Guía legal sobre privacidad en el sector *fintech*

13 de junio de 2016

El *fintech*, término que surge de la unión de las palabras "*finance*" y "*technology*", consiste en la prestación de servicios financieros mediante la utilización de herramientas tecnológicas. Se trata de un concepto amplio en el que se incluyen servicios muy diferentes, como los que permiten a sus usuarios realizar transferencias de pequeñas cantidades de dinero, los diseñados para la gestionar de gastos o los que ponen en contacto a personas que necesitan financiación con inversores a través de redes *peer to peer*. Debido a su propia actividad y al tipo de clientes a los que se dirigen, la adaptación a la normativa de protección de datos personales se erige en uno de los principales retos a que se enfrentan las compañías que prestan servicios *fintech*.

Esta guía repasa algunas de las principales implicaciones jurídicas que debe tener en cuenta una compañía *fintech* en materia de privacidad, tanto en la actualidad como con la próxima entrada en vigor del Reglamento general de protección de datos.

1. Titularidad y tratamiento de la información.

Los servicios *fintech* llevan a cabo tratamientos de datos personales de gran relevancia, tanto desde un punto de vista cualitativo como desde un punto de vista cuantitativo. Y es que estas compañías tratan datos de índole financiera -con una especial sensibilidad- de gran cantidad de individuos: la totalidad de sus usuarios.

Esta actividad otorga a la compañía *fintech* la condición de Responsable, en tanto que sujeto que determina los medios que utiliza para tratar los datos y los fines exactos del tratamiento. Para que este tratamiento sea lícito, el Responsable deberá observar, entre otras cuestiones, los principios que rigen la normativa de protección de datos, entre los que destaca (i) el principio de calidad de los datos, (ii) el principio de consentimiento informado o licitud del tratamiento o (iii) el principio de seguridad de los datos.

La compañía *fintech* sólo deberá obtener los datos mínimos e imprescindibles para prestar su servicio, y deberá mantenerlos únicamente durante el tiempo necesario. Además, deberá informar al usuario de cuestiones como su identidad y datos de contacto, los fines para los que va a utilizar los datos, los posibles destinatarios de los mismos, el tiempo durante el que va a conservarlos, la posibilidad de ejercitar sus derechos ARCO y el derecho a la portabilidad de los datos, el derecho a reclamar ante la autoridad de control correspondiente o si va a elaborar perfiles individuales, entre otras cuestiones.

Para garantizar la confidencialidad de la información, la compañía también deberá adoptar medidas de seguridad de índole técnica y organizativa adecuadas. El Reglamento (UE) 2016/679 (en adelante, "Reglamento general de protección de datos") complementa este deber de seguridad introduciendo principios como el *privacy by design*, el *privacy by default* o el principio de *accountability*. El *privacy by design* exige al Responsable aplicar las medidas de seguridad adecuadas para el tratamiento de los datos desde un momento inicial, es decir, aún antes del propio tratamiento. El *privacy by default*, por su parte, establece necesidad de restringir por perfiles el acceso a los datos de la compañía. Por último, el principio de *accountability* exige al Responsable que sea capaz de demostrar el cumplimiento de todas las obligaciones establecidas en la norma.

Así, la aprobación de este nuevo Reglamento General de Protección de Datos también incluye otras novedades como el derecho al olvido y el derecho a la portabilidad de datos de los usuarios que lo soliciten, la obligación de realizar evaluaciones de impacto en la protección de datos (PIAs – *Privacy Impact Assesment*) y la obligación de notificar las brechas de seguridad que pongan en riesgo datos de carácter personal.

Las compañías que prestan servicios *fintech* deben ir adaptando sus procesos a las novedades que introduce el Reglamento General de Protección de Datos, pero sin descuidar el cumplimiento que la normativa actual les exige.

