

Inspecciones a las Bases de Datos de la empresa

Autor: Monserrat Guitart Piguiellén y Marcos Masserini

[Carranza Torres & Asociados](#)

Asesoramiento Legal en Tecnología

Fecha Publicación: 30 de agosto de 2008

No cabe duda que con la sanción de la [Ley 25.326 de Protección de Datos Personales](#), su Decreto Reglamentario 1558/01 y las sucesivas disposiciones que la [Dirección Nacional de Protección de Datos Personales \(DNPDP\)](#) ha dictado desde su creación, la Argentina se ha propuesto firmemente garantizar la protección de los datos personales.

Para ello y con el claro afán de que este derecho no quede en la categoría de expresión de deseos, como tantos otros de nuestras constituciones, la DNPDP ha sido dotada de distintas prerrogativas en su carácter de órgano de control de la Ley 25.326.

La más reciente de ellas, contenida en la Disposición 5/2008, es la de efectuar inspecciones que consistirán en una o más visitas presenciales del inspector y de personal técnico debidamente acreditado, quienes verificarán in situ -pudiendo acceder a la totalidad de los locales, equipos o programas de tratamiento de datos personales del responsable de la base de datos controlada- el cumplimiento de las disposiciones legales y reglamentarias vigentes.

Se ha previsto que este procedimiento pueda iniciarse de oficio, a discreción de la DNPDP o por denuncia de otro organismo estatal o de un particular. El espacio para estas denuncias es generado por la propia DNPDP a través de su página web (<http://www.jus.gov.ar/dnpdpnew/>), que contiene todas las instrucciones para reportar abusos en el tratamiento de los datos personales del denunciante.

Por regla, la inspección será notificada al responsable de la base de datos con una antelación de 10 días hábiles, salvo que se considere que la previa notificación puede afectar el resultado, en cuyo caso y siempre de modo fundado, se omitirá este aviso con el objeto de preservar el estado de cosas que quiere constatar. La inspección finalizará con un acta que quedará en poder del inspeccionado y otra que se agregará al expediente.

Un minucioso detalle del alcance, procedimientos y objetivos de la inspección está contenido en el Anexo I de la disposición comentada.

Los objetivos enunciados en el Anexo son dos: evaluar el grado de cumplimiento de lo prescripto por la Ley 25.326 y realizar recomendaciones para el mejor desempeño del responsable de la base de datos. Pero no debe pensarse que esto queda allí, ya que teniendo la DNPDP facultades sancionatorias, puede darse el caso que luego de constatar la violación corresponda imponer alguna de las sanciones previstas en la Disposición 7/2005 y que, según la gravedad de la falta, pueden consistir en apercibimientos, multas de entre \$3.001 y \$100.000 y clausuras.

En cuanto al alcance y procedimientos, las facultades de fiscalización conferidas parecen elevar el estándar vigente, ampliando el universo de conductas deseables por parte de quienes utilizan bases de datos. Esta asimetría, posiblemente genere conflictos interpretativos entre lo deseado por la administración pública y lo exigible conforme a la legislación vigente.

En concreto, se verificarán las medidas técnicas y organizativas en los siguientes campos: capacitación del personal, legalidad de los datos que posee y gestiona, idoneidad de los tratamientos de datos y en toda gestión anexa y correcto tratamiento de los datos personales, mediante el análisis de documentación y

entrevistas con el personal de las áreas de sistemas, de atención a titulares y usuarios y de legales.

A tal efecto, la DNPDP puede requerir:

- Acreditaciones de personería, CUIT, ANSES, municipalidad e inscripción y renovación de las Bases de Datos.
- Se pruebe la licitud en la recolección de los datos, su origen y que se ha informado la finalidad del tratamiento a los titulares, como así también los derechos que les caben.
- Que la empresa demuestre que posee una política de privacidad y confidencialidad y que ha instrumentado mecanismos para cumplirla.
- La presentación de los contratos de confidencialidad firmados por los empleados, usuarios o terceros.
- Constancias de que los titulares han prestado el consentimiento para el tratamiento y cesión de los datos.
- El Documento de Seguridad de Datos Personales y la adopción de medidas técnicas y organizativas relativas a la incorporación y destrucción de datos, la idoneidad de los medios de tratamiento de datos, software y hardware y en general todas las contenidas en la Disposición 11/2006.
- Se demuestre la capacitación del personal, para lo que se evaluarán títulos y acreditaciones del responsable de la base de datos, su participación en actividades académicas, las publicaciones efectuadas por el mismo y sus inscripciones, inhabilitaciones e inhibiciones, capacitaciones internas y externas del personal, estudios básicos y relacionados a datos personales, conocimiento de los empleados de sus responsabilidades vinculadas al tratamiento de los datos personales, capacidad de trato y respuesta ante reclamos.
- Verificar procedimientos de atención a usuarios y de reclamos, personas a cargo, recepción de solicitudes, verificación de identidad del solicitante, respuesta al titular de los datos, registro y seguimiento del caso, procedimientos internos de rectificación, actualización, supresión y bloqueo, plazos de respuesta, etc.

