

Opinión

MERCADO ÚNICO DIGITAL Y 'BIG DATA' ¿QUIÉN TIENE EL CONTROL DE LOS DATOS?



Isabel Martínez Moriel

Asociada Senior de Andersen Tax & Legal

La Comisión Europea parece totalmente decidida a seguir dando pasos que faciliten una economía de datos europea, en el marco del Mercado Único Digital, sin que ello menoscabe los derechos fundamentales a la privacidad y la intimidad de los ciudadanos europeos. Así lo ha demostrado con la adopción del Reglamento EU General de Protección de Datos (que entra en vigor en mayo del año que viene) y la propuesta de la nueva Directiva de Comercio Electrónico y Privacidad, cuya aprobación se espera este año, y que supone un refuerzo de los derechos del ciudadano al exigir el consentimiento previo incluso para el tratamiento de los datos generados automáticamente por los dispositivos electrónicos.

Debemos resaltar que el requisito de contar con el consentimiento para el uso de los datos denominados *metadata* empodera aún más al ciudadano en el control de su privacidad, pues si bien es cierto que estos datos generados automáticamente no identifican a las personas físicas, usados de forma combinada

con los datos personales, pueden aportar mucha información del ciudadano, su comportamiento y su personalidad (por ejemplo, datos de localización, tiempo de consulta de las webs, tipo de webs consultadas, etc).

Es evidente que el desarrollo de este sector, basado en el análisis y tratamiento masivo de datos o *big data*, con tasas de crecimiento de un 40 por ciento anual según los últimos datos correspondientes al ejercicio pasado, es clave para el presente y el futuro de la industria europea y su competitividad en el mercado

Es esencial que los ciudadanos puedan prestar su consentimiento de forma "libre"

global frente a operadores de terceros países. De ahí que la Comisión Europea, tras cerrar el pasado abril un periodo de consulta con los operadores afectados, esté inmersa en la preparación de una propuesta normativa que otorgue soluciones jurídicas y políticas para impulsar la economía de datos y elimine las restricciones innecesarias que impidan su crecimiento.

En este proceso, las instituciones europeas tratan de equilibrar los beneficios de las empresas que utilizan el *big data* con el principio de transparencia y confianza de los ciudadanos, que informados adecuadamente y de forma transparente del uso de sus datos, participen activamente en la construcción de esta industria. No son pocas las ventajas de estas técnicas desde el punto de vista del consumidor, pues su normalización puede

ayudar a mejorar la calidad de los productos ofertados a los mismos, permite la personalización conforme a sus gustos, reduce costes de transporte, aprovechando la cercanía de su localización y mejora los servicios de atención al cliente y de postventa.

Sin embargo, ya hay voces que apuntan otros riesgos para los derechos e intereses legítimos de los ciudadanos, como consumidores, no tan evidentes y que aún no han recibido la atención merecida.

Y es que, cada vez es más frecuente la concentración de los operadores con importantes bases de datos, sobre las que comercializan no sólo sus productos, sino también productos en mercados conexos. Ejemplos recientes es la adquisición de *WhatsApp* por *Facebook* (sobre la que la Comisión Europea ha abierto un procedimiento sancionador contra *Facebook* por no aportar la información veraz sobre la transferencia de datos entre los dos servicios y que finalmente llevó a cabo). Tal concentración de poderes en unos cuantos operadores podría consolidar monopolios y prácticas abusivas, en detrimento de los derechos de los consumidores y de la libre competencia, impidiendo así mismo la entrada de operadores alternativos.

Como ha puesto de manifiesto la Oficina Federal Alemana de Cárteles (*German Fede-*

ral Cartel Office) en su investigación reciente a *Facebook*, este operador podría haber abusado de su posición de dominio en el mercado de redes sociales, a través de sus términos y condiciones de privacidad, que vulneraban además la normativa alemana de protección de datos. Otras autoridades de competencia han resaltado los posibles efectos anticompetitivos del uso de datos recogidos de forma masiva para su utilización en campañas publicitarias en mercados conexos y la capacidad de los titulares de estas bases de datos de

excluir a otros competidores (veáse el caso de Google pendiente de resolución por la Comisión Europea).

