera remota, por ejemplo: Slack, Microsoft Teams, Google Workspace, etc.

Juegos en línea: plataformas y comunidades virtuales donde los usuarios pueden jugar videojuegos con otros jugadores, por ejemplo: Steam, PlayStation Network, Xbox Live, etc.

Servicios de Almacenamiento Nube: servicios que ofrecen almacenamiento en línea para archivos y datos, permitiendo a los usuarios acceder a sus datos desde cualquier lugar, por ejemplo: Google Drive, Dropbox, OneDrive, etc.

Foros y Comunidades en Línea: sitios web donde los usuarios pueden discutir temas de interés, hacer preguntas y compartir información, por ejemplo: Reddit, Quora y foros especializados.

Recomendaciones generales

Para proteger tus datos personales en línea, puedes seguir estos consejos:

- Crea contraseñas seguras y únicas para cada una de tus cuentas en línea.
- Activa la autenticación de múltiples factores en tus cuentas
- Revisa las políticas de privacidad de las aplicaciones y los sitios web que usas. (Averigua qué tipo de información recopilan sobre ti, cómo la usan y con quién la comparten).
- Puedes realizar copias de seguridad de tu información personal y corporativa en un servicio de almacenamiento en la nube seguro.
- Reporta cualquier intento de fraude, extorsión o robo de identidad a las autoridades competentes.

- Puedes adquirir y utilizar el servicio de red privada virtual (VPN) cuando te conectes a Internet desde una red pública o desconocida (oculta la dirección IP de tu dispositivo y encripta tu tráfico).

La protección de la privacidad en las aplicaciones móviles

El uso de aplicaciones móviles plantea importantes consideraciones sobre la protección de datos personales, por tanto, al ser instaladas el usuario cede gran cantidad de información sensible por lo que es fundamental observar que los desarrolladoras cumplan con aspectos o especificaciones clave como:

Consentimiento Informado: Los usuarios deben otorgar su consentimiento informado y previo para que la aplicación acceda a sus datos personales.

Finalidad del Tratamiento: La finalidad del tratamiento de los datos debe estar claramente definida y comprensible para el usuario, por tal motivo, no deben recopilar datos que no sean esenciales para su funcionamiento.

Política de Privacidad: Las aplicaciones deben contar con una política de privacidad que informe a los usuarios sobre la gestión de sus datos personales, que debe incluir detalles como la identidad del responsable del tratamiento, los datos a los que accederá la app y la finalidad del tratamiento.

¿A cuáles datos pueden acceder las aplicaciones móviles?

Al descargar aplicaciones móviles, y para realizar de forma correcta la instalación, es necesario que el usuario les otorgue permisos para acceder a los recursos de los dispositivos móviles, desde los físicos como: la cámara y el micrófono, y a su vez a los recursos digitales, que en su mayoría, cuentan con datos personales e información sensible, que pueden ser:

- Lista de contactos de teléfono y de correo.
- Fotografías y videos.
- Registro de llamadas.
- Datos bancarios.

- Datos de navegación en internet.
- Datos de mensajería.
- Datos de Geolocalización.
- Información del calendario.
- Código de identificación del aparato (Direcciones IP, e IMEI), entre otros.

Es de suma importancia observar y analizar los permisos que se otorgan a los dispositivos personales, ya que recopilan gran cantidad de información: incluyendo la dirección de correo electrónico, nombre, edad, sexo, entre otros datos sensibles, con la capacidad de generar perfiles específicos de los usuarios.

Para proteger esta información, es fundamental seguir algunas recomendaciones de buenas prácticas: como verificar los permisos de las aplicaciones, descargar de las tiendas autorizadas, mantener los dispositivos actualizados, utilizar contraseñas fuertes y educarse sobre la privacidad en la red . Además, es crucial que las aplicaciones cumplan con la normativa de protección de datos, solicitando siempre el consentimiento de los usuarios para recopilar sus datos personales y proporcionando una política de privacidad clara y completa.

¿Qué son los datos personales y su tratamiento?

Los datos personales son cualquier información que se refiere a una persona física identificada o identificable[8], es decir, que permite conocer su identidad directa o indirectamente. Los datos personales pueden ser, por ejemplo, el nombre, el apellido, la fecha de nacimiento, el correo electrónico, el número de teléfono, la fotografía, la huella digital, etc.

La protección de los datos personales es importante para evitar el uso indebido o ilícito de la información que se relaciona con la identidad, la vida privada, el patrimonio, las preferencias, las creencias, la salud, entre otros aspectos de las

[8] Ley Federal De Protección De Datos Personales En Posesión De Los Particulares, *Diario Oficial de la Federación*, H. Cámara de Diputados, México, 20 de marzo de 2025, *https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm*

personas, lo cual podría causar un daño o riesgo a su seguridad física o moral, o afectar sus derechos y libertades.

Diariamente proporcionamos a terceras personas datos personales y/o datos personales sensibles, ya sea consciente o inconscientemente, sin pensar en las consecuencias de que una tercera persona tenga nuestra información, en razón de eso, la Constitución Política reconoce y garantiza la protección de los datos personales[9], así como existen normativas que regulan el tratamiento llevado por las autoridades públicas y los particulares estableciendo principios, deberes y obligaciones para asegurar el respeto a este derecho humano.

La leyes y reglamentos establecen que el tratamiento de datos personales sensibles requiere del consentimiento expreso del titular, a menos que exista una o más de las excepciones establecidas en la ley. Además, impone a quienes manejan datos personales la obligación de implementar medidas de seguridad adecuadas para proteger la información.

La normativa también otorga a los titulares de los datos una serie de derechos, conocidos como derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), que les permiten tener control sobre la información que proporcionan y cómo se utiliza.

Los datos personales se pueden clasificar en dos categorías principales: datos personales y datos personales sensibles. Esta clasificación se encuentra en leyes de protección de datos de diferentes países, y es aplicable en el contexto de la protección de la privacidad y la regulación del tratamiento de la información personal. En México, los datos personales se definen y regulan principalmente bajo la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)[10], que establece que los datos personales pueden ser sensibles o no sensibles.

Datos Personales: Nombre y apellidos, fecha de nacimiento, nacionalidad, género, dirección, número de teléfono, correo electrónico, ocupación, etc.

---

[9] Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos personales, “La Importancia del INAI en la Protección de Datos Personales (PDP)”, México. *https://micrositios.inai.org.mx/todasytodos/?page_id=426*

[10] Ley Federal De Protección De Datos Personales En Posesión De Los Particulares, “Artículo 3º fr. V y VI”, *Diario Oficial de la Federación*, H. Cámara de Diputados, México, 20 de marzo de 2025, *https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm*

Datos Personales Sensibles: Salud, orientación sexual, creencias religiosas o filosóficas, afiliación política, afiliación sindical, datos biométricos (características físicas o comportamentales únicas, como huellas dactilares, forma de caminar, complexión física, etc.), origen étnico o racial, información financiera (detalles sobre ingresos, cuentas bancarias, historial crediticio, etc.)

*** Las clasificaciones de los datos personales son a título enunciativo y no limitativo.**

Es importante destacar que al realizar un tratamiento conjunto de varios de los datos personales se pueden considerar sensibles, ya que se generan perfiles específicos de las personas, esto quiere decir, que todos los datos idealmente deben ser considerados o tratados como sensibles.

La Ley Federal de Protección de Datos Personales en Posesión de Particulares tiene como objetivo proteger la privacidad y el derecho a la autodeterminación informativa de las personas. Establece que quienes recopilen, manejen, utilicen o almacenen datos personales deben cumplir con ciertos principios, como el consentimiento del titular para el tratamiento de sus datos, la finalidad legítima del tratamiento, la proporcionalidad y la seguridad de la información.

Además, en México se cuenta con un organismo constitucional autónomo garante, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que es la autoridad encargada de supervisar el cumplimiento de las normativas y garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) que tienen los titulares de datos personales[11].

¿Qué son los datos biométricos y su manejo?

Los datos biométricos son las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son

[11] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "¿Qué es el INAI?", México, *https://home.inai.org.mx/?page_id=1626*

medibles[12], de conformidad con el grupo de trabajo del Artículo 29[13], los datos biométricos son:

1. Universales, ya que son datos con los que contamos todas las personas;

2. Únicos, ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas;

3. Permanentes, ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona,

4. Medibles de forma cuantitativa.

Entre los datos biométricos que refieren a características físicas y fisiológicas se encuentran la huella digital, el rostro (reconocimiento facial), la retina, el iris, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, la piel o textura de la superficie dérmica, el ADN, la composición química del olor corporal y el patrón vascular, pulsación cardíaca, entre otros[14].

El manejo de los datos biométricos debe incluir los siguientes aspectos[15]:

1. Necesidad y Efectividad: Se debe analizar si el uso de datos biométricos es necesario y efectivo para atender una necesidad específica o innecesaria.

2. Evaluación de Costo - Beneficio: Es importante comparar el beneficio obtenido por el uso de estos datos con el costo potencial de una violación a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

---

[12] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Guía para el tratamiento de datos biométricos", México, primera edición, marzo de 2018, *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf*

[13] Comité Europeo de Protección de Datos (CEPD), "12168/02/ES. WP 80", *Grupo de trabajo del Artículo 29*, *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_es.pdf*

[14] *Ibidem*, p. 04.

[15] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Guía para el tratamiento de datos biométrico", *op cit.*

3. Alternativas Menos Invasivas: Se debe considerar la existencia de métodos menos invasivos para lograr el mismo objetivo.

4. Seguridad y Localización: La implementación de sistemas biométricos debe tener en cuenta la localización y los riesgos de seguridad.

5. Cumplimiento Normativo: Se deben tratar los datos biométricos de acuerdo con las normativas vigentes, asegurando que se respeten los derechos de los individuos.

Los datos biométricos son herramientas poderosas para autenticar identidades, cuando estos datos se cruzan con información personal (nombre, dirección, historial financiero), el peligro se amplifica. Al vincularse directamente con características físicas únicas, cualquier fallo en su gestión puede escalar a consecuencias irreversibles para la privacidad y seguridad de las personas.

¿Qué son los Derechos ARCO? [16]

Estos derechos se conocen así por las siglas de Acceso, Rectificación, Cancelación y Oposición de los datos personales.

Derecho de Acceso: aquel que permite al titular de los derechos conocer qué datos personales se encuentran en posesión de una tercera persona, ya sea particular o una autoridad.

Derecho de Rectificación: es el que permite a la persona titular solicitar que quien tiene sus datos realice modificaciones a dichos datos, y para llevar a cabo dicha solicitud siempre se debe aportar los documentos que lo acrediten como el titular.

Derecho de Cancelación: este derecho permite a la persona titular de los datos personales solicitar a quien cuenta con sus datos (responsable) proceda a la eliminación de dicha información, los registros o bases de datos con los que cuente.

[16] Ley Federal de Protección de Datos Personales en Posesión de Particulares, “Artículo 27”, *Diario Oficial de la Federación*, H. Cámara de Diputados, México, 20 de marzo de 2025, *https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm*

Derecho de Oposición: aquel que permite a la persona titular de los datos personales solicitar a quien (responsable) cuenta con sus datos que se abstenga de utilizar dicha información personal.

¿Qué es el consentimiento?

En México, el consentimiento es el principio fundamental para garantizar el derecho a la autodeterminación informativa; para que las personas puedan otorgar de manera libre, informada, expresa y previa su autorización[17] para que sus datos personales sean recopilados, utilizados, almacenados, transferidos o procesados por una empresa, organización o entidad gubernamental.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece que el consentimiento debe ser obtenido por medios electrónicos, escritos o cualquier otro medio que permita su posterior consulta, a menos que exista una excepción legal para su obtención[18]. Por lo que el responsable debe proporcionar información clara y detallada sobre la finalidad del tratamiento, qué datos de recopilan, cómo se van a utilizar y así las personas puedan tomar decisiones informadas sobre el uso de su información.

¿Qué es un aviso de privacidad?

El aviso de privacidad, como su nombre lo dice, es un documento legal que describe cómo una entidad, ya sea una empresa, una organización o un sitio web, recopila, utiliza, divulga y gestiona los datos personales de los usuarios.

En México, la normativa que regula la protección de datos personales en el uso de aplicaciones móviles es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), y dicho ordenamiento tiene como objetivo garantizar el derecho a la *autodeterminación informativa* de las personas, es decir, que los usuarios decidan qué información sensible compartir, con quién o quiénes y que finalidad va a tener, por lo que las apps deben incluir:

[17] Ley Federal De Protección De Datos Personales En Posesión De Los Particulares, *op cit.*, p. 03.
[18] *Idem.*

- El responsable (persona física o moral) del tratamiento de los datos personales y domicilio.
- Finalidad del tratamiento de los datos personales.
- Los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y los procedimientos o medios de protección.
- Los mecanismos y procedimientos para informar al titular sobre los cambios en el aviso de privacidad.
- Medidas de seguridad que el responsable implementa para proteger los datos personales contra el daño, pérdida, alteración, acceso o tratamiento no autorizado.
- Los terceros con los que el responsable comparte los datos personales, así como las finalidades de dicha transferencia y los medios para que el titular pueda manifestar su consentimiento o negativa al respecto.
- Los datos personales sensibles que se recaban, es decir, aquellos que afectan a la esfera más íntima del titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, como los relativos a su origen racial o étnico, estado de salud, preferencias sexuales, creencias religiosas, filosóficas o morales, afiliación sindical, opiniones políticas[19], etc.

Análisis de casos prácticos

Caso Temu

El auge global en popularidad y aceptación que han experimentado las aplicaciones chinas como Temu y TikTok ha sido impactante, sin embargo, este éxito no ha estado exento de controversias, especialmente en dos vertientes, al ofrecer compras a precios extremadamente bajos, y en lo que respecta a la privacidad y la recopilación masiva de datos personales. La preocupación principal radica en la

[19] Ley Federal de Protección de Datos Personales en Posesión de Particulares, "Artículo 2º fr. VI", *Diario Oficial de la Federación*, H. Cámara de Diputados, México, 20 de marzo de 2025, *https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm*

cantidad y el tipo de información que estas aplicaciones recolectan, así como en el posible uso indebido o la supuesta transferencia de datos a entidades gubernamentales chinas. Uno de los problemas centrales es la falta de transparencia en las políticas de privacidad de estas aplicaciones, debido a que, los usuarios aceptan términos y condiciones complejos sin comprender por completo el alcance del consentimiento que otorgan.

Temu es una plataforma emergente de comercio electrónico siendo la aplicación de compras más descargada a nivel mundial, cerrando el año 2024 con casi 550 millones de descargas[20], que tiene como objetivo comercial conectar a los consumidores con millones de socios comerciales, fabricantes y marcas de todo el mundo, que ofrece como misión *empoderar* a los consumidores para mejorar su vida. Se ha vuelto en extremo popular en México, Estados Unidos y algunos países de Europa, principalmente España, tomando en consideración que su fundación fue en el año 2022, en Boston, Massachusetts, Estados Unidos[21].

Temu ha sabido diferenciarse a través de la innovación, generando un impacto significativo en la industria del e-Commerce, y su agresiva política de precios y promociones. Ha logrado un rápido crecimiento en el mercado americano y europeo, por la popularidad generada por los precios asequibles, envíos rápidos y la amplia gama de productos, donde los descuentos exagerados al valor de los productos hace cuestionarse la viabilidad comercial de la empresa, con acusaciones de “negocio fraudulento”, además, de las intervenciones mercadológicas en los eventos deportivos del Super Tazón, y las alianzas comerciales con Facebook, donde la empresa china y su competidor Shein representan gran parte de los ingresos del año anterior de la compañía Meta Platforms, Inc, lo que ha generado suspicacias a nivel internacional, pero principalmente en territorio norteamericano.

[20] Statista, “Leading shopping apps worldwide in 2024, by number of downloads (in millions)”, Alemania, enero 2025, *https://www.statista.com/statistics/1428596/most-downloaded-shopping-apps-worldwide/#statisticContainer*

[21] Whaleco Inc., “¿Qué es Temu?”, Estados Unidos, 2025, *https://www.temu.com/us-es/about-temu.html?refer_page_name=search_result&refer_page_id=10009_1711334553185_t0zi8p12sx&refer_page_sn=10009&_x_sessn_id=gs1ozkt9ql*

La firma de investigación financiera forense Grizzly Research acusa a la empresa Pinduoduo (PDD Holdings) como fraudulenta y a su aplicación (TEMU)[22] de esconder un programa espía (spyware) que suponen una amenaza urgente para los intereses de seguridad nacional de Estados Unidos, el Malware es un software malicioso diseñado para dañar, explotar u obtener acceso no autorizado a dispositivos y datos, y del mismo se desprende varios tipos, entre ellos, el Spyware, dedicado a recopilar información del dispositivo y hacerla llegar a un tercero sin el consentimiento de la víctima[23].

Para el óptimo funcionamiento, la aplicación solicita a los usuarios el consentimiento para recopilar sus datos de contacto básicos, es decir, lo que hace la mayoría de aplicaciones, pero en el ejercicio tiene alcances mayores; como el armado de perfiles con bases de datos externas, información del dispositivo de donde se hace la conexión, la ubicación y el rastreo de las actividades que desarrollamos en la red, y finalmente, como lo explica en su política de privacidad, al dar el consentimiento la aplicación obtiene la facultad de compartir su información con quien consideren un socio comercial.

