LA PRIVACIDAD EN LAS APLICACIONES DE MENSAJERÍA INSTANTÁNEA

Autor: Eduard Blasi Casagran

Abstract

Hace ya más de un siglo que el teléfono se encuentra en nuestra sociedad. En 1876, cuando Alexander Graham Bell inventó el teléfono nadie podía imaginar que su idea sería el antecesor de nuestros dispositivos de hoy en día, los teléfonos inteligentes o *smartphones*.

Ciertamente el teléfono se ha mantenido en esencia, pero en lo que respecta a sus funciones ha tenido que adaptarse a las nuevas necesidades marcadas por los cambios en los hábitos de comunicación. En un primer momento, la comunicación por voz se vio reemplazada por los mensajes cortos o SMS. Años más tarde, tras la aparición de los *smartphones*, los propios SMS quedaron obsoletos abriendo paso a lo que es hoy en día el sistema de comunicación por excelencia: la mensajería instantánea.

Las razones del éxito de las aplicaciones de mensajería instantánea han sido varias: La gratuidad o el bajo coste del servicio, la sencillez de las prestaciones, y la incorporación de nuevas funcionalidades que permiten al usuario una interacción mayor (envío de archivos, ubicación, etc.), entre otras.

Sin embargo, no todo son ventajas. Se ha comprobado que el uso de aplicaciones de mensajería instantánea a menudo pone en peligro la privacidad de sus usuarios, y estos no siempre son conscientes de ello. Toda la información recabada puede ser utilizada posteriormente con fines diversos o incluso cedida a terceras empresas. Resulta más que habitual que los usuarios no conozcan realmente qué se hace con sus datos. La falta de transparencia parece ser el mal común de las aplicaciones y en especial las de mensajería instantánea. Lo cierto es que lamentablemente la mayoría de aplicaciones de mensajería instantánea no cuentan con una política de privacidad o la información que contemplan es sesgada u obsoleta, situando al usuario en un escenario de incertidumbre e indefensión frente al uso indebido de su información.

El auge de las aplicaciones de mensajería instantánea ha conllevado que los usuarios utilicen estas aplicaciones en su entorno profesional aumentando con ello el riesgo sobre la información transmitida, por su condición de confidencial o sensible en la mayoría de los casos. La realidad es que la inmensa mayoría de los usuarios acepta los términos y condiciones de las aplicaciones sin leerlos debidamente. Sin embargo, es bien sabido que la gran parte de las aplicaciones de mensajería instantánea prohíbe de forma expresa el uso profesional o corporativo en sus propios textos legales.

Estos últimos años, las autoridades de control europeas han alertado de los riesgos de utilizar algunas de las aplicaciones de mensajería instantánea y han instado a determinados colectivos profesionales a cesar su uso en entornos corporativos. No obstante, a fecha de hoy parece no haber todavía un posicionamiento común sobre el cese de estas aplicaciones.

La privacidad tiene un precio

Actualmente existen gran cantidad de aplicaciones de mensajería instantánea en el mercado. La mayoría de ellas ofrecen un servicio gratuito o prácticamente gratuito y en ocasiones resulta un verdadero misterio saber cómo logran sustentar su negocio.

Algunas de las principales *apps* de mensajería instantánea ponen a disposición del usuario servicios de primera calidad sin solicitar el pago directo del producto. El auge de las aplicaciones ha llevado a los usuarios a un escenario de ficción donde les hacen creen que es posible adquirir productos y servicios en Internet sin coste alguno. Sin embargo, el usuario, en el momento de descargarse el *software* que pretende adquirir debe ser consciente de que la empresa que le presta el servicio no es ni mucho menos una organización sin ánimo de lucro sino, en su mayoría, empresas pioneras en Internet y con unos índices de crecimiento anuales muy elevados.

El usuario que se descarga una *app* busca en definitiva un producto de primera calidad, con un buen servicio y a coste cero. ¿Es esto posible? La realidad es que no, porque todo tiene un coste, y no podemos esperar de modo alguno que un buen producto o servicio sea 100% gratuito.

Estas empresas de Internet, como el resto de empresas, tienen unos costes que deben sufragar de algún modo. *A grosso modo,* algunos de los costes mínimos son los derivados del mantenimiento y uso de servidores, la programación y actualización de las plataformas, la corrección de 'bugs' (errores de software) e implementación de medidas de seguridad constantes, el servicio de asistencia en caso de problemas/incidencias del servicio, etc. Un servicio bueno supone por tanto un coste elevado para estas empresas.

Muchas empresas de Internet han cubierto estos costes mediante el pago por adquisición de licencias de software. Sin embargo, cuando el producto no supone un coste directo para el usuario generalmente se utilizan vías alternativas tales como el uso de los datos personales del mismo. Tal como apuntó el periódico estadounidense 'The New York Times' los datos son el petróleo del s. XXI. Por tanto, los datos personales de los usuarios son una vía de ingresos para las empresas ya que mediante la gestión de los mismos éstas pueden ofrecer a los usuarios publicidad relacionada con sus gustos e intereses, o incluso vender esta información a terceras empresas.

