La seguridad del dato en el ciberespacio: una aproximación legal

Gonzalo Menéndez Margolles // Abogado del Área de Privacidad, IT y Entornos Digitales de Broseta Abogados

El derecho a la protección de datos personales

Desde que en 1890 Samuel D. Warren y Louis D. Brandeis definieran la privacidad como el derecho a ser dejado solo o a no ser molestado –*"the right to be let alone"*–[1], la humanidad ha asistido a una evolución tecnológica sin precedentes, tanto por su velocidad como por sus repercusiones e incidencia en todos los ámbitos de nuestras vidas.

Una de las principales consecuencias de dicha evolución es la elevada vinculación y dependencia tecnológica que caracteriza a las sociedades desarrolladas actuales. En este contexto, alcanza una relevancia cada vez mayor la preocupación por la ciberseguridad y la amenaza que suponen los ciberataques para el normal desarrollo de las actividades económicas y sociales y, por supuesto, para nuestros derechos fundamentales, como el derecho a la privacidad o a la protección de datos personales.

Así lo ha reconocido, a modo de ejemplo, la Estrategia de Seguridad Nacional española de 2017, que identifica las vulnerabilidades del ciberespacio como unas de las principales amenazas y desafíos a los que debe hacer frente nuestro país en la actualidad. Por su parte, en la Estrategia Nacional de Ciberseguridad de 2019 se afirma que *"(L)as actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio uno de los principales riesgos para nuestro desarrollo como nación"*.

En España, ya en 1978 el constituyente fue consciente de las amenazas que podrían derivarse para nuestros derechos del desarrollo tecnológico, lo cual se tradujo en la inclusión de la previsión contenida en el artículo 18.4 de nuestra Constitución: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

Nuestro Tribunal Constitucional declaró en su sentencia núm. 292/2000 que el precepto transcrito contiene, *"un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos […], lo que se ha dado en llamar "libertad informática" […] derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención "*.

De esta manera, el Tribunal Constitucional reconoció la existencia de un derecho fundamental autónomo, más amplio que la intimidad y la privacidad: el derecho a la protección de datos personales, que *"atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática"*; y que *"persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado […] un poder de disposición sobre esos datos"*.

El alcance de este derecho, el objeto de la protección que ofrece, son los datos personales, que el artículo 4.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, el **"RGPD"**), define como *"toda información sobre una persona física identificada o identificable («el interesado»)"*. En este sentido, tal y como también ha señalado nuestro Tribunal Constitucional en la sentencia citada, el derecho a la protección de datos alcanza a todos aquellos datos *"que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean*

1 WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. En: *Harvard Law Review*, 1890. Vol. 4, n. º 5, págs. 193-220.

o no derechos constitucionales y […] no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo […]. Por consiguiente, también alcanza a aquellos datos personales públicos […] accesibles al conocimiento de cualquiera […]", de tal forma que *"los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona"*.

La seguridad de los datos personales: régimen legal

Hoy en día, la práctica totalidad de los tratamientos de datos personales se llevan a cabo mediante dispositivos y sistemas informáticos, de tal forma que la adecuada protección de los mismos redunda en beneficio de la seguridad de los datos personales. Como consecuencia de lo anterior, en este apartado no sólo se hará referencia a la normativa en materia de protección de datos personales, sino también a las normas sobre seguridad de las redes y sistemas de información, toda vez que las mismas imponen determinadas obligaciones íntimamente vinculadas con la salvaguarda de dichos datos debido a la estrecha relación entre estos dos ámbitos.

El RGPD y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

El artículo 5.1 del RGPD consagra como uno de los principios esenciales de cualquier tratamiento de datos el principio de integridad y confidencialidad, de acuerdo con el cual debe garantizarse una seguridad adecuada de los datos personales para evitar su uso no autorizado o ilícito, pérdida, destrucción o daño accidental.

Desarrollando dicho principio, el artículo 32 del RGPD dispone que todo aquél que lleve a cabo un tratamiento de datos personales deberá aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad de los datos adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento, así como los riesgos para los derechos y libertades de los interesados derivados de una eventual brecha de seguridad.

No obstante, el citado Reglamento no especifica ni enumera, ni siquiera a título ilustrativo, las concretas medidas que debe adoptar quien trate datos personales. Esta indeterminación deriva de otro de los principios fundamentales que inspira la regulación contenida en el RGPD, el de responsabilidad proactiva o *accountability*, de conformidad con el cual corresponde a la persona o entidad responsable de un tratamiento de datos personales el análisis de los riesgos a que los mismos se encuentran expuestos y la adopción las medidas que considere apropiadas para garantizar su seguridad.

