diariolaley

El uso ilícito de datos personales un año después de la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre

Francisco MARTÍNEZ VÁZQUEZ
Letrado de las Cortes Generales. Profesor de Derecho Administrativo de la Universidad Pontificia Comillas (ICADE)

Diario La Ley, Nº 34, Sección Ciberderecho, 5 de Diciembre de 2019, **Wolters Kluwer**

Comentarios

En la decimocuarta edición del **Informe de Riesgos Globales** (*The Global Risks Report, 14th Edition*), elaborado por el Foro Económico Mundial y publicado en enero de 2019 se constata, al igual que sucedió en la edición de 2018, que los cinco principales riesgos de impacto global a los que se enfrenta la sociedad contemporánea, en términos de probabilidad de materialización, son de naturaleza medioambiental y tecnológica. Así, frente al evidente predominio de riesgos de carácter económico o social que encontramos en ediciones anteriores, en 2019 el Foro Económico Mundial refleja en su informe anual que los riesgos más probables están relacionados con el cambio climático y con el uso ilícito o fraudulento de las tecnologías digitales. En concreto, el cuarto riesgo global, en términos de probabilidad vuelve a ser en 2019, como lo fue en 2018, **el robo o uso fraudulento de** datos (*data fraud or theft*).

Asimismo, junto a esta percepción del robo de datos personales en una destacada posición en el mapa de riesgos globales de la próxima década, el estado de ánimo pesimista se aprecia en las conclusiones alcanzadas en el informe, entre las cuales llama la atención que un 82% de los encuestados en este macroestudio afirmase que el uso fraudulento de datos personales evolucionaría de forma negativa en 2019.

En la misma línea, EUROPOL advierte en su informe anual sobre cibercrimen —Internet Organised Crime Threat Assessment (IOCTA) 2019—, de la gravedad del robo de datos, toda vez que constituye, por su volumen e impacto, la segunda ciberamenaza después del ransomware, al tiempo que constituye un instrumento para la realización de otros delitos, especialmente el fraude de medios de pago, en concreto el denominado CNP (*card not present fraud*).

El Pew Reserch Center en un interesante estudio titulado "***Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information***", publicado en noviembre de 2019, muestra que seis de cada diez norteamericanos consideran que es imposible evitar que los datos personales sean recopilados en el desenvolvimiento de nuestra vida cotidiana, bien por los poderes públicos, bien por empresas del sector privado. El 81% de los encuestados estima que los riesgos asociados a la captación de datos por compañías privadas son superiores a los beneficios, si bien ese porcentaje se reduce al 66% cuando se pregunta por el tratamiento de datos que realizan los poderes públicos. En esta misma línea, se acerca al 50% la proporción de encuestados que considera aceptable el tratamiento de datos personales por autoridades públicas con la finalidad de prevenir amenazas terroristas o esclarecer delitos. Otro resultado impactante que refleja la pésima percepción que los estadounidenses tienen sobre la protección de su privacidad es que el 86% de los encuestados considera que tiene muy poco o nulo control sobre el acceso no autorizado por parte de terceros a sus conversaciones e intercambio de mensajes en medios digitales.

La extendida percepción del riesgo de uso ilícito, abusivo o fraudulento de los datos es, por tanto, una medida de la vulnerabilidad del derecho fundamental a la protección de datos personales, que ha pasado al primer plano del nuevo catálogo de derechos que deben ser protegidos en la sociedad digital, con la particularidad de que en el caso de la protección de datos las agresiones no proceden principalmente de los poderes públicos sino de compañías privadas que son, al mismo tiempo, los grandes actores de una nueva actividad económica en la que los datos constituyen el principal objeto de transacciones e intercambios comerciales.

Al cumplirse un año desde la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (LA LEY 6637/2016) (GDPR (LA LEY 6637/2016) según el popular acrónimo en inglés), el conocimiento de los nuevos derechos protegidos por esta norma parece, a juzgar por los estudios publicados por el Eurobarómetro de junio de 2019, razonablemente satisfactorio. Mientras dos tercios de los ciudadanos europeos afirman que conocen la existencia del Reglamento, casi tres cuartas partes de los encuestados declaran conocer, al menos, uno de los derechos protegidos por esta norma y seis de cada diez dicen ser conscientes de la existencia de una autoridad nacional dedicada a la protección de datos personales.

En el primer año de vigencia del Reglamento **se notificaron casi 90.000 violaciones de datos personales** mientras que el volumen total de sanciones económicas impuestas se aproxima a los **56 millones de euros**, entre las cuales destacan, por su elevado importe, las impuestas a redes sociales y empresas de comunicación digital, aunque también es significativo el número de centros sanitarios sancionados, sin perder de vista otros casos relevantes y mediáticos como la sanción impuesta por la Agencia Española de Protección de Datos a la Liga de Fútbol Profesional.

En España se cumple un año desde la promulgación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018). Es evidente que, a estas alturas, nadie pone en duda que el derecho a la protección de datos personales tiene **naturaleza jurídica de auténtico derecho fundamental**, tal como recoge la Carta los derechos fundamentales de la Unión Europea en su artículo 8, según el cual "*toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*". El carácter de derecho fundamental es el punto de partida de todo el régimen jurídico europeo en materia de protección de datos personales, al igual que lo es en el ordenamiento jurídico español, donde el Tribunal Constitucional reconoció tempranamente la existencia de este derecho fundamental con anclaje en el artículo 18.4 CE. (LA LEY 2500/1978) Así, en la relevante STC 292/2000 (LA LEY 11336/2000) el intérprete de la Constitución afirma que "*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso*". Esta misma doctrina ha sido reiterada en pronunciamientos posteriores, incluida la reciente STC 76/2019, de 22 de mayo (LA LEY 59154/2019).

