HABEAS DATA, PROTECCIÓN DE DATOS E INTIMIDAD.

RETOS EN MATERIA DE SEGURIDAD DE LA INFORMACION PARA LAS EMPRESAS.

ACIS

PREMISAS FUNDAMENTALES EN MATERIA DE PROTECCION DE DATOS DE LA EMPRESA:

- ✓ Actualmente la información de las empresas constituye uno de sus principales activos a proteger.
- ✓ La información puede ser propia (de la empresa) o de terceros (stakeholders) .
- ✓ La ley comercial obliga a los administradores a guardar la debida diligencia en el cuidado de los "activos" sociales. Estos Activos pueden ser tangibles o intangibles.
- ✓ La información es un activo intangible.

ANTECEDENTES:

- Tradicionalmente, la protección de la información se realizaba a través de las normas de **PROPIEDAD INTELECTUAL** (Propiedad Industrial y Derechos de Autor), **NORMAS DE GESTIÓN DOCUMENTAL Y ARCHIVÍSTICA** y las relativas a los **LIBROS Y PAPELES DEL COMERCIANTE** contenidas en el Código de Comercio. (Capítulo I, Título IV, Libro I del Código de Comercio).

ACIS

- Otra información, relativa a los negocios de las empresas, se protegía y se sigue protegiendo a través de los **ACUERDOS DE CONFIDENCIALIDAD** y **CLÁUSULAS DE CONFIDENCIALIDAD.** (Extensibles a los contratos laborales o de prestación de servicios de las personas que colaboran con las empresas -trabajadores y/o contratistas-).

- El desarrollo tecnológico y la incorporación de nuevas tecnologías en los procesos industriales, que ha motivado el paso de la *"Sociedad Industrial"* a la "*Sociedad de la Información"*, requieren de una nueva visión en el tratamiento de la información: Uso de herramientas de **seguridad informática y un sistema de gestión de seguridad de la información,** para proteger toda información que ahora se considera *"de valor"*, y cuya revelación no autorizada o pérdida puede generar inconvenientes de toda índole:

  - Bases de Datos de Clientes;
  - Bases de Datos de Empleados, Afiliados, etc.;
  - Información de reservas de productos de la empresa;
  - Información de planes de negocio;
  - Confiabilidad de datos financieros; etc.

ACIS

- El uso de estas soluciones de Seguridad Informática y la implementación de un Sistema de Gestión de Seguridad de la Información, plantean por primera vez un conflicto para las empresas: **SEGURIDAD INFORMÁTICA e INFORMACION Vrs. INTIMIDAD y HABEAS DATA / PROTECCIÓN DE DATOS PERSONALES e INFORMACION Vrs. INTIMIDAD y HABEAS DATA / INFORMACIÓN** Vrs. **INTIMIDAD y HABEAS DATA**.

- **RETO DE LA EMPRESA**: Proteger y Conciliar.

- La Corte Constitucional ha reconocido la existencia de tres (3) derechos fundamentales independientes en el artículo 15 C.P.: (i) Derecho a la Intimidad, (ii) Derecho al Buen Nombre, (iii) Derecho/Garantía al *Habeas Data* (Protección de Datos Personales).

- La C.P. consagra el Derecho fundamental a la Información, en el artículo 20 C.P.

- No hay derechos absolutos.

ACIS

- El primer paso para resolver el conflicto, es a través de la clasificación de la información en: (i) Pública, (ii) Semi-Privada, (iii) Privada, y (iv) Restringida (datos sensibles) y en que se cuente con un Sistema de Gestión de Seguridad de la Información, para asegurar que en el tratamiento de la información:

  (i) Se proteja la información como activo fundamental de la empresa, con un importante valor patrimonial. (Art. 196 y Art. 200 C.Com.)

  (ii) Debe garantizarse que con la protección de la información y la implementación de los mecanismos para su tratamiento, se garantice el ejercicio del derecho fundamental a la información, y no se violen derechos fundamentales de terceros como la intimidad y/o el habeas data (Arts. 15 y 20 C.P).

  (iii) Se garantice el derecho a la protección de los datos personales de la empresa y de aquellas personas naturales y jurídicas con las que la esta tenga vínculos.

- El sistema de Gestión de Seguridad de la Información (SGSI), a su vez, debe apoyarse en la implementación de herramientas de Seguridad Informática que garanticen la (i) Confidencialidad, (ii) Integridad, (iii) Disponibilidad, (iv) Confiablidad (Enron / act II SOX), y (v) El Consentimiento. (ISO 27001 + ordenamiento legal) de la información. La sumatoria de tales factores debe culminar en la implementación de una Política de Seguridad de la Información de la empresa.

SGSI

SEGURIDAD INFORMÁTICA

+

NORMAS LEGALES

= POLITICA DE SEGURIDAD DE LA INFORMACION

ACIS

¿CUÁL ES EL MARCO LEGAL EN EL CUAL DEBEN BASARSE LAS EMPRESAS PARA GARANTIZAR EL DERECHO A LA INTIMIDAD, Y EL DERECHO/GARANTÍA AL HABEAS DATA Y LA PROTECCIÓN DE LOS DATOS PERSONALES?

Rta: **La Jurisprudencia de la Corte Constitucional Colombiana (Sentencia T-729/2002) y la Ley 1266 de 2009.**

ACIS

DESARROLLO JURISPRUDENCIAL (Sentencia T -729/ 02). **:**

- **Habeas Data** (*Autodeterminación Informática*) : *"Facultad del titular del dato personal para exigir a la* ***administradora*** *del dato personal el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos,* ***así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos****, conforme a los* ***principios*** *que informan la administración de bases de datos personales (…)."* (Sentencia T 792/ 02).