2. Invalidación del Safe Harbor agreement.

En octubre de 2015 se publicó la sentencia del Tribunal de Justicia de la Unión Europea que resolvía el asunto C-362/14, invalidando el Acuerdo de Puerto Seguro (*Safe Harbor Agreement)* suscrito entre la Unión Europea y Estados Unidos en el año 2000, y que tenía por objeto facilitar la legitimación de las transferencias de información personal a compañías establecidas en Estados Unidos. Esta sentencia trae causa en las revelaciones que realizó en 2013 Edward Snowden, que hizo público que las compañías estadounidenses permitían a las agencias gubernamentales de inteligencia el acceso indiscriminado a la información y las comunicaciones de usuarios residentes en la UE. Su invalidación afecta a cualquier compañía que transfiera información personal a compañías estadounidenses, entre las que se encuentran los prestadores de servicios *fintech*.

La normativa de protección de datos establece que los Responsables o Encargados del tratamiento que realicen transferencias de datos personales a países que no garanticen un nivel de protección equivalente al exigido en la UE, como sucede con Estados Unidos, tienen que solicitar una autorización expresa a la Agencia Española de Protección de Datos o acogerse a una serie de casos excepcionales.

Con la invalidación del Acuerdo de Puerto Seguro se produce un retorno a la situación anterior: las compañías estadounidenses que se encontraban adheridas ya no garantizan el nivel de protección adecuado. El TJUE indicó en los párrafos 21 y 22 de la sentencia señalada que *"en la práctica un número elevado de empresas certificadas no respetaban, o no lo hacían plenamente, los principios de puerto seguro" y que "aparentemente todas las empresas involucradas en el programa PRISM [programa de recogida de informaciones a gran escala], y que conceden a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro» y que ello «ha hecho del puerto seguro uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que han sido tratados inicialmente en la [Unión]"*. Añade en el párrafo 94 que *"se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada"*.

Por tanto, las entidades que realizan transferencias internacionales a compañías estadounidenses deben legitimar tal transferencia por una nueva vía, distinta del Acuerdo de Puerto Seguro. Esta sentencia afecta especialmente a las compañías de servicios *fintech*, que suelen valerse de compañías estadounidenses para cuestiones como el desarrollo o soporte de su sitio web o aplicación móvil, la prestación de servicios de seguridad de la información o, en mayor medida, la utilización de servicios de *cloud*.

Actualmente, las compañías españolas deben legitimar esta transferencia mediante la obtención de la autorización de la AEPD o siguiendo alguno de los casos excepcionales que prevé la normativa. En el caso de los servicios *fintech*, podrán legitimar la transferencia obteniendo el consentimiento inequívoco del usuario del servicio mediante la aceptación de una versión actualizada de las condiciones de uso.

No obstante, Estados Unidos y la Unión Europea se encuentran en pleno proceso de negociación de un nuevo acuerdo que vuelva a legitimar las transferencias internacionales a este país: el denominado *Privacy Shield*, cuyo primer borrador ha recibido las críticas del Grupo de Trabajo del artículo 29. Parece que este nuevo acuerdo no será aprobado hasta dentro de varios meses.

3. Big Data.

Una de las principales utilidades del *Big Data* consiste en el análisis de grandes cantidades de información con el objeto de extraer patrones individuales o colectivos de conducta que faciliten la toma de decisiones. En el contexto de los servicios *fintech*, el *Big Data* puede utilizarse para múltiples aplicaciones, pero todas ellas pueden agruparse en dos categorías. Por un lado, el *Big Data* se utiliza para analizar información relacionada únicamente con una persona determinada, como conocer cuántas veces al año cena fuera de casa o en qué sitios. Por otro, se emplea para obtener patrones generalizados de conducta o tendencias de un conjunto más o menos amplio de personas.

