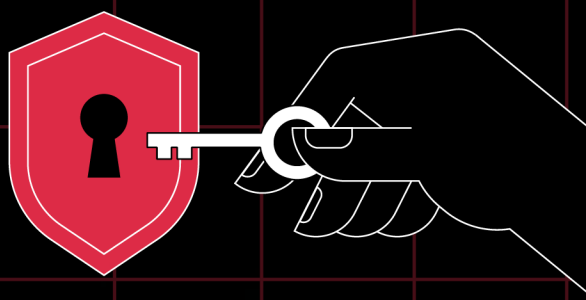
Datos y AdTech:

¿a dónde van los ductos del petróleo digital?

Fundación Karisma <K+LAB>



Bogotá, Colombia
Mayo 2024

Autores
Santiago Sáenz
Andrés Velásquez
Stéphane Labarthe

Dirección Fundación Karisma
Catalina Moreno Arocha
Juan Diego Castañeda

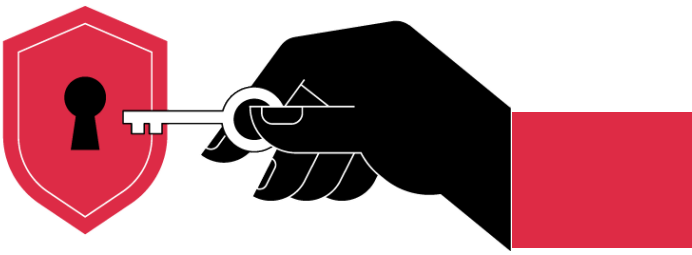
Coordinación de la investigación
Pilar Sáenz

Coordinacación K-Lab
Zia Kandler

Coordinación editorial
Natalia Andrade Fajardo

Diseño editorial
Natalia Noriega Gómez

Identidad gráfica
Daniela Moreno Ramírez



En un esfuerzo para que todas las personas tengan acceso al conocimiento, la Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluida las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.

Contenido

01

02

03

Introducción

Internet ha revolucionado cómo nos comunicamos y accedemos a la información, siguiendo principalmente un modelo económico de aparente gratuidad para las personas usuarias, pero sin saberlo hemos pagado un costo: el riesgo de vulneraciones a nuestros datos y a nuestra privacidad por parte de empresas privadas a través de tecnologías de seguimiento y publicidad dirigida. La publicidad, que ha sido una de las bases del financiamiento de las grandes empresas de internet desde sus inicios, ha mutado con el paso de los años hacia una industria tecnológica dedicada a la individualización de patrones de uso y seguimiento de intereses con el fin de ofrecer publicidad personalizada.

Una enorme cantidad de aplicaciones utilizan estas tecnologías. Incluso las aplicaciones que no tienen espacios publicitarios usan tecnologías de seguimiento ofrecidas por compañías publicitarias con el fin de obtener estadísticas de uso de sus servicios (por ejemplo, Google Analytics), o para ofrecer interacciones sociales dentro de la aplicación (por ejemplo, Facebook Pixel). La simple integración de estas tecnologías es capaz de filtrar inadvertidamente información de los usuarios que es utilizada posteriormente para el direccionamiento publicitario. Aunque en principio esta actividad parezca inofensiva, la recolección de datos en tal magnitud puede convertirse fácilmente en una amenaza para la privacidad e incluso para la seguridad de las personas usuarias.

En el año 2022, una usuaria de Twitter denunció que tras comprar una prueba de embarazo en Walgreens - una de las cadenas de farmacias más grande de los Estados Unidos - y usar su tarjeta de recompensas, recibió en su casa una caja con productos para bebé de parte de Enfamil, una marca de fórmula infantil. La usuaria en cuestión se había realizado la prueba solamente por recomendación de su médico. No estaba embarazada. Su hilo despertó discusiones alrededor de la importancia de la privacidad y, además, propuso preguntas sobre posibles afectaciones a los derechos de las mujeres a quienes fue dirigida la campaña: ¿qué hubiera pasado si la caja se hubiera enviado a una mujer tratando desesperadamente de quedar en embarazo? ¿qué significado tendría la campaña si fuera dirigida a mujeres en estados en los cuales el aborto es legal o ilegal? ¿qué pasa con las mujeres que son objetivos de la campaña y han tenido un aborto?

Aunque el caso ilustra una situación derivada de una compra física, existen técnicas de marketing que permiten conectar las compras en el "mundo real" -cuando se usan "los puntos" o una cuenta asociada de cliente frecuente- y en el "mundo digital", en general usando el correo electrónico cómo punto de conexión. Además, las tecnologías de seguimiento en internet funcionan de una forma muy similar: realizando cruces de la información recolectada en bases de datos por diversas compañías. En el mundo digital se utilizan métodos como cookies, identificadores de publicidad y fingerprinting de dispositivos que permiten recolectar información sobre quién está navegando, qué está buscando o dónde se ubica. Posteriormente, como si fueran una refinería, los algoritmos de procesamiento desarrollados por las compañías convierten estos datos crudos en el recurso más valioso del siglo: información sobre quiénes somos, qué hacemos y en qué estamos interesados.

Además, hay que entender que estos datos no siempre se quedan en el mundo del marketing digital y pueden ser obtenidos, comprados y usados para finalidades muy distintas como el análisis de riesgo, el otorgar créditos bancario o seguros, y hasta por los servicios de inteligencia de los gobiernos. Un artículo reciente de Wired mostró por ejemplo cómo el Pentágono usó datos de las plataformas de subastas en tiempo real de la publicidad dirigida (RTB, Real Time Bidding) para obtener informaciones, incluyendo datos sensibles y de localización sobre personas fácilmente y de manera masiva.