- **Principio de Libertad**: Los datos sólo pueden ser registrados y divulgados con el **CONSENTIMIENTO LIBRE, PREVIO y EXPRESO** del titular. Prohíbe la obtención y divulgación de datos de manera ilícita: (i) Sin previa autorización del Titular, (ii) En ausencia de mandato legal o judicial. (Sentencia T 792/ 02).

- **Principio de Finalidad**: El acopio, procedimiento y divulgación de datos personales debe estar definido de manera **CLARA, SUFICIENTE y PREVIA**. Queda prohibida la divulgación **INDISCRIMINADA** de datos personales.

ACIS

- **Información Pública**: Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno.

- **Información Semi-Privada**: Presenta para su acceso y conocimiento un grado mínimo de limitación. Sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales.

- **Información Privada**: Información que sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.

- **Información Reservada**: Estrecha relación con los derechos fundamentales del titular —dignidad, intimidad y libertad— se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones (“Datos Sensibles“).

- Para la Corte, clasificación es útil por que delimita: (i) La información que se puede publicar (derecho a la información), y (ii) Aquella está prohibido publicar como consecuencia de los derechos a la intimidad y al habeas data.

DESARROLLO LEGAL: LEY 1266 DE 2009.

OBJETO (Art. 1):

- Desarrollar el Derecho constitucional de las personas a conocer, actualizar, y rectificar información personal en bases de datos. (¿Todo tipo de *información* o solo la *financiera, crediticia, comercial y proveniente de terceros países*?).

- Desarrollar los demás derechos, libertades y garantías relacionadas con el tratamiento de datos personales a que se refiere el artículo 15 C.P (Intimidad, Buen Nombre, Habeas Data), así como el Derecho a la Información consagrado en el artículo 20 C.P. (Información). (¿Los desarrolla?)

- Desarrollarlos ***particularmente*** en relación con la ***información financiera, crediticia, comercial y proveniente de terceros países***. (¿Qué pasa con los demás datos? ¿Aplica por analogía?).

ACIS

- No Aplica a:

  - Bancos de Datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos, o para garantizar el orden público.

  - Bases de Datos del DAS y de la Fuerza Pública (Seguridad Nacional).

  - Registros Públicos de las Cámaras de Comercio.

  - Bases de Datos personales o domésticos y ***de circulación interna.*** (¿?)

B) **TIPOS DE INFORMACION**:

- **Dato Personal**: Información vinculada a una persona.

- **Dato Público**: Todo lo que no es privado o semiprivado según la Constitución o la Ley (Documentos Públicos, Sentencias Judiciales no sometidas a reserva, estado civil de las personas).

- **Dato Semi-Privado**: Aquel cuyo conocimiento puede interesar a un grupo determinado de personas o la sociedad en general: Dato Financiero o Crediticio, Actividad Comercial y/o de Servicios.

- **Dato Privado**: Aquel que por su naturaleza íntima o reservada solo es relevante para el titular.

- **Información Financiera, Crediticia Comercial, de Servicios y Proveniente de Terceros Países:** La referida al nacimiento, ejecución y extinción de **obligaciones dinerarias**, así como la información relativa a las demás **actividades propias del sector financiero** o sobre el **manejo financiero o los estados financieros del titular.**

C) PRINCIPIOS DE LA ADMINISTRACIÓN DE DATOS:

- Principio de Veracidad o Calidad de los “registros” o Datos.
- Principio de la Finalidad (Autorización).
- Principio de Circulación Restringida (Internet / Medidas de Seguridad).
- Principio de Temporalidad (Asociado a la finalidad del dato).
- Principio de Interpretación Integral de Derechos Constitucionales.
- Principio de Seguridad (Medidas Técnicas).
- Principio de Confidencialidad.

ACIS

PARTICULARIDADES DE LA NORMA:

- La administración de datos privados y semiprivados requiere del **CONSENTIMIENTO PREVIO Y EXPRESO** del titular de los datos, **EXCEPTO** en el caso del *dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países.* (Art. 6 Parágrafo I2).

- Los Operadores deberán adoptar un Manual Interno de Políticas y Procedimientos para garantizar el adecuado cumplimiento de las disposiciones de la Ley, especialmente para la atención de consultas y reclamos por parte de los titulares .

- Las Fuentes deberán mantener **ACTUALIZADA** la información de la base de datos.

- El Usuario deberá conservar *"con las debidas seguridades"* la información recibida para impedir su deterioro, pérdida, alteración y uso no autorizado o fraudulento.

ACIS

VIGILANCIA Y SANCIONES:

- **Superintendencia de Industria y Comercio** a los operadores, las fuentes y los usuarios de *información financiera, crediticia, comercial, de servicios y la proveniente de terceros países*.

- **Superintendencia Financiera**: Cuando el operador, la fuente o el usuario de *información financiera, crediticia, comercial, de servicios y la proveniente de terceros países* sea una entidad vigilada por la Superintendencia Financiera de Colombia.

- **Sanciones**: Establece las aplicables a los Operadores, Fuentes y Usuarios de *información financiera, crediticia, comercial, de servicios y la proveniente de terceros países*

¿ Y LOS DEMÁS ADMINISTRADORES DE DATOS?

¿QUIÉN LOS VIGILA?

¿QUIÉN LOS SANCIONA?

ACIS

GRACIAS

macanosac@gmail.com

ACIS