El Foco

La nueva regulación de datos no es una revolución

El reglamento obligará a adoptar otras reglas del juego, pero no son tan nuevas

AMAYA GARCÍA
Abogada de Cremades & Calvo-Sotelo

Con cierta perplejidad asisto al ataque de nerviosismo colectivo que ha invadido a todos los sectores y empresas, de todos los tamaños y colores, con la entrada en vigor del Reglamento General de Protección de Datos.

Efectivamente, la norma introduce novedades y refuerza los principios de la protección de datos, en aras de que ciudadanos y usuarios puedan tener un mayor control de sus datos de carácter personal. Lo cual significa que las empresas que manejan este tipo de información deben ser más cuidadosos y menos aventureros cuando tratan esta información. Pero, en mi opinión, no es el giro copernicano que se trata de hacer ver, la realidad, es que la norma se asienta sobre los principios ya existentes en materia de protección de datos, reforzando como decíamos el control de sus titulares sobre los mismos.

Como principal novedad, sobre la que se han escrito ríos de tinta, es el consentimiento, que no es que antes no se exigiese, es simplemente que ya no se puede basar en la inacción del titular. Lo que no se permite es que para informar a nuestros clientes, empleados, proveedores, usuarios web o cualquier otro colectivo enviemos una carta informándole de nuevas finalidades para las que trataremos sus datos y, si no contesta, pues los cedemos o los vendemos o le enviamos publicidad. Adicionalmente, no siempre necesitamos el consentimiento para el envío de publicidad o para fines de mercadotecnia, como indica el considerando (47) del propio texto del reglamento y la Agencia Española de Protección de Datos en su *Informe sobre el interés legítimo*.

En este sentido, si tenemos una relación contractual con nuestros clientes y enviamos publicidad o promociones relacionadas con los productos que haya contratado o sobre los que exista una expectativa razonable de recibir comunicaciones, estaríamos actuando sobre la base de nuestro interés legítimo y no necesitamos recabar el consentimiento expreso. Cuestión diferente es que si el receptor no está interesado, tenga la oportunidad de decirnos que no quiere recibir más información u ofertas y las empresas tengan que respetar esta elección.

Por otra parte, se están solicitando consentimientos de forma innecesaria, como tratar los datos para la prestación del servicio contratado o para ceder los datos a terceros cuando es necesario para la prestación del servicio o el cumplimiento de obligaciones legales. Todos estos usos de los datos son legítimos y no precisan de consentimiento, pues igual que sucedía con nuestra querida LOPD, están amparados por la relación contractual o la existencia de una norma que obliga a la recogida y comunicación de datos a determinados terceros.

> **En mi opinión, la norma no constituye el giro copernicano que se trata de hacer ver**

Lo que, al igual que siempre, no es posible hacer es utilizar los datos que hemos recabado con la intención de prestar un servicio o por una obligación legal para otros fines como publicidad, elaboración de perfiles, creación de bases de datos para comunicación a terceros, sin contar con el consentimiento de los afectados o estar amparado en alguno de los supuestos permitidos en el artículo 6 del RGPD.

Más allá, es cierto, que cuando realmente es necesario recabar el consentimiento la cosa se complica, pues al basarse en la acción del usuario, se requiere de un esfuerzo de adaptación de políticas y procedimientos internos considerables y, no lo olvidemos, los consiguientes costes de adaptación, pero, también lo es, que necesitamos el consentimiento de los afectados para las mismas finalidades que antes, todas aquellas que exceden el ámbito de la relación jurídica o contractual, no vienen impuestas por una norma o no están amparadas en el interés legítimo.

Lo mismo sucede con otras novedades introducidas por el RGPD, como el delegado de protección de datos. El hecho de que nuestro negocio requiera utilizar datos personales –pues como mínimo serán necesarios para la firma del contrato, entrega del producto o la prestación del servicio–, no implica necesariamente que necesitemos un delegado. Solo será necesario si nuestra actividad principal requiere de una observación sistemática de datos, lo que incluye la elaboración de perfiles (zonas públicas con videovigilancia, aplicaciones y otros servicios de la información que obtienen grandes cantidades de datos y elaboran perfiles o patrones de comportamiento en virtud de la información obtenida, etc.) o que nuestra actividad principal requiera de la recogida de datos de carácter sensible (salud, afiliación sindical, opiniones, vida sexual) y además dicha recogida sea a gran escala, por ejemplo, como indica el grupo del artículo 29, en el caso de hospitales sería necesario nombrar un delegado de protección de datos, pero no lo sería en el ámbito de la consulta privada de un médico, ya que esto último no sería gran escala. Ahora bien, es cierto que la definición o, más bien, los criterios proporcionados por el grupo del artículo 29 para valorar si un tratamiento es a gran escala son ambiguos y no cerrados, de forma que, salvo cuando son tratamientos muy obvios (colegios, hospitales, bancos), resulta muy complejo delimitar cuando estamos ante un tratamiento a gran escala o no. Así, el propio grupo, en su directrices sobre el delegado de protección de datos, señala que no es posible definir el concepto gran escala atendiendo únicamente al número de afectados, sino que se deben tener en consideración los siguientes factores:

- el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
- el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
- la duración, o permanencia, de la actividad de tratamiento de datos;
- el alcance geográfico de la actividad de tratamiento.

Atendiendo al ejemplo anterior respecto al tratamiento de datos por un hospital y un único médico, la diferencia entre el volumen y alcance geográfico del tratamiento es enorme, dejando una amplia zona gris en medio en la que es muy difícil establecer una valoración. Como consecuencia es probable que, al igual que sucede con los consentimientos, se estén nombrando delegados en casos en los que realmente no es necesario y viceversa.

En todo caso, la función del delegado es velar por que se cumplan con las normas de protección de datos internamente y se adopten medidas suficientes para proteger la información. No significa que, si tenemos obligación de nombrarlo, no podamos seguir tratando los datos, ni que nuestras medidas no sean suficientes, sino que es necesario tener un controlador y revisar qué estamos haciendo con los datos.

Sin perjuicio de todo lo anterior y otras novedades introducidas por el RGPD, lo que sí está claro es que la polémica está servida y que aún nos espera tener que revisar políticas y clausulas, durante los próximos meses, para acostumbrarnos y adaptarnos a las nuevas reglas del juego, que insisto, no son tan nuevas.

PIXABAY