El panorama ha cambiado con la irrupción de empresas asiáticas como Temu, AliExpress y Shein, la primera, en particular, ha ganado terreno rápidamente, impulsada por su creciente popularidad, fenómeno que se ha hecho visible en el volumen de miles de paquetes diarios que llegan al aeropuerto de Zúrich, lo que atrajo la atención del gobierno suizo, que ha dado paso a investigaciones, como el *Análisis de Seguridad Técnica de la App Móvil Temu: Un Vistazo Profundo*[24]

Temu ha enfrentado acusaciones sobre posibles riesgos de ciberseguridad, se ha sugerido que la aplicación podría espiar a los usuarios o mostrar comportamientos similares a los de un *malware*, como fue sostenido por Grizzly

[22] Grizzly Research LLC, "We believe PDD is a Dying Fraudulent Company and its Shopping App TEMU is Cleverly Hidden Spyware that Poses an Urgent Security Threat to U.S. National Interests", Estados Unidos, 2023, *https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/*

[23] Nord VPN, ¿Qué es spyware?, *Blog ciberseguridad*, *https://nordvpn.com/es/blog/que-es-spyware/*

[24] Castagna, Tobias, "Technical Security Analysis Mobile App Temu", *National Test Institute for Cibersecurity*, Suiza, versión 1.0, diciembre 2024, *https://www.ntc.swiss/hubfs/temu-security-analysis-ntc-en.pdf*

Research. Identificar comportamientos problemáticos en aplicaciones móviles requiere conocimientos técnicos especializados, lo que representa un desafío para la mayoría de los usuarios, dada la capacidad para recopilar datos sensibles a través de sensores de los teléfonos inteligentes, por lo que es fundamental analizar objetiva y detenidamente los riesgos asociados con aplicaciones chinas.

El análisis realizado por *The National Test Institute for Cybersecurity* (NTC) no encontró vulnerabilidades críticas evidentes ni pruebas de vigilancia de usuarios en la aplicación Temu, en general, el comportamiento observado y los permisos solicitados son similares a los de otras aplicaciones de comercio electrónico, en comparación con competidores como Amazon, Ali-Express o Shein, Temu solicita menos permisos y menos problemáticos.

Si bien la aplicación no parece acceder al micrófono, la cámara y el GPS sin el consentimiento del usuario, la organización suiza hizo hincapié en algunos comportamientos inusuales que merecen atención:

Banderas rojas: la aplicación tiene la capacidad de cargar dinámicamente código similar a JavaScript, esto quiere decir, se refiere a la posibilidad de incorporar y ejecutar fragmentos de código o módulos solo cuando son necesarios, en lugar de cargarlos todos al inicio de la aplicación, lo que permite modificar su comportamiento en tiempo de ejecución, si bien no es una característica exclusiva de esta aplicación, su implementación es inusual y dificulta la predicción y prueba de todos los posibles comportamientos de la aplicación. Otro aspecto crítico es el uso de capas adicionales de cifrado, que podrían ocultar transmisiones de datos no deseadas, si bien estas medidas pueden ser positivas en la protección de los datos del usuario, también dificultan el análisis del tráfico de red y la identificación de posibles riesgos.

Recomendaciones: si bien el análisis no encontró evidencia directa de actividad maliciosa, en el estudio **se recomienda el no usar la aplicación Temu, especialmente en contextos empresariales o gubernamentales**, tomar medidas técnicas y organizativas para mitigar los riesgos, como conceder solo los permisos necesarios, mantener el sistema operativo actualizado y limitar el uso de la aplicación al mínimo, como alternativa se recomienda el acceder al servicio a través del

navegador web del dispositivo móvil, lo que reduce la superficie de ataque y las oportunidades de vigilancia permanente.

Cabe señalar que, para su óptimo funcionamiento, la aplicación solicita el consentimiento para recopilar los datos de contacto como nombre, apellido, correo electrónico, dirección de facturación, número de teléfono, además, información demográfica, es decir, sexo, ciudad, estado, código postal y país de residencia, así como la fotografía del perfil, nombre de usuario y contraseña, información de pago y los enlaces de redes sociales, así pues, lo que hace la mayoría de aplicaciones.

Lo que hace diferente a TEMU, es que con el consentimiento obtiene:

- **Accede a su lista de contactos:** para autocompletar la información de los contactos del teléfono móvil, para enviarles ofertas o acceder fácilmente a la dirección de envío registrada de una amistad de la lista de contactos.

- **Información de terceros:** accede a fuentes de vendedores, fuentes públicas (agencias gubernamentales y plataformas de redes sociales), proveedores de datos, socios de marketing y terceros (Cookies).

- **Recopilación automática de datos:** la empresa, sus proveedores de servicios y socios comerciales pueden registrar automáticamente su equipo o dispositivo móvil: tipo de sistema operativo, modelo de dispositivo móvil, fabricante, especificaciones técnicas del equipo, compañía del dispositivo móvil, IP e IMEI (números de identificación de los equipos o dispositivos), etc.

- **Datos de actividad en línea:** las páginas visitadas anteriormente, tiempo de conexión en la red, el sitio web que se visitó antes de acceder al servicio, horarios y otros datos más.

- **Datos de ubicación:** accede a los datos de geolocalización de los equipos y dispositivos móviles a través de la dirección IP, y la ubicación exacta de su móvil.

Expresamente, la aplicación explica en su política de privacidad que al aceptar la descarga de la aplicación obtiene el consentimiento del usuario, y la facilidad de compartir la información personal con quien ellos consideren prudente.

Caso TikTok

Las aplicaciones Douyin y TikTok, ambas propiedad de ByteDance[25], son plataformas que aunque comparten similitudes en su interfaz y funcionalidad, presentan diferencias significativas en términos jurídicos y jurisdiccionales.

Douyin es la versión exclusiva para China, lanzada en el año 2016, mientras que TikTok se expandió globalmente en 2017[26]. La primera, solo se puede descargar y utilizar dentro de China, mientras que la segunda está disponible en más de 150 países alrededor del mundo[27]. Esto significa que solo en China se puede acceder a Douyin, y TikTok almacena su información en servidores según la región geográfica, por lo que la aplicación china está sujeta a las estrictas regulaciones de contenido del gobierno chino, lo que implica un mayor control sobre el tipo de información permitida en la plataforma, esto incluye limitaciones en ciertas temáticas de publicaciones (contenido seguro para niños) y mayores restricciones para menores de edad (límites de tiempo de uso diario)[28], en cambio, TikTok se sujeta a las regulaciones y restricciones de los diversos países donde tiene presencia, lo que le ha permitido captar una base de usuarios considerable, especialmente adolescentes y jóvenes adultos, que se distingue por su enfoque en videos de corta duración que se reproducen en bucle, lo que fomenta un consumo continuo y adictivo. Desde su lanzamiento, ha experimentado un crecimiento explosivo, su atractivo radica en su capacidad para viralizar contenido rápidamente, lo que ha llevado a debates sobre la necesidad de regular de manera más estricta a estas empresas o incluso prohibir su uso en ciertos contextos, especialmente en Estados Unidos.

La popularidad de esta aplicación, contrasta con las crecientes advertencias de los políticos estadounidenses sobre los riesgos que plantea para la privacidad y la seguridad de los datos, la principal preocupación radica en ByteDance, la empresa china propietaria de la aplicación, y la sujeción de la cual puede ser objeto a las

[25] Global Data Plc, "Beijing ByteDance Technology Co Ltd: Locations", United Kingdom, 2025, *https://www.globaldata.com/company-profile/beijing-bytedance-technology-co-ltd/locations/*

[26] González, Abel, "Douyin, la versión de TikTok exclusiva para China"*, Asilo Digital,* Venezuela, 20 de junio de 2021, *https://www.asilodigital.com/douyin-version-china-tiktok/*

[27] *Idem.*

[28] Juárez Aguilar, María Beatriz, "RedNote, TikTok y las nuevas fronteras del desafío chino", *dpl news*, México, 3 febrero de 2025, *https://dplnews.com/rednote-tiktok-y-las-nuevas-fronteras-del-desafio-chino/*

regulaciones del gobierno chino, lo que prevé podría derivar en la filtración de datos de usuarios estadounidenses, y la posibilidad de que el gobierno chino utilice la aplicación para difundir propaganda y desinformación en territorio norteamericano.

Ante estas amenazas, se han aplicado diversas medidas para restringir o prohibir el uso de la aplicación, por ejemplo, en los dispositivos de trabajo de los contratistas y empleados del gobierno federal norteamericano, y 34 estados han impuesto restricciones similares a sus empleados, el estado de Montana ha prohibido el uso de TikTok a todos sus residentes[29].

Para mitigar las preocupaciones, TikTok ha impulsado el "Proyecto Texas", una iniciativa que busca trasladar el control de los datos de usuarios estadounidenses, cuyo acceso estaría controlado por una subsidiaria independiente llamada U.S. Data Security (USDS)[30], a pesar de estas medidas, en marzo de 2024, la Cámara de Representantes aprobó la *Ley de Protección de los Estadounidenses frente a Aplicaciones Controladas por Adversarios Extranjeros*[31], que busca forzar la separación de TikTok de ByteDance, donde de no cumplirse la exigencia la aplicación sería prohibida en Estados Unidos, sin embargo, el Senado frenó su aprobación, lo que vino a dar un respiro a la plataforma, además, surge la interrogante de si otras empresas y plataformas chinas que se expanden a nivel internacional enfrentarán restricciones similares.

La prohibición de TikTok no es un fenómeno exclusivo de Estados Unidos, varios países han vetado o parcialmente prohibido la plataforma: resalta el caso de India, donde contaba con 150 millones de usuarios aproximadamente, y debido a un enfrentamiento en la frontera con China por el Himalaya, se anunció su prohibición y la de más de 50 aplicaciones chinas, las prohibiciones de uso de la aplicación

[29] Tian, Zhe, Zakaria, Aqib, Latif, Adam, “Bridging Digital Divides: Navigating Data Governance and Security in the U.S.-China Technological Arena”, Fudan-Harvard China-U.S. Young Leaders Dialogue 2024, Fudan university center for American studies, China, 2024, *https://cas.fudan.edu.cn/info/1206/16673.htm*

[30] González, Fernanda, “TikTok se compromete a eliminar los datos de usuarios de EE UU para evitar la prohibición en el país”, *Wired*, México, 23 de marzo de 2023, *https://es.wired.com/articulos/tiktok-se-compromete-a-eliminar-los-datos-de-usuarios-de-ee-uu*

[31] Protecting Americans from Foreign Adversary Controlled Applications Act, “H.R.7521”, *Senado De Los Estados Unidos*, EUA, 14 de marzo de 2024, *https://www.congress.gov/bill/118th-congress/house-bill/7521/text?s=1&r=5&q=%7B%22search%22%3A%22tiktok%22%7D*

impuestas al personal de la Comisión, el Consejo y Parlamento Europeos, Canadá, Australia, Gran Bretaña, Nueva Zelanda y Taiwán con la prohibición de uso en los teléfonos gubernamentales, y finalmente Nepal, Pakistán, Somalia, Indonesia y Afganistán lo consideran de impacto perjudicial para sus ciudadanos, lo que hace imposible negar el rechazo internacional[32].

Caso Oxxo Smart Grab & Go

El caso que demanda atención en México es la reciente apertura de la tienda Oxxo Grab & Go (10 de febrero de 2023), perteneciente a la cadena comercial FEMSA. Ubicada en Monterrey, Nuevo León, en el campus del Tec de Monterrey, destaca por ser la primera tienda en toda Latinoamérica en operar bajo un sistema totalmente digital, con un modelo innovador que descarta la necesidad de realizar el pago en caja, utilizando inteligencia artificial y tecnología avanzada para automatizar el proceso de compra[33].

El funcionamiento de la tienda es sencillo y a la vez con un despliegue tecnológico importante, donde los usuarios deben descargar la aplicación *Oxxo Smart Tec Grab & Go (citar)*, registrar los datos personales y vincular una tarjeta de crédito o débito, al ingresar la información permite generar un código QR que al pasar por el escáner ubicado en la puerta permite ingresar a la tienda. Una vez dentro, los usuarios pueden tomar los productos directamente de los estantes y salir sin necesidad de pasar por una caja tradicional, al ser monitoreados por un sistema que a través de cámaras avanzadas y el uso de la inteligencia artificial identifica a los usuarios y los productos seleccionados para realizar el cobro automático al salir, y el recibo de compra se envía directamente al celular del cliente[34].

Este modelo fue creado para ser replicado en espacios como universidades, hospitales, oficinas y plazas comerciales[35], y como toda innovación se encuentra en

---

[32] Taylor, Adam, Hassan, Jennifer, Francis, Ellen, Mellen, Ruby, "Countries banned TikTok", *Washington Post*, EUA, 17 de enero de 2025, *https://www.washingtonpost.com/world/2025/01/17/countries-banned-tiktok/*

[33] Grupo FEMSA, "Comunicado de Prensa: OXXO abre la primera tienda Grab & Go, con un sistema totalmente digital y sin fricciones", México, 10 febrero de 2023, *https://www.femsa.com/es/sala-de-prensa/comunicado/oxxo-abre-la-primera-tienda-grab-go-con-un-sistema-totalmente-digital-y-sin-fricciones/*

[34] Animal Político, "Entrevista OXXO Grab & Go", *YouTube*, México, 15 de marzo de 2023,*https://www.youtube.com/watch?v=9saVFTvZkTs&ab_channel=AnimalPol%C3%ADtico*

[35] Grupo FEMSA, *Comunicado de Prensa, op. cit.*

una fase de adaptación, de ajustes para desarrollarse de manera funcional, pero, especialmente existe preocupación sobre la privacidad y seguridad en la protección de la información de los usuarios (datos personales sensibles; financieros y biométricos),

Grupo FEMSA asegura que el tratamiento de los datos personales cumple con las regulaciones aplicables y que estos son utilizados únicamente para mejorar la experiencia del cliente y realizar las transacciones automatizadas, no obstante, la dependencia de tecnologías avanzadas plantea riesgos potenciales al enfrentar desafíos derivados de la falta de transparencia en los mecanismos de protección de la privacidad de los usuarios y la confiabilidad hacia el sistema.

El cual opera a través de un software de visión por computadora y el uso de inteligencia artificial, donde me permito citar al Gerente de Innovación y Tecnología de OXXO, Abraham Leos Gutiérrez[36]:

> *… el contenedor tiene alrededor de 38 cámaras que tienen detectado todo el espacio para no tener puntos ciegos, cuando tú entras con tu código QR, detecta tu altura, tu complexión, la ropa que estás usando y te asigna un identificador, al salir tenemos una cámara, - que llamamos la cámara de check out -, entonces la cámara te detecta que sales y es cuando te hace el cobro.*
>
> *… nosotros protegemos la identidad de los usuarios, y simplemente detecta siluetas o formas, y cuando tú entras y tomas los productos de los estantes, te los agrega a tu carrito virtual de compras, y todo esto es por medio de estas cámaras.*

Los datos personales y la inteligencia artificial guardan una relación íntima, estrecha, y a través de ella se logra el funcionamiento optimo, lo que nos lleva a considerar que el mayor activo de la IA son los datos biométricos, por lo que, es importante poner en contexto ambos conceptos, de inicio, la Red Iberoamericana de Protección de Datos Personales propone que la Inteligencia artificial es *un término sombrilla que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, particularmente se vincula el uso de algoritmos a la IA, los cuales son un conjunto de*

[36] Animal Político, “Entrevista OXXO Grab & Go”, *op. cit.*

reglas o una secuencia de operaciones lógicas que proporcionan instrucciones para que las máquinas tomen decisiones o actúen de determinada manera[37]*.,* y posteriormente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en la Guía para el Tratamiento de Datos Biométricos[38], los reconoce como datos personales, al referir características físicas, fisiológicas del comportamiento y de la personalidad, que permiten las distinción de las personas, por lo que se espera que el manejo de esta categoría jurídica de información sea respetuoso de los derechos humanos y del marco jurídico aplicable al tratamiento de datos personales.

Como fue mencionado anteriormente en las palabras del representante del Grupo FEMSA, al recabar información: al captar rostros, complexión física, e inclusive la forma de caminar de los usuarios, se pueden trazar perfiles, que fácilmente se pueden relacionar e identificar, lo que en un escenario trágico, visiblemente puede derivar en resultados catastróficos, si son extraídos sin autorización y compartidos irresponsablemente, al dejar en vulnerabilidad y sin protección la privacidad de los usuarios de dicha aplicación.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), obliga a los Particulares como Responsables de garantizar la privacidad y el derecho a las personas de estar informadas sobre el uso de sus datos personales, así mismo, en su estructura establece la figura de la *transferencia de datos* cuando la información es compartida con terceros nacionales o extranjeros, que si bien, *asumirán las mismas obligaciones que correspondan al responsable que transfirió los datos*[39], a la par con el responsable, solo queda en una simple asunción, como lo muestra puntualmente este ejemplo, que en su aviso de privacidad establece que:

---

[37] Red Iberoamericana de Protección de Datos, "Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial", México, 21 de junio de 2019, *https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf*

[38] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Guía para el tratamiento de datos biométricos", *op. cit.*, p. 09

[39] Ley Federal de Protección de Datos Personales en Posesión de Particulares, "Artículo 35", *Diario Oficial de la Federación*, H. Cámara de Diputados, México, 20 de marzo de 2025, *https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm*

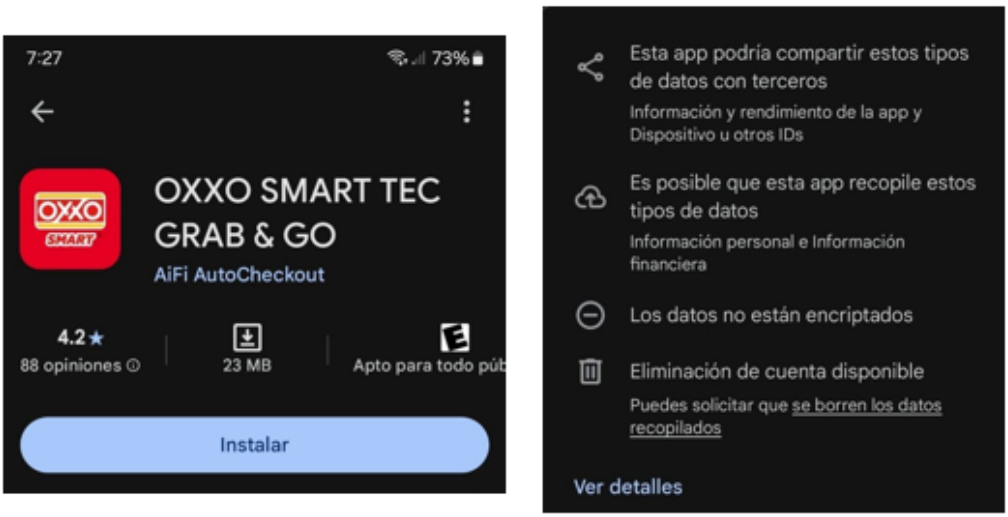
OXXO podrá compartir sus datos personales sin requerir de su consentimiento en los siguientes supuestos[40]:

Terceros con los que OXXO tenga una relación jurídica y su transferencia sea necesaria para poder llevar a cabo el cumplimiento de las finalidades para las que fueron recabados los datos personales.

