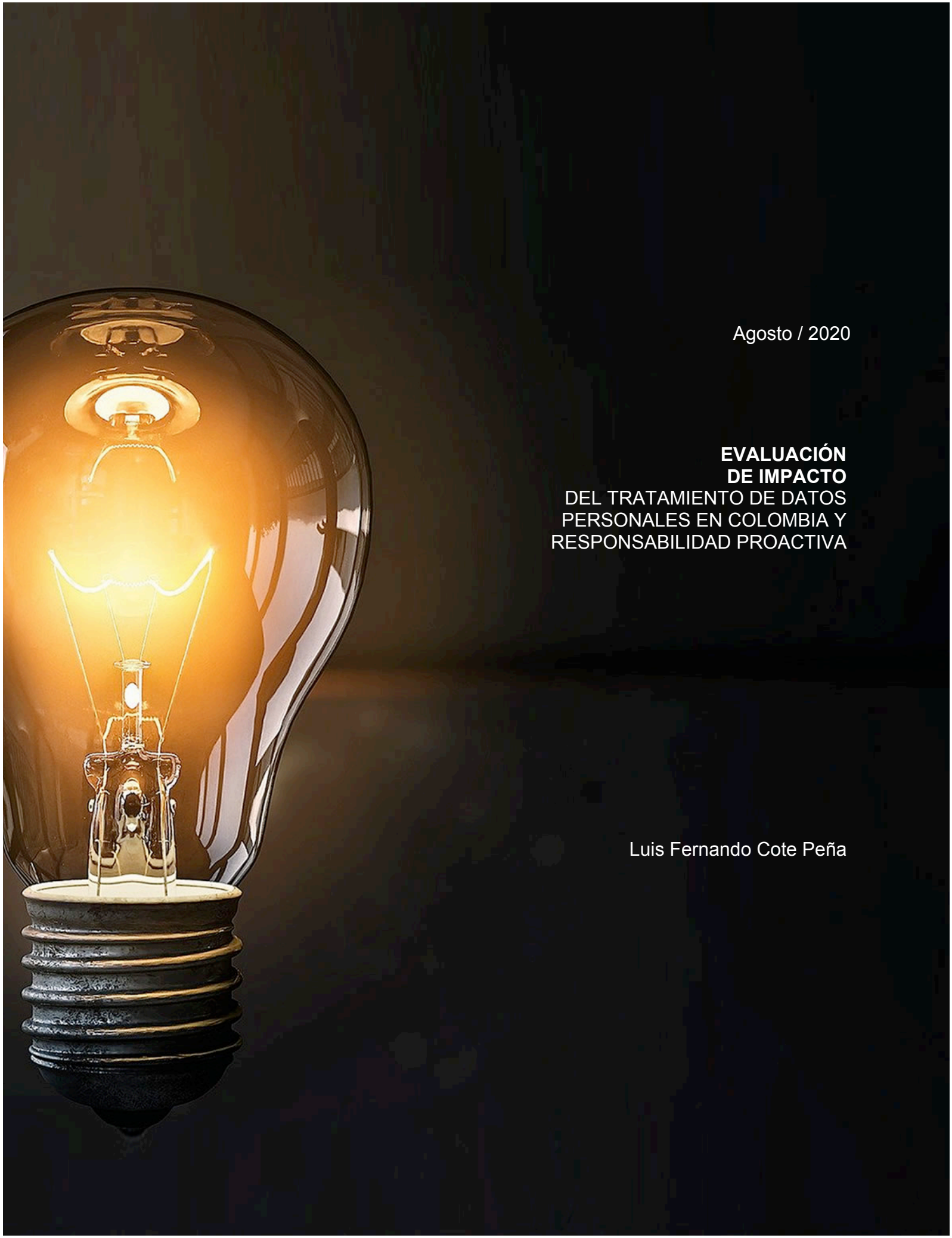


Agosto / 2020

EVALUACIÓN DE IMPACTO
DEL TRATAMIENTO DE DATOS PERSONALES EN COLOMBIA Y RESPONSABILIDAD PROACTIVA

Luis Fernando Cote Peña

Luis Fernando Cote Peña

Abogado, Especialista en Derecho Comercial de la U. Externado de Colombia, Especialista en Instituciones Jurídico Políticas y Derecho Público de la U. Nacional, Magister en Planes de Desarrollo Urbano Regional de la Pontificia Universidad de Valparaíso de Chile, Magister en Derecho de la U. Santo Tomás, Premio Internacional de Datos Personales 2015 de la Agencia Española de Protección de Datos Personales Versión XIX, Auditor Certificado en ISO 27001, Ex Alcalde de Bucaramanga, Ex Conjuez del Tribunal Administrativo de Santander, con experiencia docente universitaria en pregrado y posgrado por más de 11 años, autor de publicaciones especializadas en Protección de Datos, colaborador de Tribuna, publicación virtual de la Red Iberoamericana de Protección de Datos, y actual gerente de FERSACO S.A.S., empresa especializada en protección de datos personales, reconocido en el Ranking Nacional de Innovación de la Revista Dinero y Nominado al Premio de Innovación Tecnológica por Fenalco Santander 2018, por el desarrollo de la plataforma *SaaS* para cumplimiento de protección de datos *1581 – SPD*.

Contacto:
luisfernandocotep@fersaco.com
Derechos Reservados

EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES EN COLOMBIA Y RESPONSABILIDAD PROACTIVA

Tabla de Contenido

DE LA RESPONSABILIDAD ACTIVA A LA PROACTIVA EN EL TRATAMIENTO DE LOS DATOS PERSONALES 5

Responsabilidad activa en la protección de datos personales 5

Responsabilidad proactiva en la protección de datos personales 6

LA EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS COMO EXIGENCIA DE LA RESPONSABILIDAD PROACTIVA..... 8

