INSEGURIDAD EN LA PROTECCIÓN DE DATOS PERSONALES

El desarrollo alcanzado en el diseño y la utilización de bases de datos por parte de organizaciones públicas y privadas, ha posibilitado sistematizar información sobre las personas a niveles sin precedentes.

La suma de información acumulada representa un grave peligro para el derecho de las personas, y quienes manejan esta información tienen una responsabilidad primaria sobre su uso y sobre el destino que se le dará a los datos que administran. Si la venta de datos se establece como una práctica generalizada -y no nos consta que ya no lo sea- empresas y entidades inescrupulosas podrán cruzar datos personales de distintos orígenes para construir un conocimiento no autorizado sobre distintos aspectos de cada individuo. Y esto comprende una amplia gama de información privada, que incluye desde enfermedades y adicciones penalizadas socialmente hasta creencias religiosas y adscripciones políticas.

En la Argentina, la ley 25.326 de Protección de Datos Personales (también llamada ley de Hábeas Data) establece la obligación para el responsable o usuario del archivo de datos, de adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales. Y también penaliza con prisión de un mes a dos años a quien insertara datos falsos en un archivo de datos personales, o a quien revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar.

Sergio Massa es el titular del ANSES. Poco tiempo atrás, Massa efectuó una seria denuncia vinculada al tráfico de información dentro de esa institución. Concretamente, acusó a funcionarios de su administración de vender a una empresa privada, los archivos de unos 12 millones de personas registradas en el organismo. Con ello, tendió un manto de sombras sobre la seguridad con la que se manejan los datos personales en los ámbitos públicos. Sombras que no sólo se extienden a todas las instituciones del Estado, sino que también alcanzan a las empresas y organizaciones privadas que gastan sumas considerables para conocer los gustos y hábitos de consumo de sus potenciales clientes.

Esta manifiesta inseguridad técnica en el

manejo de datos personales conspira abiertamente contra la declarada voluntad del gobierno nacional de instaurar lo que denomina “gobierno electrónico”, una iniciativa que consiste básicamente en facilitar a los ciudadanos a través de Internet, el acceso a una amplia gama de información sobre la gestión de los organismos públicos, que va desde trámites personales hasta el acceso a las licitaciones que realiza el Estado. Más allá del poco feliz nombre con el que se le ha bautizado, la utilización de un mecanismo de este tipo facilita el control ciudadano y puede ayudar a hacer más transparente la gestión pública.

Lamentablemente, hechos como el denunciado por el titular de la ANSES no ayudan a confiar en que los procedimientos establecidos en el Estado para administrar información, observen las normas básicas de seguridad que se requieren. Por el contrario, resulta contraproducente que los ámbitos administrados por quienes tienen la responsabilidad de brindar seguridad jurídica y de gestión a los ciudadanos, sean escenario de este tipo de delitos.

Proveer a la seguridad de las personas constituye una responsabilidad básica e ineludible del Estado. Urgentemente deben establecerse procedimientos preventivos obligatorios que protejan los datos personales de los ciudadanos, a ser cumplimentados por la totalidad de las empresas y organizaciones que administran dicha información.

El Registro Público de Bases de Datos que funciona en el Ministerio de Justicia y Derechos Humanos de la Nación es un paso adelante, pero inscribir las bases no resulta suficiente para asegurar un mínimo de control en su funcionamiento y acceso.

Es necesario en primer lugar, establecer procedimientos de administración de las bases de datos que contengan información sobre las personas, para que observen normas de seguridad informática aceptadas internacionalmente. Luego, resulta imprescindible auditar a las organizaciones en forma permanente, para asegurar que esos procedimientos sean respetados y sostenidos en el tiempo.

Sólo de esta manera será posible reducir los riesgos de que el tráfico de información se convierta en el más novedoso de esos “negocios” que en nuestro país florecen al amparo de la desidia.