Esto quiere decir, que la cadena comercial, al tener una relación jurídica y comercial con la empresa AiFi Inc., como tercero al ser el desarrollador de la aplicación, mediante un instrumento jurídico (cualquier expresión relacionada con "agreement"), está en cumplimiento con las finalidades para que fueron recabados los datos personales, como se establece el artículo 35 de la LFPDPPP, anteriormente citado.

En lo que respecta a la Aplicación *Oxxo Smart Tec Grab & Go*[41], al ingresar a buscar la aplicación en las plataformas de descarga de Apps, en este caso se expone el sistema Android como ejemplo, donde se observan varios factores importantes:

Seguridad de los datos: el desarrollador fue el responsable de proporcionar la información que se presenta a continuación:



Imágenes tomadas de Google Play Store (2024)

[40] Grupo FEMSA, "Aviso de Privacidad Integral para clientes", México, febrero de 2024, *https://www.oxxo.com/aviso-de-privacidad-integral*

[41] Google LLC, "Oxxo Smart Tec Grab & Go", *Google Play Store*, 2025, *https://play.google.com/store/apps/details?id=io.aifi.autocheckout.oxxoo&pc*

Observaciones:

a) Datos recopilados: nombre, dirección de correo electrónico, ID de usuario, número teléfono y la información de pago del usuario. Los datos personales, al unirse generan un perfil, con identificación del usuario, con nombre e información de pago, ya se puede considerar datos personales sensibles.

- Los datos no son encriptados: tus datos no se transfieren mediante una conexión segura. No es necesario hacer mayor hincapié en la falta de seguridad en la transferencia de datos.

- Eliminación de cuenta disponible: puedes solicitar que se borren los datos recopilados. Al ingresar al enlace para la eliminación de los datos personales, el desarrollador presenta un enlace hacia su política de privacidad, la cual, no concuerda con el propósito del caso, como se muestra en la página web del desarrollador, , la *"Privacy Policy – Aplicants"* está dirigida a establecer el procesamiento de la información en el reclutamiento y selección de los solicitantes de posiciones laborales en AiFi Inc[42].

En segunda instancia los prestadores de servicios internacionales cuentan con la protección jurisdiccional y territorial de sus países de origen, que por desagracia la falta de estandarización en la protección internacional del derecho a la privacidad, la falta de organización entre naciones y la laguna en nuestro ordenamiento legal aún no ha sido atendida puntualmente, como sucede en este caso en particular, ya que la empresa se encuentra establecida legalmente en el estado de California, por lo que goza de la protección de las leyes de ese estado y en su consideraciones solo se encuentra la referencia del Reglamento de Protección de Datos de la Unión Europea y de la Ley de Privacidad del Consumidor de California (CCPA)[43].

[42] AiFi Inc., "Privacy Policy – Applicants", EUA, 23 de febrero de 2024, *https://aifi.com/privacy-policy-for-applicants/*

[43] California Consumer Privacy Act ("CCPA"), "Cal. Civ. Code §§ 1798.100–1798.199", *Department of Justice State of California*, EUA, 2018, *https://oag.ca.gov/privacy/ccpa*

La gestión enfocada en la seguridad de la información y la protección de la privacidad de los usuarios son consideraciones primordiales para generar confianza en los entornos digitales. Los usuarios se enfrentan al dilema de disfrutar de los servicios que ofrecen las aplicaciones a cambio de ceder una gran cantidad de información personal, con riesgos potenciales para su privacidad y seguridad. Lo que nos lleva a considerar:

¿Las imágenes que captan las cámaras son resguardadas de forma segura? ¿Al no saber específicamente el funcionamiento puntual de dicha tecnología, estamos en la capacidad de ejercer los derechos ARCO[44] sobre dichas imágenes?, ¿Se hace un manejo adecuado y conforme a la legislación mexicana para el resguardo de datos biométricos? ¿Se ha considerado que la filtración de los datos personales otorgados y consentidos en la Aplicación y de los captados en las cámaras pudieran ser relacionados y generar perfiles específicos de los usuarios?

Comisión de Protección de Datos de Irlanda impuso infracción administrativa a TikTok por un importe total de 530 millones de euros[45].

El 2 de mayo de 2025, la Comisión de Protección de Datos de Irlanda (DPC) anunció una multa histórica de 530 millones de euros a TikTok Technology Limited, tras una investigación sobre el cumplimiento de los requisitos de transparencia en las transferencias de datos personales hacia China como lo establece el Reglamento General de Protección de Datos (RGPD) para los usuarios del Espacio Económico Europeo (EEE), por lo que expongo los puntos principales:

- Transferencia ilícita de datos personales a China, TikTok infringió el artículo 46(1) del Reglamento General de Protección de Datos, porque no verificó, garantizó, ni demostró que las medidas complementarias y

[44] Constitución Política de los Estados Unidos Mexicanos, "Artículo 16", *Diario Oficial de la Federación*, H. Cámara de Diputados, 5 de febrero de 1917, *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf*

[45] The Data Protection Commission (DPC), "Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China", Irlanda, 2 de mayo de 2025, *https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following*

las cláusulas contractuales fueran eficaces para garantizar que los datos personales de los usuarios del EEE, al no realizar las evaluaciones necesarias sobre el marco jurídico chino, que difiere significativamente de los estándares de protección de datos de la Unión Europea, especialmente en la Ley de Ciberseguridad y la Ley de Inteligencia Nacional China.

- Infracción del artículo 13(1)(f) del RGPD, al no informar adecuadamente a los usuarios sobre las transferencias de datos a terceros países, incluyendo China, ni sobre la naturaleza de los tratamientos realizados.

- Multa total: 530 millones de euros (45 millones por falta de transparencia y 485 millones por transferencias ilícitas de datos).

- TikTok debe adecuar sus operaciones de tratamiento de datos personales en un plazo de 6 meses o se suspenderán las transferencias de datos a China, así como demostrar que cualquier transferencia futura cumple con el nivel de protección exigido por la Unión Europea.

- TikTok inicialmente negó almacenar datos de usuarios del EEE en China, pero posteriormente admitió que una cantidad limitada de datos sí fue almacenada allí, lo cual agravó la situación y podría derivar en acciones regulatorias adicionales.

La decisión de la DPC refuerza la necesidad de que las empresas tecnológicas que operan en la Unión Europea respeten los altos estándares de protección de datos personales, garantizando transparencia y seguridad en las transferencias internacionales de datos. TikTok debe implementar cambios sustanciales para cumplir con la normativa europea y proteger adecuadamente los datos de sus usuarios.

Informe de la Comisión Federal de Comercio de los Estados Unidos (Federal Trade Commission *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*)[46].

En diciembre de 2020 la Comisión Federal de Comercio (FTC, por sus siglas en inglés) de Estados Unidos solicitó información a las nueve empresas más importantes en redes sociales y streaming de video (Amazon.com, Inc., Facebook, Inc. (ahora Meta Platforms, Inc.), YouTube LLC, Twitter, Inc. (ahora X), Snap Inc., ByteDance Ltd., (TikTok), Discord Inc., Reddit, Inc., y WhatsApp Inc.), para comprender mejor el impacto de estos servicios en los consumidores estadounidenses. El informe presentado en septiembre de 2024 analiza prácticas de recolección, uso y retención de datos, publicidad dirigida, uso de inteligencia artificial y algoritmos, tratamiento de menores y adolescentes, y cuestiones de competencia, donde surgieron varios hallazgos a resaltar:

- Las empresas recolectan y retienen grandes volúmenes de datos (de usuarios y no usuarios) con información personal, demográfica y de comportamiento, tanto en su plataforma como en fuentes externas, en su mayoría, sin políticas claras de eliminación de datos.

- La mayoría de estas empresas tienen modelos de negocio basados en publicidad dirigida, emplean algoritmos, análisis de datos e inteligencia artificial para el seguimiento y recopilación desmedida de datos sensibles, sin que los usuarios sean plenamente conscientes de ello.

- Las empresas no protegen adecuadamente a niños y adolescentes: suelen limitarse a cumplir con los requerimientos básicos de la Ley de Protección de la Privacidad Infantil en Línea (Children's Online Privacy Protection Rule, COPPA por sus siglas en inglés)[47] pero caen en incumplimiento ya que al generar los infantes y adolescentes perfiles

[46] Federal Trade Commission," A look behind the screens: Examining the data practices of social media and video streaming services", EUA, 18 de septiembre de 2024, *https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services*

[47] Children's Online Privacy Protection Rule ("COPPA"), *"*15 U.S.C. 6501–6505", *Federal Trade Commission,* EUA, 1998, *https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa*

son tratados como adultos, recolectando sus datos y sin restricciones específicas.

- El dominio del mercado por las grandes plataformas les permite imponer sus prácticas monopólicas de privacidad, creando barreras para nuevos competidores y reduciendo la calidad y privacidad de los servicios para los usuarios.

Resolución de la Segunda Sala de la Suprema Corte de Justicia de amparo en revisión sobre la recolección de datos de geolocalización[48].

El 29 de enero de 2025, la Segunda Sala de la Suprema Corte de Justicia de la Nación resolvió, por mayoría de tres votos contra uno, negar el amparo en revisión 74/2024 y validar la recolección masiva e indiscriminada de datos de geolocalización de personas usuarias de servicios de banca en línea en México. Esta decisión ha generado preocupación por sus implicaciones en la protección de datos personales y derechos fundamentales, por lo que me permito expresar los puntos más relevantes de la resolución:

- La Suprema Corte de Justicia consideró constitucional la obligación de recolectar, almacenar y entregar los datos de geolocalización de usuarios de la banca en línea, con el argumento central de que la geolocalización no constituye un dato personal sensible, porque “lo que se geolocaliza es el aludido dispositivo, no la persona” y, por lo tanto, no se afecta nuestra esfera más íntima.

- Esta postura contradice los estándares internacionales que reconocen la geolocalización como dato personal sensible, ya que es posible reconstruir rutinas, relaciones y actividades privadas, exponiendo a los usuarios a riesgos de vigilancia y afectación de su privacidad, ignorando la finalidad de la geolocalización bancaria, que es identificar y localizar a la persona, no solo al dispositivo.

[48] Red en Defensa de los Derechos Digitales R3D, “Ministras Batres, Esquivel y Pérez Dayán validan la geolocalización indiscriminada de usuarias de la banca en línea”, *Privacidad*, México, 4 de febrero de 2025, *https://r3d.mx/2025/02/04/ministras-batres-esquivel-y-perez-dayan-validan-la-geolocalizacion-indiscriminada-de-usuarias-de-la-banca-en-linea/*

- La decisión vulnera los derechos a la privacidad, protección de datos personales, presunción de inocencia, debido proceso y derecho de audiencia de millones de personas usuarias de la banca en línea.

- Si bien el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) desempeñó su papel fundamental como órgano garante en la supervisión y protección de los derechos de la titular de los datos personales, la resolución de la Suprema Corte de Justicia representa un retroceso en materia de protección de datos personales en México, al permitir la recolección y almacenamiento masivo de información sensible sin salvaguardas, priorizando intereses del sector financiero y de seguridad pública sobre los derechos fundamentales de las personas.

Capítulo 2

Análisis de intervención y comparativo de la protección de datos personales e inteligencia artificial.

Capítulo 2. Análisis de intervención, comparativos del Derecho a la Protección de Datos Personales e Inteligencia Artificial.

Este segundo capítulo describe la metodología como la base utilizada en la intervención, justificando la elección y presentando los objetivos del estudio. Se analiza la protección de datos personales a nivel internacional y en México, revisando antecedentes jurídicos y actuales. El estudio comparativo de los distintos países líderes en protección de datos e inteligencia artificial abordan los retos de privacidad y seguridad de la información, permitiendo comprender tanto el contexto local como las tendencias globales en regulación.

Metodología de intervención

Metodología es un vocablo que se genera a partir de tres palabras de origen griego: *meta* (más allá), *odos* (camino) y *logos* (estudio), por lo que el autor lo

manifiesta al *concepto que hace referencia al proyecto de investigación que permite fijar y lograr ciertos objetivos en el marco de un tema-problema en determinada área del conocimiento (unitaria, multidisciplinaria o transdisciplinaria)*[49]. Es fundamental, ya que ofrece un marco estructurado que orienta al investigador en cada una de las etapas del estudio, desde la planificación hasta el análisis de los resultados. Un diseño metodológico apropiado garantiza que los hallazgos sean fiables y replicables, lo que a su vez contribuye al avance del conocimiento en cualquier disciplina.

La metodología es un recurso concreto que deriva de una posición teórica y epistemológica (parte de la filosofía que trata de los fundamentos y los métodos del conocimiento científico), para la selección de caminos (métodos) y herramientas (técnicas) específicas de investigación[50]. Con la elección de la metodología adecuada se puede evitar la visión unidimensional, abstracta de la realidad para tomar consciencia de la naturaleza y de las consecuencias de los paradigmas que mutilan el conocimiento y desfiguran lo real[51].

La metodología es una vertiente del conocimiento… Esto es, toda ciencia tiene un método y/o una metodología, …entendemos por una metodología, en el ámbito de la investigación jurídica, a un conjunto de pasos o secuencias que deben cumplirse para llegar a metas u objetivos prefijados libremente por el investigador…[52], por lo que, este caso en particular, se consideran los métodos jurídico, inductivo y el comparado o analógico, ya que nos permite tomar el camino adecuado para generar un análisis de las acciones y el acompañamiento jurídico plasmado en la guía.

La metodología jurídica se refiere al estudio del método en el ámbito del derecho, abarcando todos los aspectos relacionados con la determinación de respuestas jurídicas a casos específicos. En términos generales, la metodología jurídica implica el análisis de cómo se establecen y aplican las normas jurídicas, así como la justificación de las decisiones legales a través de la argumentación[53]. Esta

[49] Zenteno Trejo, Blanca, Osorno Sánchez, Armando, "Elementos para el diseño de investigaciones jurídicas: Una perspectiva multidimensional", *Benemérita Universidad Autónoma de Puebla*, México, primera edición, agosto de 2015, p. 109.
[50] *Idem.*
[51] Zenteno Trejo, Blanca, Osorno Sánchez, Armando, *op. cit.*, p. 109.
[52] Witker Velásquez, Jorge, "Metodología de la Investigación Jurídica", *Universidad Nacional Autónoma de México*, México, primera edición, septiembre de 2021, *https://biblio.juridicas.unam.mx/bjv/detalle-libro/6818-metodologia-de-la-investigacion-juridica*
[53] *Idem.*

disciplina se enfoca en los procedimientos y esquemas utilizados para realizar actividades jurídicas, alcanzar objetivos legales y resolver conflictos legales de manera coherente y fundamentada, que derive en las soluciones más adecuadas a los problemas sociales de nuestra época y así poder adecuar el ordenamiento jurídico a las transformaciones y cambios sociales, de acuerdo a las palabras del Maestro Fix Zamudio. Para otorgar al ciudadano o usuario de las aplicaciones el acompañamiento y la información que le permitirá observar las normativas y regulaciones sobre la protección de derechos humanos y la protección de la esfera jurídica.

Método inductivo: de inducción (Del lat. inductĭo, -ōnis). 1. f. Acción y efecto de inducir. Se analizan solo casos particulares, cuyos resultados son tomados para extraer conclusiones de carácter general. A partir de las observaciones sistemáticas de la realidad se descubre la generalización de un hecho y una teoría. Se emplea la observación y la experimentación para llegar a las generalidades de hechos que se repiten una y otra vez[54].

La relevancia de este método es tal que podemos ejemplificarlo con el sistema jurídico del Common Law, por ejemplo, este sistema de naturaleza inductiva, parte del análisis de casos concretos para buscar precedentes aplicables, en ausencia de estos, se crea un nuevo precedente que servirá como regla general para futuros casos similares, la investigación se ha basado en una variedad de fuentes tecnológicas que, aunque no cuentan con el rigor de los estudios académicos formales, han aportado conocimientos valiosos y actualizados sobre el tema, dichos recursos, como blogs especializados en seguridad informática, foros de desarrolladores y sitios web de análisis de aplicaciones, ofrecen una perspectiva práctica y más cercana a los desafíos y oportunidades en el ámbito de la seguridad móvil.

Estos espacios virtuales permiten a expertos, entusiastas y usuarios comunes compartir sus experiencias, conocimientos y descubrimientos, por lo que, a través de la lectura de artículos y tutoriales, ha sido posible identificar las principales vulnerabilidades de las aplicaciones móviles, las técnicas utilizadas por los atacantes y las mejores prácticas para mitigar los riesgos, así como, concretar las numerosas recomendaciones de los propios desarrolladores, para establecer cuestionamientos

[54] Zenteno Trejo, Blanca, Osorno Sánchez, Armando, *op. cit.*, p. 117.

que sirvan como guía de acompañamiento en la descarga y manejo de los aplicaciones móviles. Por ejemplo, en el Proyecto Datávoros[55], que es un proyecto de investigación sobre la recolección de datos a través de aplicaciones móviles desarrolladas por gobiernos y empresas, así como, los blogs especializados como *Geeks for Geeks*[56] que han publicado un par de análisis exhaustivos sobre las prácticas de recopilación de datos de las aplicaciones más populares, sin hacer de lado las consultas en fuentes oficiales, que expresan información relacionada al tema, como la Comisión de Examen Económico y de Seguridad Estados Unidos-China[57], que publica artículos con información específica sobre seguridad en el uso de dichas aplicaciones.