Cuando nos referimos a datos personales no hablamos sólo de datos en el sentido estricto de la palabra, sino también de metadatos. Los metadatos no son otra cosa que la información asociada a un dato. En el caso de las aplicaciones de mensajería instantánea, los metadatos podrían ser, a modo de ejemplo, la hora de conexión del usuario, la hora de desconexión, el destinatario de la información, el volumen de la información transmitida, etc. Dicha información puede ser tan o más valiosa que los propios datos.

Así pues, la gratuidad de una aplicación de mensajería instantánea debería anular cualquier expectativa de privacidad del usuario ya que, de forma evidente, el usuario debe costear los gastos que conlleva el servicio utilizado.

Cuando los usuarios se disponen a adquirir alguno de los servicios de estas empresas son habitualmente informados sobre el tratamiento de sus datos en los términos y condiciones que generalmente son aceptados casi de forma automática, sin prestar atención alguna: *"he leído y acepto la política de privacidad"*. Los usuarios deberían siempre leer y prestar atención en las políticas de privacidad de los productos o servicios que adquieren para conocer exactamente qué

se hace con sus datos, y aún más, si se trata de productos o servicios gratuitos. En este sentido, tras leer la política de privacidad de la app gratuita podría suceder que el uso de los datos personales fuera excesivo y por tanto el producto o servicio que se fuera a adquirir acabase resultando verdaderamente 'caro'.

Resulta francamente alarmante la forma en que se aceptan las políticas de privacidad y condiciones de las distintas plataformas y *softwares*. A modo de ejemplo, la empresa *Gamestation*, el 1 de abril de 2010, coincidiendo con el día de los inocentes anglosajón, decidió incluir una cláusula en sus términos y condiciones que establecía que se reservaba el derecho a exigir el alma de sus clientes cuando quisiera. El resultado fue que el 88% de los usuarios aceptó ceder su alma a la empresa aquel día. Aquel caso ciertamente fue una 'broma' pero la realidad es que actualmente los usuarios facilitan gran cantidad de datos, y conceden usos y cesiones de los mismos sin ser conscientes de ello.

Sin embargo, toda la responsabilidad no es de los usuarios. Existen todavía muchas *apps* que carecen de políticas de privacidad, y los que las contemplan, frecuentemente son oscuras y poco transparentes, lo que dificulta enormemente la lectura y la comprensión de las mismas. En este sentido, un estudio de 2013 constata que sólo el 61% de las aplicaciones más descargadas, contempla una política de privacidad. La falta de política de privacidad, sumado a la gratuidad del producto, debería resultar un argumento más que suficiente para descartar determinadas aplicaciones de mensajería en el entorno corporativo, ya que ello genera indudablemente desconfianza sobre el modo en que son tratados los datos. Cabe considerar que las empresas, no sólo tratan datos personales, sino también datos confidenciales que deben ser custodiados con igual o mayor protección, aunque no exista una normativa que obligue a aplicar determinadas medidas de seguridad para estos últimos.

La seguridad no es sinónimo de privacidad

Estos últimos años, la mayoría de aplicaciones de mensajería instantánea ha incrementado de forma sustancial la seguridad en las comunicaciones. Ello ha contribuido a evitar que ciberdelincuentes y gobiernos accedan de forma indebida a las comunicaciones de los usuarios.

Los usuarios, tal como establece la propia Constitución Española en su artículo 18, tienen derecho al secreto de las comunicaciones que pretende garantizar la impenetrabilidad de la comunicación frente a terceros ajenos a ella.

En el ecosistema de las aplicaciones de mensajería, resulta prácticamente imprescindible contar con un mecanismo de cifrado. Algunas de las principales *apps* han apostado por el cifrado SSL que evita el acceso durante la comunicación entre el usuario y el servidor, otras sin embargo han preferido contar con protocolos de cifrados aún más robustos como el *end-to-end* que evitan además que el servidor pueda acceder al contenido de la comunicación, cifrándola desde el emisor hasta el destinatario.

Efectivamente la seguridad (y con ello, el cifrado) es un elemento fundamental en las comunicaciones pero no debemos olvidar que la implementación de medidas de seguridad sólo representa un aspecto en la Ley Orgánica de Protección de Datos. Por tanto, el hecho de incorporar robustas medidas de seguridad no significa *de facto* que sea conforme con la normativa de protección de datos.