La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018) no solo ha supuesto **un cambio de paradigma** en cuanto al modelo de protección adoptado, decantándose, como no podía ser de otro modo, por el enfoque de riesgo y los principios de prevención y flexibilidad, sino que ha incorporado en nuestro ordenamiento jurídico **nuevos derechos para la era digital**, no necesariamente relacionados con la protección de datos personales. Es cierto, sin embargo, que en este primer año de vida de la Ley Orgánica el alcance práctico de tales derechos digitales ha sido limitado y subsisten dudas razonables sobre la eficacia jurídica real de algunos de los enunciados solemnes que incluye el Título X de la Ley, que presentan el **riesgo de quedar desdibujados** sin llegar a incorporarse como verdaderos derechos susceptibles de ser protegidos por los órganos jurisdiccionales.

En el contexto de una Legislatura extremadamente compleja por la ausencia de mayorías parlamentarias claras que respaldasen a los sucesivos Gobiernos, la Ley Orgánica 3/2018 (LA LEY 19303/2018) fue un **extrañísimo ejemplo de consenso entre las fuerzas políticas** pues resultó aprobada por unanimidad en el Congreso de los Diputados y por una altísima mayoría de senadores. Ese inusual acuerdo parlamentario que consiguió poner de acuerdo a los diputados de todos los perfiles ideológicos y superar la profunda brecha entre grupos constitucionalistas, nacionalistas e incluso independentistas, todos los cuales votaron en el Congreso a favor de la Ley, es un evidente reflejo de la preocupación existente por incorporar a nuestro ordenamiento jurídico instrumentos eficaces para proteger el derecho más vulnerable en nuestra vida digital contemporánea, como es el gobierno de nuestros datos personales y la custodia de nuestra privacidad, todo ello intrínsecamente unido a la dignidad de la persona y al libre

desarrollo de la personalidad, que proclama el artículo 10 de nuestra Constitución (LA LEY 2500/1978) como fundamento del orden político y de la paz social. Lamentablemente el ejemplar consenso parlamentario ha quedado, en cierto modo, oscurecido por la declaración de inconstitucionalidad del artículo 58 bis de la Ley Orgánica de Régimen Electoral General (LA LEY 1596/1985), incorporado por la Ley Orgánica 3/2018 (LA LEY 19303/2018), realizada por la STC 76/2019, de 22 de mayo de 2019 (LA LEY 59154/2019).

El balance de este primer año de vigencia de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018) debe ser **prudentemente satisfactorio,** a juzgar por el grado de conocimiento y adaptación a la nueva norma. En este proceso de adecuación a las exigencias de la nueva normativa, la Agencia Española de Protección de Datos ha desempeñado un importante papel tuitivo, alineado con el enfoque de prevención que impregna el Reglamento y la Ley, dejando atrás su configuración como organismo esencialmente sancionador para asumir las competencias de un verdadero regulador en la materia.

Por delante quedan, no obstante, retos de enorme importancia para la salvaguarda del derecho a la protección de datos personales, en un contexto tecnológico disruptivo y en constante evolución. En concreto, la correcta aplicación del Reglamento europeo y de la Ley española **exigen políticas integrales de gestión de la información** por parte de los responsables y encargados del tratamiento de datos personales, que aseguren el ejercicio de los derechos reconocidos a los titulares y también la adecuada protección del interés general. Estas políticas deben incluir las diversas fases del ciclo de la información, desde la protección hasta la destrucción y borrado seguro de los datos cuando así lo exija la aplicación de la normativa.

La mayor parte de las reclamaciones presentadas antes las autoridades de los distintos países europeos están relacionadas con el marketing telefónico, con los correos electrónicos publicitarios y con los sistemas de videovigilancia.

La evolución tecnológica hace presagiar que pasarán a primer plano de la preocupación por la privacidad nuevas aplicaciones basadas en desarrollos innovadores, como los **sistemas de reconocimiento facial,** cuyas innumerables utilidades exigen un cuidadoso análisis de su impacto en los derechos afectados. En efecto, en agosto de 2019 la autoridad sueca de protección de datos imponía una sanción de 200.000 coronas suecas a una entidad local por utilizar el reconocimiento facial para controlar la asistencia a clase de los alumnos. En noviembre de 2019 la CNIL, el regulador francés en la materia, ha publicado un informe titulado "*Reconnaissance faciale: pour un débat à la hauteur des enjeux*" con orientaciones interesantes sobre esta cuestión.

Asimismo, **la vinculación entre la minería de datos y la inteligencia artificial** plantean retos enormemente interesantes que serán objeto de nuevas directrices para preservar la privacidad, al igual que en el caso de los dispositivos conectados a Internet que configuran el denominado Internet of Things, sin pasar por alto tecnologías altamente sensibles como los implantes cerebrales, a los que se ha referido expresamente el Supervisor europeo.

En definitiva, la experiencia de fugas de información, robo de datos personales o uso fraudulento de los mismos en estos doces meses de vigencia de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018), demuestra que el estatuto jurídico del ciudadano digital se construye, en gran medida, con el **fortalecimiento de los derechos asociados al propio gobierno de los datos personales,** convertidos en un valioso activo comercial si bien se trata, ante todo, de emanaciones de la propia personalidad y, por eso, merecedores de una especial tutela que garantice y preserve, en su recopilación y tratamiento, la dignidad del ser humano.