OBLIGADOS A LA REALIZACIÓN DE EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE LOS DATOS PERSONALES 14

OPERACIONES QUE HACEN OBLIGATORIO REALIZAR EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES 16

Operaciones que entrañan alto riesgo de afectación a los Titulares.....18

Operaciones incorporadas en listas de obligatoria realización.....19

EXCEPCIONES AL DEBER DE REALIZAR EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES.....21

EFECTOS DEL INCUMPLIMIENTO DEL DEBER DE REALIZAR EIPD.....24

CONLUSIONES 25

EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES EN COLOMBIA Y RESPONSABILIDAD PROACTIVA

RESUMEN

Con el presente ensayo se busca poner de relieve la nueva tendencia interpretativa que en protección de datos personales se ha venido consolidando, pasando de un mero cumplimiento material de las exigencias normativas a la proactividad que presupone entre otras la realización de evaluaciones de impacto del tratamiento de los datos personales. Por otra parte se pretende servir de apoyo conceptual para aproximarse a conceptos básicos como qué es la evaluación misma, quienes están obligados, en que operaciones se entiende obligatorio el deber de realizarse y cuando no, así como las consecuencias que pueden derivarse de su incumplimiento. Para tal fin, y habida consideración de la ausencia de normativa colombiana en la materia, se ha buscado apoyo en los desarrollos que en el caso europeo y particularmente en el Español, se han dado.

PALABRAS CLAVES: Protección de Datos Personales, PIAS, Evaluaciones De Impacto De Protección de Datos Personales – EIPD, Oficial de Protección de Datos Personales – OPD, Protección de Datos desde el Diseño y Por Defecto, Decreto 620 de 2020.

DE LA RESPONSABILIDAD ACTIVA A LA PROACTIVA EN EL TRATAMIENTO DE LOS DATOS PERSONALES

El proceso de incorporación del derecho fundamental de hábeas data en la vida colombiana, a partir de su aparición en el artículo 15 de la Constitución Política de Colombia, desde la perspectiva de la interpretación y aplicación por parte de la Superintendencia de Industria y Comercio - SIC como autoridad de inspección, vigilancia y control de protección de datos que lo es para el país, ha estado definido por dos dinámicas claramente identificables.

Responsabilidad activa en la protección de datos personales

En un segundo momento, definido con ocasión de la divulgación de los conceptos contenidos en la Ley 1581 de 2012, como ley general de hábeas data para Colombia que lo es, sumado a la aparición de la *Guía de Implementación del Principio de Responsabilidad Demostrada o Accountability*[1] de la SIC, en el cual se fueron abriendo camino los pronunciamientos sobre nuevos asuntos de hábeas data, ya no solo financieros, al punto que hoy en día unos y otros casi llegaron a un nivel similar. Podría alguien afirmar que en la *Guía de Accountability* de la SIC, al ordenar el *Programa Integral de Protección de Datos*, se dibujan los albores de la Responsabilidad proactiva, sin embargo, en su literalidad y aplicación interpretativa al momento de sancionar la violación de los deberes de protección de datos por parte de la SIC, no se percibe con claridad la presencia de nociones como la protección de datos desde el diseño y por defecto y mucho menos la evaluación de impacto del tratamiento de datos personales, figuras que aparecen claramente demarcadas en fase posterior del desarrollo del universo jurídico del hábeas data nacional.

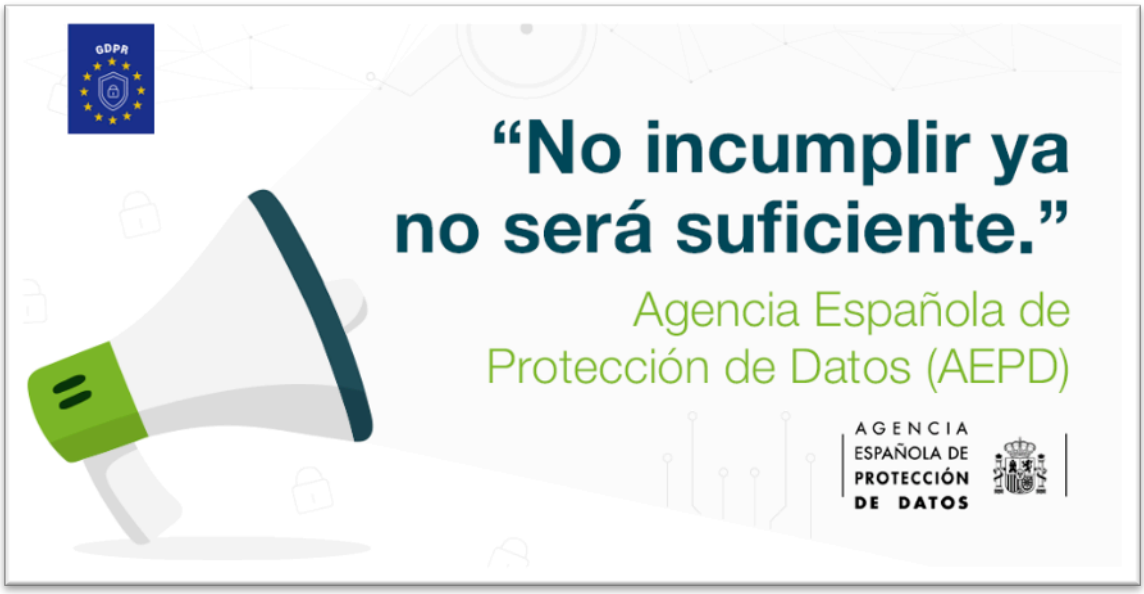
[1] Disponible en línea: www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Tanto en uno como en otro momento, las directrices de los pronunciamientos de la SIC, solo en pocos casos aplicadas por los Responsables y Encargados, así como las acciones organizacionales o las causas de sanciones, tenían que ver con verificaciones formales, esto es, tener una Política de Tratamiento de Información, contar con Procedimientos de seguridad de datos personales, haber divulgado en debida forma el Aviso de Privacidad, designar un área responsable del tratamiento de los datos, recolectar las autorizaciones cuando era debido, etc. Es decir, se trató de una fase, que podríamos llamar de mero cumplimiento formal de la ley, propio de los procesos de maduración normativa.