Sin embargo, en nuestro país, la referida indeterminación no afecta por igual a las entidades del sector privado y del sector público. Las primeras únicamente cuentan con la referencia contenida en el artículo 32.3 del RGPD, de acuerdo con el cual la adhesión a un código de conducta o a un mecanismo de certificación en materia de protección de datos podrá servir para demostrar el cumplimiento de sus obligaciones en materia de seguridad de los datos personales. Sin embargo, dicha adhesión no implica *per se* la satisfacción de dicha obligación, pues ello requiere un análisis caso por caso a fin de implementar las medidas que resulten idóneas en cada supuesto, que no tienen por qué coincidir con las previstas en dichos mecanismos. Por su parte, respecto de las entidades integrantes del sector público, la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que dichas entidades deberán aplicar las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

La Directiva NIS y su normativa de transposición

Al margen de las disposiciones contenidas en el RGPD en materia de seguridad de los datos, en el marco de la Unión Europea se ha llevado a cabo un elevado número de actuaciones de diversa naturaleza relacionadas en mayor o menor medida con la ciberseguridad, tales como **(i)** la creación y consolidación de la Agencia de la Unión Europea para la Ciberseguridad ("ENISA", por sus siglas en inglés); **(ii)** la elaboración de documentos como la Estrategia de Ciberseguridad de la Unión Europea[2] y la Estrategia de la UE para una Unión de la Seguridad[3]; o **(iii)** la aprobación de normas como la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de

2 https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.
3 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0605&from=EN.

seguridad de las redes y sistemas de información en la Unión[4] (en adelante, la **"Directiva NIS"**).

Con el objetivo de garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, la Directiva NIS impone a todas aquellas entidades que puedan calificarse, de acuerdo a los criterios que la propia norma define, como operadores de servicios esenciales y proveedores de servicios digitales, un conjunto de obligaciones relativas a **(i)** las medidas de técnicas y organizativas de seguridad que deberán ser adoptadas y **(ii)** la notificación a la autoridad competente o al equipo de respuesta a incidentes de seguridad informática ("CSIRT", por sus siglas en inglés) de referencia de los incidentes que tengan efectos significativos en la continuidad de los servicios que prestan[5]. Si bien cualquier otro agente no estará sujeto a estas obligaciones, nada impide que las utilice como criterios de referencia.

La Directiva NIS ha sido transpuesta al ordenamiento español mediante Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (en adelante, el **"RDL 12/2018"**), norma complementada por el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (en adelante, el **"RD 43/2021"**).

De acuerdo con estas normas, los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar las medidas técnicas y organizativas que resulten adecuadas y proporcionadas para **(i)** gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información que utilicen para prestar sus servicios y **(ii)** prevenir y reducir al mínimo el impacto de eventuales incidentes. A tal fin, se ofrecen un conjunto de mecanismos que pueden servir de ayuda a tales sujetos:

- Se contempla la posibilidad de que las autoridades competentes establezcan obligaciones específicas en materia de seguridad y dicten instrucciones técnicas y guías orientativas para detallar el contenido de tales obligaciones.
- Se insta a la utilización de normas o especificaciones técnicas elaboradas de conformidad con la normativa europea sobre normalización o aprobadas por organismos internacionales de normalización.
- Por último, todos aquellos sujetos que, a consecuencia del sector en el que operen, estén sometidos a una legislación específica que establezca obligaciones de seguridad con efectos equivalentes a los perseguidos por las referidas normas, podrán acudir a las previsiones de aquélla para definir sus medidas de seguridad.

A mayor abundamiento, en el caso de los operadores de servicios esenciales, el RD 43/2021 enumera los principios que deberán inspirar sus políticas de seguridad de las redes y sistemas de información, así como los aspectos mínimos que dichas políticas deberán considerar. Adicionalmente, la disposición establece que las medidas de seguridad que tales operadores están obligados a adoptar **(i)** tomarán como referencia las recogidas en el Esquema Nacional de Seguridad, en la medida en que las mismas resulten aplicables y **(ii)** estarán basadas, cuando sea posible, en otros esquemas nacionales de seguridad existentes, sin perjuicio de la posibilidad de tener en cuenta otros estándares reconocidos internacionalmente. Con ello, la norma les proporciona unos criterios que pueden servir de guía para determinar las concretas medidas de seguridad a implementar.

Finalmente, el RD 43/2021 dispone expresamente que la elaboración de las políticas de seguridad deberá tener en cuenta los riesgos derivados del tratamiento de datos personales, en los términos establecidos por el RGPD, reconociendo así la intrínseca relación entre seguridad de las redes y sistemas y seguridad de los datos personales.

En definitiva, la normativa a la que se ha hecho referencia pone de manifiesto que no existe una solución homogénea y universal para hacer frente a los ciberriesgos y ciberamenazas que afectan a los datos personales, sino que es necesario **(i)** efectuar un análisis, caso por caso, de cuáles son esos riesgos y amenazas e implementar las medidas de seguridad que se consideren más idóneas para mitigarlos; y **(ii)** establecer procedimientos de reevaluación periódica y mejora continua, pues la naturaleza, tipología y funcionamiento de los ciberataques evolucionan constantemente y las medidas de seguridad deben mantenerse a la altura para resultar efectivas. ●

4 El 16 de diciembre de 2020, tras una revisión de la Directiva NIS, la Comisión Europea presentó al Parlamento Europeo y al Consejo su propuesta para una nueva Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 ("Directiva NIS2"). https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0012.02/DOC_1&format=PDF

5 Para más información, véase la "Guía nacional de notificación y gestión de ciberincidentes", aprobada por el Consejo Nacional de Ciberseguridad el 21 de febrero de 2020. https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf.