

La protección de datos: una necesidad

José María Ayala Muñoz* y
Celia Fernández Aller**

La sociedad de la información avanza rápida y penetrante en todo el mundo; El Salvador no es la excepción. Ello trae consigo ventajas, sobre todo en lo que se refiere a la capacidad de almacenamiento y transmisión de grandes cantidades de información a velocidad impensable hace años; o también a la posibilidad para comerciar y realizar trámites a través de Internet. Sin embargo, el uso inadecuado de las tecnologías de la información y las comunicaciones conlleva amenazas potenciales para los derechos de los individuos, quienes ven cómo su información personal se distribuye en ámbitos geográficos que, por supuesto, exceden el suyo. Esto implica la pérdida de control del uso que se da a esa información, su destino y de las entidades —públicas o privadas, físicas o jurídicas— a las cuales está dirigida.

En la práctica, existe cada vez más conciencia acerca de la necesidad de proteger a las personas frente a estos riesgos. Sin embargo, el camino que queda por recorrer es largo. A los ciudadanos nos falta sensibilización sobre la importancia de proteger al respecto. Sólo cuando estalla un gran escándalo sobre el manejo de los datos o cuando se les da un tratamiento abusivo que nos concierne de forma muy directa (por ejemplo, negación de un crédito por manejo erróneo de una información sobre una deuda pasada ya cancelada), tomamos conciencia de la necesidad de que la protección de los datos sea un derecho reconocido y regulado suficientemente. A las instituciones públicas y privadas les falta comprender

* Abogado del Estado español ante el Tribunal Supremo en Madrid; y profesor de Derecho Comunitario Europeo en la Universidad Pontificia Comillas de Madrid, España.

** Doctora en Derecho Constitucional, con especialidad en Protección Constitucional de Derechos Fundamentales; y profesora de Derecho Informático en la Universidad Politécnica de Madrid, España. Correo electrónico: cfaller@eui.upm.es.

la importancia de políticas activas en materia de protección de datos personales. Éstas no acaban de entender que el cumplimiento de una normativa de protección de datos puede conseguir una mayor transparencia y respeto a los derechos individuales, y hacer más competitivas a las empresas y más eficaces a las administraciones públicas.

1. Introducción a los conceptos

1.1. El derecho a la protección de datos

El llamado derecho a la protección de datos personales se plantea, ante la revolución tecnológica actual, como un instituto que persigue garantizar a los individuos el control de sus datos personales, así como también el uso y el destino de los mismos para impedir el tráfico ilícito y lesivo de éstos. Los ordenamientos jurídicos de otros países, los pronunciamientos judiciales y los estudios de los autores proponen dos formas para reconocer este derecho: como parte del derecho a la intimidad o como un derecho autónomo.

El derecho a la intimidad protege aquellos aspectos que afectan al ámbito más esencial de la persona (datos sobre creencias, afiliación sindical, raza, salud, etc.). El derecho de autodeterminación informativa, denominado con distintos términos (libertad informática o protección de datos), pretende proteger un ámbito más amplio: la "privacidad". Se trata de un conjunto más global de facetas de la persona, las cuales no son consideradas de manera aislada. Al considerarlas de esta última forma pueden carecer de significado intrínseco, pero cuando son analizadas de forma sistemática, permiten obtener un retrato de la persona, cuyos componentes ésta tiene derecho a mantener en reserva. En el concepto de privacidad podrían incluirse datos patrimoniales, gustos personales, consumo, etc.

Creemos que la regulación del derecho a la intimidad pudiera no resultar suficiente para proteger a la persona. Fundamentalmente, porque ese derecho supone otorgar a la persona poder para controlar sus datos. Y no solo los datos íntimos, sino también cualquier

otro dato cuyo conocimiento o empleo por terceros pueda afectar sus derechos, sean o no fundamentales; porque el objeto a proteger no debiera ser solo la intimidad individual, sino los datos de carácter personal, ya sean éstos de carácter íntimo o no.