La trascendencia de la protección de datos de carácter personal es evidente en la primera categoría, ya que la obtención de patrones comportamentales de personas concretas queda circunscrito necesariamente a su régimen jurídico. Cabe resaltar, asimismo, que aunque el nuevo Reglamento general de protección de datos no contiene ninguna alusión expresa al *Big Data*, sí introduce restricciones a la elaboración de perfiles o perfilado. Pero también la delimitación de tendencias generales o estadísticas puede verse sometida a la normativa de protección de datos, ya que los recursos utilizados para su creación serán, en muchos casos, datos personales. En otras palabras, la elaboración de un perfil individualizado de conducta se considera en sí mismo información personal, pero un

patrón colectivo o estadístico se puede crear a partir de información personal.

El régimen jurídico de la protección de datos resulta de vital relevancia, puesto que el enorme potencial del *Big Data* lleva consigo importantes riesgos para la privacidad de los sujetos, cuya información personal compone buena parte de la base sobre la que se apoya el sistema. A pesar de que algunos actores han manifestado que los actuales principios rectores de la privacidad deberían ceder por suponer una barrera insalvable para el *Big Data*, las instituciones consideran que su convivencia con la privacidad es posible.

Lo cierto es que el derecho a la privacidad y, más concretamente, el derecho de una persona a decidir para qué finalidades se utiliza la información que le incumbe, se ha configurado como un derecho fundamental en instrumentos jurídicos internacionales y nacionales, tal y como ha reconocido el Tribunal Constitucional. Por tanto, el éxito del *Big Data* debe limitarse y someterse en todo caso al necesario respeto a este derecho fundamental.

3.1. Uso de *Big Data* en relación con personas concretas.

Para que el tratamiento de información personal que realiza una compañía de servicios *fintech* sea legítimo, deberá observar todos los principios rectores de la normativa ya mencionados. En el contexto del *Big Data*, adquieren una relevancia destacada los principios de la finalidad y del consentimiento, en virtud de los cuales el Responsable sólo podrá tratar los datos del interesado para la finalidad que hubiera sido consentida. De esta manera, el servicio *fintech* no podrá trazar patrones comportamentales si no hubiera obtenido una autorización explícita e independiente para ello tras haber informado al afectado de cuestiones como (i) la identidad del Responsable, (ii) los posibles destinatarios de los datos, (iii) el plazo durante el que se conservarán los datos, (iv) la posibilidad de ejercitar los derechos ARCO y el derecho a la portabilidad de los datos, (v) los fines para los que se van a tratar los datos y (vi) la existencia de elaboración de perfiles, haciendo una referencia expresa a la importancia y consecuencias del tratamiento, así como a la lógica o metodología aplicada.

El Reglamento general de protección de datos ha modificado el concepto de consentimiento que recogía la Directiva 95/46/CE, exigiendo necesariamente que tal consentimiento tenga un carácter activo. Por tanto, el usuario del servicio *fintech* deberá aceptar expresamente la utilización de su información personal para fines de *Big Data* relacionados con la individualización de su comportamiento.

Esta nueva norma rectora de la privacidad en la UE establece, también, importantes restricciones al perfilado, es decir, a la utilización de datos personales para *"analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física"*. El análisis de grandes cantidades de información relativas a una persona constituye uno de los ejemplos más claros de perfilado. Aplicado a los servicios *fintech*, sirve para predecir cuestiones como la situación económica del interesado, lo que puede ser muy valioso para las entidades de crédito, que contarán con una fuente de información ideal para determinar la concesión o no de, por ejemplo, un préstamo hipotecario.

Los usuarios de los servicios *fintech* podrán oponerse en todo momento a la elaboración de perfiles. Asimismo, esta práctica implica la obligación de realizar evaluaciones de impacto a la protección de datos (PIAs), de conformidad con el artículo 35 del Reglamento general de protección de datos.

