El nuevo Reglamento General de Protección de Datos

En búsqueda del equilibrio entre tecnología y privacidad, el Reglamento tiene la finalidad de concienciar tanto a los responsables que tratan datos personales como a los propios ciudadanos y supone un desafío importante para la sociedad en su conjunto.

Patricia Juárez | *Consultora del área jurídica de Afi*
Beatriz Castro | *Consultora del área de Servicios Financieros de Afi*

Big Data, *fintech*, globalización y digitalización son conceptos con los que estamos familiarizados y que en los últimos años han adquirido una importancia fundamental. La conocida como «cuarta revolución industrial» es ya una realidad, en la que la tecnología afecta de forma directa a la forma en la que vivimos y a las relaciones personales y profesionales. El alcance de los efectos es difícil de determinar, por la escala y la complejidad de la transformación. En este contexto, supone un desafío garantizar el **derecho a la privacidad**, derecho humano fundamental reconocido en distintos tratados internacionales, máxime cuando el dato se configura como activo de gran valor en varios ámbitos.

La Directiva 95/46/CE no era suficiente para atender las exigencias de la **Sociedad de la Información**, pues aunque sus principios sean válidos, no otorgaba la suficiente seguridad en materia de protección de datos personales, existiendo un riesgo para las personas físicas. Así, tras más de veinte años de avances tecnológicos, era una exigencia elaborar un nuevo texto normativo adaptado a la realidad actual, en la que la globalización ha ocasionado un incremento de los flujos transfronterizos de datos. Precisamente a esta exigencia responde el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 («Reglamento General de Protección de Datos»), que resultará de aplicación a partir del próximo **25 de mayo de 2018**.

Pero ¿por qué es tan relevante el Reglamento? ¿Realmente supone un cambio sustancial con respecto a la normativa anterior? La respuesta es, sin lugar a dudas, sí. Hay un cambio estructural en la definición del sistema de protección de los derechos de las personas físicas en relación con el tratamiento de sus datos personales. Quizá uno de los rasgos más relevantes del Reglamento es la **transversalidad** del mismo: no solo afecta a las entidades financieras, sino a todas las organizaciones que realicen tratamientos de datos perso-

nales. Centros docentes, colegios profesionales, entidades que exploten redes y presten servicios de comunicaciones electrónicas, centros sanitarios, organizaciones que desarrollen actividades de publicidad y prospección comercial y la propia administración pública son solo algunos de los afectados en un contexto en el que el tratamiento de datos personales está a la orden del día.

Pero, más allá de esta necesaria actualización, el Reglamento tiene la finalidad de concienciar a la sociedad en su conjunto, no solo a los responsables que tratan datos personales sino también a los propios ciudadanos propietarios de sus datos. En general, estamos más que familiarizados con la existencia de largas cláusulas de protección de datos, pero rara vez las revisamos con detalle. El lenguaje excesivamente jurídico, el tamaño de la fuente, o la extensión del texto son incentivos suficientes para que aquellos que, heroicamente, han intentado pasar del primer párrafo, desistan de tal hazaña. Ya sea en formato electrónico o en papel, se busca el espacio para la firma o el botón de «acepto», y nada más.

Sin embargo, cuando nuestro dispositivo móvil nos pide que valoremos el restaurante del que acabamos de salir, sin haber hecho nada «activamente» que le permitiera saber dónde íbamos a comer, es normal sentirse en cierta medida contrariado, incluso observado: «¿Cómo sabe que acabo de comer en este restaurante?» Seguramente hayas reservado a través de una aplicación, a la que le permitiste acceso a tu agenda, a tus contactos y a tu ubicación. De hecho, es más que posible que posteriormente recibas correos electrónicos solicitando tu valoración del restaurante, o promociones para ese local, o para otros que, por tus gustos, pueden encajar con tu perfil. ¿En qué momento has autorizado que un innumerable número de empresas conozcan, evalúen, perfilen y monitoricen tus preferencias? De forma más o menos consciente, la autorización existe desde que se pulsa el botón de «Acepto» para tener esa aplicación tan cómoda que, además, es gratis. Y como se suele afirmar, «si el servicio es gratis, el producto eres tú».