El contenido de este derecho de protección de datos es peculiar, debido a que otorga al titular una serie de facultades, consistentes en poderes jurídicos, cuyo ejercicio impone a terceros deberes jurídicos para garantizar el poder de control. Estos deberes son el derecho a pedir consentimiento previo; a informar en el momento de la recolección de los datos; y a permitir el derecho de acceso, rectificación y cancelación, oposición, indemnización e impugnación de valoraciones arbitrarias. En definitiva, el derecho de autodeterminación informativa concede al sujeto un poder de disposición, en virtud del cual decide qué datos proporciona o no; posee la facultad para consentir su registro y la posibilidad de acceso a ellos; controla el uso de los mismos; y le da derecho a ser informado en todo momento acerca de quién dispone de sus datos personales.

1.2. Principales elementos del régimen jurídico

Si se examinan las soluciones dadas por las legislaciones de otros países y los análisis técnico-jurídicos de los especialistas, se concluye que el sistema de protección de datos personales ha de tener un contenido mínimo esencial, necesario para garantizar el respeto a la privacidad y para que el individuo pueda controlar el manejo de sus datos por parte de otra persona o entidad. Hasta ahora, ningún país ha instaurado un sistema completo.

En esta cuestión hay que distinguir dos sujetos. Por un lado, el titular de los datos, es decir, el sujeto cuya información va a ser procesada y a quien se llama "afectado" o "interesado"; por el otro lado, el responsable del procesamiento, quien decide sobre su uso, contenido y finalidad, los cuales pueden ser públicos o privados. En suma, desde el punto de vista doctrinal o científico, los principales

elementos del régimen jurídico del sistema de protección de datos personales son el consentimiento del interesado; los derechos de acceso, rectificación y cancelación de los titulares de los datos; las transferencias internacionales; y el derecho a ser informado antes de otorgar consentimiento.

El consentimiento del interesado, en un sistema que pretenda proteger los datos personales, consiste en prohibir el procesamiento de éstos sin solicitud o aprobación previa de aquél. Será necesaria, por lo tanto, la reserva de ley para exceptuar dicho consentimiento. En el ámbito europeo, las excepciones comprenden la recolección de datos de fuentes accesibles al público, como los medios de comunicación, los repertorios telefónicos, etc.; los datos recogidos en el contexto de una relación de negocios, laboral o administrativa; los datos necesarios para salvaguardar un interés vital del interesado (una urgencia médica, por ejemplo); y los datos utilizados por las administraciones públicas para ejercer sus funciones en el ámbito de su competencia.

Por eso, la exigencia de recabar el consentimiento del interesado carecería de sentido si ella no fuese acompañada de una información previa. Esto es, sólo debe ser válido el consentimiento prestado por quien, debidamente informado, conoce en detalle aquello a lo que consiente. De esta manera, el llamado principio de finalidad supone que, prestado el consentimiento para un determinado tratamiento de los datos, éstos no pueden destinarse a finalidades distintas de las consideradas, bajo pena de considerar nulo el consentimiento. El responsable de recolectar los datos debe informar al afectado, por consiguiente, sobre las finalidades y los usos que va a dar a la información, así como acerca de su localización. La información también permitirá que el interesado pueda ejercer sus derechos y vigilar el cumplimiento de la normativa que protege sus datos.

Para atribuir al afectado un poder de control sobre sus datos, aun después de haber consentido su procesamiento, debe concedérsele derecho para acceder al contenido

del fichero y modificar los datos erróneos o cancelarlos cuando dejan de ser necesarios para la finalidad para la cual fueron recogidos. Complemento de esto es considerar los derechos a oponerse al procesamiento; crear un registro centralizado de archivos de tratamiento de datos y de derecho de consulta para que el afectado pueda conocer en cuántos ficheros públicos o privados se encuentra su información; el derecho de indemnización, que permite resarcir, en el caso de daños morales o patrimoniales, derivados de un tratamiento incorrecto de los datos; y el derecho de impugnación de las valoraciones arbitrarias, lo cual impide a terceros tomar decisiones sobre la persona, basadas única y exclusivamente en una valoración de datos personales. En este mismo sentido, debe exigirse al responsable del fichero que el tratamiento se haga con condiciones mínimas de calidad. El principio de calidad impone que el tratamiento de los datos sea adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las cuales se han obtenido.

