

**CONTRIBUCIÓN DE LA RECIENTE JURISPRUDENCIA
DEL TJUE A LA PLENA ASUNCIÓN DEL DERECHO A LA
PROTECCIÓN DE DATOS COMO UN DERECHO
FUNDAMENTAL DE TODOS LOS EUROPEOS**

La plena asunción del valor normativo de la Carta de los Derechos Fundamentales de la Unión Europea y, por lo tanto, de su artículo 8, ha tenido plasmación en la reciente jurisprudencia del TJUE, así como en los trabajos de elaboración de la propuesta de Reglamento General de Protección de los Datos personales que viene elaborándose desde el 2012. Supone una contribución decisiva para la configuración del derecho a la protección de los datos personales de todos los europeos, que goza de los atributos propios de un derecho fundamental, como son:

- La definición de unos elementos y rasgos específicos y singulares que lo hacen reconocible como un derecho autónomo y distinto del derecho a la vida privada del artículo 7 de la Carta, por más que entre ambos exista una intensa relación.
- La atribución de eficacia directa y de carácter vinculante *erga omnes*.
- La consiguiente determinación de un contenido esencial, inderogable e indisponible, que ha de ser observado en la regulación de las condiciones de ejercicio del mismo.
- El establecimiento de un régimen jurídico uniforme a través de un Reglamento para la protección de datos personales aplicable a toda la Unión, que garantiza la igualdad de todos sus titulares en el ejercicio del derecho y que proporciona seguridad jurídica para la libre circulación de los datos.

- La creación de un sistema de garantías adecuado a la evolución tecnológica y a la naturaleza de las relaciones jurídicas que conlleva el tratamiento en las más diversas actividades de un número incontable de datos y, en especial, el desarrollo de productos de inteligencia artificial como el *Big Data* en el contexto de la globalización.

Un sistema en el que las agencias de protección de datos tienen un papel esencial, en el plano consultivo y de prevención, así como en el de control, y que tiene como garantía última la tutela de los tribunales de justicia del lugar de residencia del titular del derecho, independientemente de dónde estén localizados los responsables de los tratamientos, ya sea dentro o fuera de la Unión Europea.

Naturalmente, este conjunto de elementos configuradores del derecho fundamental a la protección de datos personales no le confieren un carácter absoluto e inmutable. Tanto la propuesta de Reglamento como la jurisprudencia del Tribunal de Justicia de la Unión Europea se encargan de advertir que ha de conciliarse con otros derechos como, por ejemplo, el derecho a la información o la libertad de empresa, y, también, con los principios e intereses generales sobre los que se sustentan y por los que han de velar la Unión Europea y los sistemas constitucionales de los Estados miembros (caso de la seguridad nacional y de la seguridad pública). Conciliación que comprende, por lo tanto, los intereses legítimos de las empresas y otros operadores que tratan datos personales en un marco de libre circulación de los mismos.

La incesante y cada vez más rápida e intensa evolución tecnológica, en particular del *Big Data*, implica, inevitablemente, nuevos peligros para la protección de los datos de las personas, lo que equivale a decir para su libertad. Ello requiere, por consiguiente, la correlativa adecuación de la regulación, interpretación y protección de este derecho fundamental para evitar su conculcación o la ineficacia de las garantías dispuestas para su efectividad. Ineludiblemente, también exige una adaptación de la organización y de los procedimientos empleados por las empresas que garantice su respeto.

La clave de esta cuestión radica, por lo tanto, en ser capaces de hallar un punto de equilibrio entre la irrenunciable libertad a la determinación del uso de nuestros datos personales y el eficaz funcionamiento de un mercado global para cuyo desarrollo los datos constituyen un elemento esencial y del que depende el bienestar de todos. Un equilibrio que habrá de concretarse mediante la ponderación caso a caso, pero que debe sustentarse en unos principios bien establecidos y en una regulación clara y precisa de los elementos del derecho. Propósito que, como decía más arriba, se ve favorecido por la constitucionalización a escala europea del derecho a la protección de datos en los términos del artículo 8 de la Carta de los Derechos Fundamentales y de la última jurisprudencia del TJUE.

Ese es el camino seguido por las sentencias del TJUE sobre la retención de datos de las comunicaciones electrónicas (de 8 de abril de 2014, asunto C-293/12, Digital Rights Ireland Ltd.), el derecho al olvido (de 13 de mayo de 2014, C-131/12 Google Spain S.L., Google Inc. c. Agencia Española de Protección de Datos (AEPD)) y el puerto seguro (de 6 de octubre de 2015, asunto C-362/14, M. Schrems c. Facebook) que serán objeto de comentario y debate en el Foro Jurídico y Económico.

Pero si en el contexto europeo se han puesto las bases para alcanzar ese objetivo, más dificultades se presentan para su plena consecución en el ámbito de la transferencia internacional de datos, a la vista de lo sucedido con los Estados Unidos de América a raíz de la STJUE sobre el puerto seguro. Máxime, teniendo en cuenta que es en este país donde se encuentran las principales empresas del *Big Data*.

Es urgente, por ello, que, sin perjuicio de la diferencia de los modelos de protección (heterónimo e institucional, el europeo, y de autocertificación y autorregulación empresarial, el americano) que deriva de las respectivas cultura y tradición jurídicas, se ponga remedio a la inexistencia en los Estados Unidos de cauces de protección efectiva del derecho para los ciudadanos que ofrezcan garantías equivalentes a las europeas.

No obstante, cuanto mejor definido esté el derecho fundamental más fácil será encontrar la fórmula de equivalencia. Por ese motivo, la evolución normativa y jurisprudencial que suponen la propuesta de Reglamento y las sentencias antes citadas han de servir de referencia obligada para que el derecho a la protección de datos obtenga un estándar de protección equivalente en Europa y los Estados Unidos.

Todo ello representa, ciertamente, nuevos retos para las empresas, que han de asumir que la protección de los datos personales que manejan es una dimensión esencial de su actividad pero sabiendo que los recursos que hayan de emplear para garantizarla constituirán, sin ninguna duda, una inversión productiva que no solo redundará en la prevención de riesgos de exigencia de responsabilidad en esta materia sino, también, en la imagen corporativa comprometida con la dignidad de la persona y el libre desarrollo de su personalidad, que es, en definitiva, el objetivo de la protección de los datos personales. En la medida que lo consigan, mayor será la confianza de las personas que se relacionan con ellas y su disposición a facilitarles sus datos, con el beneficioso efecto que ello supone para el flujo de los mismos en un marco de libertad y seguridad.