3.2. Uso de *Big Data* para obtener datos colectivos o estadísticos.

El *Big Data* no sólo es útil para trazar perfiles individualizados, sino que también sirve para extraer tendencias o patrones conductuales de cualquier colectivo más o menos amplio de individuos. La utilización de información para fines estadísticos se encuentra contemplada de forma expresa tanto en la Directiva 95/46/CE como en el Reglamento general de protección de datos. De hecho, este último indica que *"el tratamiento ulterior de los datos personales [...] con fines estadísticos no se considerará incompatible con los fines iniciales"*, aunque se deberán establecer las garantías oportunas para proteger a los individuos afectados.

Podría parecer que este precepto habilita a los proveedores de servicios *fintech* a tratar los datos personales de sus usuarios para elaborar estadísticas. Sin embargo, su aplicación al caso resulta ciertamente improbable, ya que el propio Considerando 156 del Reglamento general de protección de datos dispone que *"El tratamiento ulterior de datos personales con [...] fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados"*. En consecuencia, los servicios *fintech* no podrán mantener información estadística de índole colectiva que permita la identificación de los individuos cuyos datos se han utilizada para la elaboración de la misma si pueden satisfacerse los mismos fines mediante la utilización de información disociada o anonimizada.

Así, los servicios *fintech* que deseen elaborar patrones colectivos de conducta deberán anonimizar de forma adecuada la información personal que se integre en su estudio. La anonimización se considera una forma de cancelación de la información personal, dado que suponer quebrar el vínculo entre un dato concreto y el individuo a que se refiere. De esta forma, la normativa de protección de datos deviene inaplicable. Resulta de utilidad, en este sentido, la Opinión 05/2014 (WP 216) del Grupo de Trabajo del Artículo 29, que analiza los puntos fuertes y las debilidades de diferentes técnicas de anonimización como la adición de ruido, la permutación, la agregación, la *k-annonymity*, la *l-diversity* o la *t-closeness*.

4. Autenticación en servicios *fintech*.

En la sociedad actual, usualmente denominada *sociedad de la información*, el número de personas que utiliza servicios digitales para solventar sus necesidades del día a día aumenta continuamente. Tareas tan rutinarias como reservar mesa en un restaurante, pedir un taxi, realizar la compra o, por supuesto, confirmar una transacción bancaria, han dejado de ser acciones que se realizan estrictamente en la esfera *offline* gracias a la proliferación de aplicaciones o plataformas digitales. Estos servicios digitales simplifican enormemente los quehaceres diarios de las personas, permitiendo optimizar el tiempo y ofreciendo mayor comodidad.

Uno de los principales desafíos de estos servicios digitales consiste en la autenticación de los usuarios, es decir, en la utilización de mecanismos que garanticen que los individuos que utilizan la herramienta son realmente quienes dicen ser. La necesidad de autenticación es relevante para cualquier plataforma, pero adquiere una trascendencia especial para aquellos servicios que, como los servicios *fintech*, están relacionados con cuestiones tan sensibles como la vida financiera de sus usuarios. La autenticación persigue varios objetivos. Por un lado, asegura que sólo la persona oportuna pueda acceder a espacios privados en los que se contiene información sensible. Por otro, garantiza que las operaciones que realizan los usuarios a través de la plataforma sean válidas desde el punto de vista jurídico, es decir, asegura la validez de los consentimientos otorgados en el mundo digital.

4.1. La autenticación como garantía de confidencialidad.

Las entidades bancarias que ofrecen herramientas *fintech* se encuentran vinculadas por el denominado secreto bancario, en virtud del cual deben asegurar la confidencialidad de la información financiera de sus clientes, no desvelándola a terceros. Además del secreto bancario, también están obligadas a guardar secreto de conformidad con la normativa de protección de datos, que los considera Responsables de los mismos. Estos deberes se relacionan con el derecho a la intimidad y el derecho de *habeas data* de las personas. Para garantizar la obligada confidencialidad, las plataformas *fintech* deben instaurar medidas de seguridad técnicas y organizativas suficientes para evitar que la información de sus clientes pueda llegar a ser conocida por terceros.

Pues bien, la restricción de acceso a los espacios personales de las aplicaciones *fintech* constituye una medida de seguridad básica de inexcusable instauración para poder asegurar la debida confidencialidad de la información de un usuario. Las compañías que prestan servicios *fintech* son conscientes de esta necesidad, por lo que tratan de ofrecer mecanismos de autenticación cada vez más seguros que contribuyan a generar confianza en los usuarios. Aunque las contraseñas, códigos PIN (*Personal Identification Number*) o tarjetas de coordenadas siguen siendo mecanismos de autenticación muy habituales en la práctica, los servicios *fintech* están tratando de desmarcarse de ellos incorporando procedimientos más seguros y cómodos.

Los mecanismos de autenticación suelen clasificarse en tres grupos: (i) los basados en algo que el individuo conoce, como una contraseña; (ii) los basados en algo que el individuo posee, como una tarjeta de coordenadas o un certificado electrónico; y (iii) los basados en rasgos biométricos del usuario, como el reconocimiento de su huella dactilar, de su voz o de su rostro. Los mecanismos de autenticación basados en biometría aseguran una nivel de seguridad superior, por los que algunas entidades que ofrecen herramientas *fintech* ya han comenzado a utilizarlos o van a hacerlo próximamente. Es el caso, por ejemplo, de Apple Pay, Android Pay o Samsung Pay, que permiten la autenticación a través de huella dactilar. También Mastercard introducirá, durante 2016, la autenticación a través de reconocimiento facial, por lo que los usuarios de su servicio podrán confirmar pagos realizando un simple *selfie*.

Además de la autenticación basada en los rasgos biométricos del usuario, los servicios *fintech* suelen utilizar mecanismos de autenticación en dos factores. En estos casos, el acceso a su espacio privado o la prestación de su consentimiento para obligarse contractualmente se realizaría mediante la combinación de dos métodos de autenticación diferentes. Ya es habitual que se combinen métodos basados en algo que el usuario conoce con métodos basados en algo que el usuario tiene: una cuenta de usuario combinada con un código recibido por SMS, por ejemplo.

La utilización de estos nuevos mecanismos permite, en definitiva, que la información relativa a un usuario sólo pueda ser conocida por él mismo.

4.2. Validez jurídica del consentimiento digital.

Los nuevos mecanismos de autenticación no sólo son útiles a la hora de permitir el acceso a un espacio privado únicamente al interesado, garantizando de esta manera el deber de confidencialidad exigido todo servicio *fintech*. También permiten que los consentimientos prestados por los usuarios sean válidos. La adhesión a las condiciones generales del servicio *fintech* en cuestión o la confirmación de un pago, entre otras acciones, implican una emisión de voluntad que deben ser válidas jurídicamente y cuya autenticidad debe poder acreditarse.

Si en el mundo físico la emisión del consentimiento se suele realizar mediante una simple firma manuscrita, este mecanismo pierde su operatividad en el mundo digital. En la esfera online, el simple trazo de unas líneas sobre una *tablet* o un *smartphone* puede ser falseado fácilmente, ya que resulta muy complicado verificar la autenticidad de una firma sin poder analizar elementos tan relevantes como el grado de presión o la continuidad del trazo.

Para asegurar que un consentimiento es válido en el mundo digital es necesario recurrir a mecanismos de autenticación como los mencionados, que se convierten en este punto en mecanismos de firma electrónica. La firma electrónica se regula en la Ley 59/2003, de 19 de diciembre, de firma electrónica, que será derogada próximamente con la entrada en vigor total, en julio de 2016, del Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. El Reglamento nº 910/2014 define la *firma electrónica* como *"los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar"*. En otras palabras, una firma electrónica es cualquier tipo de información electrónica que, unida a otra, utiliza una persona para identificarse. De la definición de firma electrónica se pueden extraer tres notas características: (i) que se utilicen un conjunto de datos electrónicos, (ii) que estén consignados junto a otros o asociados a ellos y (iii) que puedan ser utilizados para identificar al firmante.