Es importante destacar que, aun cuando las fuentes no cuentan con el respaldo de estudios académicos, su valor radica en la exposición de casos particulares, que al repetirse constantemente crean patrones de información actualizada de manera rápida y sencilla, y permiten llevar a generalizar las experiencias, lo que nos lleva a considerar en tercera instancia el *Método comparado o analógico. De comparación. (Del lat. comparatĭo, -ōnis). 1. f. Acción y efecto de comparar, que se refiere a la actividad mental lógica, presente en multitud de situaciones de la vida humana, que consiste en observar semejanzas y diferencias en dos o más objetos de estudio, también se puede entender como un procedimiento sistemático y ordenado para examinar relaciones, semejanzas y diferencias entre dos o más objetos o fenómenos observados, con la intención de extraer determinadas conclusiones[58].*

La ausencia de investigaciones formales y exhaustivas sobre el uso seguro de aplicaciones móviles y sus implicaciones en la privacidad constituye un desafío complejo, desde la rápida evolución del ecosistema móvil que dificulta que las investigaciones sean actuales y se mantengan vigentes, como la constante aparición de nuevas aplicaciones con funcionalidades y tecnologías emergentes, multiplicidad

[55] Organización Datavoros, “Aplicaciones de Redes Sociales – Análisis Técnico”*, Social TIC*, México, 5 junio de 2023, *https://datavoros.org/analisis-de-aplicaciones-de-redes-sociales/*

[56] Organización GeeksforGeeks, “Temu Review”, EUA, 1 de septiembre de 2023, *https://www.geeksforgeeks.org/temu-review/*

[57] U.S.-China Economic and Security Review Commission, “Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes”, *https://www.uscc.gov/research/shein-temu-and-chinese-e-commerce-data-risks-sourcing-violations-and-trade-loopholes*

[58] Zenteno Trejo, Blanca, Osorno Sánchez, Armando, *op. cit.*, p. 118.

de sistemas operativos, dispositivos y tiendas de aplicaciones, que impiden seguir el paso de la tecnología.

Las investigaciones siempre deben enriquecerse con perspectivas diversas, con puntos de vista alternos que converjan y generen conclusiones puntuales, que no se observe desde una sola óptica, que las diferencias sean puntos de convergencia, de objetividad, por lo que es preciso señalar que gran parte de la información a consultar proviene del lenguaje anglosajón, en traducciones o de fuentes en idioma inglés, que nos llevan a enriquecer y ampliar las perspectivas de análisis, por lo que es oportuno empatizar con el contexto de México, a forma de analogía y ejemplo el artículo, donde me permito hacer la traducción al español del título del autor: "La Decolonización de los Estudios Poscoloniales y los Paradigmas de la Economía Política: Transmodernidad, Pensamiento Decolonial, y Colonialismo Global"[59], de Ramón Grosfoguel, ya que el autor aborda la necesidad de decolonizar los estudios y los paradigmas de la economía política desde una perspectiva metodológica que desafié las estructuras de conocimiento tradicional, desarrolla una crítica al pensamiento social americano y a las estructuras de pensamiento moderno, que son consecuencia de pensamientos heredados por el continente europeo y que han sido impuestos por el poder político a través de la historia, por lo que es necesario mencionar los aspectos clave de su enfoque metodológico:

Análisis del Colonialismo. Donde la Real Academia de la Lengua Española define el concepto de *colonialismo* como el *régimen político y económico en el que un Estado controla y explota un territorio ajeno al suyo*, estructuras de poder y conocimiento que persisten hasta nuestros días y cómo las relaciones de poder continúan afectando las dinámicas sociales y económicas en el mundo actual. *Crítica Epistemológica*, Grosfoguel crítica a las teorías del conocimiento dominantes, aquellas que provienen de la modernidad eurocéntrica, y que posteriormente fueron heredadas en Norteamérica. Su metodología implica cuestionar las categorizaciones y conceptualizaciones para analizar la realidad social, sugiriendo que son insuficientes para entender las complejidades del mundo contemporáneo, especialmente desde la perspectiva de los pueblos considerados del tercer mundo.

[59] Grosfoguel, Ramón, "Decolonizing Post-Colonial Studies and Paradigms of Political-Economy: Transmodernity, Decolonial Thinking, and Global Coloniality", *Berkeley University of California*, EUA, 2011, *https://escholarship.org/uc/item/21k6t3fq*

Interdisciplinariedad, el enfoque interdisciplinario (sociología, antropología, economía y estudios culturales) dan apertura a los fenómenos sociales, como parte fundamental para superar la diferencias entre las economías, la política y los estudios culturales, permitiendo un análisis holístico de los fenómenos sociales. *Perspectiva Subalterna*, enfatiza la importancia de adoptar una perspectiva desde los pueblos del tercer mundo, es decir, desde las experiencias y conocimientos de aquellos que han sido históricamente marginados por el colonialismo y el eurocentrismo. *Transmodernidad y Pluriversalidad*, el primer concepto, como lo propone el autor, implica la coexistencia de múltiples modernidades y la aceptación de diversas formas de conocimiento, para fomentar el diálogo entre diferentes tradiciones culturales y epistemológicas, promoviendo una comprensión pluriversal que trascienda las limitaciones del pensamiento eurocéntrico, y se consideren las diversidades como factores específicos de cada región.

La metodología de Grosfoguel se centra en la crítica de las epistemologías dominantes, como la norteamericana, o la europea, de las herencias metodológicas y de las estructuras impuestas, busca promover un diálogo crítico que reconozca la diversidad de experiencias y conocimientos, abogando por un enfoque más inclusivo y pluralista en los estudios sociales y políticos, que no siempre se adaptan a las historias y a las situaciones, en este caso, de este país, que si bien estamos muy cerca del primer mundo, es necesario ofrecer una comprensión más cercana a la realidad social de México, analizar los casos en comparativa para comprender más a profundidad las diferencias, y así desmenuzar los factores culturales, económicos, sociales y políticos que generan las diferencia entre unos y otros.

Los desacuerdos sobre la gobernanza de datos y la privacidad pueden obstaculizar la colaboración en áreas críticas, para el desarrollo conjunto y la estandarización internacional. A medida que las naciones buscan proteger sus intereses, la posibilidad de cooperación entre estos se ve amenazada. Esto se ve expresado en la creciente rivalidad tecnológica entre Estados Unidos y China, donde cada país busca asegurar su lugar como líder en la innovación tecnológica. La disputa se ha intensificado con medidas como restrictivas en la exportación de tecnologías, lo que ha llevado a las naciones a acelerar los esfuerzos por eliminar los necesidad

de productos extranjeros en las cadenas de suministro industrial, por desgracia los avances son lentos y frenan el avance tecnológico[60].

El análisis de la legislación china sobre protección de datos requiere una perspectiva que vaya más allá del concepto occidental de privacidad, donde en la Unión Europea y México, así como Estados Unidos el término privacidad se vincula a derechos individuales y económicos sucesivamente, por ello, la aplicación de marcos legales occidentales al contexto chino puede generar puntos ciegos y no captar los objetivos, por lo que es importante analizar a fondo el contexto asiático, las diferencias entre los países anteriormente mencionados, y conocer los antecedentes que han dado paso al avance avasallador de China en el mundo digital, en el desarrollo de un marco jurídico robusto que vaya de la mano de la innovación y el desarrollo tecnológico.

Los principios constitucionales o valores liberales no son los principales fundamentos del régimen legal chino en protección de datos, sino la política de ciberseguridad e informatización, la cual es impulsada desde 2014 por el líder Xi Jinping, de donde surge el plan *Made in China 2025*[61], lanzado en 2015, busca dominar los sectores tecnológicos clave, convertir al país en una potencia cibernética y redefinir su rol en la economía global. Con un enfoque en diez industrias prioritarias: generación de tecnología de información de última generación, robótica avanzada, equipo avanzado de transporte ferroviario, equipos aeroespaciales, vehículos y equipos de bajo consumo energético, ingeniería marítima de alta tecnología, semiconductores, maquinaria agrícola, y por último biofarmacéutica y nuevos dispositivos médicos[62], con el objetivo de transformar al gigante asiático de una potencia manufacturera a un líder en innovación, donde las empresas no solo controlen la producción, sino también el diseño, el desarrollo de software y la propiedad intelectual en cadenas de valor críticas, reduciendo la dependencia de tecnologías extranjeras.

---

[60] Yong, Nicholas, "Cómo China consigue robarle sus secretos tecnológicos a Estados Unidos", *BBC News Mundo*, Reino Unido, 26 de enero de 2023, *https://www.bbc.com/mundo/noticias-internacional-64355527*

[61] Zamarrón, Israel, "Made in China 2025: así es el ambicioso plan tecnológico chino que amenaza el dominio de EU", *Revista Forbes*, México, 16 de marzo de 2023, *https://forbes.com.mx/made-in-china-2025-asi-es-el-ambicioso-plan-tecnologico-chino-que-amenaza-el-dominio-de-eu/*

[62] *Idem.*

La iniciativa ha intensificado la rivalidad tecnológica con Estados Unidos, donde el Congreso estadounidense ha expresado preocupación por el posible desplazamiento de su liderazgo en áreas como inteligencia artificial, tecnología 5G y los semiconductores, donde China pretende dominar estos últimos, como punto neurálgico.

> *En el contexto más amplio de la globalización, la transmisión de datos comerciales se ha convertido en una faceta integral de las operaciones diarias de las corporaciones multinacionales*[63]*.*

La creciente interdependencia entre la transmisión de datos comerciales y *el aumento de las preocupaciones por la seguridad nacional, acentuadas por la pandemia de COVID-19, la guerra de Rusia en Ucrania y la intensificación de las rivalidades geopolíticas*[64] han transformado los desafíos de la globalización en la era digital. Los flujos de información, que en el pasado eran vistos como simples facilitadores de las operaciones empresariales, ahora se consideran activos estratégicos con profundas implicaciones geopolíticas. Este cambio manifiesta cómo los gobiernos, las corporaciones nacionales y multinacionales manejan los datos, no solo como herramientas de registro, sino también como elementos críticos para la soberanía y la estabilidad económica.

Este nuevo paradigma ha transformado las plataformas digitales y aplicaciones tecnológicas en blancos estratégicos en un campo de batalla geopolítico. En este escenario, potencias como China y Estados Unidos se restringen mutuamente en el uso de herramientas tecnológicas, citando riesgos de ciberseguridad y manipulación de datos. Mientras tanto, la Unión Europea avanza con regulaciones como el Reglamento General de Protección de Datos (RGPD)[65], que busca garantizar el control ciudadano sobre la información personal. Sin embargo, esta falta de estandarización global lleva a los estados a priorizar estrategias unilaterales, limitando la interoperabilidad tecnológica a nivel mundial.

---

[63] Tian, Zhe, Zakaria, Aqib, Latif, Adam, “Bridging Digital Divides”, *op. cit.*, p. 02.

[64] Jakubik, Adam, Van Heuvelen, Elizabeth, “La Globalización Hoy”, *Fondo Monetario Internacional*, Estados Unidos, junio de 2024, *https://www.imf.org/es/Publications/fandd/issues/2024/06/B2B-Globalization-Today-Adam-Jakubik-and-Elizabeth-Van-Heuvelen*

[65] General Data Protection Regulation (GDPR), *European Union*, 27 April 2016, *https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng*

El desafío reside en equilibrar la protección de intereses nacionales con la cooperación económica, evitando que la desconfianza mutua descarrile décadas de cooperación beneficiosa entre ambas naciones, donde los datos pueden fungir como un puente o una barrera, donde el manejo transparente podría fomentar confianza, pero la politización excesiva amenaza con polarizar el mundo en bloques tecnológicos incompatibles, donde ya no exista la neutralidad en los datos, la gestión positiva de la información puede definir no solo el comercio internacional exitoso, sino la estabilidad global en un mundo donde la seguridad nacional y la economía digital son dos caras de la misma moneda.

Análisis en protección de datos personales e inteligencia artificial

Principales instrumentos normativos internacionales

Convenio No.108 del Consejo de Europa: Para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal[66].

El Convenio fue concebido inicialmente como un instrumento de carácter universal, ha evolucionado desde sus primeras recomendaciones no vinculantes hasta convertirse en un tratado internacional obligatorio para los Estados Parte. Su ámbito de aplicación trasciende las fronteras europeas, consolidándose como el único instrumento jurídicamente vinculante de alcance global dedicado a la protección de los datos personales de los ciudadanos. Ha sido ratificado por 47 Estados miembros del Consejo de Europa, otros Estados no miembros del Consejo, que son Parte del Convenio son Uruguay, Mauricio, Senegal y Túnez, Argentina, México, Burkina Faso, Cabo Verde y Marruecos, y en acorde a lo establecido en él me permito expresar las características principales:

- Dividido en 7 capítulos en los cuales se establecen las reglas generales, los principios básicos para proteger los datos personales, los flujos transfronterizos de datos, la cooperación entre las Partes, el Comité Consultivo, las Enmiendas y la Clausulas Finales.

[66] Convenio No.108 del Consejo de Europa: Para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, *Consejo de Europa*, Francia, 28 de enero de 1981, *https://rm.coe.int/16806c1abd*

- Establece los Principios básicos para la protección de datos: el compromiso de las partes, la calidad de los datos (leal y legítimamente, finalidad, pertinencia, exactitud, conservación limitada), categorías particulares de datos, garantías complementarias y seguridad de los datos, excepciones y restricciones, sanciones y recursos, y la protección más amplia.

- Establece un Comité Consultivo constituido por un representante y un suplente de cada Parte y la opción de contar con observadores de cualquier Estado miembro del Consejo de Europa que no sea Parte del Convenio.

- En forma de complemento los Estados Parte acordaron un Protocolo Adicional que fue adoptado por el Comité de Ministros en mayo de 2001.

Al ratificar este instrumento, México cuenta con una herramienta internacional que permite el intercambio efectivo y seguro de la información, además de fortalecer las relaciones comerciales al establecer un flujo transfronterizo con reglas homogéneas entre los miembros[67], lo que en teoría resuelta muy atractivo para nuestro país, pero en la práctica estamos muy retrasados en las adecuaciones a las normativas mexicanas para ajustarnos al Convenio y tener la capacidad de garantizar la completa protección del flujo transfronterizo de datos.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos Personales.

Surge del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos del 1 al 6 de junio de 2003, celebrado en La Antigua, Guatemala. Se establece como:

> *"Foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos*

[67] Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, "Convenio 108 permite a México el intercambio efectivo y seguro de información", *Foro INFOEM*, México, 2 de agosto de 2021, *https://www.infoem.org.mx/es/contenido/noticias/convenio-108-permite-méxico-el-intercambio-efectivo-y-seguro-de-información*

necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho."[68]

Características principales de los Estándares:

- Busca responder a las necesidades y exigencias nacionales e internacionales del derecho a la protección de datos personales en la sociedad del conocimiento y la información.

- Buscan ser el modelo de referencia para que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, para la regulación futura en el derecho de protección de datos, así como para aquellos países que aún no cuentan con estas normativas, o como referente para la modernización y actualización de las legislaciones existentes .

- Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y fuera de sus fronteras (cooperación internacional entre las autoridades).

- Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento para la libre circulación y favorecer las actividades comerciales.

- Integrado por: Una Presidencia, actualmente ostentada por la Unidad Reguladora y de Control de Datos Personales de Uruguay (URCDP-AGESIC), una Secretaría Permanente¸ representada por la Agencia Española de Protección de Datos (AEPD), y Tres Vocalías (INAI-México, SIC-Colombia y AAIP-Argentina).

[68] Red Iberoamericana de Protección de Datos, "Historia de la Red Iberoamericana de Protección de Datos", Guatemala, 2024, *https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd*

Su objetivo principal es establecerse como un marco regulatorio de referencia para los países que aún no cuentan con normativa de protección de daros personales o en la actualización de lo que ya cuentan y así lograr la estandarización de los parámetros de las naciones parte.

Memorándum de Montevideo sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes[69]

El escrito manifiesta las recomendaciones adoptadas en el *Seminario Derechos, Adolescentes y Redes Sociales en Internet*, realizado en Montevideo en el año 2009, con la participación de diversos expertos en el tema. Su ámbito de aplicación se establece en el documento considerando a América Latina y el Caribe como regiones donde se están realizando esfuerzos, dentro de la diversidad social, cultural, política y normativa existente para lograr un consenso irracionalidad de modo tal de establecer un equilibrio entre la garantía de los derechos y la protección ante los riesgos en la Sociedad de la Información y el Conocimiento, y en acorde a lo establecido en él me permito expresar las características principales:

- Es un documento que reúne a representantes de la industria, medios de comunicación, legisladores, jueces, padres de familia, organizaciones de la sociedad civil y autoridades en educación con el objetivo de fomentar el diálogo y definir estrategias para la protección de los menores en Internet.

- Utiliza como referente normativo la Convención de las Naciones Unidas sobre los Derechos del Niño (CDN).

- Establece como valor el derecho a la vida que toda su sociedad que se considere democrática debe respetar.