Responsabilidad proactiva en la protección de datos personales

En los últimos años, coincidente con la aparición del *Reglamento General de Protección de Datos Europeo - RGPD*[2], en Colombia, la forma de abordar la protección de datos personales ya no basta con el cumplimiento activo de los deberes exigidos en la norma, ha tenido una variación sustancial. La nueva visión incorpora una gestión proactiva que traslada el quehacer de la protección de datos, del análisis de los riesgos para al Responsable o al Encargado por el hecho del tratamiento, al análisis de los riesgos a los que puede estar expuesto el titular de los datos personales, llevando la operación del cumplimiento a enfocarse esencialmente en la garantía del derecho fundamental del hábeas data, reglado de por sí, como los demás derechos fundamentales incorporados en la Carta Constitucional de 1991, para la protección de la dignidad humana como principio fundante del Estado[3].

[2] Parlamento Europeo y del Consejo. Reglamento General de Protección de Datos Europeo. Disponible en línea: www.boe.es/doue/2016/119/L00001-00088.pdf
[3] Cote Peña, Luis Fernando. Habeas Data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001:2013, disponible en línea en: drive.google.com/file/d/1v2nNVi78nnVi3TBadsV1W3dGeVspMUcO/view. 2016. P 21-51.



Al tradicional enfoque del *Accountability,* muy sucintamente descrito en el RGPD al afirmar que *“Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la* autoridad *de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento”* [4] , se sumó la obligación para responsables y encargados consistente en tener que adoptar las medidas efectivas y necesarias que garanticen “*un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación*

[4] Parlamento Europeo y del Consejo. Op. Cit. Considerando 82.

o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales."[5]

La Red Iberoamericana de Protección de Datos - RIPD, el 20 de junio de 2017, dentro de los Estándares De Protección De Datos Personales Para Los Estados Iberoamericanos que fueron adoptados en el XV Encuentro Iberoamericano de Protección de Datos, señaló claramente las medidas preventivas que permiten *"(…) al responsable responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales como son la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia; la designación de un oficial de protección de datos personales; la elaboración de evaluaciones de impacto a la protección de datos personales y la privacidad por defecto y por diseño, entre otras, lo cual resulta esencial en el ámbito de las tecnologías de la información y las telecomunicaciones"*[6].

LA EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS COMO EXIGENCIA DE LA RESPONSABILIDAD PROACTIVA

Este nuevo enfoque de protección de datos proactivo se ve manifiesto, para el caso europeo, entre otros, con la advertencia que el mismo RGPD, cuando se presentes eventos en los cuales *"sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas"*, en cuyo caso se deberá realizar una *"evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo"*, para que con base en ellas se adopten las medidas adecuadas que deban tomarse. Esta exigencia es de tal nivel que, si con ocasión

[5] Ibíd. Considerando 83.
[6] Red Iberoamericana de Protección de Datos, Estándares de Protección de Datos Personales. Disponible en línea: www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf. Pág. 11.

del resultado de la correspondiente evaluación se advierte que la operación objeto de análisis conlleva un alto riesgo que para el responsable no le resulta posible mitigar con medidas dispuestas a su alcance y conforme a la tecnología disponible, debe reportar a la autoridad de control correspondiente antes de efectuar el correspondiente tratamiento.