Es evidente que la situación que se muestre al inspector debe coincidir con las manifestaciones efectuadas en el formulario de inscripción o renovación de datos, que tiene carácter de declaración jurada. Por lo que, para enfrentar con éxito estas inspecciones será indispensable un sinceramiento de las empresas en cuanto al estado real de sus bases de datos con la finalidad de adoptar medidas correctivas y preventivas cuanto antes.

Y es que, disparados los mecanismos de control, no habrá lugares donde esconderse. Por ello entendemos que la política de la empresa no puede ser la de buscar el resquicio legal para ampararse o la de confiar en la quietud del Estado. La política de la empresa no puede ser otra que la de transformar sus comportamientos, acercándolos poco a poco a las Best Practices internacionales en la materia.

Una ayudita por favor

El 3 de septiembre de 2008 se publicó en el Boletín Oficial (B.O.) la Disposición 9/2008 de la Dirección Nacional de Protección de Datos Personales (DNPDP) por la cual se prorrogan los plazos para adoptar medidas de seguridad sobre las bases de datos.

Por medio de la Disposición 11/06 la Dirección concretó un régimen de seguridad dividido en tres niveles y escalonó el cumplimiento de cada uno de ellos, en uno, dos y tres años a contar a partir del día 22 de septiembre de 2006, fecha en la que fue publicada en el B.O. la mencionada norma. Esos plazos, ahora vencerán para el nivel medio el día 3/09/09 y para el nivel crítico el día 3/10/09. Las de nivel mínimo, que incluyen la obligación de redactar el Documento de Seguridad, ya se encuentran vigentes.

El lento avance de la implementación de las medidas de seguridad en las empresas y la falta de internalización de las mismas, ha sido el motivo por el cual se decidió extender el plazo en el cual estas medidas serán exigibles. No es la primera vez que esto ocurre, ya que una prórroga similar se acordó respecto de las inscripciones de las bases de datos privadas en el año 2006.

Pero esto no es todo, ya que la DNPDP avanzó un poco más poniendo a disposición de los administrados un modelo orientativo de Documento de Seguridad de Datos Personales, allanando de ese modo el camino que han emprendido aquellos que son conscientes del valor de sus bases de datos y de las responsabilidades que acarrea su posesión.

Debe recordarse que la DNPDP está facultada para imponer sanciones y para realizar inspecciones consistentes en una o más visitas a las empresas por parte de inspectores y personal técnico, quienes podrán acceder a la totalidad de los locales, equipos o programas de tratamiento de datos personales del responsable de la base de datos controlada con el objeto de verificar el cumplimiento de las disposiciones legales y reglamentarias vigentes. La inspección puede dispararse por una denuncia o por una decisión de la DNPDP y puede hacerse sin previo aviso.

En una inspección la DNPDP puede requerir:

- Acreditaciones de personería, CUIT, ANSES, Municipalidad e inscripción y renovación de las Bases de Datos.
- Se pruebe la licitud en la recolección de los datos, su origen y que se ha informado la finalidad del tratamiento a los titulares, como así también los derechos que les caben.
- Que las empresas demuestren que poseen una política de privacidad y confidencialidad y que han instrumentado mecanismos para cumplirla.
- La presentación de los contratos de confidencialidad firmados con los empleados, usuarios o terceros.
- Constancias de que los titulares han prestado el consentimiento para el tratamiento y cesión de los datos.
- El Documento de Seguridad de Datos Personales y la adopción de medidas técnicas y organizativas relativas a la incorporación y destrucción de datos, la idoneidad de los medios de tratamiento de

datos, software y hardware y en general todas las contenidas en la Disposición 11/2006.

- Se demuestre la capacitación del personal y la correcta atención a los reclamos de los titulares de los datos.

Aunque el sólo cumplimiento de la ley tiene un valor innegable, esta iniciativa de la DNPDP es una oportunidad inmejorable para auditar la legalidad de las bases de datos de las empresas y revisar las conductas corporativas relacionadas con las mismas.

El Documento de Seguridad propuesto por la normativa comentada, no hace otra cosa que reflejar las Best Practices de la materia, y debe ser considerado un norte para los directivos de las empresas y encargados de sistemas, quienes tienen el desafío de modificar los comportamientos de la organización, mejorándolos. Esta ayuda que el Estado ha otorgado, no debe ser desaprovechada.