Puede suceder que, al traspasar las fronteras, los titulares de los datos pierden la posibilidad de controlar su destino. Y si el país receptor cuenta con un nivel de protección de datos inferior al país emisor, los derechos de la persona pueden verse vulnerados. De este modo, para que los derechos hasta aquí expuestos sean eficaces y no puedan ser defraudados por la salida de los datos fuera del territorio nacional del Estado que establece la regulación, deben imponerse limitaciones o restricciones a su exportación.

Existen dos modelos para regular estas transferencias. El modelo estadounidense utiliza los principios de "puerto seguro", establecidos por el Departamento de Comercio el 19 de abril de 1999. Las empresas estadounidenses que quieran contar con el beneficio de "puerto seguro" deben satisfacer unas condiciones mínimas: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación. De esta forma, cualquier empresa estadounidense que quiera negociar con una europea ha de cumplir estos

estándares de protección de datos. Sin embargo, este modelo cuenta con muchas limitaciones, tal y como ha detectado el Dictamen 2/99 de la Unión Europea sobre la idoneidad de los “Principios internacionales de puerto de seguro”¹.

Por su parte, el modelo europeo exige, para transferir datos personales a otros países, un tratamiento adecuado, de acuerdo a los criterios siguientes²: (a) principio de finalidad; (b) principio de proporcionalidad y calidad de los datos; (c) principio de transparencia; (d) principio de seguridad; y (e) derecho de acceso, rectificación y oposición. Además, existen restricciones para hacer transferencias sucesivas a terceros países: solo se permiten transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último garantice, asimismo, un nivel de protección de datos adecuado. Este modelo también tiene limitaciones, por ejemplo: cómo definir qué es la “protección adecuada” y cuáles son las excepciones; la diferente regulación entre países; y la cuantía de las sanciones pecuniarias.

1.3. Mecanismos especiales de control

La garantía eficaz de protección de datos de carácter personal no solo exige la declaración legal de los derechos hasta aquí expuestos, sino que también el establecimiento de mecanismos adecuados para —por la vía administrativa y judicial— asegurar una reacción de los poderes públicos contra los actos lesivos a tales derechos. Con este fin, puede crearse un organismo de carácter administrativo, dotado de suficiente autonomía para controlar no solo los ficheros en poder de empresas privadas, sino también en poder de la administración pública.

También existe la posibilidad de reconocer un proceso judicial, el hábeas data. Se trata éste de un remedio constitucional contra los abusos de poder y las ilegalidades cometidas

por los servidores o los agentes públicos, y relacionadas con las informaciones y los datos de los administrados. En algunos países, solo se refiere a datos públicos; en otros, incluye los datos de los ficheros de titularidad privada. Normalmente, no se distingue si las bases de datos están o no informatizadas. Este remedio constitucional debe ser activado a instancia de la parte interesada, no de oficio. En algunas constituciones se establece que el sujeto activo y peticionario debe ser el titular de los datos personales; en otras, se faculta, además, a los familiares, en caso de que el titular hubiere fallecido o no pudiese hacerlo.

El procedimiento suele ser breve. Los plazos de presentación de pruebas y alegaciones son cortos y las resoluciones deben hacerse efectivas con prontitud. La tramitación está a cargo de un órgano judicial, para lo cual los tribunales ordinarios o una sala de justicia determinada podrían tener competencia. Sin embargo, el hábeas data, por sí mismo, no garantiza una protección adecuada de los datos. En tanto que su finalidad es corregir irregularidades en el tratamiento de los datos personales, no es un medio idóneo para prevenir acciones que atenten contra los derechos y las libertades; así como tampoco sirve para regular cómo debe ser tratada la información. De hecho, de los seis principios del documento del Grupo de Autoridades Europeas de Protección de Datos (GT29), el hábeas data incluye solo el quinto (y de modo parcial).

1.4. Exclusiones de la normativa de protección de datos

En ciertas ocasiones, el bien jurídico protegido por estas normas, la privacidad de individuo, ha de ceder ante razones de interés público. Dentro de estas razones estarían el mantenimiento de la seguridad nacional e internacional, la lucha contra el terrorismo, etc. En todas las normativas de protección de datos, se establecen excepciones en el ámbito de aplicación. Así, en el Artículo 2.2 de la ley

1. Disponible en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp19es.pdf.

2. El Grupo de Autoridades Europeas de Protección de Datos (GT29) estableció dichos criterios.