- Busca asegurar la autonomía de los individuos para decidir los alcances de su vida privada, por lo que debe limitarse tanto el poder del estado como de

[69] Memorándum De Montevideo, Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, *Instituto de Investigaciones Jurídicas* UNAM, México, 2019, *https://archivos.juridicas.unam.mx/www/bjv/libros/12/5667/12.pdf*

organizaciones privadas, de cometer intromisiones ilegales o arbitrarias, particularmente en la información personal de niñas, niños y adolescentes.

Las Cinco Recomendaciones del Memorándum:

1. *Recomendaciones para los Estados y entidades educativas para la prevención y educación de niñas, niños y adolescentes* (obligación de proveer información y fortalecer capacidades de los progenitores y personas responsables, sobre los riesgos a los que se enfrentan los niñas, niños y adolescentes en los ambientes digitales).

2. *Recomendaciones para los estados sobre el marco legal* (la creación, reforma o armonización normativa debe hacerse tomando como consideración primordial el interés superior de niñas, niños y adolescentes, todo esto considerando que se requiere el desarrollo de una normativa nacional).

3. *Recomendaciones para la aplicación de las leyes por parte de los estados* (las autoridades deben garantizar que los procesos judiciales y administrativos sean acorde a las necesidades de los menores).

4. *Recomendaciones en materia de políticas públicas* (el interés superior del niño sea considerado como principio rector de toda medida que se tome la materia, particularmente en las políticas públicas para regular las redes sociales digitales).

5. *Recomendaciones para la industria* (enfocada a las empresas que proveen los servicios de acceso a internet, hoy desarrollan aplicaciones por redes sociales digitales, los cuales deben comprometerse en materia de protección de datos personales y la vida privada particularmente de niñas niños y adolescentes).

Desafortunadamente, en México todavía no se cuenta con normativa o reglamento específico para regular la protección en el entorno digital de niñas, niños y adolescentes, si bien la Ley General de Protección de Niñas, Niños y Adolescentes, en su Capitulo Décimo Séptimo establece el derecho a la intimidad personal y familiar, y a la protección de los datos personales de los menores, los salvaguarda, pero no

por completo y de no de forma integral como lo haría una regulación especializada en el tema.

Análisis comparativo de las legislaciones sobre protección de datos personales: perspectivas desde Estados Unidos, China y la Unión Europea

> *Las cuestiones relacionadas con los datos, incluidos el flujo de datos, la protección de la privacidad y la inteligencia artificial generativa, se están convirtiendo cada vez más en factores fundamentales para dar forma a la relación entre Estados Unidos y China (Fudan-Harvard China-U.S. Young Leaders Dialogue Spring 2024: Bridging Digital Divides: Navigating Data Governance and Security in the U.S.-China Technological Arena[70]).*

La transferencia de datos entre países es crucial para las operaciones comerciales y el desarrollo tecnológico, pero las diferencias en las regulaciones al recopilar, compartir y almacenar datos han causado tensiones, debido a que el marco legal de cada nación refleja sus valores y prioridades, lo que resalta las diferencias culturales, políticas y económicas de cada país.

La legislación sobre datos en Estados Unidos, China y la Unión Europea presenta diferencias significativas, en la primer nación no existe un marco regulatorio federal integral para la protección de datos, a diferencia de los mencionados. Estados Unidos depende de un conjunto de leyes federales específicas, órdenes ejecutivas y regulaciones a nivel estatal para supervisar la protección de datos, por ejemplo, la Orden Ejecutiva 14034, emitida en junio de 2021 por la administración Biden[71], es una política clave que rige la recopilación de datos de consumidores estadounidenses por parte de softwares o aplicaciones móviles extranjeros, la cual busca clarificar y evaluar las políticas existentes relacionadas con los riesgos que ciertas aplicaciones extranjeras pueden representar para la privacidad y seguridad de los datos de los ciudadanos, especialmente aquellas que podrían estar bajo la influencia de gobiernos extranjeros considerados adversarios.

---

[70] Tian, Zhe, Zakaria, Aqib, Latif, Adam, *op. cit.*

[71] Executive Order 14034 - Protecting Americans' Sensitive Data From Foreign Adversaries, *The White House*, EUA, 09 de junio de 2021, *https://www.presidency.ucsb.edu/documents/executive-order-14034-protecting-americans-sensitive-data-from-foreign-adversaries*

La orden mencionada adopta un enfoque más amplio para los *adversarios* en general, pero es imposible desmarcar le inclinación hacia las aplicaciones chinas, debido a que, esta orden deroga las órdenes ejecutivas 13942, 13943 y 13971, que fueron específicas para aplicaciones chinas como TikTok y WeChat, entre otras.

En términos de legislación federal, el país de las barras y las estrellas se ha enfocado en abordar las problemáticas de sectores concretos con leyes específicas, como la Ley de Protección de la Privacidad Infantil en Internet (COPPA)[72], la Ley Gramm-Leach-Bliley (GLBA)[73], la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)[74], la Ley de Derechos Educativos y Privacidad de la Familia (FERPA)[75], y la Ley de Privacidad de 1974[76], donde a pesar de los esfuerzos expresados en estas leyes no cuentan con un marco legal coherente que unifique su aplicación, lo que resulta en una protección de datos inconsistente y fragmentada.

La Ley de Modernización de la Revisión del Riesgo de Inversión Extranjera (FIRRMA)[77], introducida en 2018, amplió las competencias del Comité de Inversión Extranjera en los Estados Unidos (CFIUS) para revisar inversiones extranjeras en empresas estadounidenses que puedan representar riesgos para la seguridad nacional.

La falta de una legislación federal integral, holística, adecuada tiene un efecto negativo en las transferencias internacionales de datos, dado que no hay un marco de protección de datos coherente y sólido, y las empresas pueden encontrar obstáculos al transferir información personal desde otros países, lo que deriva en la

[72] Children's Online Privacy Protection Rule ("COPPA")", *op. cit.*

[73] Gramm-Leach-Bliley Act ("GLBA"), "15 U.S.C. §§ 6801–6827", *Federal Trade Commission*, EUA, 1999, *https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act*

[74] Health Insurance Portability and Accountability Act ("HIPAA"), "Public Law 104-191", *U.S. Department of Health & Human Services*, EUA, 1996, *https://www.hhs.gov/hipaa/for-professionals/privacy/index.html*

[75] Family Educational Rights and Privacy Act ("FERPA"), "20 U.S.C. § 1232g; 34 CFR Part 99", *U.S. Department of Education*, EUA, 1974, *https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html*

[76] Privacy Act of 1974, "5 U.S.C. § 552a", *U.S. Department of Justice*, EUA, 1974, *https://www.justice.gov/opcl/privacy-act-1974*

[77] Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA"), "Public Law 115-232", *Senate of the United States*, EUA, 2018, *https://www.congress.gov/bill/115th-congress/house-bill/5841/text*

creación de acuerdos específicos, como el Privacy Shield[78], donde se han enfrentado desacuerdos legales, generando incertidumbre en el flujo de datos entre los Estados Unidos y la Unión Europea.

La protección de la privacidad se vuelve esencial a medida que los datos se convierten en un recurso cada vez más valioso, por ende, las preocupaciones han aumentado las regulaciones y las propuestas de nuevos instrumentos jurídicos, como ejemplo, la Ley de Privacidad del Consumidor de California (CCPA)[79], donde el estado norteamericano ha sido pionero en la implementación de leyes de privacidad más estrictas, para otorgar a los consumidores más control sobre la recopilación de datos, la reclamación de daños y perjuicios por violaciones de datos.

La ausencia de un marco regulatorio federal sólido en Estados Unidos muestra un panorama regulador fragmentado y potencialmente menos seguro para los consumidores, no obstante, la cooperación entre ellos y China, en materia de gobernanza de datos, podría beneficiarse de la reciente renovación del *Acuerdo de Cooperación Científica y Tecnológica*[80], por otros cinco años, proyectado antes de la llegada de Donald Trump a la presidencia, que incluye nuevas disposiciones sobre seguridad y protección de la propiedad intelectual, como parte de los esfuerzos de ambas administraciones por estabilizar las relaciones y considerando que China ha expresado su disposición para trabajar con la administración entrante para fortalecer el diálogo y la cooperación, lo que podría abrir oportunidades para abordar desafíos comunes en la gobernanza de datos.

La Protección de Datos en China

Entre 1994 y 2011, China estableció las bases de su modelo actual de protección de datos[81], impulsado por la rápida transformación digital y la necesidad de gestionar riesgos emergentes graves. Durante este período, el país equilibró la

[78] U.S. Department of Commerce, “Privacy Shield Program Overview”, EUA, 2017, *https://www.privacyshield.gov/ps/program-overview*
[79] California Consumer Privacy Act (CCPA), *op. cit.*
[80] El Economista, “Como cada 5 años: EU y China renuevan su acuerdo de cooperación tecnológica”, México, 13 de diciembre de 2024, *https://www.eleconomista.com.mx/internacionales/5-anos-eu-china-renuevan-acuerdo-cooperacion-tecnologica-20241213-738261.html*
[81] *Idem.*

modernización tecnológica con mecanismos de control, anticipando desafíos que hoy son centrales en su gobernanza de datos.

En la década de 1990, se lanzaron los Proyectos Dorados[82], que digitalizaron sectores claves como: impuestos, seguridad pública y comercio, optimizando la digitalización estatal, pero también normalizando la recolección masiva de datos ciudadanos, lo que derivó en una infraestructura de vigilancia sin precedentes, que terminó exponiendo las vulnerabilidades por la falta de un marco regulatorio sólido, con casos de fugas de información sensible y venta ilegal de bases de datos.

A diferencia de Europa o Estados Unidos, donde la protección de datos se cimentó en los derechos fundamentales, en China la privacidad se utilizó como un instrumento de gobernanza, subordinada a los intereses públicos, lo que sentó las bases para un régimen de seguridad nacional y control social, creando una sinergia indisociable de la protección de datos ciudadana y la soberanía cibernética nacional, donde la privacidad se convirtió en una herramienta de protección, pero no del ciudadano, sino de la estabilidad política.

Entre 2012 y 2018, el país asiático buscó consolidar un marco integral de protección de datos, un proceso marcado por contradicciones entre su ambición regulatoria y las realidades de una economía digital en crecimiento exponencial, bajo el liderazgo de Xi Jinping[83]. Este período reflejó el control del Partido Comunista en el flujo de información social-política, sin desacelerar la innovación tecnológica, siendo ésta clave para la proyección global. La explosión del internet móvil alcanzó una penetración del 70% de la población, lo que impulsó a gigantes como Alibaba y Tencent, cuyos modelos tienen como base explotar datos de usuarios, a generar hábitos de consumo, ubicaciones y patrones médicos[84], que generó un mercado negro de datos. Durante este período se establecieron precedentes clave: como

[82] Stanford Project Torfix, “The Great Firewall of China: Background, Stanford University”, EUA, 1 de junio de 2011, *https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html*

[83] Israel Zamarrón, “Made in China 2025”*, op. cit.*

[84] Creemers, Rogier, “China’s Emerging Data Protection Framework, Journal of Cybersecurity”, *Journal of Cybersecurity Oxford Academic*, Reino Unido, Volume 8, 24 de agosto de 2022, *https://academic.oup.com/cybersecurity/article/8/1/tyac011/6674794*

ejemplo, la Ley de Ciberseguridad[85], que priorizó la seguridad nacional sobre los derechos individuales.

En un movimiento estratégico para reafirmar su soberanía en la era digital, China promulgó en 2021 la Ley de Seguridad de Datos (DSL) y la Ley de Protección de Información Personal (PIPL), marcando su enfoque hacia la gobernanza de datos, estos instrumentos legislativos no solo formalizan el valor de los datos como un *factor de producción esencial para el desarrollo*, *al igual que la tierra, el capital y el trabajo*, sino que a la par refleja una ambición mayor: establecer el nuevo orden digital que equilibre el crecimiento económico con la seguridad nacional y el control estatal[86].

La Ley de Protección de Información Personal representa un acontecimiento con dos vertientes en la gobernanza de datos: un intento de equilibrar la protección de la privacidad ciudadana pero sin soltar el control estatal y la seguridad nacional en un contexto digital en rápida evolución[87]. Inspirada en el Reglamento General de Protección de Datos de la Unión Europea. La ley establece que la recolección de datos personales debe ser consensuada, a la par incluye excepciones por razones de interés público, muy similar al contexto de México (por -seguridad nacional-), y de la misma forma que nuestro país es de aplicación tanto a las empresas privadas, como a las entidades gubernamentales que manejan información personal. Conjuntamente, la PIPL tiene implicaciones extraterritoriales, lo que significa que puede aplicarse a empresas extranjeras que ofrezcan productos o servicios a ciudadanos chinos, tal como se observa en legislaciones como el Reglamento General de Protección de Datos de la Unión Europea.

La Ley de Seguridad de Datos (DSL) redefine la gobernanza de datos en el país, estableciendo un marco regulatorio sin precedentes que trasciende la mera protección de la privacidad individual, erigiéndose como un instrumento de soberanía

[85] Creemers, Rogier, Webster, Graham, Triolo, Paul, "Translation: Cybersecurity Law of the People's Republic of China", *Stanford University*, EUA, junio 29 de 2018, *https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/*

[86] Creemers, Rogier, *China's Emerging Data Protection Framework*, *op cit.*, p. 05.

[87] Creemers, Rogier, *China's Emerging Data Protection Framework*, *op cit.*, p. 06.

digital que busca asegurar el control sobre la información estratégica para el desarrollo económico y la estabilidad política del país[88].

El alcance de la DSL es amplio, abarcando no solo la información personal, sino cualquier tipo de dato que no esté categorizado como secreto de Estado, que le otorga al gobierno asiático un control exhaustivo sobre la información en poder de entidades gubernamentales, empresas y otros actores dentro del país, permitiendo una supervisión general de los flujos de datos y una la capacidad de gestionar de forma centralizada los riesgos asociados.

En particular, introduce una categoría nueva llamada *Datos fundamentales del Estado* (guojia hexin shuju)[89], que abarca datos relacionados con la seguridad nacional, aspectos críticos de la economía y la vida pública, lo que implica que estos datos se evalúan según su nivel potencial de riesgo y su relevancia para los intereses del estado. La Ley refuerza la obligación de las organizaciones de cooperar con las entidades de seguridad pública nacional, lo que significa que la legislación busca equilibrar la protección de datos con la necesidad de garantizar que las autoridades puedan cumplir con sus responsabilidades.

La ley tiene como objetivo crear un ecosistema que no solo proteja a las personas, sino que también impulse el desarrollo de la economía digital del país. Esto sugiere que no se trata únicamente de una ley de seguridad, sino también de un instrumento de política industrial, lo que nos conecta directamente con el enfoque norteamericano, que aunque se basa en la protección de la privacidad, tiene una base comercial. Al final, ambas naciones comparten más aspectos de lo que podrían admitir.

Desde el comienzo del siglo XXI, China ha estado construyendo un modelo de protección de datos único, moldeado por sus propias circunstancias y necesidades, de la mano de la naturaleza vigilante del régimen chino, donde el proceso ha sido gradual, cauteloso y fue incrementando acorde a las dificultades derivadas de la reestructuración administrativa en la gobernanza cibernética[90], pero, todavía resta un largo camino donde la investigación podría manifestar las diferencias, similitudes,

[88] *Idem.*
[89] Creemers, Rogier, *China's Emerging Data Protection Framework*, *op cit.*, p. 07.
[90] Creemers, Rogier, *China's Emerging Data Protection Framework*, *op cit.*, p. 08.

fortalezas y debilidades de estos diversos enfoques entre las potencias, para comenzar a identificar áreas viables de conflicto entre naciones.

Los últimos cinco años, el gigante rojo ha intensificado la creación de leyes para la protección de datos, con la promulgación de la Ley de Protección de Información Personal (PIPL, por sus siglas en inglés)[91] y la Ley de Seguridad de Datos (DSL, por sus siglas en inglés)[92], estos instrumentos legales han marcado una nueva era en la regulación de datos en el país asiático[93], con implicaciones tanto internas como para entidades extranjeras, especialmente aquellas con fuertes lazos digitales con la República Popular, por lo que el análisis comparativo resulta crucial para comprender el impacto y su potencial influencia en otras legislaciones internacionales.

Aunque el gigante asiático tardó en adoptar normas específicas de protección de datos, la rápida expansión de los servicios digitales y los incidentes de seguridad de alto perfil impulsaron la creación de un marco legal integral.

La administración del Presidente Joe Biden realizó investigaciones exhaustivas a empresas como *China Mobile*, *China Telecom* y *China Unicom* debido a sus supuestas conexiones con los servicios de inteligencia chinos y el potencial acceso no autorizado a datos estadounidenses a través de sus negocios en la nube y en la red. Estas medidas emplean regulaciones más estrictas a las empresas a cumplir con para asegurar la protección de los datos, impuestas por los legisladores y reguladores de telecomunicaciones norteamericanos[94].

Las restricciones y la presión política influyen negativamente en la viabilidad de las empresas chinas en el mercado estadounidense, porque los consumidores o las autoridades ven a estas empresas como una amenaza a la seguridad, lo que afecta sus ingresos y su capacidad para competir en el mercado. Esto se refleja en la

---

[91] Personal Information Protection Law, *National People's Congress of the People's Republic of China*, China*,* 22 de mayo de 2022*, https://personalinformationprotectionlaw.com/*

[92] Data Security Law Popular Republic of China*, National People's Congress of the People's Republic of China,* China Law Translate*,* China, 25 de junio de 2021, *https://www.chinalawtranslate.com/en/datasecuritylaw/*

[93] Creemers, Rogier, *China's Emerging Data Protection Framework*, *op cit.*, p. 05.

[94] El Observador, "Estados Unidos pone más empresas de comunicación chinas bajo la lupa: desconfianza por el uso de los datos", Uruguay, 25 de junio 2024, *https://www.elobservador.com.uy/estados-unidos/estados-unidos/estados-unidos-investiga-china-telecom-y-china-mobile-internet-y-los-riesgos-la-nube-n5947856*

creciente desconfianza hacia aplicaciones y plataformas chinas, como DeepSeek, que ha sido criticada por enviar datos de usuarios estadounidenses a servidores en China[95].

