Pontificia Universidad JAVERIANA Bogotá

LA RESPONSABILIDAD DEMOSTRADA FRENTE AL TRATAMIENTO DE DATOS PERSONALES Y SU RELEVANCIA PARA LA GRADUACIÓN DE LA SANCIÓN AL INTERIOR DE PROCEDIMIENTOS ADMINISTRATIVOS SANCIONATORIOS

DIEGO FERNANDO MONTEZUMA CHAVEZ

OBJETIVOS

GENERAL

Identificar los elementos y criterios que ha tenido en cuenta la SIC para aplicar el principio de responsabilidad demostrada como un factor de fijación de la sanción en las actuaciones administrativas sancionatorias adelantadas contra empresas responsables y encargadas del tratamiento de datos personales que han incumplido con sus deberes establecidos en el artículo 17 de la Ley 1581 de 2012 y demás concordantes.

ESPECÍFICOS

a. Identificar en qué casos la SIC empleó criterios divergentes al momento de aplicar el principio de Responsabilidad Demostrada e imponer la sanción administrativa.

b. Encontrar aquellos criterios que han sido reiterados en las decisiones en las que la SIC ha aplicado el principio de Responsabilidad Demostrada.

c. Realizar un planteamiento crítico sobre la eficiencia del Régimen de Protección de Datos personales en Colombia.

DELIMITACIÓN Y MÉTODO

En desarrollo de la investigación se estudió:

i) La potestad Sancionatoria de la Administración – Facultad sancionatoria por violación del Régimen de Protección de Datos Personales en Colombia.[1]
ii) La importancia del Sistema General de Protección de Datos Personales.
iii) El principio de Responsabilidad Demostrada en el Sistema de Protección de Datos Personales.
iv) La aplicación de dicho principio por parte de la SIC frente al tratamiento de datos personales y sus beneficios.
v) Los criterios de la SIC al encontrar infracciones respecto del tratamiento de datos personales

1: En adelante, RPDP.

La Potestad Sancionatoria de la Administración -SIC- por violación al RPDP

Constitución política

- **Art. 15**
- **Arts. 16 y 20**

→ **Derecho Fundamental al Habeas Data**

Ley 1581 de 2012

- **Art. 22:** Trámite para la imposición de sanciones.
- **Art. 23:** Lista las sanciones que puede imponer la SIC.
- **Art. 24:** criterios para la graduación de la sanción.

Importancia del Sistema General de Protección de Datos Personales

Pontificia Universidad JAVERIANA Bogotá

- **Sentencia C-748 de 2011**
- **“Big Data”** ¿De quién son? ¿Qué uso les puedo dar?
- **Derecho Fundamental.**
- **Responsabilidad Social.**
- **Régimen de Protección de Datos Personales.**

Principio de Responsabilidad Demostrada en el Sistema de Protección de Datos Personales

“Guidelines on the protection of Privacy and Transborder Flows of Personal Data” - Organización de Cooperación y Desarrollo Económico

El responsable del tratamiento de Datos Personales será garante en acatar las medidas necesarias para la implementación de los principios de recolección, calidad de la información, especificación, limitación, salvaguardas de la seguridad, apertura u participación del individuo.

El principio de Responsabilidad demostrada implica que el responsable del tratamiento de datos personales está llamado a responder por la inobservancia de los mencionados principios, pues es quien decide respecto del uso procesamiento de los datos personales recolectados, por lo que no puede escindir de su responsabilidad en el caso de que el tratamiento este efectuado por un encargado y/o tercero.

Principio de Responsabilidad Demostrada frente al responsable del tratamiento de datos personales

Grupo de Trabajo de Protección de Datos del artículo 29 (hoy Comité Europeo de Protección de Datos) Dictamen 3/2010

Planteó dos elementos, a saber: i) la necesidad de que el responsable del tratamiento adopte medidas adecuadas y eficaces para aplicar los principios de protección de datos y; ii) la necesidad de demostrar, si así se requiere, que se han adoptado medidas adecuadas y eficaces, así pues, el responsable del tratamiento de datos deberá aportar pruebas.

La eficacia de las medidas dependerá: i) sensibilidad de los datos; ii) la masa de datos objeto de tratamiento y; iii) los riesgos especiales planteados por el tratamiento.

Decreto 1377 de 2013

Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este Decreto, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.

2. La naturaleza de los datos personales objeto del tratamiento.

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas.

Aplicación del Principio de Responsabilidad Demostrada por parte de la SIC

Su empleo se ve ligado a la consideración que realice la autoridad respecto del responsable de tratamiento de datos personales, así como la existencia de medidas y políticas adecuadas al momento de evaluar la imposición de una sanción.

Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability):

"Tal y como sucede con el modelo recogido en el Decreto (1377 de 2013), y en los mismos términos en que la Superintendencia de Industria y Comercio ha venido diseñando su sistema de supervisión, el énfasis de la comunidad dedicada a la protección de la información tiende a volcarse hacia un modelo que privilegia la gestión del riesgo y la asignación de responsabilidades en cabeza del Responsable del Tratamiento".

Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability):

En este documento se construyó el **Programa de Gestión de Datos Personales** y está dirigido a quienes están sometidos al RPDP y sean vigilados por la SIC.

→ Con este Programa se busca estar preparados para demostrarle a la autoridad la implementación de medidas efectivas en la organización y generar confianza en el mercado.

→ Tiene como base el artículo 27 del Decreto 1377 de 2013 que trata las políticas efectivas que buscan garantizar:

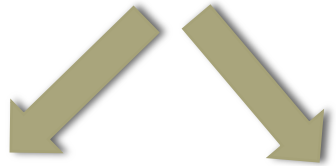
i) Que exista una estructura administrativa proporcional a la estructura del responsable para implementarlas
ii) Que se adopten mecanismos internos para poner en práctica políticas que incluyan herramientas de implementación, entrenamiento y programas de educación
iii) La adopción de procesos par la atención de reclamos y consultas de los titulares.

Elementos esenciales que debe tener un Plan Integral de Gestión de Datos Personales

1. Compromiso de la Organización
   - Desde la Alta Dirección
   - Oficial de Protección de Datos
   - Presentación de informes

2. Controles del programa
   - Procedimientos operacionales
   - Inventario de las bases de datos con información personal
   - Políticas
   - Sistema de Administración de Riesgos Asociados al Tratamiento de Datos Personales
   - Requisitos de formación y educación
   - Protocolos de respuesta en el manejo de violaciones e incidentes
   - Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales
   - Comunicación externa

EVALUACIÓN Y REVISIÓN DEL PLAN INTEGRAL



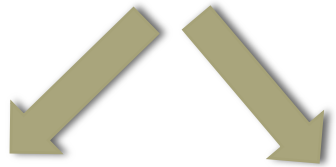
Desarrollar un Plan de Supervisión y Revisión

Evaluar y revisar los controles del Programa.

En materia de transferencias internacionales de datos personales

- Circular Externa 5 de 10 de agosto de 2017: i) Transferencia a países con nivel adecuado de protección y; ii) los responsables de datos deben demostrar que han implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de datos personales.

Responsable del tratamiento de datos



Garantizar el adecuado tratamiento de los datos personales que se transfieren a otro País.

Conferir la seguridad de los “registros al momento de efectuar dicha transferencia”.

Beneficios que trae la implementación del Principio de Responsabilidad Demostrada

	A PRIORI	A POSTERIORI
EL VIGILANTE	Permite enfocar los esfuerzos de vigilancia donde sea más necesario.	Tendrá un marco pre existente en el cual basar su decisión sancionatoria.
EL VIGILADO	Beneficio reputacional, así como disminución de los riesgos de violación de las disposiciones legales.	La existencia de un sistema de protección de datos recolectados por parte del investigado deberá tenerse en cuenta al momento de imponer sanciones.
EL TITULAR DE LOS DATOS	Conocerá de forma inequívoca sus derechos respecto de sus datos, podrá solicitar actualizaciones, supresiones, información adicional, entre otros.	Conocerá el marco en el cual se presentó la recolección, uso, transferencia, análisis y/o procesamiento indebido de sus datos.

Los criterios de la SIC al encontrar infracciones respecto del tratamiento de datos personales.

Pontificia Universidad JAVERIANA Bogotá

1. Tramitar consultas y reclamaciones en el término legal establecido.
2. Garantizar siempre y en todo lugar el ejercicio pleno y efectivo del *habeas data* al titular de la información.
3. Conservar la información bajo óptimas condiciones de seguridad.
4. Solicitar y conservar copia de la autorización previa y expresa de los titulares para el tratamiento de datos personales.
5. Contar con políticas de tratamiento de datos personales.

CONCLUSIONES

- El Sistema de Protección de Datos Personales que no tome en consideración fenómenos como el Big Data, la transmisión transfronteriza de información, la capacidad ilimitada de procesamiento de datos personales y, las implicaciones económicas, sociológicas y políticas de estos fenómenos está llamado a fracasar.

- El Sistema de Protección de Datos colombiano se encuentra permeado por las directrices de la OCDE y el Sistema Europeo de Datos Personales, los que también consideran al Habeas Data como un derecho fundamental.

- La implementación de un sistema adecuado de protección de datos, cuyo diseño y aplicación permita tener a las empresas que lo implementen una serie de beneficios en caso de que haya lugar a imponer una sanción administrativa.

- La imposición de sanciones administrativas por la violación al RPDP en Colombia responde a una visión integral de los derechos de los particulares, pues de una lectura sistemátic de las normas que regulan su protección, se comprenden que todos ellos componen la integridad de un sistema equilibrado y garantista.

Pontificia Universidad
JAVERIANA
Bogotá

G R A C I A S