# Cumplimiento de la Protección de Datos en Venezuela

## Recursos Administrativos

No existe una entidad administrativa específica a cargo de los asuntos de privacidad.

Lo más probable es que los casos de privacidad se decidan en los tribunales y dicha entidad determinará las medidas cautelares aplicables según el caso específico.

## Recursos Civiles

La Ley de Delitos Informáticos prevé sanciones civiles que van desde las 200 unidades tributarias hasta las 600 unidades tributarias.

Actualmente, una unidad tributaria equivale a Bs. 127 (que equivale a USD 2,43 al tipo de cambio oficial SICAD 2 de 52,10 por USD), sujeto a los ajustes anuales posteriores realizados por la Administración Tributaria normalmente dentro del primer trimestre de cada año y de acuerdo con la inflación del año anterior.

Además, en caso de un procedimiento judicial civil, el tribunal determinará la indemnización que se otorgará a un demandante si se prueban los daños y perjuicios.

## Recursos Penales

El incumplimiento de lo dispuesto en la Ley de Protección de la Privacidad de las Comunicaciones, somete al infractor a sanciones de prisión que van desde un mínimo de tres meses hasta un máximo de cinco años.

El incumplimiento de lo dispuesto en la Ley de Delitos Informáticos, dará lugar a sanciones de prisión que van desde los dos años hasta un máximo de seis años.

## Otros remedios

Ninguno.

## Acciones de cumplimiento seleccionadas/Comentarios generales

Las normas contenidas en la legislación venezolana en relación con la privacidad de los datos y la transferencia de datos personales se limitan a algunas disposiciones contenidas en (i) la Constitución de la República Bolivariana de Venezuela y, (ii) leyes especiales que sancionan determinadas conductas relacionadas con la violación del derecho a la privacidad de los datos. Como se dijo, es muy probable que cualquier asunto relacionado con la privacidad sea decidido por un tribunal. Algunos ejemplos de acciones de cumplimiento recientes en Venezuela:

- En una decisión emitida por la Corte Suprema el 14 de marzo de 2001, la Corte hizo una interpretación de los artículos 28 (derecho a acceder a los registros oficiales) y 60 (derecho a la protección de la privacidad) de la Constitución. Esta sentencia rectora (a) determinó la información privilegiada que se encuentra protegida por las normas constitucionales; y (b) estableció un proceso de hábeas data y la información que puede ser objeto de dicho proceso (la "Decisión"). Al respecto, la Sentencia indicó que la información privilegiada sujeta a protección constitucional es aquella contenida en uno o más registros que combinadas pueden crear un perfil completo o parcial de la persona cuyos datos se incluyen en dicho registro.
- Con base en lo anterior, bajo esta decisión podría interpretarse que una base de datos de empleadores cumple con los estándares constitucionales, si de la información de la base de datos no se puede afirmar un perfil completo de una persona registrada, es decir, un empleado.
- Es importante señalar que la decisión no define claramente qué debe significar la expresión "perfil completo o parcial".
- I Asimismo, el 4 de agosto de 2011, la Sala Constitucional del Tribunal Supremo emitió la Sentencia No. 1318 ("Sentencia 1318"), la cual es la primera sentencia judicial que aborda los principios contenidos en el artículo 28 de la Constitución venezolana.

- De conformidad con la Decisión 1318, los principios fundamentales que regulan la privacidad de datos en Venezuela son los siguientes:

- I Principio de Autonomía de la Voluntad –

  Toda persona cuyos datos se encuentren incluidos en una base de datos tiene derecho a ser informada sobre: (i) la recolección de sus datos; (ii) la entidad responsable de sus datos; (iii) las finalidades para las que se recabaron los datos; y (iv) la forma en que podrá ejercer el derecho a la libre determinación. Todos ellos están sujetos a la existencia de un "consentimiento previo, libre, informado, inequívoco y revocable" por parte del afectado, en caso de que la entidad responsable de los datos necesite comunicarlos.

- I Principio de Legalidad –

  El derecho a la "autodeterminación informativa" sólo puede ser limitado mediante normas con rango de ley, siempre que ello esté justificado por el interés público, y tales normas deben ser interpretadas restrictivamente. Al respecto, la Sala aclara que la información recabada (i) no puede ser utilizada para fines contrarios a los principios enunciados en la sentencia bajo análisis oa las garantías constitucionales; o (ii) procesado por métodos ilegales o desleales.

- I Finalidad y Principio de Calidad –

  Las organizaciones que deseen recopilar datos personales de personas físicas, deberán hacerlo en estricto cumplimiento de las leyes y normas constitucionales y sectoriales, y ello deberá hacerse con un propósito, razón o causa clara. Este principio se considera esencial para que el consentimiento de la persona sea válido. De acuerdo con este principio, la recolección y uso de los datos personales de las personas físicas debe obedecer al principio de buena fe y proporcionalidad, pues sólo pueden recabarse los datos que sean adecuados, pertinentes y no excesivos para la finalidad perseguida.

- I Principio de Temporalidad y Conservación –

  Con fundamento en el derecho a la protección de datos, a la intimidad y a la actualización de la información contenida en bases de datos y en archivos de personas públicas y privadas, la Sala sostuvo que la información contenida en tales sistemas debe ser actualizada periódicamente a fin de evitar el deterioro de las personas como consecuencia de la obsolescencia de los datos. Asimismo, la Sala adoptó las decisiones adoptadas por los

tribunales colombianos en relación con el "derecho al olvido", que es el derecho de todas las personas a que se actualicen sus datos personales una vez subsanado el incumplimiento o la morosidad en que hayan incurrido.

- I Principio de Precisión y Autodeterminación –

  Los datos personales deben reflejar la verdadera condición de la persona. En este sentido, los datos no solo deben estar actualizados, sino también precisos y completos. Para lograr la eficacia de este principio, se deben establecer procedimientos claros y expeditos para asegurar que las personas tengan acceso y conocimiento de los datos que las instituciones públicas y privadas conservan sobre ellas. Esto también implica el derecho de las personas a exigir la rectificación o cancelación de los datos incompletos, inexactos, inadecuados y excesivos, y a ser advertidos de su corrección.

- I Principio de Prospectiva e Integralidad –

  Los avances tecnológicos exigen un análisis del almacenamiento, compilación y uso de los datos personalizados en conjunto con otras bases de datos o registros en los que se encuentran almacenados los datos personales del individuo, ya que si se muestran en su conjunto pueden ser perjudiciales para el individuo o sus intereses o derechos.

- I Principio de Seguridad y Confidencialidad –

  Todas las entidades que manejan la compilación, almacenamiento y uso de bases de datos tienen la obligación de mantener la seguridad requerida respecto de dichos datos, y de impedir la modificación de los mismos por parte de terceros ajenos.

  Esta obligación subsiste incluso después de la terminación de la relación entre la entidad y la persona correspondiente.

  Adicionalmente, la Sala señaló que este principio incluye la prohibición de transferir el contenido de las bases de datos a otros estados que no cuenten con normas que garanticen la protección de la información de las personas.

- I Principio de Protección –

  La protección judicial no es suficiente.

  Es necesario contar con entidades públicas con competencia para elaborar e implementar modelos basados en normas técnicas mediante los cuales se proteja la información de estas bases de datos.

- I Principio de Responsabilidad –

  Cualquier infracción del derecho a la protección de datos dará lugar a sanciones civiles, administrativas y penales.

  La responsabilidad por la infracción de este derecho no sólo recaerá sobre el funcionario del sector bancario, sino que se extiende a cualquier otro sector encargado del sistema de información.