Este clima regulatorio puede desalentar la inversión y la innovación, ya que las empresas enfrentan obstáculos legales cada vez más complejos y restrictivos, además, de la inclusión de empresas chinas en listas negras por su supuesta colaboración con las Fuerzas Armadas Chinas[96], donde han incrementado las tensiones comerciales y políticas entre ambos países durante la transición entre las administraciones de Trump y Biden, intensificando el debate y la revisión de las políticas hacia China.

Análisis comparativo de las regulaciones de Inteligencia Artificial (Estados Unidos, China y la Unión Europea)

En la inteligencia artificial, especialmente las tecnologías generativas (que pueden crear contenido nuevo a partir de datos existentes), ocupan un lugar central en el debate sobre el futuro tecnológico entre las potencias mundiales, compitiendo encarnizadamente para liderar en este campo emergente, la IA generativa[97], que plantea preguntas sobre el uso ético en la propiedad de los datos y los derechos de autor, agregando tensión a la relación internacional entre China y Estados Unidos.

El gigante asiático ha lanzado un ambicioso plan nacional de inteligencia artificial con el objetivo de convertirse en el líder mundial en IA para 2035[98], mientras que el país de las barras y las estrellas ha hecho lo mismo, con la implementación de políticas de para impulsar la investigación y el desarrollo de la IA, pero en un afán más combativo que propositivo, lo que hace visible que ambos países están compitiendo para asegurar el dominio en este campo emergente, en la búsqueda de

[95] Burgess, Matt, Newman, Lily Hay, “DeepSeek’s Popular AI App Is Explicitly Sending US Data to China”, *Wired*, EUA, 27 de enero de 2025, *https://www.wired.com/story/deepseek-ai-china-privacy-data/*

[96] Forbes, “China critica la decisión de EU de incluir a más de 20 empresas en su lista negra”, *Forbes México*, México, 1 de febrero de 2024, *https://forbes.com.mx/china-critica-la-decision-de-eu-de-incluir-a-mas-de-20-empresas-en-su-lista-negra/*

[97] Shih, Silva, Lin, Yixuan, “Made in China 2025: How China Thrives Despite Tech Sanctions”, *CommonWealth Magazine*, Taiwán, vol. 809, 15 de octubre de 2024, *https://english.cw.com.tw/article/article.action?id=3789*

[98] Zamarrón, Israel, *Made in China 2025*, *op cit*.

crear localmente sus propios suministros y dejar de depender de la importación de materiales extranjeros.

Cada región también ha adoptado enfoques distintos, en la Unión Europea aprobaron la primera norma jurídica integral sobre inteligencia artificial a nivel internacional: el Reglamento de Inteligencia Artificial[99], basado en un enfoque de riesgo, clasificando los sistemas de IA según su nivel de seguridad, con requisitos más estrictos para aquellos que presentan un alto riesgo, para evitar los sesgos, la discriminación y las lagunas en la rendición de cuentas, y así promover la innovación y fomentar la adopción de la IA[100].

Estados Unidos, no cuenta con un instrumento legal integral sobre inteligencia artificial, por lo que ha promovido un entorno regulatorio centrado en el comercio, que permite un enfoque más flexible para la innovación y la adaptación a nuevas tecnologías, como ejemplo, la *Orden Ejecutiva 14110:* "*Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*" del Ex presidente Joe Biden, que introduce un conjunto de directrices éticas para garantizar que las agencias federales utilicen la inteligencia artificial de manera responsable y confiable, enfocándose en aspectos clave como: la responsabilidad institucional, la claridad informativa, la justicia algorítmica, la protección de sistemas y la protección de datos personales[101], es importante destacar que esta regulación no afecta a las empresas privadas ni a las aplicaciones militares, limitándose a las operaciones gubernamentales.

Algoritmos: Implicaciones y Aplicaciones

Las aplicaciones chinas han experimentado un crecimiento acelerado, superando a las norteamericanas en términos de popularidad y uso. Los objetivos con los que fueron creadas estas plataformas y sus algoritmos permiten conectar a personas de todo el mundo, facilitando la interacción global y el intercambio cultural.

---

[99] Reglamento de Inteligencia Artificial de la Unión Europea, *Consejo Europeo*, 29 de abril de 2025, *https://www.consilium.europa.eu/es/policies/artificial-intelligence/#what*

[100] *Idem.*

[101] Executive Order 14110 - Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Federal Register, EUA, 30 de octubre de 2023, *https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence*

aplicaciones como Temu y TikTok, han demostrado ser capaces de adaptarse rápidamente a las preferencias de los jóvenes norteamericanos, gracias a su avanzado algoritmo y al extenso contenido les otorgan una ventaja competitiva significativa en el mercado global, pero también han generado desafíos significativos en términos de privacidad y seguridad de datos.

La prohibición de TikTok en Estados Unidos ha llevado a muchos usuarios a buscar alternativas chinas, lo que ha aumentado la visibilidad y el uso de plataformas como *RedNote (Xiaohongshu, 小红书), volviéndola la aplicación más descargada en ese país* [102]. Esta aplicación tiene una particularidad, como lo establece en su artículo la Dra. Beatriz Juárez plantea que es una App que respeta las *Disposiciones de gestión de las recomendaciones algorítmicas en servicios de información de Internet* de China, que específicamente el artículo 18 establece que los proveedores de servicios de recomendación algorítmica tienen la obligación de proteger a los menores de edad conforme a la ley, facilitarles acceso a información beneficiosa para su salud física y mental, asimismo, prohíbe la difusión de contenido dañino y prohíbe el uso de algoritmos que generen adicción en línea.

Colectivismo vs. Exclusivismo

El algoritmo utilizado en TikTok ha sido objeto de críticas y controversias, especialmente en cuanto a su posible uso para difundir propaganda del Partido Comunista Chino mediante la manipulación del algoritmo con información tendenciosa, lo que podría aumentar la visibilidad de ciertos temas y generar adicción en los usuarios, así fue expresado en la entrevista en TED, del CEO de TikTok, Shou Chew[103], en la réplica, Chew explicó que la diferenciación entre su algoritmo y el de las demás redes sociales está en la ideología, en la estructura y en la construcción de la misma, esto quiere decir, que la misión de la plataforma (“Inspire creativity and to bring joy”, “Inspirar creatividad y aportar alegría”) expresa el objetivo de la creación del algoritmo, comparó TikTok con plataformas como Facebook e Instagram, que fueron construidas con la premisa - personas que sigan a personas-, la interacción entre personas famosas y sus seguidores, donde las personajes famosos logran gran

[102] Juárez Aguilar, María Beatriz, *op. cit.*
[103] TED, TikTok CEO Shou Chew on Its Future — and What Makes Its Algorithm Different, *YouTube*, EUA, 21 de abril de 2023, *https://youtu.be/7zC8-06198g?si=hkagahxLwF-j6dmC*

aceptación, que expresa un mensaje de exclusividad, y la aplicación china construyó su algoritmo centrado en las necesidades de las personas “del día a día”, ofreciendo una ventana para el descubrimiento, conectando a las personas a través del talento y el contenido, teniendo como base la ideología colectiva, lo que puede sonar en extremo romantizado, pero concuerda con el objetivo de su creación. Asimismo, Chew destacó que el algoritmo funciona de manera sencilla, guiándose por el reconocimiento de patrones basados en las señales de los intereses y aspiraciones de los usuarios, como los videos que observan, los "me gusta" y los contenidos compartidos, utilizando datos que cada usuario ha autorizado previamente.

Otro tema controvertido es la jurisdicción del almacenamiento de información, donde los datos generados por la compañía china en territorio norteamericano son procesados por el gigante texano Oracle, a pesar de que en Beijing se encuentra la sede de ByteDance[104], han surgido preocupaciones bien fundamentadas, ya que empleados de la empresa matriz en Beijing fueron sorprendidos vigilando a periodistas estadounidenses que investigaban la aplicación, monitorearon las fuentes y documentos compartidos.

Sin embargo, no debemos olvidar que incidentes similares ocurren en todas partes del mundo, no olvidemos el famoso caso de Cambridge Analytica[105], que reveló la explotación indebida de datos de hasta 87 millones de perfiles de usuarios de Facebook, cuya información se utilizó para dirigir mensajes diseñados para influir en la decisión de los votantes, la manipulación en la información en el entorno digital no es una cuestión de oriente u occidente, sino un tema de responsabilidad y respeto a la privacidad de las personas.

El Derecho a la Protección de Datos Personales en México.

En México, los antecedentes del derecho de la protección de datos personales tienen la primera referencia en la abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en el 2002[106], que fue la primera en

[104] Global Data Plc, *op. cit.*
[105] Amnistía Internacional, ““El gran hackeo”: Cambridge Analytica es sólo la punta del iceberg”, 24 julio 2019, *https://www.amnesty.org/es/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/*
[106] Parra Noriega, Luis, “El Derecho a la Protección de Datos Personales en México”, *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales - Guía Orientadora “La*

contemplar apartados específicos en materia de protección de datos personales en el sector público[107], sentando el precedente para la reforma al artículo 6º constitucional en el año 2007, donde se estableció el reconocimiento de la protección de la vida privada y del término "datos personales"[108].

Sin embargo, la protección de datos personales se restableció como derecho hasta la reforma de los artículos 16 y 73 en el año 2009[109], donde se reconoce a las empresas como responsables del tratamiento de los datos y nacen los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), y finalmente en el 2010 se promulgó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que estableció el marco específico para la protección de los datos personales que obran en posesión de los particulares.

El incremento desmesurado en el uso de dispositivos electrónicos y aplicaciones móviles han revolucionado la forma en que interactuamos con la tecnología, debido a la generación, recopilación y procesamiento de grandes cantidades de datos personales. Los grandes avances desarrollados en las aplicaciones móviles se han enfocado en cuestiones de innovación tecnológica y mercadotecnia, dejando de lado los derechos a la protección de datos personales y la privacidad.

Las aplicaciones móviles funcionan con base en la captación de estos datos para la creación de perfiles que identifiquen a los usuarios, por lo que es prioridad hacer consciencia e informar a las personas sobre las afectaciones que genera dar un clic en los términos y condiciones, y en las políticas de privacidad que permiten el uso indiscriminado de la información personal.

La guía práctica busca informar, acompañar y hacer conscientes a las personas en la protección de sus datos personales al utilizar aplicaciones móviles,

---

Protección de Datos Personales en Plataformas Digitales", México, 2021, *https://www.infoem.org.mx/doc/publicacionesExternas/20211025_GuiaOrientadoraProteccionDatosPersonales.pdf*

[107] Reyes Krafft, Alfredo, "Ley Federal de Protección de Datos en Posesión de Particulares Comentada, Capitulo I.", *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, México, 2019, *https://www.cide.edu/wp-content/uploads/2021/03/LFPDPPP-Comentada_digital.pdf*

[108] Parra Noriega, Luis Gustavo, *op cit.*, p. 18.

[109] *Idem.*

este caso en particular, la aplicación Temu, la más descargada en México y Estados Unidos.

Capítulo 3

Cuestionario de Evaluación de Seguridad

Capítulo 3. Cuestionario de Evaluación de Seguridad.

El cuestionario de seguridad se constituye como una herramienta esencial que permite a los usuarios evaluar de manera consciente, minuciosa y crítica los posibles riesgos asociados antes, durante y después del proceso de descarga de aplicaciones móviles. Este instrumento va más allá de una simple lista de verificación: facilita la identificación de aspectos clave y sensibles, tales como los permisos que la aplicación solicita, el origen y la legitimidad del desarrollador, así como las vulnerabilidades conocidas que podrían comprometer la seguridad del dispositivo y la privacidad del usuario.

El cuestionario de seguridad extendido no solo funciona como herramienta técnica para la evaluación de riesgos, sino también promueve la reflexión responsable sobre las prácticas digitales cotidianas, al incentivar a los usuarios a adoptar una postura preventiva y crítica frente a las tecnologías con las que interactúan, lo que contribuye a la detección temprana de posibles amenazas y fomentar la conciencia más profunda sobre la importancia de mantener hábitos para proteger la información personal y la integridad digital.

Cuestionario de seguridad extendido para descarga de aplicaciones móviles en dispositivos electrónicos.

Previo a la descarga:

¿Va a descargar la aplicación de fuentes oficiales?

Descargar aplicaciones solo de tiendas oficiales como Google Play Store[110], Huawei App Gallery[111] (Android), o App Store[112] (iOS), es la forma más segura, ya que implementan mecanismos de seguridad para filtrar aplicaciones maliciosas.

Las tiendas oficiales requieren que los desarrolladores sigan estándares de calidad y seguridad, brindando la posibilidad de denunciar y atender irregularidades.

¿Ha comprobado que el desarrollador de la aplicación sea TEMU, y coincida con el icono y las capturas de pantalla oficiales?

Para verificar que el desarrollador de la aplicación TEMU sea legítimo y coincida con el logotipo y las capturas de pantalla oficiales, siga estos pasos:

Verifique el nombre del desarrollador:

- Al abrir la aplicación en Google Play Store, Huawei App Gallery en la sección "Asistencia de la aplicación" o en la sección “Ficha Técnica” de App Store, verifique que el nombre del desarrollador coincida exactamente con "Temu Inc." o “WhaleCo, Inc.”.

Compruebe el logotipo y las capturas de pantalla:

- Compare el logotipo de la aplicación en la tienda con el icono oficial de Temu que puede encontrar en el sitio web oficial o en otras fuentes confiables.
- Examine las capturas de pantalla de la aplicación en la tienda para asegurarse de que coincidan con el diseño y la interfaz de la aplicación oficial de TEMU.

Tenga cuidado con aplicaciones no oficiales:

- Evite descargar la aplicación TEMU de fuentes no oficiales, como sitios web de terceros o tiendas de aplicaciones no autorizadas. Estas aplicaciones pueden ser falsificaciones o contener malware.

[110] Google Play Store, EUA, 2025, *https://play.google.com/store/apps*
[111] Huawei App Gallery, EUA, 2025, *https://appgallery.huawei.com/#/Featured*
[112] Apple Store, EUA, 2025, *https://www.apple.com/mx/app-store/*

¿He leído las reseñas y comentarios de otros usuarios para tener una idea de la confiabilidad y experiencia de la aplicación?

Revise las calificaciones y los comentarios de usuarios:

- Antes de descargar la aplicación, revise las calificaciones y comentarios de los usuarios para detectar posibles problemas relacionados con la aplicación o la autenticidad del desarrollador.

¿He verificado la fecha de publicación de la aplicación y la frecuencia de actualizaciones?

Para verificar la información en la aplicación TEMU, siga estos pasos:

Verifique la fecha de publicación y actualizaciones:

- Ingrese a la tienda oficial de aplicaciones Google Play Store o Huawei App Gallery, busque la aplicación TEMU, y en la sección "Asistencia de la aplicación", y en la sección “Información de la app” encontrará la fecha de publicación original de la aplicación. En ambas encontrará la fecha de la última actualización.

- Ingrese a la tienda oficial de aplicaciones App Store, busque la aplicación TEMU, en la sección "Novedades", encontrará el “Historial de versiones” y las actualizaciones enlistadas por fecha y número de versión.

- Mantenga la aplicación actualizada con la última versión para garantizar que tenga acceso a las últimas funciones, correcciones de errores y mejoras de seguridad, ya que las actualizaciones a menudo incluyen parches de seguridad críticos que protegen su dispositivo y sus datos de vulnerabilidades conocidas.

Verifique la configuración de la aplicación:

- Abra la aplicación y acceda a la configuración. En la mayoría de los casos va a encontrar una opción para habilitar las actualizaciones automáticas, para que no tenga la necesidad de hacerlo manualmente.

¿He descargado la aplicación exclusivamente desde el sitio web oficial de TEMU?

Lo más seguro es descargar la aplicación directamente del sitio web oficial en lugar de utilizar fuentes no oficiales. Algunas razones clave son:

a) El sitio web oficial ofrece instrucciones claras para descargar la aplicación de forma segura.

b) Sitios web no oficiales podrían contener versiones modificadas de la aplicación con funcionalidades adicionales no deseadas.

c) Descargar de sitios web oficiales ayuda a evitar riesgos como malware, spyware u otras amenazas que podrían estar presentes en versiones no oficiales.

Conexión vía página web:

¿Ha considerado usar la versión web en lugar de la aplicación?

Si tiene preocupaciones sobre la recopilación de datos, considere utilizar el sitio web para tener un mayor control sobre la privacidad:

Mayor seguridad:

- La aplicación ha sido objeto de críticas por su recopilación excesiva de datos del usuario, lo que genera dudas sobre la privacidad. La versión web ofrece mayor control sobre la información que se comparte, ya que no requiere la instalación de una aplicación en su dispositivo.

- Se han reportado casos de malware y spyware ocultos en aplicaciones móviles, y al utilizar la versión web elimina este riesgo, ya que se accede a través de un navegador web seguro.

Comodidad y accesibilidad:

- La versión web se puede usar en cualquier dispositivo con conexión a internet, incluyendo computadoras, laptops, tabletas y smartphones. Esto ofrece mayor flexibilidad y comodidad que la aplicación.

Mejores Prestaciones:

- La versión web suele ofrecer opciones de búsqueda más avanzadas que la aplicación, lo que permite a los usuarios encontrar productos específicos con mayor facilidad.
- Facilita la comparación de diferentes productos, lo que puede ser útil para tomar decisiones de compra informadas.

Sin actualizaciones:

- No requiere descargas ni actualizaciones, lo que ahorra espacio de almacenamiento en su dispositivo.

