Capítulo

XI

LOS DATOS PERSONALES

POR DISTINTAS RAZONES, A DIARIO ENTREGAMOS A LAS AUTORIDADES UNA GRAN CANTIDAD DE INFORMACIÓN RELACIONADA CON NUESTRA VIDA PERSONAL; por ejemplo para realizar un trámite, obtener un servicio o cumplir con ciertas obligaciones. Pensemos en el expediente médico que se encuentra en las clínicas del IMSS o del ISSSTE, en nuestro historial escolar, en los datos respecto de nuestro domicilio, número telefónico, edad, religión y dependientes económicos, o en nuestros ingresos anuales que declaramos para fines fiscales. Imaginemos qué sucedería si toda esta información fuera pública y cualquiera pudiera conocerla. Obviamente se estaría afectando nuestra vida privada y, con ello, nuestro derecho a preservarla del conocimiento público. En efecto, la Suprema Corte de Justicia ha dicho que "el derecho a la vida privada consiste en la facultad que tienen los individuos para no ser interferidos o molestados por persona o entidad alguna, en todo aquello que desean compartir únicamente con quienes ellos eligen"[41]. Es por ello que todos estos datos –que se conocen como datos personales– merecen un trato especial y privilegiado.

Un dato personal es una información que concierne a una persona física, identificada o identificable. Ejemplos de datos personales son el nombre asociado a las características físicas o emocionales, el estado de salud, la cuenta de correo electrónico, el patrimonio, la religión, la huella digital, la fotografía o el número de seguridad social de una persona. Lo importante es la asociación de dos o más datos que permitan referirlos a una persona física específica e identificable. Esto es especialmente delicado ahora que las nuevas tecnologías de información permiten el tratamiento de estos datos de manera tal, que la información personal se puede comunicar, manipular o usar para muy diversos fines[42].

En la dimensión internacional, particularmente en Europa, el derecho a la protección de los datos personales es considerado como un derecho fundamental a título propio, distinto del derecho a la intimidad[43]. En México, este derecho fue reconocido recientemente como tal en la Constitución[44]. Por su parte, la fracción II del segundo párrafo del artículo 6° constitucional estableció la protección de los datos personales en posesión de las autoridades, pues el Constituyente Permanente identificó claramente que era necesario proteger esos datos de la posibilidad que fueran divulgados indiscriminadamente o usados para propósitos distintos de aquellos por los que fueron recolectados.

De esta manera, las leyes de acceso a la información son también en muchos casos leyes de protección de datos personales respecto de aquellos datos personales que se encuentran en posesión de las entidades gubernamentales, tal como sucede en la mayor parte de las entidades federativas; en algunas de ellas, como el Distrito Federal, Guanajuato, Colima y Oaxaca se ha optado por expedir leyes distintas, una para regular el

acceso a la información y otra para la protección de los datos personales.

Existe un conjunto de principios internacionalmente reconocidos que rigen la protección de los datos personales, que son los de consentimiento, información previa, licitud, calidad de la información, confidencialidad y seguridad[45]. A continuación los examinaremos brevemente[46].

El principio del consentimiento es el eje fundamental a partir del cual se ha construido el derecho a la protección de los datos personales, y conlleva la idea de la autodeterminación informativa. Implica que todo tratamiento de datos personales requiere ser autorizado previamente por el titular de los mismos. En este sentido, la manifestación de voluntad por parte del titular de los datos deberá ser libre, informada y específica. En otras palabras, el titular de los datos es el "único que tiene derecho a decidir quién, como, cuándo y para qué se tratan sus datos"[47].

El segundo de los principios es el de información. Supone que el responsable del tratamiento de los datos tiene la obligación de dar a conocer a las personas que sus datos serán organizados en una base de datos, los fines para los cuáles se utilizarán, así como la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición (véase *infra*). Del cabal cumplimiento de este principio depende que el consentimiento sea válido, pues de no conocerse de manera precisa los alcances del tratamiento, éste puede considerarse como inválido.

El tercer principio es el de calidad. Propone que los datos recabados deben ser adecuados, exactos, pertinentes y no excesivos, según sea la finalidad para la que fueron recabados. Por su parte, el principio de licitud consiste en que las entidades gubernamentales sólo deben desarrollar o tener sistemas de datos personales relacionados directamente con sus facultades y atribuciones. La posesión de sistemas de datos personales que no estén directamente relacionados con las atribuciones de una entidad gubernamental violenta directamente este principio.

El principio de confidencialidad establece que los sujetos obligados deben asegurar el manejo confidencial de los sistemas de datos personales, y que su transmisión o divulgación sólo puede darse previo consentimiento del titular.

EXISTE UN CONJUNTO DE PRINCIPIOS INTERNACIONALMENTE RECONOCIDOS QUE RIGEN LA PROTECCIÓN DE LOS DATOS PERSONALES, QUE SON LOS DE CONSENTIMIENTO, INFORMACIÓN PREVIA, LICITUD, CALIDAD DE LA INFORMACIÓN, CONFIDENCIALIDAD Y SEGURIDAD.

Finalmente, el principio de seguridad conlleva la obligación de quien recaba los datos de adoptar las medidas de carácter técnico y organizativo que aseguren un tratamiento seguro. En esta materia se reconoce que no todos los datos personales requieren del mismo grado de seguridad, por lo cual pueden establecerse diferentes niveles. Así, los datos de identificación de una persona –por ejemplo, el domicilio, el número telefónico, el RFC o la fecha de nacimiento– requieren de un nivel de protección bajo, a diferencia de los "datos sensibles", que son aquellos relacionados, por ejemplo, con las preferencias ideológicas, religiosas, la vida sexual o la salud, que necesitan un nivel de protección alto.

Desde luego que todos los principios arriba descritos admiten excepciones, principalmente cuando los datos hayan sido recabados por un mandato legal o para el cumplimiento de las facultades legales de las entidades gubernamentales.

Ahora bien, estos principios se complementan con cuatro derechos distintos e independientes, que son los de acceso, rectificación, cancelación y oposición, que la doctrina reconoce como los "derechos ARCO", y que brevemente describiremos a continuación.

El derecho de acceso corresponde a cualquier persona física para obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento por una entidad gubernamental, así como las transmisiones hechas o que se prevea realizar de los mismos. El de rectificación es el derecho de modificar o corregir los datos cuando sean inexactos o incompletos. El de cancelación es el derecho de solicitar el bloqueo de los datos personales cuando hayan sido objeto de tratamiento en violación a alguno de los principios arriba referidos. Finalmente, las personas tienen derecho a oponerse al tratamiento de sus datos cuando hayan sido recabados sin su consentimiento.