Por esta razón, la concienciación y formación son dos elementos esenciales para el éxito de la implementación del nuevo Reglamento que, junto con la obligación de informar de forma concisa, transparente, inteligible y fácilmente accesible, garantizan de forma efectiva el control por parte de los interesados de sus datos personales. Atrás quedaron aquellas extensas cláusulas pocas veces leídas y, en ocasiones, aceptadas con demasiada facilidad.

Implicaciones para el sector bancario. Un cambio de paradigma

Desde que se publicó el Reglamento en abril de 2016, muchos fueron los que se llevaron las manos a la cabeza pensando en cómo afectaría esta nueva normativa a la actividad diaria de cualquier banco. Después de años interiorizando la idea de que «el valor está en los datos», invirtiendo millones en grandes proyectos para «extraer el valor de los datos», e implementando nuevas tecnologías que favoreciesen esta tendencia (*Big Data*, modelos predictivos, *Machine Learning*, computación cognitiva, etc.), el Parlamento Europeo y el Consejo de la Unión Europea publican un nuevo Reglamento que parece que dificulta estos esfuerzos. Durante los dos años que se han otorgado como periodo de adaptación al Reglamento, las entidades «más aplicadas» que empezaron a trabajar en su implantación de forma temprana se han enfrentado a numerosos escollos.

En primer lugar, identificar los flujos de datos personales en un banco es una tarea complicada y ambiciosa, y es que, en definitiva, el **concepto de dato personal** comprende *cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*. Por tanto, la mayor parte del trabajo de las entidades financieras se realiza sobre datos personales: las cuentas, los movimientos, los productos contratados, etc.

La definición de dato personal es tan amplia que abarca prácticamente toda la información que se utiliza en las entidades financieras, a excepción de dos grandes categorías: la **información anónima** y los datos referentes a las **personas jurídicas**. En el primer caso, el Reglamento no resulta de aplicación, si bien en el segundo conviene apuntar una serie de matices. ¿Toda la información relativa a las personas jurídicas está excluida del ámbito de aplicación del Reglamento? En efecto, así sucede con datos como la razón social, el domicilio, los estados financieros, etc. (sin perjuicio, en su caso de las obligaciones de confidencialidad). Ahora bien, **¿qué sucede con los conocidos como datos profesionales?** La interpretación mayoritaria es clara, y señala que este tipo de datos, característicos del ámbito mercantil, se encuentran dentro del ámbito de aplicación del Reglamento, pero su tratamiento se encuentra amparado por el interés legítimo, concepto que veremos más adelante.

Una vez acotado el perímetro de aplicación del nuevo Reglamento (tan complejo y tan sencillo a la vez como decir «toda la organización») la siguiente pregunta es «¿quién se va a hacer cargo de todo esto?» Tradicionalmente, el grueso de responsabilidad de la antigua normativa de protección de datos («LOPD») residía en los departamentos de tecnología y operaciones (Seguridad de la Información, Administración Central, etc.), con apoyo de las áreas de Asesoría Jurídica y/o Cumplimiento Normativo. Esto tiene sentido si nos paramos a pensar cómo se configuran las obligaciones de la antigua LOPD: declaración de ficheros a la Agencia Española de Protección de Datos (AEPD), elaboración

de un Documento de Seguridad, procedimiento para garantizar el ejercicio de los derechos a los interesados y aplicación de diferentes medidas de seguridad a aplicar de acuerdo al nivel de seguridad de los datos.

Sin embargo, este modelo de gobierno deja de ser válido bajo el nuevo Reglamento debido al nuevo **principio de responsabilidad proactiva**. Este principio implica que las medidas correctivas en materia de protección de datos no son suficientes, sino que es necesario introducir la protección de datos en la **cultura de la organización,** desde las capas operativas hasta las de dirección y gestión, de tal forma que todas las medidas preventivas que se adopten queden documentadas para poder demostrar el cumplimiento con la norma. Por tanto, el Reglamento supone el cambio desde un modelo «paternalista», con unas instrucciones más o menos claras para cumplir con la norma, hacia un modelo de **autorregulación** en el que la norma puede resultar ambigua (quedando sujeta a la interpretación de la misma, en línea con la *Common law* anglosajón). Algunas de las consecuencias son las siguientes:

• No será necesario declarar los ficheros a la AEPD, pero será preciso elaborar un **registro interno** de los tratamientos de datos personales.

• Se sustituyen las medidas de seguridad asociadas a las diferentes categorías de datos debiendo llevarse a cabo una evaluación de impacto (*DPIA, Data Protection Impact Assesment*, por sus siglas en inglés) y, en función del resultado de este análisis, aplicar las medidas se seguridad que sean más apropiadas.

• En el supuesto de que se produzca una incidencia de seguridad de datos personales, la organización deberá notificar tal hecho a la a la AEPD y, en algunos casos, a los propios afectados. No es suficiente la gestión interna de la incidencia, aumentando por tanto el riesgo reputacional de las entidades.

Todas estas modificaciones hacen que sea imposible definir una única figura dentro de los bancos que pueda encargarse del cumplimiento del Reglamento, siendo más aconsejable definir un **órgano de gobierno multidisciplinar**, compuesto por integrantes de diferentes áreas, responsable de supervisar las medidas necesarias para garantizar la adecuada implementación del Reglamento. Este órgano, en línea con el carácter transversal de los tratamientos de datos personales en los bancos, debería estar formado, al menos, por miembros de Cumplimiento Normativo, Asesoría Jurídica, Tecnología y Operaciones, Riesgos, Recursos Humanos y Áreas Comerciales (Negocio, Marketing, etc).

Uno de los fallos más comunes a la hora de implementar el Reglamento es el relativo a las funciones del **Delegado de Protección de Datos** (*DPO, Data Protection Office* por sus siglas en inglés). Esta nueva figura que introduce el Reglamento, obligatorio para todas las entidades financieras, debe ser la responsable de supervisar el cumplimiento de la norma y el punto de contacto dentro de la organización, tanto para autoridades como para interesados, en lo que a protección de datos personales se refiere.

¿Cuál es el malentendido que se está produciendo con respecto al DPO? Muchas entidades que han designado al DPO le han responsabilizado de la adaptación completa al Reglamento. Se trata de una trasgresión del modelo de las tres líneas de defensa, por el cual el DPO debería situarse en la tercera línea, al igual que las áreas de Auditoría Interna, y no en la primera línea de operaciones. Esta confusión genera dentro de los bancos un **conflicto de intereses**, al convertir al DPO en juez y parte. Por ejemplo, si el DPO establece la metodología de evaluación de impacto de los tratamientos de datos personales, al supervisar dicha metodología estará **autoevaluándose**, por lo que es cuestionable afirmar que efectivamente se aplica un criterio objetivo.

Pánico a la protección de datos: el consentimiento

Acotado el ámbito de aplicación del Reglamento y establecidas las responsabilidades, llega el momento de máximo pánico dentro de las entidades financieras, al revisar la nueva definición de **consentimiento**: «*Acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen (…) Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento*» [Considerando (32) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016]. Es entonces cuando las entidades llegan a la fatídica conclusión: «Ya no podemos enviar ninguna comunicación comercial a nuestros clientes». Es conveniente matizar esta afirmación pues, en líneas generales, el Reglamento es más flexible de lo que pudiera parecer y no supone un impedimento en la práctica para las áreas de comunicación.

Efectivamente, la nueva definición de consentimiento hace que los conocidos como «consentimientos tácitos», derivados de la inacción o el silencio, pierdan su validez. La máxima de «salvo que me indiques lo contrario, entiendo que estás conforme» no es suficiente. Además, ya no podemos intercalar las cláusulas relativas a protección de datos entre los eternos clausulados que acompañan a la mayoría de contratos, y considerar que la firma de ese contrato en cuestión supone un consentimiento expreso. Hay que informar, de manera clara y sencilla de los aspectos clave del tratamiento siguiendo el **principio de transparencia** que introduce el Reglamento, y obtener un consentimiento activo y afirmativo. Tampoco se podrá supeditar la prestación de un servicio o comercialización de un

producto a la obtención de un consentimiento que no sea necesario para la ejecución de ese contrato. Por ejemplo, un comercial bancario que esté comercializando tarjetas de crédito no puede condicionar la prestación de su servicio a la obtención de un consentimiento para poder enviar publicidad sobre seguros.