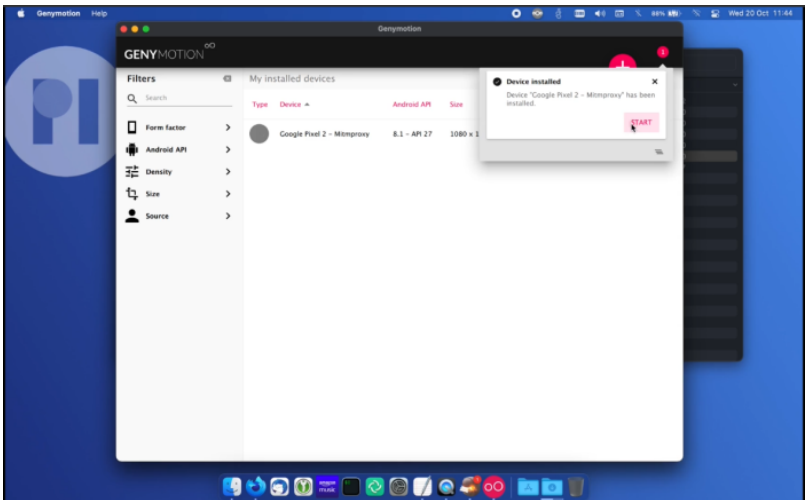
Comprender cómo funcionan estas tecnologías y desarrollar estrategias para el análisis y detección de indicadores de uso inadecuado de datos es esencial para vigilar a las empresas de Internet y abogar por una web libre, transparente y respetuosa con la privacidad. En 2023, desde Karisma hemos estado trabajando junto a la ONG británica Privacy International en el análisis de aplicaciones de amplio uso en Latinoamérica (principalmente en Colombia) para evaluar la amplitud de este rastreo publicitario, identificar los actores involucrados y las técnicas usadas, particularmente en sectores que involucran información confidencial.

Realizamos análisis detallados de aplicaciones de salud (privadas y estatales), finanzas y entretenimiento. Los hallazgos fueron cuanto menos preocupantes en la mayoría de los casos. Parece que los datos, el petróleo digital, se filtran por muchas partes y raras veces hay información sobre hacia dónde se dirigen, tampoco son claras las garantías para proteger la privacidad de quienes usamos internet.

Este artículo resalta algunos puntos sobresalientes de esta investigación.

01
La metodología

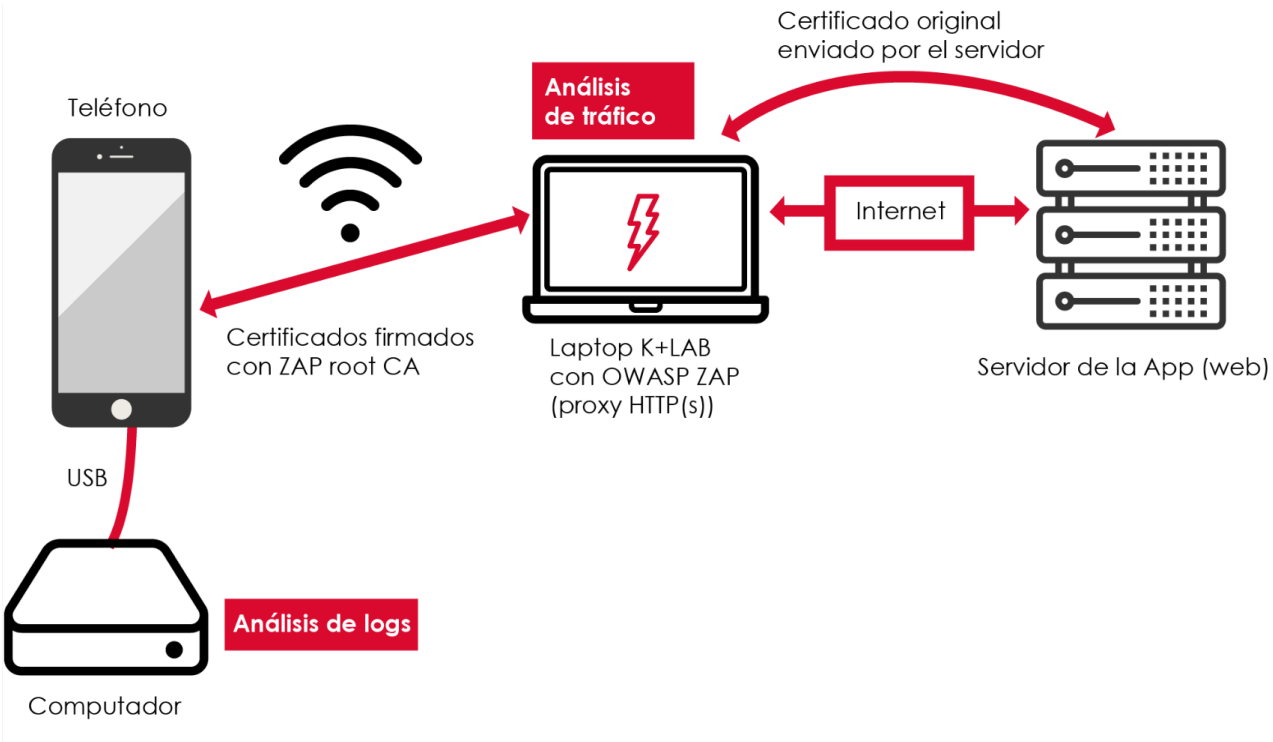
Para lograr detectar indicadores de uso indebido, Privacy International (PI) desarrolló y publicó un entorno de código abierto, el "Data Interception Environment", en el que a través de máquinas virtuales (que son computadores y/o teléfonos emulados dentro de otro computador) se logra interceptar todos los datos enviados por una aplicación hacia internet.



Los datos interceptados fueron analizados en el Laboratorio de seguridad digital y privacidad (K+Lab) de la Fundación Karisma con el fin de detectar qué información personal se envía a terceros y determinar en cuáles casos podría existir una violación a la seguridad o la privacidad de las personas usuarias.