En esta misma línea, el Reglamento de la Ley Orgánica de Protección de Datos, que regula el conjunto de medidas de seguridad que deben aplicarse durante el tratamiento de datos personales en función de su naturaleza, establece que en tratamientos de datos sensibles que requieran la aplicación de medidas de seguridad de nivel alto, la transmisión de dichos datos "*(...) se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que*

garantice que la información no sea inteligible ni manipulada por terceros". Así pues, el cifrado de las comunicaciones resulta a su vez sólo una medida de seguridad de todas las contempladas por el citado Reglamento.

Por tanto, el hecho de incorporar un cifrado robusto en la comunicación no conlleva el cumplimiento de la normativa de protección de datos y por tanto no debería asumirse la privacidad en la comunicación. La normativa de protección de datos busca conciliar tanto la seguridad como la privacidad. Dichos términos pueden parecer sinónimos en un principio, pero revisten de notables diferencias.

La privacidad en las aplicaciones de mensajería sólo existiría en el caso de que éstas pudieran demostrar de forma efectiva garantías sobre el cumplimiento del derecho a la intimidad y el derecho a la protección de datos, en su totalidad.

La cesión de datos personales en las apps

Como norma general, la cesión de datos de carácter personal precisa el consentimiento del afectado.

La normativa de protección de datos, en España, permite recabar el consentimiento para la cesión de datos, de forma expresa (mediante el marcado de una casilla) o de forma tácita. El consentimiento tácito, si bien no resulta una forma válida de obtención del consentimiento según el Reglamento General de Protección de Datos (UE) que será de plena aplicación el 25 de mayo de 2018, resulta todavía un mecanismo permitido en España. Este se encuentra regulado en el Reglamento de la Ley Orgánica de Protección de Datos:

> *"Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.*
>
> *En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento."*

Así pues, las *apps* en el momento de descargarlas pueden solicitarnos de forma expresa o tácita el consentimiento para la cesión de los datos personales. Tal como hemos comentado anteriormente, la información tiene un valor económicamente cuantificable y por ello algunas aplicaciones de mensajería instantánea han optado por ceder determinados datos de sus usuarios. Según datos contrastados del informe de Technology Science "*Who Knows What About Me"*de 30 de octubre de 2015 algunas de las principales *apps* de mensajería instantánea ceden determinados datos de sus usuarios.

Los usuarios de estas (y otras) aplicaciones de mensajería instantánea pueden no ser consientes de las cesiones de sus datos personales, bien porque las cláusulas legales resultan oscuras o poco claras, o bien porque las políticas de privacidad simplemente no hacen mención de ello. En cualquier caso, resulta evidente que existen intereses diversos sobre los datos de los usuarios y raramente la cesión de información se realiza con carácter altruista.

Las apps deben incorporar las obligaciones del nuevo Reglamento (UE)

El pasado 27 de abril de 2016 se publicó en el Diario oficial de la UE el Reglamento General de protección de Datos. Esta disposición normativa incorpora, entre otras cosas, determinadas novedades enfocadas a las aplicaciones móviles. En especial los conceptos "*privacy by design"* y el *"privacy by default"* ya desarrollados en el Dictamen 02/2013 del Grupo de Trabajo de Artículo 29.

El concepto de "*privacy by design"* o privacidad desde el diseño exige que los fabricantes de dispositivos o aplicaciones incorporen las salvaguardas necesarias para garantizar la protección de datos y la intimidad de sus usuarios. Esto incluye garantizar la disponibilidad de mecanismos apropiados para informar y educar al usuario final sobre lo que las aplicaciones pueden hacer y los datos a los que pueden acceder, así como proporcionar configuraciones adecuadas para que los usuarios de *apps* modifiquen los parámetros del tratamiento. A modo de ejemplo, ninguna aplicación de mensajería instantánea que no permitiese evitar o revocar el acceso a su agenda de contactos en cualquier momento, sería conforme al Reglamento.

Por otro lado, el concepto de *"privacy by default"* o privacidad por defecto exige que los fabricantes de dispositivos o de aplicaciones incorporen la protección de datos desde el inicio de su diseño, es decir, la máxima protección desde el momento en que el usuario se instala la *app* en su dispositivo. Las aplicaciones por tanto deberán poder acceder únicamente a los datos que realmente necesitan para funcionar correctamente y deberá ser el usuario quien, libremente y bajo su voluntad, facilite o decida revelar más información. A modo de ejemplo, ninguna *app* debería solicitar en su registro más datos de los estrictamente necesarios ni recabarse más información sobre comportamiento del usuario (*logs*) salvo que el mismo lo consienta.

Sin duda el Reglamento aprobado recientemente establece unas nuevas "reglas de juego" en el ecosistema de las *apps* que a los desarrolladores y a los fabricantes no les quedará más remedio que aplicar. La gran ventaja de este nuevo Reglamento es su aplicación extraterritorial, ello significa que todas las empresas que traten datos de ciudadanos europeos quedaran sujetas a dichas obligaciones, aunque el tratamiento no se efectúe en territorio europeo.