Cabe recordarse que la Evaluación de Impacto de Tratamiento de Datos, se define como una herramienta que permite *"la identificación proactiva de los riesgos que el tratamiento de datos personales genera en los sistemas, procesos, infraestructura y actividades del talento humano y su gestión adecuada, para evitar su ocurrencia en las organizaciones. Constituye una traslación normativa europea, como la inmensa mayoría de las normas colombianas de protección de datos, que conforme al artículo 35 del Reglamento General de Datos Personales - RGPD, se volvió obligatoria en Europa para ciertas organizaciones cuando existe alto riesgo para los derechos y libertades de los Titulares."*[7]

Justamente la Red Iberoamericana de Protección de Datos - RIPD, imprimió el nuevo sentido de la protección de datos proactiva, incorporando en su numeral 41, que *"Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales"*[8], sentir que quedó refrendado posteriormente el 21 de junio de 2019, al momento de aprobar las Recomendaciones Generales Para el Tratamiento de los Datos en

[7] Red Iberoamericana de Protección de Datos, Cote Peña, Luis Fernando. Servicios Ciudadanos Digitales. Disponible en línea: https://www.redipd.org/sites/default/files/2020-06/servicios-ciudadanos-digitales-Luis-Fernando-Cote.pdf. 2020. Ítem iii. numeral 1.
[8] Red Iberoamericana de Protección de Datos, Estándares de Protección de Datos Personales. Op. Cit. P. 31.

la Inteligencia Artificial[9], donde igualmente dejó también plateada la evaluación de impacto como herramienta misma desde el diseño y por defecto. A propósito la RIPD al respecto enunció *que "previo al diseño y desarrollo de productos de IA, y en la medida en que sea probable que los productos entrañen un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, se debe realizar una evaluación de impacto".*[10]

Para el caso colombiano, podría afirmarse que la nueva orientación de la responsabilidad proactiva se vio claramente manifiesta en la exigencia de la evaluación de impacto para las operaciones asociadas a los servicios ciudadanos digitales, consagrada en el artículo 2.2.17.6.2. del Decreto 1413 del 25 de agosto de 2017[11], subrogado por el artículo 1º del Decreto 620 de 2020, donde se advirtió como obligatorio para los operadores de servicios ciudadanos digitales que *"antes de dar inicio a la prestación del servicio"*, evaluar el impacto en el tratamiento de datos personales de las operaciones asociadas a dichos servicios, la cual debería, al tenor de lo normado, incluir como mínimo lo siguiente:

> *"1. Una descripción detallada de las operaciones de tratamiento de datos personales que involucran la prestación de los servicios ciudadanos digitales y de los fines del tratamiento.*
> *2. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.*

[9] Red Iberoamericana de Protección de Datos, Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial. Disponible en línea: https://www.sic.gov.co/sites/default/files/files/pdf/1%20RIPD%20(2019)%20RECOMENDACIONES%20GENERALES%20PARA%20EL%20TRATAMIENTO%20DE%20DATOS%20EN%20LA%20IA.pdf.
[10] Ibíd. Pág. 15.
[11] Ministerio de Tecnologías de la Información y las Comunicaciones, Decreto 1413 del 25 de agosto de 2017. República de Colombia. Disponible en línea: https://www.sic.gov.co/sites/default/files/files/Boletin-juridico/2017/Decreto1413DE25AGOS2017ServiciosCiudadanosDigitales.pdf

3. Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales.

4. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, tecnologías y mecanismos que garanticen la protección de datos personales, pudiendo realizar diseño de software, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas"[12].

A nivel doctrinal es importante traer a referencia el pronunciamiento que la Superintendencia de Industria y Comercio realizó el 28 de enero de 2019, en el marco de las actividades anuales que la entidad desarrolla con ocasión del día internacional de la protección de datos personales. En esta fecha que a la postre resulta icónica, se dio a conocer la Resolución 1321 de 2019, producida 4 días atrás, por medio de la cual exigió a Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited, incorporar en sus operaciones un conjunto de acciones dirigidas a proteger los datos de los habitantes del territorio colombiano, usuarios de los servicios de las referidas empresas, en razón del tratamiento que de los mismos realizan.