En el marco de la investigación, el K+Lab expandió la metodología desarrollada por PI con el fin de cubrir todos los sistemas operativos móviles presentes en el mercado en la actualidad, no solamente a través de simulaciones en máquinas virtuales, sino también en dispositivos físicos hasta Android 13 e iOS 16. Esto permitió trabajar con las versiones más actualizadas de las aplicaciones, haciendo uso de todas las funcionalidades ofrecidas por los sistemas operativos modernos.

La captura de datos se realiza conectando el dispositivo (real o simulado) a una red de internet creada en el K+Lab a través de software de código abierto para la interceptación de datos como OWASP ZAP y MITMProxy. Una vez conectado (y gracias a configuraciones adicionales que permiten capturar el tráfico cifrado HTTPS) es posible visualizar con todo detalle cada uno de los paquetes de datos que son enviados desde el celular y aislar o filtrar los que son generados por la aplicación que se quiere analizar.



En esta investigación, en el rastreo y la privacidad, nos centramos en la búsqueda de:

- Servicios que instalan cookies de seguimiento.
- Servicios que transmiten identificadores de publicidad del dispositivo (AAID de Android e IDFA de iOS) u otros identificadores de seguimiento.
- Servicios que identifican a la persona usuaria a través de mecanismos de fingerprinting.
- Conexiones a dominios pertenecientes a empresas de publicidad, analítica, perfilamiento o identificación de las personas usuarias y/o geolocalización.
- Transmisión de datos sensibles a terceros y fugas/transmisiones de datos personales.

Además de este análisis se usó Exodus Privacy para realizar "análisis estático". Exodus hace un escaneo rápido de las aplicaciones Android y lista los elementos de tracking y de otros terceros (cómo crash reporters) encontrados en el código fuente, así como los permisos del dispositivo a los cuales tiene acceso la aplicación.

Aunque no nos fue tan útil en el marco de estos análisis, estos se pueden complementar con la revisión de los logs generados por el sistema operativo del teléfono cuando la aplicación está funcionando. En Android se puede acceder a los archivos de logs con el Android Debug Bridge (ADB). En iPhone se puede usar la herramienta nativa propietaria Apple Configurator o la herramienta idevicesyslog de la librería open source libmobiledevice.

02 Hallazgos

El K+Lab realizó análisis sobre 12 aplicaciones de amplio uso. En todas las aplicaciones excepto una (“Conoce tu Riesgo” de MinSalud) se encontró, de una forma u otra, la implementación de tecnologías de seguimiento sin consentimiento previo de las personas usuarias. En muy pocos casos las tecnologías sólo se implementaron para obtener estadísticas de uso de la aplicación y, en la gran mayoría de casos, se encontraron tecnologías de múltiples empresas de publicidad o seguimiento, en varios casos decenas de ellas. A continuación presentamos algunos de los hallazgos más interesantes.

Aplicaciones creadas para rastrear: AMMA Pregnancy & Baby Tracker

AMMA es una aplicación desarrollada por Mobile Dimension, una compañía desarrolladora de software con sede en Moscú, Rusia. Curiosamente la política de privacidad de la aplicación no hace responsable del tratamiento de datos a Mobile Dimension, sino a una entidad legal registrada en Hong Kong solamente para el desarrollo de esta aplicación. Cuenta con más de 10 millones de descargas solamente en la Google Play Store y se encuentra en los tops de apps de maternidad en varios países de Latinoamérica (ocupa el primer puesto en México y el tercero en Brasil).

El análisis estático de la aplicación mostró la presencia de 25 rastreadores distintos. Este número excesivo hace sospechar que el propósito de la aplicación no es otro que la monetización de minería de datos sensibles de mujeres en estado de embarazo. En el mundo del marketing, la información detallada de grupos poblacionales con intereses específicos como este es muy valiosa. Este tipo de información permite dirigir las campañas publicitarias a las personas con mayor probabilidad de adquirir productos de alto valor durante un tiempo amplio y predecible.

El análisis de tráfico de la aplicación confirmó las excesivas transferencias de datos hacia servidores de terceros. En este caso, la información estaba siendo transmitida a empresas publicitarias, pero también de forma directa a empresas que realizan producción de alimentos para la primera infancia. Resulta relevante la detección de indicadores que sugieren una transferencia de datos hacia Nestlé de Colombia sin el consentimiento explícito de las usuarias, lo cual se puede ver en el análisis de tráfico y no está especificado en los términos y condiciones de la aplicación.

Los términos y condiciones de la aplicación (que no son accesibles ni claros sobre la forma en que realizan el tratamiento de datos) indican transferencias de datos hacia Procter & Gamble de Rusia y “otras empresas”. Aunque el documento legal no especifica cuáles son estas empresas, publicaciones en el sitio web de Mobile Dimension sugieren que AMMA tiene o ha tenido alianzas con Pepsico, Pampers, Huggies, Medela, Elevit y otras empresas dedicadas a los productos de consumo inmediato y a la industria farmacéutica.

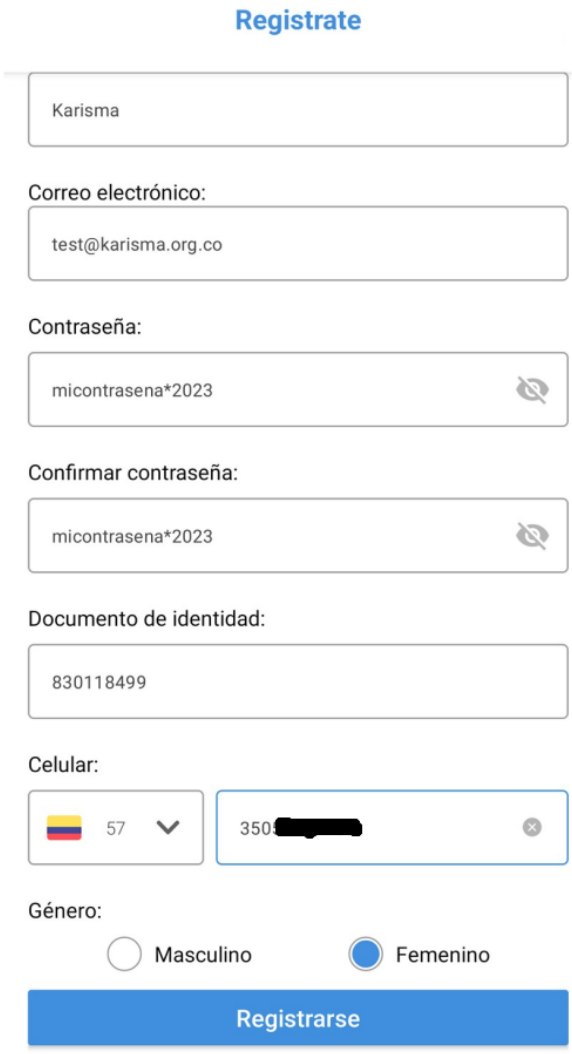
Además de la gran cantidad de servicios de seguimiento, la aplicación solicita acceso a 22 permisos del teléfono. Estos permisos incluyen acceso preciso a la ubicación GPS (que es transmitida al servidor de la aplicación), a la cámara y al control de las funciones de llamadas telefónicas.