Si bien la aplicación TEMU ofrece grandes ventajas, como la capacidad de reconocimiento de usuario, sección de favoritos, y la de realizar compras rápidas y fáciles desde su teléfono móvil, la versión web ofrece menor exposición de sus datos personales, comodidad, funciones adicionales y una experiencia más segura.

Es importante destacar que la decisión final sobre qué plataforma utilizar depende de las preferencias, necesidades y consideraciones individuales de cada usuario.

Observar la barra de direcciones del navegador:

¿Ha verificado qué el certificado de seguridad del sitio web sea válido y que la conexión sea “https”?

Existen diversas maneras de verificar la validez del certificado de seguridad de un sitio web:

- Un sitio web con certificado SSL válido muestra un candado verde o un ícono de "sitio seguro" en la barra de direcciones.

El certificado SSL[113] (Secure Sockets Layer) es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada entre un servidor

[113] Kaspersky Lab, “Qué es un certificado SSL: definición y explicación”, *https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate*

web y un navegador web. Debe ser emitido por una Autoridad de Certificación de confianza y estar presente en la computadora del usuario final para que el navegador muestre que la conexión es segura.

- La URL del sitio debe comenzar con "https://" en lugar de "http://".

El Hyper Text Transfer Protocol Secure[114], es un protocolo de comunicación seguro que se utiliza para transferir datos entre un navegador web y un servidor web de forma encriptada. Esto es especialmente importante cuando se transmiten datos sensibles como información personal, contraseñas o datos financieros.

Revisar los detalles del certificado:

1. Haga clic en el ícono de candado o "sitio seguro" en la barra de direcciones.
2. Seleccione la opción "Ver certificado" o "Detalles del certificado".
3. Verifique lo siguiente: que el nombre del dominio coincide con el nombre del sitio web, y el certificado está vigente.

Seguridad del dispositivo:

¿Mi dispositivo tiene un sistema operativo actualizado con las últimas correcciones de seguridad instaladas?

Asegúrese de que su dispositivo tenga un software antivirus o de seguridad actualizado para detectar posibles amenazas, es muy importante mantener su sistema operativo actualizado con las últimas correcciones de seguridad contra malwares, virus y otras amenazas cibernéticas, ya que estas incluyen parches críticos que corrigen vulnerabilidades de seguridad, por lo que no se debe deshabilitar las actualizaciones automáticas ya que pueden poner en riesgo su dispositivo y sus datos personales. Las actualizaciones de seguridad ayudan a proteger la información personal sensible, como contraseñas, datos financieros y archivos privados contenidos en el sistema operativo y así evitar accesos no autorizados o filtraciones de datos.

[114] The Cyber Security Agency of Singapore (CSA), “What is HTTPS? Hypertext Transfer Protocol Secure”, Singapur, 20 de enero de 2025, *https://www.csa.gov.sg/Tips-Resource/internet-hygiene-portal/information-resources/https*

Los desarrolladores de software descubren constantemente vulnerabilidades y errores en los sistemas operativos, que los ciberdelincuentes aprovechan para crear malware, virus y otras amenazas que pueden robar información personal, dañar archivos o tomar el control de su dispositivo. Las actualizaciones no solo incluyen correcciones de seguridad, sino también mejoras de rendimiento y estabilidad. Estas mejoras pueden hacer que su dispositivo funcione más rápido, sea más eficiente y tenga menos errores.

¿Tengo un antivirus de confianza instalado y actualizado en mi dispositivo?

- Los antivirus modernos ofrecen protección al instante, lo que significa que pueden analizar y bloquear amenazas de forma instantánea mientras usa el dispositivo.
- Esto le protege contra las últimas amenazas emergentes, incluso antes de que tengan la oportunidad de dañar su dispositivo.
- Un antivirus de confianza puede detectar y eliminar el malware de su dispositivo, evitando que cause daños, robo de información personal o interrumpir el funcionamiento normal de tu sistema.
- Los ataques de phishing[115] intentan engañarle para que revele información personal o financiera, como contraseñas o números de tarjetas de crédito, a través de correos electrónicos, sitios web o mensajes falsos, el antivirus con protección antiphishing puede ayudarle a identificar y evitar estos sitios web peligrosos.
- Los virus y otras amenazas de malware evolucionan constantemente, por lo que es importante tener un antivirus que se actualice regularmente con las últimas definiciones.

[115] Microsoft Corporation, "¿Qué es el phishing?", *Seguridad de Microsoft*, 2025, *https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing*

- Saber que tiene un antivirus de confianza actualizado en su dispositivo le brinda tranquilidad y le permite usar internet y su dispositivo con mayor seguridad.

Permisos de la aplicación:

¿Ha revisado los permisos que solicita la aplicación antes de aceptar la descarga? ¿Ha evitado consentir permisos no esenciales para el funcionamiento de la aplicación?

Los permisos específicos que solicita la aplicación Temu pueden variar ligeramente dependiendo de su dispositivo y la versión de la aplicación. Sin embargo, en general, Temu solicita los siguientes permisos:

Permisos esenciales:

- Almacenamiento: Este permiso es necesario para que la aplicación pueda almacenar datos en tu dispositivo, como imágenes de productos, información de tu cuenta y datos de compra.
- Cámara: Este permiso puede ser necesario para que pueda tomar fotos de productos o usar la función de escaneo de códigos QR de la aplicación.
- Micrófono: Este permiso puede ser necesario para que pueda usar la función de búsqueda por voz de la aplicación.
- Ubicación: Este permiso puede ser necesario para que la aplicación le muestre ofertas y recomendaciones personalizadas según tu ubicación.

Permisos adicionales:

- Contactos: Este permiso puede ser necesario para que la aplicación pueda acceder a su lista de contactos para encontrar amigos que también usen la aplicación.
- Teléfono: Este permiso puede ser necesario para que la aplicación pueda verificar su número de teléfono o para que pueda usar la función de llamadas dentro de la aplicación.

- SMS: Este permiso puede ser necesario para que la aplicación pueda enviarle mensajes SMS con información sobre pedidos u ofertas.

Es importante tener en cuenta que:

- Puede revisar y administrar los permisos que ha otorgado a Temu en cualquier momento en la configuración de su dispositivo.
- No es obligatorio otorgar todos los permisos solicitados por la aplicación para que funcione. Sin embargo, algunas funciones pueden no estar disponibles al negar ciertos permisos.
- Debe leer la política de privacidad de Temu para comprender cómo se recopilan, utilizan y comparten sus datos.

Recomendaciones:

- Se recomienda otorgar a Temu solo los permisos que considere estrictamente necesarios para el uso que le dará a la aplicación. Si tiene dudas sobre algún permiso en particular, no lo otorgue y contacte el servicio de soporte de Temu para más información.
- Revise la política de privacidad de Temu antes de otorgar cualquier permiso.

¿He concedido solo los permisos que son estrictamente necesarios para que la aplicación funcione correctamente?

Los ajetreos de la vida diaria complican el tomarse el tiempo para el análisis necesario en cada una de las descargas de aplicaciones tecnológicas, es de suma importancia concienciar al momento de realizar descargas móviles y prácticamente en todas las interacciones en la red que requieran de su consentimiento y otorgamiento de información, los datos personales son suyos, cuídelos.

Existen algunas estrategias que puedes seguir para tener una mejor idea de qué permisos son necesarios:

- En la tienda de aplicaciones (Google Play Store, Huawei App Gallery o App Store) se debe proporcionar información sobre los permisos que solicita y por

qué son necesarios para su optimo funcionamiento, preste atención a las redacciones vagas o genéricas, pueden ser una señal de ser una aplicación dañina.

- Compare los permisos que solicita la aplicación con los de otras aplicaciones similares, el exceso de permisos más que otras aplicaciones similares no es buena señal.
- Si el desarrollador tiene una reputación cuestionable o ha creado aplicaciones en el pasado que han sido problemáticas, es posible que esta aplicación también solicite permisos innecesarios.

- Si una aplicación necesita un permiso sospechoso en particular, es mejor no concedérselo.
- Siempre puede desinstalar la aplicación si descubre que necesita permisos que no está cómodo otorgando.

Datos personales:

¿Consultó la política de privacidad de la aplicación y comprende cómo se recopilan, utilizan y comparten sus datos personales?

Lea la política de privacidad de Temu[116] para entender qué datos recopila y cómo los utiliza. Tenga en cuenta que se ha informado que la aplicación puede acceder a muchos datos personales.

Para el óptimo funcionamiento, la aplicación solicita a los usuarios el consentimiento para recopilar sus datos de contacto como nombre, apellido, correo electrónico, dirección de facturación, número de teléfono, además, información demográfica, esto quiere decir; sexo, ciudad, estado, código postal y país de residencia, así como su fotografía, nombre de usuario y contraseña, información de pago y sus enlaces de redes sociales, prácticamente, lo que hace la mayoría de aplicaciones.

[116] WhaleCo Inc., “Temu - Política de privacidad”, EUA, 12 de mayo de 2025, *https://www.temu.com/mx/privacy-and-cookie-policy.html*

Lo que hace diferente a Temu, es que con su consentimiento obtiene:

- **Información de terceros:** accede a fuentes de vendedores, fuentes públicas (agencias gubernamentales y plataformas de redes sociales), proveedores de datos, y socios de marketing y terceros (Cookies).

- **Accede a su lista de contactos.**

- **Recopilación automática de datos:** la empresa, sus proveedores de servicios y socios comerciales pueden registrar automáticamente tu computadora o dispositivo móvil: tipo de sistema operativo, tipo de dispositivo móvil, fabricante, modelo, especificaciones técnicas del equipo, IP e IMEI, compañía del dispositivo móvil, etc.

- **Datos de actividad en línea:** las páginas que visitó, tiempo que pasó conectado, el sitio web que visitó antes de entrar al servicio, horarios y otros datos más.

- **Datos de ubicación:** sus datos de ubicación general: desde su computadora a través de la dirección IP, hasta la ubicación exacta de su móvil.

Expresamente, la aplicación explica en su política de privacidad que al consentir la descarga la aplicación obtiene del usuario la autorización de compartir toda la información con quien ellos consideren un “socio comercial”, en pocas palabras, con el mejor postor comercial.

Pregunta sin respuesta:

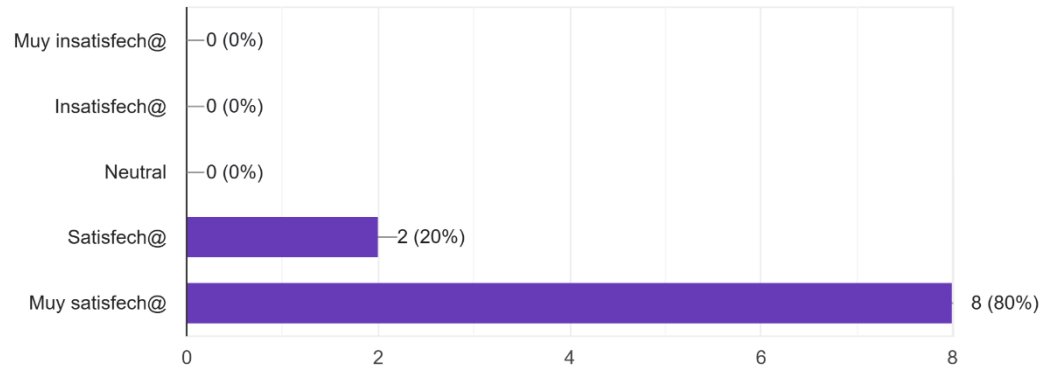
¿Ha considerado que las ofertas o promociones son tan exageradamente buenas para generar margen de ganancia a la compañía?, ¿y qué la mercadotecnia, en su totalidad, va enfocada a la descarga de la aplicación?

Evaluación del Cuestionario:

Con base en el análisis anterior, se proponen las siguientes preguntas para evaluar si el cuestionario fue útil o no:

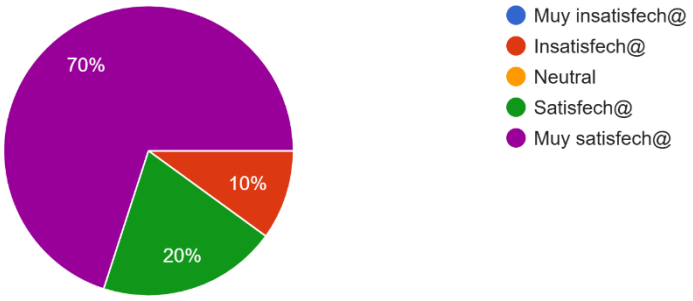
1. ¿Considera que las preguntas del cuestionario le ayudaron a identificar riesgos antes de descargar la aplicación TEMU?

10 respuestas



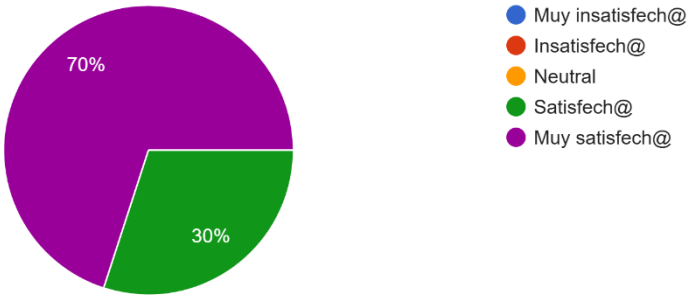
2. ¿Le resultaron claras las instrucciones para verificar la legitimidad del desarrollador de la aplicación?

10 respuestas



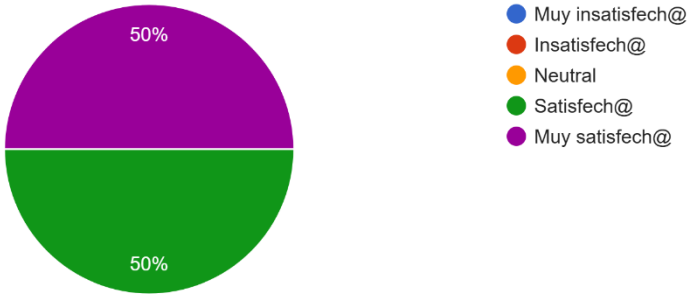
3. ¿Las recomendaciones sobre leer reseñas y verificar actualizaciones le parecieron relevantes para evaluar la confiabilidad de TEMU App?

10 respuestas



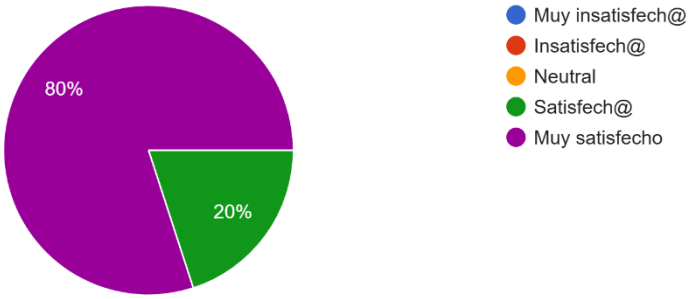
4. ¿La información sobre los permisos solicitados por TEMU le ayudó a tomar decisiones más informadas sobre su privacidad?

10 respuestas



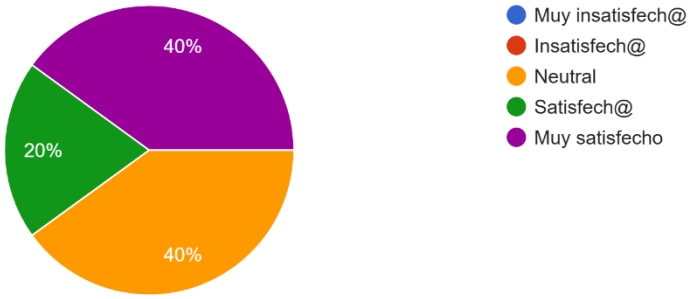
5. ¿Le pareció útil la alternativa propuesta de usar la versión web en lugar de descargar la aplicación?

10 respuestas



6. ¿Después de leer el cuestionario, realizó alguna acción adicional, como actualizar su sistema operativo o instalar un antivirus?

10 respuestas



Las respuestas reflejan varias conclusiones:

- Dentro de los entrevistados, uno de los participantes consideró que la información otorgada para verificar la legitimidad del desarrollador es insuficiente.
- En relación a la reflexión sobre realizar una acción posterior con la protección de un antivirus no fue exitosa, lo que causa desacierto debido a que la información fue dedicada para la concienciación de la seguridad, pero los usuarios, al menos el 40% no consideran importantes la instalación del antivirus.

Conclusiones Generales

La captación masiva de datos personales en las aplicaciones de comercio electrónico es un fenómeno que tiene profundas consecuencias sociales, económicas y políticas. Cada segundo, este monstruo voraz crece sin medida debido a la desinformación y el desinterés de las personas al compartir su información. Es así, que surge la guía, por la necesidad de concienciar y educar sobre la gestión responsable y el mal uso de la información privada, la recopilación excesiva de información está resultando en afectaciones a la probidad, fama y reputación de las personas, facilita la comisión de delitos informáticos y la creación de perfiles personales en extremo detallados, que convertirán la privacidad en un lujo inalcanzable.

Dedicar tiempo al análisis en la protección de su seguridad y privacidad es fundamental al usar cualquier aplicación móvil, por lo que este cuestionario de seguridad va enfocado en brindarle un acompañamiento, en forma de guía detallada, para evaluar los riesgos potenciales y tomar medidas informadas al descargar y usar cualquier aplicación, adoptar un enfoque preventivo y consciente le ayudará a minimizar las vulnerabilidades y proteger su información personal.

La recopilación desmedida de datos personales permite, en situaciones de mal uso, la creación de perfiles detallados de los ciudadanos, lo que pone en vulnerabilidad a la población, que puede resultar en estados de vigilancia masiva, invasión a la privacidad personal, manipulación en el ejercicio de la democracia y el desgaste de la confianza en las instituciones. Al informar y capacitar a las personas sobre el ejercicio de los derechos a la información y la protección de la privacidad, así como los riesgos asociados, da pie a una sociedad más responsable y consciente, por ende, a una de mayor exigencia en la transparencia y la responsabilidad en el manejo de los datos personales por parte de los gobiernos y las empresas.