Así, la unión de una huella dactilar digital o de un código recibido por SMS a una cuenta de usuario supone realizar una firma electrónica, ya que se cumplen las tres notas características de las mismas. En primer lugar, se utilizan datos electrónicos, ya que la huella dactilar digital o el código recibido por SMS es información en formato electrónico. En segundo lugar, esta información está consignada junto a otra: el nombre de usuario o ID del firmante. Por último, se utilizan para identificar al firmante, ya que sólo él dispondrá del conocimiento o los medios necesarios para realizar la acción. En consecuencia, la utilización de estos mecanismos permiten realizar firmas electrónicas.

Estas firmas electrónicas son plenamente válidas jurídicamente, como reconocen tanto la Ley 59/2003 como el Reglamento (UE) nº 910/2014, que la sustituye. Este último indica expresamente que *"No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada"*. Así, la normativa aplicable establece claramente que estas firmas electrónicas (i) tienen eficacia jurídica y (ii) son admisible como prueba en procedimientos judiciales.

Por otro lado, la posible impugnación de la autenticidad de esta clase de firmas podrá ser rebatida mediante un informe pericial o cualquier otra prueba válida que detalle el funcionamiento técnico del mecanismo.

5. Notificación de violaciones de seguridad.

Una de las principales novedades que introduce el Reglamento general de protección de datos consiste en la obligación de notificar a la autoridad líder y, en ocasiones, al afectado, aquellas violaciones o brechas de seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado de terceros.

El artículo 33 del nuevo Reglamento obliga a notificar estas quiebras

en un plazo máximo de 72 horas desde que tuvieran constancia de la misma, aunque es posible hacerlo más tarde si se acreditan los motivos de la dilación. La notificación debe contemplar, al menos, cuestiones como (i) la descripción de la naturaleza de la violación, (ii) el grado de sensibilidad de los datos y el número de interesados afectados, (iii) la identificación del delegado de protección de datos o persona que vaya a gestionar la incidencia con la autoridad líder, (iv) la descripción de las posibles consecuencias de la violación y (v) las medidas que se proponen para mitigar o remediar los efectos de la violación de seguridad.

Por otro lado, también se deberá notificar la quiebra de seguridad a los propios afectados, sin dilación, cuando sea probable que la misma suponga un riesgo alto para sus derechos, de forma que puedan llevar a cabo con la máxima rapidez las medidas oportunas para proteger sus intereses. La especial sensibilidad de los datos que manejan los prestadores de servicios *fintech*, que disponen de información financiera de sus usuarios, supone que el riesgo vaya a ser considerado alto en buena parte de los casos, aunque este extremo deberá determinarse específicamente mediante la elaboración previa de una evaluación de impacto (PIA). No obstante, el Responsable podrá evitar esta notificación, que genera un daño reputacional difícilmente reparable a la compañía, mediante la adopción de medidas que hagan ininteligibles los datos personales afectados. El Reglamento considera que una vía adecuada para lograr la ininteligibilidad de los datos personales es el cifrado de los mismos, por lo que los servicios *fintech* deben considerar la implantación de esta medida.

La obligación de notificar brechas de seguridad a la autoridad competente y a los usuarios afectados ya existe en la actualidad para un tipo de compañías determinadas: los prestadores de servicios de comunicaciones electrónicas, pues así lo establece la Directiva 2002/58/CE. Esta obligación ha sido transpuesta en España mediante el artículo 41 de la Ley General de Telecomunicaciones y desarrollada a través del Reglamento (UE) nº 611/2013. Finalmente la obligación se extenderá, a partir de mayo de 2018, a cualquier Responsable que trate datos personales, sin importar su sector de actividad.

ONTIER

Departamento: Tecnología y Propiedad Intelectual
Contacto: Joaquín Muñoz jmunoz@ontier.net