El pronunciamiento histórico de la SIC, coincidente con similares manifestaciones realizadas por diversas autoridades de protección de datos de otros países tales como The Data Protección Commission of Ireland (2012), The Federal Trade Commision de los Estados Unidos de Norteamérica (2011), The Office of the Australian Information Commisiones (2012), The Office of the Privacy Commissioner of Canada y The Standing Committee on Access to Infomation Privacy and Ethics del mismo país (2009), The Information Commissioner´s Office de Gran Bretaña (2017), The Commision Nationale de L'informatique et des

[12] Ibíd, Pág. 15-16.

Libertés de Francia (2017), The Dutch Data Protection Authority de los Países Bajos (2017), The Office of the Privacy Commissioner of New Zealand (2018), The Office of the Attorney General for the District of Columbia (2018), abrió la línea doctrinal sancionatoria de la SIC en la nueva dimensión proactiva de protección de datos que la generalidad del universo europeo había adoptado.[13]

En la mencionada Resolución 1321/19 mencionada, la SIC exigió a Facebook la realización de una evaluación de impacto relativa a la protección de datos, figura que para ese momento y aún hoy, no había sido expresamente reglada en la legislación colombiana con el mismo carácter general que se ha realizado en el caso europeo, no siendo aplicable la norma de servicios ciudadanos digitales mencionada por tratarse de norma especial no aplicable al asunto.

No obstante, si bien no existía norma expresa general, a diferencia de lo que sucede en la unión europea con el artículo 35 del RGPD que lo hace universalmente obligatorio entre otros a los casos ya advertidos, puede decirse que de la lectura de los literales a. de los artículos 17 y 18 de la Ley 1581 de 2012, en concordancia con la responsabilidad de los administradores derivada de la Ley 222 de 1995 en sus artículos 22 y 23, si se deriva un mandato de cumplimiento de protección de datos proactiva, con materializaciones obligacionales tales como el aseguramiento de los datos desde el diseño y por defecto, apalancados en la evaluación de impacto del tratamiento de los datos, pues constituyen justamente una clara manifestación del sentir normativo que ordena garantizar al Titular *"en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data".*

[13] FERSACO SAS, Cote Peña, Luis Fernando. ¿Podrá cumplir Facebook exigencias de la sic en protección de datos? Disponible en línea: fersaco.wordpress.com/2019/04/06/podra-cumplir-facebook-exigencias-de-la-sic-en-proteccion-de-datos/

Como se ha señalado, en el caso colombiano no se tiene aún reglamentación acerca del proceso de la evaluación de impacto, para identificar cuándo o en qué eventos se está obligado, cuales han de ser las características mínimas que ella debe entrañar, cuáles son las consecuencias derivadas de la falta de ejecución de la misma, etc. Esta actividad de reglamentación que se encuentra pendiente de parte de las autoridades de protección de datos en la SIC, de seguro en proceso de incubación entre otras teniendo en cuenta la actividad evidenciada en sus pronunciamientos, fue advertida como compromiso por el conjunto de las autoridades de Iberoamérica al dejarlo así plantado en el texto de los Estándares de Protección de Datos Personales, al señalar en el apartado 41.2 que "*La legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia señalará los tratamientos que requieran de una evaluación de impacto a la protección de datos personales; el contenido de éstas, los supuestos en que resulte procedente presentar el resultado ante la autoridad de control, así como los requerimientos de dicha presentación, entre otras cuestiones.*"

Sin embargo, se estima de interés compartir algunos aspectos orientadores que pueden resultar útiles para quienes se aproximan hasta ahora en este tema, de manera que, con base en las fuentes institucionales que han abordado la evaluación de impacto en el tratamiento de datos personales, puedan ir incorporando en su conocimiento y probablemente en sus prácticas también, el cumplimiento de la obligación que, como quedó dicha, se entiende ínsita en los deberes de los Responsables, advertidos en los artículos 17 y 18 de la Ley 1581 de 2012.