En el futuro, sin lugar a dudas, las personas se arrepentirán de haber otorgado información personal sin medida. La creciente dependencia de la tecnología y la automatización con la inteligencia artificial en el manejo de la información puede llevar a una pérdida de autonomía en las decisiones y a una mayor desigualdad social. Por lo que es vital mantener actualizada la información respecto a las experiencias, expresiones y necesidades que surjan del estudio de las aplicaciones móviles, buscando seguir de cerca los pasos agigantados de los avances tecnológicos, por lo que considero, este trabajo como un inicio de una sinergia imprescindible, así como el análisis continuo de las fortalezas, oportunidades, debilidades y amenazas que están y surgirán en los diversos sistemas jurídicos de las diversas naciones, en constante evolución. Todo este proceso ha sido una experiencia muy enriquecedora, al tener la oportunidad de observar, analizar, comparar y juzgar como los sistemas jurídicos del *Common Law*, el sistema jurídico *Romano Germánico* y el sistema jurídico *Socialista* con características chinas, se contraponen en enfoques de forma, pero en el fondo tienen amplias y profundas convergencias, y cómo los valores y expectativas sociales, políticas y económicas de las naciones siempre son las base del pensamiento que las guía y las acompaña en su evolución.

Para el desarrollo de este trabajo se seleccionaron dos casos prácticos con enfoques y alcances contrastantes, lo que permitió enriquecer el análisis sobre la protección de datos personales en la aplicación móvil Temu.

Por un lado, el caso de **TikTok** fue elegido debido a la enorme cantidad de información disponible y su constante presencia en el debate público y regulatorio internacional. La empresa ByteDance se ha mantenido en el "ojo del huracán" por sus prácticas de manejo de datos personales, lo que ha generado abundantes investigaciones, reportes y resoluciones – como la reciente multa impuesta por la Comisión de Protección de Datos de Irlanda –. Esta visibilidad facilitó el acceso a fuentes confiables y actualizadas, permitiendo un análisis a profundidad y respaldado por evidencia sólida.

Por otro lado, el caso de **Oxxo Smart Grab and Go** representa un reto metodológico distinto. Al tratarse de una innovación reciente en el contexto mexicano, la información pública es escasa y restringida. Para su análisis fue necesario realizar una búsqueda exhaustiva, invirtiendo horas de indagación en la red y consultando diversas fuentes para reunir datos relevantes. Este esfuerzo busca abrir brecha en un tema novedoso, sobre el cual no se han encontrado estudios integrales previos en el país, aportando así un enfoque original y pionero.

La combinación de ambos casos, así como los informes y la resolución referida permitieron contrastar realidades: por un lado, el escrutinio internacional y los pocas investigaciones formales sobre una aplicación global; y por el otro, el desafío de investigar un caso nacional emergente y con información a cuenta gotas. Esto enriquece la comprensión de los retos y oportunidades en la protección de datos personales, y subraya la importancia de analizar tanto los ejemplos ampliamente documentados como aquellos que apenas comienzan a surgir en el entorno digital mexicano.

Bibliografía

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO DE URUGUAY, "¿Qué entendemos por entorno digital?", *Construyendo ciudadanía en entornos digitales. Punto de partida*, Uruguay, capítulo 3, 2025, *https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/construyendo-ciudadania-entornos-digitales-punto-partida/ construyendo-4#*

AIFI INC., "Privacy Policy – Applicants", EUA, 23 de febrero de 2024, *https://aifi.com/privacy-policy-for-applicants/*

AMAZON MÉXICO, "Condiciones de Uso", *https://www.amazon.com.mx/gp/help/customer/display.html?nodeId=GLSBYFE9MGKKQXXM*

ANIMAL POLÍTICO, "Entrevista OXXO Grab & Go", *YouTube*, México, 15 de marzo de 2023, *https://www.youtube.com/watch?v=9saVFTvZkTs&ab_channel=AnimalPol%C3%ADtico*

APPLE INC., Apple Store, EUA, 2025, *https://www.apple.com/mx/app-store/*

APPLE INC., "Apple Reinvents the Phone with iPhone", *Apple UK and Ireland Public Relations,* United Kingdom, 09 January 2007, *https://www.apple.com/uk/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/*

CASTAGNA, Tobias, "Technical Security Analysis Mobile App Temu", *National Test Institute for Cibersecurity,* Suiza, versión 1.0, diciembre 2024, *https://www.ntc.swiss/hubfs/temu-security-analysis-ntc-en.pdf*

Children's Online Privacy Protection Rule ("COPPA")", "15 U.S.C. 6501–6505", *Federal Trade Commission*, EUA, 1998, *https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa*

Constitución Política de los Estados Unidos Mexicanos, *Diario Oficial de la Federación*, H. Cámara de Diputados, 5 de febrero de 1917, *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf*

Convenio No.108 del Consejo de Europa: Para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, *Consejo de Europa*, Francia, 28 de enero de 1981, *https://rm.coe.int/16806c1abd*

EL OBSERVADOR, "Estados Unidos pone más empresas de comunicación chinas bajo la lupa: desconfianza por el uso de los datos", Uruguay, 25 de junio 2024, *https://www.elobservador.com.uy/estados-unidos/estados-unidos/estados-unidos-investiga-china-telecom-y-china-mobile-internet-y-los-riesgos-la-nube-n5947856*

EXECUTIVE ORDER 14034 - Protecting Americans' Sensitive Data From Foreign Adversaries, *The White House*, EUA, 09 de junio de 2021, *https://www.presidency.ucsb.edu/documents/executive-order-14034-protecting-americans-sensitive-data-from-foreign-adversaries*

EXECUTIVE ORDER 14110 - Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Federal Register, EUA, 30 de octubre de 2023, *https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence*

FEDERAL TRADE COMMISSION, ”A look behind the screens: Examining the data practices of social media and video streaming services”, EUA, 18 de septiembre de 2024, *https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services*

FIX-ZAMUDIO, Héctor, *Metodología, Docencia e Investigación Jurídicas*, Porrúa, México, 1997, p. 240.

FORBES, “China critica la decisión de EU de incluir a más de 20 empresas en su lista negra”, *Forbes México*, México, 1 de febrero de 2024, *https://forbes.com.mx/china-critica-la-decision-de-eu-de-incluir-a-mas-de-20-empresas-en-su-lista-negra/*

General Data Protection Regulation (GDPR), *European Union*, 27 April 2016, *https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng*

GLOBALDATA, “Beijing ByteDance Technology Co Ltd: Locations”, United Kingdom, 2025, *https://www.globaldata.com/company-profile/beijing-bytedance-technology-co-ltd/locations/*

GONZÁLEZ, Abel, “Douyin, la versión de TikTok exclusiva para China”, *Asilo Digital*, Venezuela, 20 de junio de 2021, *https://www.asilodigital.com/douyin-version-china-tiktok/*

GONZÁLEZ, Fernanda, “TikTok se compromete a eliminar los datos de usuarios de EE UU para evitar la prohibición en el país”, *Wired*, México, 23 de marzo de 2023, *https://es.wired.com/articulos/tiktok-se-compromete-a-eliminar-los-datos-de-usuarios-de-ee-uu*

GOOGLE LLC, Google Play Store, EUA, 2025, *https://play.google.com/store/apps*

GOOGLE LLC, “Oxxo Smart Tec Grab & Go”, *Google Play Store*, 2025, *https://play.google.com/store/apps/details?id=io.aifi.autocheckout.oxxoo&pcampaignid=web_share*

GRIZZLY RESEARCH LLC, “We believe PDD is a Dying Fraudulent Company and its Shopping App TEMU is Cleverly Hidden Spyware that Poses an Urgent Security Threat to U.S. National Interests”, Estados Unidos, 2023, *https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/*

GROSFOGUEL, Ramón, “Decolonizing Post-Colonial Studies and Paradigms of Political-Economy: Transmodernity, Decolonial Thinking, and Global Coloniality”, *Berkeley University of California*, EUA, 2011, *https://escholarship.org/uc/item/21k6t3fq*

GRUPO FEMSA, “Aviso de Privacidad Integral para clientes”, México, febrero de 2024, *https://www.oxxo.com/aviso-de-privacidad-integral*

GRUPO FEMSA, “Comunicado de Prensa: OXXO abre la primera tienda Grab & Go, con un sistema totalmente digital y sin fricciones”, México, 10 febrero de 2023, *https://www.femsa.com/es/sala-de-prensa/comunicado/oxxo-abre-la-primera-tienda-grab-go-con-un-sistema-totalmente-digital-y-sin-fricciones/*

HUAWEI TECHNOLOGIES CO., LTD, Huawei App Gallery, EUA, 2025, *https://appgallery.huawei.com/#/Featured*

IBM, “¿Qué es el malware?”, *Think*, International Business Machines, México, 14 de abril de 2022, *https://www.ibm.com/mx-es/think/topics/malware*

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS, “Convenio 108 permite a México el intercambio efectivo y seguro de información”, *Foro INFOEM*, México, 2 de agosto de 2021, *https://www.infoem.org.mx/es/contenido/noticias/convenio-108-permite-méxico-el-intercambio-efectivo-y-seguro-de-información*

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, “Guía para el tratamiento de datos biométricos”, México, primera edición, marzo de 2018, *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf*

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, “La Importancia del INAI en la Protección de Datos Personales (PDP)”, México, *https://micrositios.inai.org.mx/todasytodos/?page_id=426*

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, “¿Qué es el INAI?”, México, *https://home.inai.org.mx/?page_id=1626*

JAKUBIK, Adam, Van Heuvelen, Elizabeth, “La Globalización Hoy”, *Fondo Monetario Internacional*, EUA, junio de 2024, *https://www.imf.org/es/Publications/fandd/issues/2024/06/B2B-Globalization-Today-Adam-Jakubik-and-Elizabeth-Van-Heuvelen*

JUÁREZ AGUILAR, María, “RedNote, TikTok y las nuevas fronteras del desafío chino”, *dpl news*, México, 3 febrero de 2025, *https://dplnews.com/rednote-tiktok-y-las-nuevas-fronteras-del-desafio-chino/*

KASPERSKY LAB, *“Qué es un certificado SSL: definición y explicación”,*

https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

Ley Federal De Protección De Datos Personales En Posesión De Los Particulares, *Diario Oficial de la Federación*, H. Cámara de Diputados, México, 20 de marzo de 2025, *https://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp.htm*

Memorándum De Montevideo, Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, *Instituto de Investigaciones Jurídicas* UNAM, México, 2019, *https://archivos.juridicas.unam.mx/www/bjv/libros/12/5667/12.pdf*

MICROSOFT CORPORATION, "¿Qué es el phishing?", *Seguridad de Microsoft*, 2025, *https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing*

MOBILE PHONE MUSEUM, "Nokia 6110", *Phone detail, https://www.mobilephonemuseum.com/phone-detail/nokia-6110*

NORD VPN, ¿Qué es spyware?, *Blog ciberseguridad*, *https://nordvpn.com/es/blog/que-es-spyware/*

ORGANIZACIÓN DATAVOROS, "Aplicaciones de Redes Sociales – Análisis Técnico", *Social TIC*, México, 5 junio de 2023, *https://datavoros.org/analisis-de-aplicaciones-de-redes-sociales/*

ORGANIZACIÓN DE LAS NACIONES UNIDAS, "Medición de las tecnologías de la información y la comunicación (TIC) en educación: manual del usuario", *IIEP Learning Portal*, Canadá, 2009, *https://learningportal.iiep.unesco.org/en/glossary/information-and-communication-technologies-ict*

ORGANIZACIÓN GEEKS FOR GEEKS, "Temu Review", EUA, 1 de septiembre de 2023, *https://www.geeksforgeeks.org/temu-review/*

PARRA NORIEGA, Luis Gustavo, "El Derecho a la Protección de Datos Personales en México", Guía Orientadora "La Protección de Datos Personales en Plataformas Digitales", México, 2021. Disponible en: https://www.infoem.org.mx/doc/publicacionesExternas/20211025_GuiaOrientadora ProteccionDatosPersonales.pdf , Consultado el 5 de octubre de 2023, p. 18.

Protecting Americans from Foreign Adversary Controlled Applications Act, "H.R.7521", *Senado De Los Estados Unidos*, EUA, 14 de marzo de 2024, *https://www.congress.gov/bill/118th-congress/house-bill/7521/text?s=1&r=5&q=%7B%22search%22%3A%22tiktok%22%7D*

REAL ACADEMIA ESPAÑOLA, "Diccionario de la Lengua Española", España, 2024, *https://dle.rae.es/método*

RED EN DEFENSA DE LOS DERECHOS DIGITALES R3D, "Ministras Batres, Esquivel y Pérez Dayán validan la geolocalización indiscriminada de usuarias de la banca en

línea", *Privacidad*, México, 4 de febrero de 2025, *https://r3d.mx/2025/02/04/ministras-batres-esquivel-y-perez-dayan-validan-la-geolocalizacion-indiscriminada-de-usuarias-de-la-banca-en-linea/*

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS, "Historia de la Red Iberoamericana de Protección de Datos", Guatemala, 2024, *https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd*

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS, "Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial", México, 21 de junio de 2019, *https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf*

Reglamento de Inteligencia Artificial de la Unión Europea, *Consejo Europeo*, 29 de abril de 2025, *https://www.consilium.europa.eu/es/policies/artificial-intelligence/#what*

REYES KRAFFT, Alfredo, "Ley Federal de Protección de Datos en Posesión de Particulares Comentada, Capitulo I.", *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, México, 2019, *https://www.cide.edu/wp-content/uploads/2021/03/LFPDPPP-Comentada_digital.pdf*

SHIH, Silva, Lin, Yixuan, "Made in China 2025: How China Thrives Despite Tech Sanctions", *CommonWealth Magazine*, Taiwán, vol. 809, 15 de octubre de 2024, *https://english.cw.com.tw/article/article.action?id=3789*

SOFTCORP, "Definición y cómo funcionan las aplicaciones móviles", Venezuela, 2010, *https://servisoftcorp.com/definicion-y-como-funcionan-las-aplicaciones-moviles/*

STATISTA COMPANY, "Leading shopping apps worldwide in 2024, by number of downloads (in millions)", Alemania, enero 2025, *https://www.statista.com/statistics/1428596/most-downloaded-shopping-apps-worldwide/#statisticContainer*

TAYLOR, Adam, Hassan, Jennifer, Francis, Ellen, Mellen, Ruby, "Countries banned TikTok", *Washington Post*, EUA, 17 de enero de 2025, *https://www.washingtonpost.com/world/2025/01/17/countries-banned-tiktok/*

THE CYBER SECURITY AGENCY OF SINGAPORE (CSA), *"What is HTTPS? Hypertext Transfer Protocol Secure", Singapur, 20 de enero de 2025, https://www.csa.gov.sg/Tips-Resource/internet-hygiene-portal/information-resources/https*

THE DATA PROTECTION COMMISSION (DPC), "Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China", Irlanda, 2 de mayo de 2025, *https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following*

TIAN, Zhe, Zakaria, Aqib, Latif, Adam, “Bridging Digital Divides: Navigating Data Governance and Security in the U.S.-China Technological Arena”, *Fudan-Harvard China-U.S. Young Leaders Dialogue 2024*, Fudan University Center for American studies, China, 2024, *https://cas.fudan.edu.cn/info/1206/16673.htm*

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, “Tienda de Apps UNAM”, *Dirección General de Cómputo y de Tecnologías de la Información y la Comunicación*, Universidad Nacional Autónoma de México, México, 2023, *https://sistemas.tic.unam.mx/wp-content/uploads/2023/09/20230804_DSSI_CSC_DTE_Aplicaciones_Moviles.pdf*

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, “Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes”, *https://www.uscc.gov/research/shein-temu-and-chinese-e-commerce-data-risks-sourcing-violations-and-trade-loopholes*

U.S. DEPARTMENT OF COMMERCE, “Privacy Shield Program Overview”, EUA, 2017, *https://www.privacyshield.gov/ps/program-overview*

WHALECO INC., “¿Qué es Temu?”, Estados Unidos, 2025, *https://www.temu.com/us-es/about-temu.html?refer_page_name=search_result&refer_page_id=10009_1711334553185_t0zi8p12sx&refer_page_sn=10009&_x_sessn_id=gs1ozkt9ql*

WHALECO INC., “Temu - Política de privacidad”, EUA, 12 de mayo de 2025, *https://www.temu.com/mx/privacy-and-cookie-policy.html*

WITKER VELÁSQUEZ, Jorge, “Metodología de la Investigación Jurídica”, *Universidad Nacional Autónoma de México*, México, primera edición, septiembre de 2021, *https://biblio.juridicas.unam.mx/bjv/detalle-libro/6818-metodologia-de-la-investigacion-juridica*

YONG, Nicholas, “Cómo China consigue robarle sus secretos tecnológicos a Estados Unidos”, *BBC News Mundo*, Reino Unido, 26 de enero de 2023, *https://www.bbc.com/mundo/noticias-internacional-64355527*

ZAMARRÓN, Israel, “Made in China 2025: así es el ambicioso plan tecnológico chino que amenaza el dominio de EU”, *Revista Forbes*, México, 16 de marzo de 2023, *https://forbes.com.mx/made-in-china-2025-asi-es-el-ambicioso-plan-tecnologico-chino-que-amenaza-el-dominio-de-eu/*

ZENTENO TREJO, Blanca, Osorno Sánchez, Armando, “Elementos para el diseño de investigaciones jurídicas: Una perspectiva multidimensional”, *Benemérita Universidad Autónoma de Puebla*, México, primera edición, agosto de 2015, *http://ru.juridicas.unam.mx/xmlui/handle/123456789/13153*