Rastreo a través servicios de analíticas de datos: estadísticas, fugas de datos personales sensibles y "session replay"

En el artículo Fuga de datos por rastreo publicitario habíamos alertado de una situación común que pone en riesgo la privacidad de las personas usuarias: los y las desarrolladoras suelen integrar librerías o SDKs de terceros porque ofrecen funcionalidades pero sin considerar las posibles consecuencias de la transmisión de datos, sin realizar un análisis de las políticas de privacidad de los terceros asociados y sin tener en cuenta el consentimiento de las personas usuarias.

Además, las interfaces de estas herramientas -así puedan en ciertos casos permitir una configuración de los datos que se transmiten- no suelen usar una configuración predeterminada que minimice la transmisión de datos personales. En el marco de esta investigación pudimos detectar transmisión de datos personales privados y sensibles debido a la integración de SDKs en varias de las aplicaciones analizadas. El caso que mostramos aquí tiene que ver con servicios de analítica de datos -que es el servicio externo más usado dentro de los sitios web y las aplicaciones- usado en un contexto de una aplicación relacionada con la salud. Mostramos como no sólo se mandaban a estas empresas de analítica de datos informaciones personales (nombre, apellido, correo electrónico, número de teléfono, número de documento de identificación), sino también datos sensibles, potencialmente vinculados con la salud o la sexualidad de la persona usuaria, en función de los productos farmaceúticos de interés o comprados.

Resultaron particularmente interesantes los hallazgos sobre las librerías de Amplitude (detectada en 3 de las 12 aplicaciones analizadas) y Braze (detectada en 1 de las 12 aplicaciones analizadas). Estas librerías, que tienen como propósito facilitar actividades de analítica de datos, reporte de uso o marketing digital, tienen la capacidad de recolectar y transmitir a sus propios servidores la totalidad de los datos de las aplicaciones en las que están integradas. Notamos con preocupación que éste era el caso en una de las aplicaciones, en la que toda la actividad de las personas usuarias (que incluía envío de datos de identificación personal, búsqueda y compras de artículos de salud) era transmitida sin la autorización explícita de estas personas a los servidores de Braze y Amplitude, como lo muestra la tabla siguiente que muestra en la columna izquierda el formulario de inscripción de una aplicación vinculada con la salud y en la derecha los datos que se envían a las analíticas de datos:

Datos ingresados en el formulario de registro de la aplicación *(captura de pantalla)*	Transmisión de los datos del formulario hacía Braze y Amplitude *(extracto de captura de tráfico de la app)*
	<u>Transmisión de datos a Amplitude:</u> **POST https://api2.amplitude.com/** HTTP/1.1 [...] **“user_id”:”212400d2-2e7a-47f9-a5e6-4ccae7f98063”** [...] **{“androidADID”:”52cc-c9b6-3ae9-498a-818b-d715af-31d1aa”**,”limit_ad_tracking”:false,”-gps_enabled”:true},”event_proper-ties”:{},”user_properties”:{“$set”:{“First Name”:”**Fundacion** “,”Last Na-me”:**”Karisma** “,”Phone”:”**57350[...]**”,”-Gender”:””,”Email”:”**test[at]karisma.org.co**”,”Country”:”CO””,”**Identifica-tion”:”ODMwMTE4NDk5**” [...] <u>Transmisión de datos hacia Braze:</u> **POST https://sdk.iad-06.braze.com/api/v3/data [...]** **{“device_id”:”a-c66a91a-d678-4712-a60d-2cf7d4e-105c6”**,”time”:1675206137,{“first_na-me”:”**Fundacion** “,”custom”:{“Signed up”:”EMAIL”,**”Identification”:”OD-MwMTE4NDk5”**,”Vip”:false,”Logged in”:”EMAIL”,”Prime”:false},”last_na-me”:**”Karisma “**,”phone”:”**57350[...]**”,”-**gender”:”u”,”email”:”test[at] karisma.org.co**”,”country”:”CO”,**”u-ser_id”:”212400d2-2e7a-47f9-a5e6-4ccae7f98063”}]**

Aquí los datos personales del formulario de registro de la aplicación se mandan hacía URL de terceros (Amplitude y Braze), incluso el documento de identidad que se encuentra codificada en base64. Estos datos son además asociados a un identificador común (user_id), y en el caso de Amplitude al identificador de publicidad de Android (androidADID).