OBLIGADOS A LA REALIZACIÓN DE EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE LOS DATOS PERSONALES

Un primer aspecto que se estima necesario, es precisar que la obligación de realizar la EITD no recae en cabeza del Oficial de Protección de Datos – OPD, cuyas funciones están advertidas en la Guía Para la Implementación del Principio de Responsabilidad Demostrada o *Accountability* en el apartado IV, sin que sean las únicas, sino en el Responsable, pues es a él a quien la ley impone, como se ha advertido ya tantas veces, el deber de garantizar al Titular, en todo momento, el pleno y efectivo ejercicio del derecho de hábeas data, que entre otras implica el tratamiento seguro de sus datos, garantizando su confidencialidad, integridad y disponibilidad. Es por tanto el Responsable, con la orientación y apoyo del OPD, sobre quien primigeniamente recae el deber de realizar la EITD cuando se den las circunstancias que lo ameriten.

Así entonces, surge la inquietud en relación con si el Encargado está o no obligado a realizar EITD. Recuérdese que siendo el Responsable aquél que trata los datos por su cuenta y riesgo, y además puede "disponer"[14] de los mismos,

[14] Cote Peña, Luis Fernando. Habeas Data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001:2013. Op. Cit. Pág. 125.

conforme a la ley y al marco de relacionamiento jurídico que surge de la autorización previa, expresa e informada que se recolecta, el Encargado, por su parte, es aquel que realiza tratamiento de datos por cuenta y riesgo del Responsable.

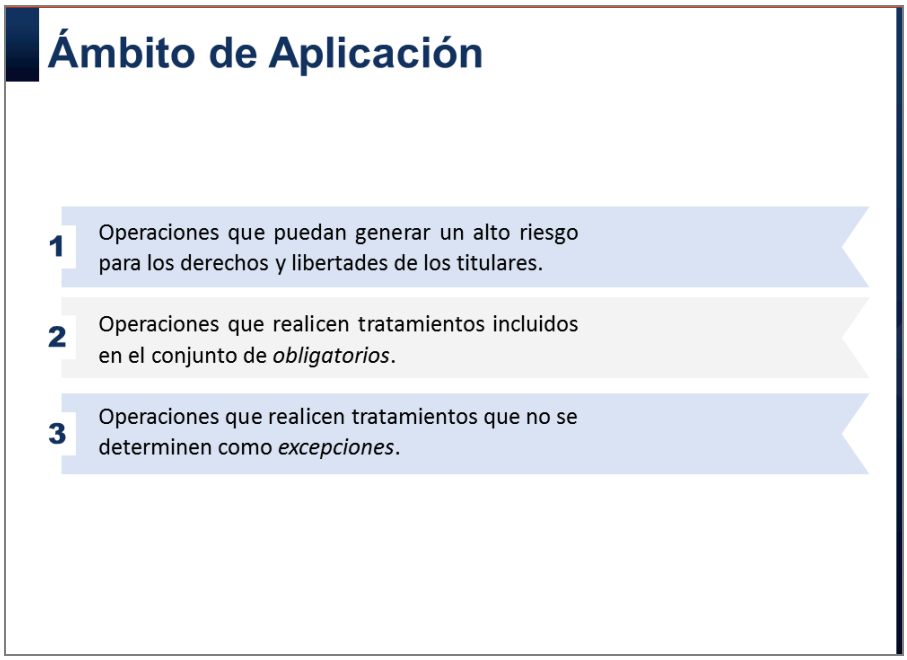
A este respecto debe aclararse que el Encargado, en relación con una operación en particular objeto de verificación del deber de hacer EITD y de la cual se deriva su calidad de Encargado, no le corresponde llevarla cabo. Esto se explica teniendo en cuenta que la EITD se tiene como una herramienta *ex ante*, es decir que debe desarrollarse antes de que una operación que ha de tratar datos personales se ponga en ejecución, representando un instrumento básico para realizar protección de datos desde el diseño y por defecto en cumplimiento de la responsabilidad proactiva que corresponde a la nueva tendencia jurídica de cumplimiento de hábeas data. Es justamente al Responsable a quien interesa la operación misma y quien está en capacidad de resolver si se hace o no, con qué características, soportado en qué tecnologías, involucrando qué áreas de la organización han de participar y por tanto definiendo si se verán vinculados o no terceros que, de llegar a tratar datos, adquirirán la calidad de Encargados.