En definitiva, si es esencial que el ciudadano conozca las consecuencias del consentimiento que otorga, no lo es menos que dicho consentimiento se preste de forma "libre", esto es, que el ciudadano

Los operadores no deben imponer condiciones y permitir que las empresas compitan

/consumidor no acepte los términos y condiciones de un operador por el mero hecho de no contar con alternativas que presten un servicio igual o similar. En definitiva, que los operadores de los servicios de *big data* no utilicen su posición en el mercado para imponer sus condiciones sino que compitan igualmente por obtener el beneplácito de los consumidores y que cualquier empresa que desee competir pueda hacerlo en igualdad de condiciones.

EL VALOR DE LA CERTIFICACIÓN UNE 19601



Salvador Román

Gerente de Governance y Corporate Compliance de AENOR

La reforma del Código Penal (Ley 1/2015) reconoce los modelos de prevención de delitos como instrumentos clave para prevenir y detectar la comisión de conductas contrarias a la Ley en las empresas.

Por su parte, la Fiscalía General del Estado (Circular 1/2016) estableció que las empresas que implanten sistemas de *compliance* pueden no sólo atenuar, sino incluso ser eximidas de su responsabilidad penal. El Art. 31 bis del CP establece los requisitos mínimos de estos modelos.

En este contexto, la Asociación Española de Normalización, UNE, formó un grupo de trabajo con la finalidad de diseñar una norma de sistema de gestión de prevención de delitos, que diera respuesta y concretase en mayor medida los requisitos exigidos por el CP y que a su vez estuviera alineado con los estándares internacionales más avanzados en la materia.

Fruto de estos trabajos, se ha publicado la

UNE 19601 *Sistemas de gestión de compliance penal*, con la participación y el consenso de expertos representativos de los principales grupos de interés del ámbito del *compliance* penal.

La UNE 19601 establece los requisitos de un sistema de gestión de *compliance* penal con el objetivo de ir más allá del cumplimiento de la legislación, y ayudar a las empresas y organizaciones a prevenir la comisión de delitos y reducir el riesgo penal y con ello, favorecer una cultura ética y de cumplimiento.

UNE 19601 está estructurada en 10 grandes apartados comunes a los establecidos en los estándares internacionales más avanzados en la materia, lo que facilita su uso, e integración en otros sistemas de gestión como el *compliance* (ISO 19600) o la prevención del soborno (ISO 37001).

Los requisitos de la Norma UNE 19601 son exigentes. Entre otros se requiere un análisis del contexto y partes interesadas; establecer responsabilidades para los órganos de gobierno, alta dirección y la función de cum-

plimiento; compromiso con la cultura de cumplimiento; evaluar los riesgos penales; determinar objetivos y planes; formar y sensibilizar; establecer controles generales y específicos (financieros, no financieros, *due diligence*, a las filiales y a los socios de negocio); incluir cláusulas contractuales o canales de comunicación de incumplimientos e irregularidades, entre otros.

Cumplir con la norma, implica dar respuesta a todos sus requisitos. Una manera de evidenciar este cumplimiento y además transmitir confianza a las partes interesadas y autoridades judiciales es mediante la certificación por una tercera parte independiente y competente como Aenor.

Las autoridades judiciales considerarán la certificación como una prueba relevante a aportar en caso necesario. Y es que la finalidad de la implantación y certificación conforme a la norma UNE 19601 es la prevención de delitos y reducción del riesgo penal. La Circular 1/2016 de la Fiscalía General del Estado pone en valor la certificación como

Cumplir con la norma ayuda a las empresas a prevenir delitos y a reducir riesgos penales

un elemento muy significativo que se considerará, llegado el caso, en la valoración de la eficacia de los modelos de prevención penal y en la exoneración de la responsabilidad penal de las personas jurídicas.

Por esta razón, las certificaciones tienen que tener el rigor suficiente para que puedan ser valoradas en sede judicial. El proceso de certificación debe ser realizado por un tercero independiente, con reconocimiento, competente y con la experiencia necesaria para ello.

La certificación genera confianza a las empresas, personas y autoridades judiciales, ya que es realizada por una tercera parte independiente y competente y va más allá del cumplimiento de requisitos legales.

Es una ayuda para acreditar la diligencia debida ante terceros (clientes, autoridades judiciales) y aporta una seguridad razonable en la prevención de delitos y reducción de riesgos penales y de incumplimiento. No garantiza la imposibilidad de comisión de un delito pero si ayudan a reducir en gran medida el riesgo de su materialización y a su prevención, y a que la organización ha hecho todo lo razonablemente posible para prevenir los delitos, y con ello atenuar e incluso exonerar la responsabilidad penal de las personas jurídicas.