En el caso de Amplitude, el K+Lab no encontró motivo -ya que esta herramienta se usaba únicamente como analítica de datos y no tiene sentido hacer estadísticas sobre datos personales cómo el apellido o el número de documento- que justificara la transferencia de los datos a esa herramienta, lo cual nos fue confirmado por la empresa encargada de la aplicación. Sin embargo estos tipos de herramientas no suelen ser diseñados para minimizar la colecta de datos personales ("privacy by design") sino al contrario debido a su modelo de negocio. En el caso de Amplitude, se menciona claramente en su sitio web que por defecto rastrea todas las interacciones con los formularios incluso desde antes que se haga clic para enviar los datos:

Tracking form interactions

Amplitude tracks form interaction events by default. A form start event is tracked when the user initially interacts with the form. An initial interaction can be the first change to a text input, radio button, or dropdown. The event type for session start is "[Amplitude] Form Started". A form submit event is tracked when the user submits the form. The event type for session start is "[Amplitude] Form Submitted". If a form is submitted with no initial change to any form fields, both "[Amplitude] Form Started" and "[Amplitude] Form Submitted" are tracked.

Extracto del sitio web de Amplitude, https://www.docs.developers.amplitude.com/data/sdks/browser-2/#tracking-default-events, 27/03/2024

El caso de Amplitude permite plantear el tema de las soluciones de analítica de datos y sus importantes capacidades de recolección de datos, además de resaltar cómo ciertas compañías usan los datos recolectados para finalidades de publicidad y marketing propias. En este campo, las herramientas más populares son las de Google ("Firebase analytics" para las apps y "Google Analytics" para los sitios webs). No todas las soluciones tienen el mismo impacto en términos de privacidad -esto se abordará de forma diferencial en el apartado de recomendaciones- por tanto, se requiere analizar los términos y condiciones para descartar las más intrusivas o determinar cuáles cumplen con las funciones requeridas sin poner en riesgo los datos de las personas usuarias.

Antes de la publicación de este informe, el K+Lab contactó a la empresa encargada del desarrollo de la aplicación de venta de medicamentos y productos de higiene que integraba las librerías de Amplitude y Braze para señalar las preocupaciones con respecto a esta situación. Se debe señalar que varias observaciones fueron atendidas prontamente por el equipo legal y los encargados del desarrollo.

La empresa asumió compromisos para mejorar, hasta cierto punto, la información de la aplicación y la

privacidad y seguridad de sus clientes. En concreto, nos informaron que se habían suscrito a la oferta paga de ambas soluciones que incluían la garantía de no compartir los datos con otros terceros. Además, cambiaron la información de la aplicación en el PlayStore y en el AppStore; ahora es claro que comparten información con terceros, se incluyeron detalles sobre el tipo de información y la finalidad. En el sitio web implementaron un banner de información de cookies con un enlace hacia una nueva "política de cookies/privacidad". Creemos que estos cambios mejoran la información hacia las personas usuarias y, en este caso, las acciones pueden resaltarse como resultado de este análisis. Lo anterior también muestra que este tipo de análisis y vigilancia desde la sociedad civil tiene resultados positivos.

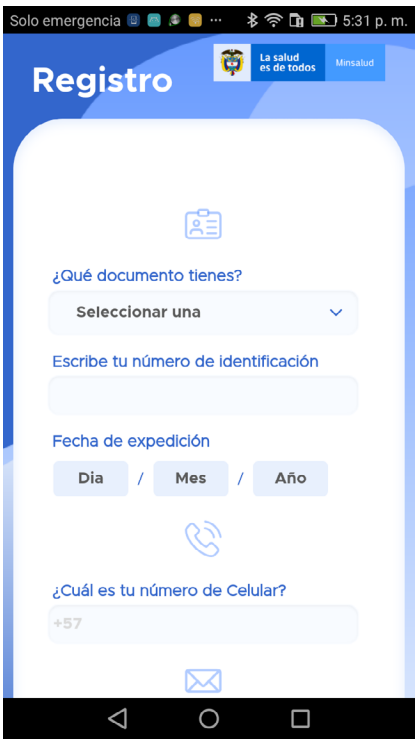
Sin embargo, mantenemos nuestra preocupación sobre la forma como Amplitude, Braze y otras empresas con servicios de analítica de datos (como Google/Firebase Analytics), al facilitar servicios de analítica de datos y/o marketing digital a terceros, recolectan cada vez más datos de las aplicaciones en las que están integradas. Hasta ofrecen nuevos servicios como el "session replay" que permite hacer volver a reproducir la sesión de cada usuario, desde cada movimiento del mouse hasta cada caracter teclado (ver por ejemplo la función "microscopio" de Amplitude).

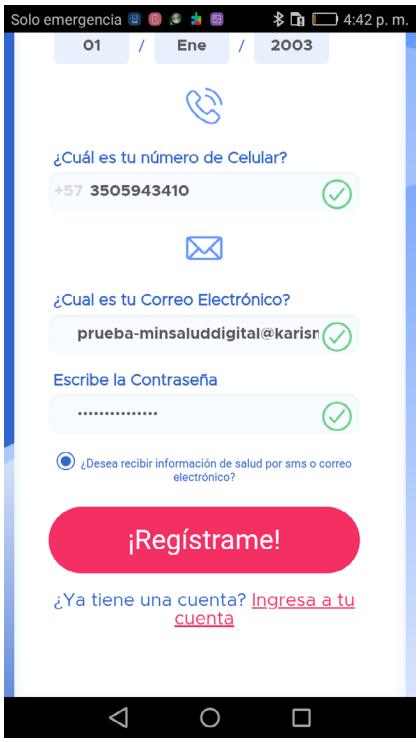
Minsalud Digital: una aplicación fantasma que sigue mandando datos a Google y OneSignal

Finalmente se puede resaltar un caso que, aunque no es grave, muestra una situación común para las aplicaciones desarrolladas por entidades del Estado. En nuestro análisis se detectó una aplicación que, a pesar de ser descargable en las tiendas de aplicaciones, ya no funcionaba, es decir, los servidores no respondían.