En este punto entra en juego otro principio de marcada importancia en el Reglamento, el **principio** de **minimización de datos**, que presenta una doble vertiente. Así, la minimización de datos se aplica **de forma general**, tratando solamente aquellos datos que sean necesarios para la finalidad del tratamiento en cuestión, y **se minimiza la extensión temporal**, debiendo retener los datos para su tratamiento por el mínimo tiempo necesario. En el caso de los bancos, la tendencia ha sido la de almacenar a lo largo de los años todos los datos de antiguos clientes sin que, en muchos casos, se hayan adoptado medidas para protegerlos o aislarlos (seudonimización o encriptación de datos). Por tanto, en el listado de tareas para la implantación del Reglamento se debe definir cómo garantizar la minimización temporal de los datos, entre otras cuestiones.

En muchos casos los bancos han tratado de abordar el problema de los consentimientos analizando el estado actual de los consentimientos de su stock de clientes. Con frecuencia, la dificultad que se han encontrado es que no contaban con un solo consentimiento (válido o no) por cada cliente, sino que los consentimientos se habían ido recogiendo históricamente por producto o servicio. Por tanto, cada cliente tenía tantos consentimientos como contratos firmados con la entidad. Estos consentimientos variaban en cuanto a forma (digitales o en documento físico) o contenido (diferentes clausulados), haciendo inviable llegar a un estado de situación sobre los mismos. Por tanto, la pregunta más repetida en los bancos ha sido, **¿tengo que pedir consentimientos a todos mis clientes?**

A estos efectos, el Reglamento establece cuatro bases legales válidas para realizar tratamientos de datos personales:

• **Cumplimiento de una obligación legal** (aplicable al responsable), como puede ser la normativa de Prevención de Blanqueo de Capitales y Financiación del Terrorismo (PBC FT).

• **Ejecución de un contrato en el que el interesado es parte**, o aplicación a petición de este de medidas precontractuales: por ejemplo, en el caso de un contrato de cuenta corriente, el banco necesita obligatoriamente tratar datos personales para poder prestar este servicio.

• **Consentimiento válido**, en los términos señalados en el Reglamento, que será necesario cuando se trate de cualquier tratamiento con una finalidad comercial (envío de comunicaciones comerciales, cesión de datos a terceros, estudios y perfiles con fines comerciales).

• **Interés legítimo**. El Reglamento determina que un tratamiento de datos es válido si este es necesario para satisfacer el interés legítimo del responsable, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del afectado.

Es, precisamente, el **interés legítimo** el que está generando mayor incertidumbre, al configurarse como concepto jurídico indeterminado y, en consecuencia, entrar en juego la interpretación en el momento de su aplicación práctica.

La mayoría de los tratamientos de datos personales de los bancos se pueden apoyar en la base de la ejecución de un contrato, exceptuando todos aquellos con finalidades comerciales. Dada la inviabilidad de comprobar la validez de los consentimientos históricos, las entidades se enfrentan a la disyuntiva de solicitar nuevos consentimientos a todos sus clientes para poder seguir usando sus datos con fines comerciales, o bien basarse en el interés legítimo y seguir tratando los datos sin obtener nuevos consentimientos. Los más conservadores opinan que tratar de justificar la existencia de un interés legítimo sin que prevalezcan los derechos y libertades de los interesados es difícilmente justificable. Otros, en cambio, señalan que, tras haber mantenido una relación comercial con los clientes, durante varios años en algunos casos, justifica ese interés legítimo y, por tanto, se puedan seguir realizando tratamientos de datos con fines promocionales.

No obstante, aunque se opte por la vía del interés legítimo, debido al principio de transparencia previamente comentado y a los nuevos requisitos de información recogidos en el Reglamento, será necesario que las entidades realicen, al menos, una comunicación informativa a todos los interesados.

No cabe duda de que la adaptación al Reglamento supone un desafío para la sociedad en su conjunto. Empresas, administración pública y ciudadanos en general deben concienciarse y conocer el valor de los datos, y el efecto de difundir o ceder información no autorizada. La experiencia de Facebook con el escándalo de Cambridge Analytica, las dimisiones de altos cargos por la difusión de información referente a los mismos o el incremento de las amenazas de seguridad, son solo algunos de los casos que ponen de manifiesto la necesidad de controlar los datos personales para garantizar el **derecho a la privacidad** de las personas. Es fundamental implementar las nuevas exigencias, pues de lo contrario la Sociedad de la Información quedará desvirtuada. Y, en este punto, es de nuevo el Reglamento el que en su Considerando (4) nos recuerda que «El tratamiento de datos personales debe estar concebido para servir a la humanidad» y, por tanto, en ningún caso las personas están al servicio de los datos ::