28 de Enero - Día Internacional de la Protección de Datos Personales

El 28 de enero de 1981, se firmó el Convenio 108 del Consejo de Europa, por el cual se establecía que ese día de cada año se celebrase el Día Internacional de la Protección de Datos Personales. El objetivo de la conmemoración era crear conciencia sobre la importancia de la **privacidad**, la **protección de datos personales en el mundo**, difundir los **derechos y mejores prácticas** en esta materia y sensibilizar a la población sobre las **implicaciones de compartir los datos personales con terceros**.

En nuestro país, la protección de datos personales se encuentra garantizada a través de la acción de hábeas data, incorporada en el Artículo 43 párrafo tercero de la Constitución Nacional, en oportunidad de la reforma constitucional de 1994. Posteriormente se sancionó la **Ley 25.326 de Protección de Datos Personales**, norma de orden público que tiene por objeto el resguardo integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, ya sean públicos o privados, destinados a dar informes para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que se registre sobre ellas.

En 2014 la **Ley 26951** creó el **Registro Nacional "*No Llame*"** cuya finalidad es proteger a los titulares o usuarios autorizados de los servicios de telefonía, en cualquiera de sus modalidades (fija, celular, IP, etc.) de los abusos de procedimiento de contacto, publicidad, oferta, venta y regalo de bienes y servicios no solicitados. En dicho registro **podrá inscribirse toda persona física o jurídica titular o usuario autorizado del servicio de telefonía** en cualquiera de sus modalidades **que manifieste su voluntad de no ser contactada**.

En la actualidad, la **Agencia de Acceso a la Información Pública**, ente autárquico que funciona en el ámbito de la Jefatura de Gabinete de Ministros, actúa como **autoridad de aplicación** de la Ley 25.326 de Protección de Datos Personales según el Decreto Reglamentario 206/2017.

Cabe señalar, por un lado, que la Ley 25.326 abarca a las personas físicas y a las de existencia ideal y, por otro, define los **datos sensibles**, los cuales revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. **Ninguna persona está obligada a proporcionar datos sensibles**. Los datos sensibles sólo pueden ser abordados y tratados cuando medien razones de interés general autorizadas por ley o con fines estadísticos o científicos cuando no puedan ser identificados sus titulares. Además está prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles.

¿**Es obligatorio obtener el consentimiento en todos los casos para acceder a los datos**? **No será necesario dicho consentimiento** cuando: a) los datos se obtengan de fuentes de acceso público irrestricto; b) se recaben para el ejercicio de funciones propias de los poderes del Estado o de una obligación legal; c) se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) deriven de una relación contractual, científica o profesional del titular de los datos y

resulten necesarios para su desarrollo o cumplimiento, e) se trate de operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.
Vinculada con este tema se encuentra la **nueva Ley de Protección de Datos de la Unión Europea (*General Data Protection Regulation* – Regulación General de Protección de Datos** y es el marco legal que entrará en vigencia el **25 de mayo de 2018**. El propósito de la GDPR es proteger los datos personales y la forma de procesamiento, almacenamiento y destrucción de esos datos cuando ya no son requeridos por las organizaciones.

Esta normativa otorga **ocho derechos específicos**, a saber: a estar informado, al acceso, a la rectificación, a ser borrado (o derecho a ser olvidado), a restringir el procesamiento, a la probabilidad de datos, a objetar, sobre la toma de decisiones y creación de perfiles automáticos. **Si una organización o procesador viola alguna condición las penalidades son muy altas**: podrían llegar a la suma de diez millones de euros o del 2% de su volumen de ventas globales.

Asimismo, la GDPR aplicará su regulación a:

- Organizaciones con presencia física en al menos algún país miembro de la Unión Europea.
- Organizaciones que procesan o almacenan datos sobre individuos que residen en la Unión Europea.
- Organizaciones que utilizan servicios de terceros que procesan o almacenan información sobre individuos que residen en la Unión Europea.