La aplicación "Minsalud Digital" que antes se llamaba "Coronapp_Colombia" (identificada en al Playstore cómo "co.gov.ins.guardianes") fue desarrollada por el Instituto Nacional de Salud y usada ampliamente en el marco de la pandemia de COVID-19. Al final de su implementación y sin que se tuviera claridad sobre su futuro, su gestión fue entregada al Ministerio de Salud y Protección Social de Colombia quien finalmente desistió de su uso. Sin embargo, en el momento de nuestro análisis, aún se podía encontrar en tiendas y se promocionaba en la página del Ministerio. Al iniciar la aplicación en el teléfono, se ejecutaba el código de varios terceros (gracias a las SDK integradas) cuyas transmisiones de datos irónicamente sí eran recibidas por los servidores de compañías publicitarias.

La siguiente tabla muestra cómo aunque el servidor de la aplicación está inactivo (no respondía a las solicitudes e incluso tenía el servicio/puerto web desactivado) la aplicación sigue mandando datos a terceros:

Pantallazos de la aplicación	Solicitudes/respuestas al/del servidor de la aplicación mostrando que no funciona	La app se comunica con servidores de terceros
	**OPTIONS https://minsaluddigital.ifxcorp.com/v1/session/register HTTP/1.1** **Host: minsaluddigital.ifxcorp.com** **[solicitud hacia el servidor web de MinSalud Digital]** [...] User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 Accept-Language: es-419,es;q=0.9 Content-Length: 0 **HTTP/1.1 404** **[Respuesta con código de error que significa "no encontrado"]** Server: nginx/1.18.0 (Ubuntu) Date: Tue, 04 Oct 2022 23:03:22 GMT Content-Length: 0 Connection: keep-alive	**Hacía Google Analytics:** **POST https://www.google-analytics.com/**g/collect?v=2&tid=G-Z84LNPFZVL&gtm=2oe9l0&_p=19809237&_fid=frNYAnl9Kt-DN4we_fHsMY&ci d=649954200.1664144451&ul=es-co&sr=360x640&_z=ccd.v9B&_s=4&sid=1664144451&sct=1&seg=1&dl=http://localhost/**register&dt=MinSalud Digital**&en=opn_registro&_ee=1&ep.origin=firebase&_et=98781 HTTP/1.1 Host: www.google-analytics.com [...]



La aplicación no dejaba ir más allá del formulario de registro. Al hacer clic en "Registrarme" no pasaba nada.

Escaneo del servidor mostrando que el servicio web no está activo:

host minsaluddigital.ifxcorp.com
minsaluddigital.ifxcorp.com is an alias for minsaluddigital.trafficmanager.net.
minsaluddigital.trafficmanager.net has address 200.91.252.123

nmap -Pn 200.91.252.123
Starting Nmap 7.80 (https://nmap.org) at 2023-01-23 22:17 EST
Nmap scan report for hapifhir.api.ifxcorp.com (200.91.252.123)
Host is up (0.042s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
53/tcp open domain
Nmap done: 1 IP address (1 host up) scanned in 7.23 seconds

Hacía OneSignal:

POST https://api.onesignal.com/players HTTP/1.1
SDK-Version: onesignal/android/040603
[...]
{"app_id":"3a52108e-597b-4f25-81c1-d68123326c27","device_os":"6.0","timezone":-18000,"timezone_id":"America\/Bogota","language":"es","sdk":"040603","sdk_type":"cordova","**android_package":"co.gov.ins.guardianes"**,"device_model":"ALE-L23","game_version":206,"net_type":0,"rooted":false,"identifier":"e_ZW-FLw-Nfk:APA91bEcF-T5X-dsu8H-mRZ2n-Q1EY6ynFLfcSDnGWcz-7maS0SzWg0ZoEc_PV3aY_TPh9lAenRJZ-n51Xi6sgzQkzvurxps-pBJwyLZaHXpSG_6J-6NaCDFT1tKuoR7cpiO-jrFouMwIIyrvet","device_type":1}

Nota: se hicieron pruebas desde un teléfono Android y desde un iPhone. Estos datos son los de Android (no se observó el envío hacía terceros desde iPhone).

Informamos al Ministerio de este hallazgo junto con un reporte de una vulnerabilidad menor en otra aplicación y, a diferencia de lo que sucedió con administraciones previas, recibimos una pronta respuesta mostrando el interés de la entidad por mejorar la situación:

> *"Validado el informe con el área encargada de la publicación de las aplicaciones en el sitio web del Ministerio, se establecieron mesas de trabajo internas para revisar el ciclo de vida de las aplicaciones en mención y tomar los correctivos necesarios con el fin de mitigar los riesgos de seguridad digital que se puedan presentar." (Tomado de la respuesta del Ministerio de Salud de Colombia a la Fundaciòn Karisma, fecha del 2 de marzo del 2023).*

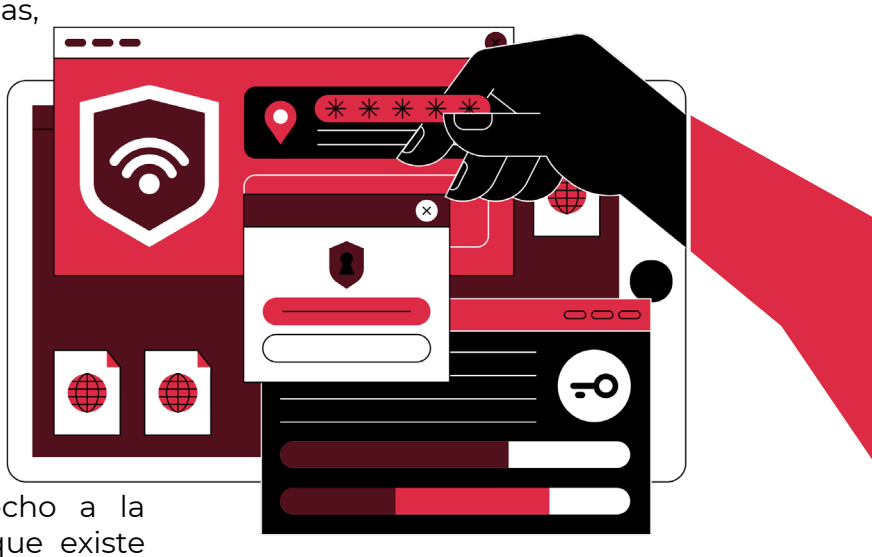
Desde entonces la aplicación fue retirada de las tiendas. Conviene indicar además que a raíz de este ejercicio el K+Lab fue invitado a una reunión con el recién creado grupo de seguridad de información y protección de datos personales del Ministerio de Salud que escuchó las preocupaciones y agradeció el reporte.

03
Conclusiones y recomendaciones

El análisis realizado por K+Lab confirma que el ecosistema actual de internet y de los negocios que se han desarrollado en torno a esta red tiene demasiados incentivos para la extracción, comercialización y uso de datos sin importar otras consideraciones. Privacy International por ejemplo ya había realizado un estudio sobre los datos recolectados por aplicaciones de menstruación usando otra metodología (pidiendo por derecho de acceso a los datos personales previsto en el RGPD).

El análisis de K+Lab permite confirmar lo que ya avanzaron otros estudios: hay aplicaciones dirigidas a nichos de mercado cuyos datos son muy apetecidos en publicidad. Los incentivos para que se recolecten datos -incluso sensibles- son grandes y por tanto es evidente que se ignoran aspectos claves de privacidad de las personas. Pero además de los casos en los cuales el rastreo es consecuencia de la inclusión voluntaria y consciente, por parte del desarrollador de la aplicación, de publicidad con el fin de generar ingresos (cómo en AMMA), hay otros casos en los cuales el desarrollador incluye código fuente de terceros (SDK) que proveen funcionalidades gratuitas a cambio de la recolección de datos de las personas usuarias. Parece que los y las desarrolladoras no han cultivado el hábito de analizar las integraciones que hacen de aplicaciones de terceros en el mercado; aparentemente con muy poco análisis integran funcionalidades que usan código de terceros para incluir funciones concretas que aprovechan (por estos terceros) para extraer los datos de las personas usuarias de la aplicación que integra su código. Sin embargo, esos detalles no se mencionan en las políticas de las aplicaciones que están en el mercado. Aunque durante el ejercicio conseguimos que mejorara la información para las personas usuarias de una de las aplicaciones, nos queda la duda de si esto generó cuestionamientos al interior de la empresa. Es decir, es posible que los cambios de componentes en una aplicación ya en el mercado sea tan costoso como impensable, aún así la pregunta es ¿si pudieran, cambiarían la tercera aplicación por una alternativa más respetuosa de los derechos de las personas usuarias?

Finalmente, en el frenesí de la transformación digital nacen muchas aplicaciones cada día y muchas otras mueren, dejan de ser usadas, son abandonadas, desechadas. No existe un cementerio donde queden enterradas esas aplicaciones que ya fueron desechadas, todo indica que muchas de ellas quedan en un limbo y se convierten en fantasmas que pueden seguir acechando los datos de las personas, transmitiéndolos a terceros y generando problemas. Es necesario llamar la atención a quienes se comprometen con el despliegue de aplicaciones para que pongan también interés en su retiro.



Este informe tampoco ofrece un panorama alentador para el derecho a la privacidad en la red. A pesar de que existe un creciente número de servicios, tanto de código abierto como propietario que buscan ofrecer características más respetuosas con la privacidad de las personas usuarias, la cultura de las aplicaciones parece que no se ha apropiado de tales oportunidades. Por otro lado, tampoco hay incentivos suficientes para que esto cambie.

Recomendaciones a las y los legisladores y autoridades de América Latina

Es posible tomar un rumbo hacia una Internet respetuosa con la privacidad, pero requiere de esfuerzos desde diferentes sectores.

Las y los legisladores y hacedores de política pública en la región deben abordar las particularidades de las aplicaciones para celulares y su apetito por los datos personales de quienes las usan para determinar posibles reformas legislativas que ofrezcan mecanismos más efectivos en la garantía de derechos.

Las autoridades de protección de datos deben seguir analizando la situación a la luz de las normas existentes y así buscar las oportunidades que tienen en el marco legal existente para garantizar algún nivel de protección.

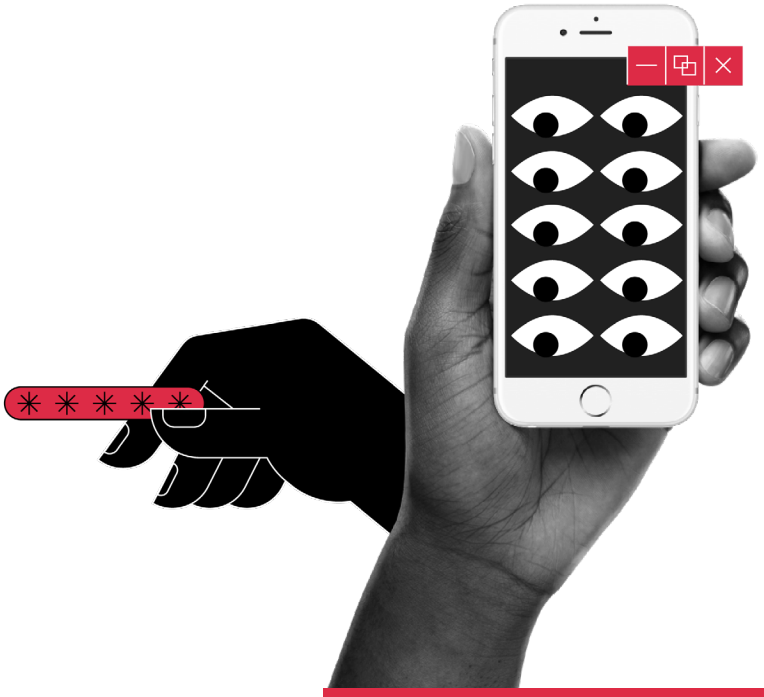
En Colombia, el nuevo proyecto de ley de protección de datos personales puede ser una oportunidad.

Esta es una actividad que se ya ha realizado, por ejemplo, en agosto de 2016 la Superintendencia de Industria y Comercio colombiana afirmó que el tratamiento de datos a través de cookies de rastreo exige el respeto de la ley de protección de datos (Ley 1581 de 2012). Probablemente la SIC deba precisar mejor su interpretación de la ley y los requisitos resultantes frente al uso de cookies y tecnologías similares para rastrear las personas usuarias (identificadores de publicidad, fingerprinting etc.), comunicar ampliamente en este tema y tomar las medidas cuando aplicaciones que involucren datos personales sensibles en gran volumen no las respeten.

Por fin, las entidades públicas como responsables de aplicaciones en el mercado deben mantener un inventario actualizado de las mismas, hacer evaluaciones periódicas de seguridad digital y privacidad -para verificar que el software esté actualizado, por ejemplo-, pero también para establecer que sigan teniendo un propósito.

Recomendaciones a las personas que desarrollan aplicaciones para celulares

Cuando los desarrolladores integran publicidad y rastreo en las aplicaciones con el fin de generar ingresos, es importante dar una información adecuada y obtener el consentimiento de las personas usuarias en línea con las legislaciones de protección de datos vigentes, aún más cuando se trate de datos sensibles. Cuando se integran funcionalidades de terceros, es esencial analizar con detenimiento los riesgos y beneficios de incluir este código de terceros en una aplicación antes de integrarlo en su código. En aquellos casos en los cuales es importante obtener métricas de uso o realizar análisis del funcionamiento de la aplicación, considere el uso de alternativas de analytica amigables con la privacidad de las personas usuarias, en lugar de hacer uso de código propietario creado por compañías de publicidad. Por ejemplo, Plausible y Piwik les han permitido a muchas compañías, en años recientes, migrar desde servicios como Google Analytics hacia una alternativa libre y mucho más privada. Esta recomendación se aplica también a todos los otros servicios externos que se integran en una aplicación o sitio web: vídeos, botones de redes sociales, reporte de crash/bugs, chats de ayuda, etc.



Recomendaciones para casos en los que se incluyen códigos de terceros:

01 Antes de integrar un servicio externo/SDK en su aplicación, tome en cuenta el modelo económico de éste, su política de privacidad y los impactos potenciales para sus usuarios. Considere usar servicios alternativos que minimicen la recolección de datos (por ejemplo Plausible y Piwik para las analíticas de datos).

02 Tenga en cuenta la importancia de la información y del consentimiento de las personas que van a usar la aplicación, en especial cuando se manejan datos personales sensibles (relacionados por ejemplo con la salud, la sexualidad o las opiniones políticas).

03 Ofrezca opciones claras y accesibles que permitan revocar el rastreo y la autorización de transferencia de datos a terceros.

04 Si tiene la capacidad o puede contratarla, haga un análisis detallado del funcionamiento de su aplicación con las librerías que integra y de la información que transmite a compañías externas antes de poner en riesgo la información de las personas. Puede usar la metodología que usamos aquí o una metodología similar.

05 Maneje con extremo cuidado la información de identificación, bancaria, contraseñas, de localización o datos personales sensibles.

Recomendaciones a las personas usuarias:

A diferencia de cuando se usan los navegadores en portátiles o computadores de escritorio (a través de software como Chrome o Firefox), las personas usuarias no tienen muchas opciones a la hora de proteger sus datos cuando usan aplicaciones móviles. Actualmente la responsabilidad de mejora y las opciones que se pueden ofrecer a las personas para mitigar los efectos del ecosistema descrito es de quienes desarrollan las aplicaciones.

Algunos factores agravan la situación: ausencia de mecanismos efectivos en las leyes de protección de datos de la región, la falta de acción de las autoridades de protección de datos por enfrentar la situación con las herramientas que tienen y la poca atención que las entidades o empresas quienes desarrollan ponen a esta situación.

A pesar del panorama pesimista hay algunas acciones que las personas pueden tomar por sí mismas para minimizar la transferencia de datos y facilitar la identificación de aplicaciones abusivas o poco seguras:

01 Consulte la sección de privacidad de cada aplicación en la tienda de aplicaciones antes de descargarla. Evalúe la necesidad de su uso si esta declara que realiza transmisión de datos a terceros o si la aplicación recolecta datos personales que considere sensibles. Considere elegir una aplicación similar que ofrezca una mejor privacidad.

02 Si es usuario de Android, considere instalar aplicaciones de código abierto que, por tener modelos económicos diferentes y por respetar un principio de transparencia, suelen rastrear mucho menos.

03 Tenga cuidado con los permisos que otorga a las aplicaciones al instalarlas, en particular el acceso a la localización, a los contactos, al micrófono y cámara. Revisa regularmente estos permisos, en particular de acceso a la ubicación que se gestiona aparte.

04 Ingrese a la configuración de sus cuentas en cada aplicación y verifique si es posible desactivar la transferencia de datos a terceros y la personalización de anuncios.

05 En Android, ingrese a la configuración de su cuenta de Google y desactive el seguimiento y los datos de personalización y el ID de publicidad. En versiones de Android previas a la 12 no se puede desactivar el ID de publicidad pero puede cambiarlo regularmente.

06 En Apple, ingrese a la configuración del dispositivo y en la sección de privacidad y seguridad y desactive los anuncios personalizados.

07 En Android es posible usar aplicaciones que monitorean y limitan el rastreo. Tracker Control y la aplicación de Exodus Privacy. Estas aplicaciones permiten conocer cuáles son los rastreadores en las aplicaciones que están instaladas en su dispositivo.

Para más información sobre cómo proteger sus datos personales, consulte los tips que se ofrecen en la página del nuevo proyecto de la ONG Social Tic, Datávoros: https://datavoros.org/gestiona-tu-privacidad/.

Datos y AdTech:

¿a dónde van los ductos del petróleo digital?

<K+LAB>

Karisma.org.co

Karismacol @Karisma Karismacol fundacionKarismaa