Ahora bien, lo anterior no significa que pueda llevarse a cabo una EITD de una determinada operación sin la colaboración de un Encargado, cuando su relacionamiento con la misma es indispensable. Cabe mencionar por ejemplo, si para llevar a cabo un perfilamiento de titulares se necesita una herramienta de Inteligencia Artificial que la proveerá un tercero, claramente este será un Encargado sin cuya colaboración no se podría completar la EITD, pues resulta esencial conocer el ambiente tecnológico en el cual se desarrollaría la operación misma a efectos de estimar los análisis de riesgos pertinentes.

En conclusión, si bien es cierto el deber de la realización de una EITD es del Responsable, cuando se involucren Encargados en la operación a evaluar, deberá contar la colaboración de este, a riesgo de quedar inane la EITD que se desarrolle o en el mejor de los casos incompleta.

OPERACIONES QUE HACEN OBLIGATORIO REALIZAR EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES

La siguiente tarea es precisar en qué operaciones se debe realizar una evaluación de impacto del tratamiento de datos personales, tanto para proteger la dignidad de los titulares como para precaver los efectos nocivos del incumplimiento legal del debido tratamiento.



A este respecto se estima de importancia definir que, para efectos de las EITD, por operación se entiende un conjunto de acciones humanas y/o automatizadas que, en el marco de un proceso organizacional, conllevan el tratamiento de datos

personales por cuenta de un Responsable. A partir de ello, se infiere que una determinada operación puede implicar uno o varios tratamientos de datos. Esta es la razón que lleva a adoptar tal denominación, a diferencia de la conceptualización española al respecto, para no confundir, para el ámbito de la dogmática colombiana, la noción de tratamiento (recolección, almacenamiento, uso, circulación o supresión) con la noción que acaba de exponerse de operación, que de por sí es más compleja. Son ejemplos de operaciones el registro biométrico de acceso a las instalaciones de una determinada entidad, en el marco de las actividades de seguridad física, o el control de signos vitales mediante relojes inteligentes, en el marco del servicio de control de salud.

Precisado entonces qué se entiende por operación, debe decirse que no todas las operaciones demandan la realización de una EITD, lo que no significa para nada, y se hace énfasis en ello, que no deban estar siendo desarrolladas en el marco de un sistema de protección de datos personales, a riesgo de violar la ley. Hay operaciones, por ejemplo el registro de acceso a un edificio en sistemas físicos de registro, que escaparían al deber de realización de una EITD, al igual que la toma de signos vitales que realiza un médico y registra en su historia clínica física o en herramientas ofimáticas.

En contraste con lo reseñado, existen operaciones donde la utilización de nuevas tecnologías, por su naturaleza, alcance, contexto o fines pueden exponer de manera grave los derechos y libertades de los titulares a quienes están referidos los datos. Así lo expresa justamente el artículo 35 del RGPD de Europa al señalar: *"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. (…)"*

¿Cuáles son entonces las operaciones que deben ser objeto de EITD? Para responder tal interrogante, apalancados en la normativa europea consagrada en el RGPD y en la Guía Práctica para Las Evaluaciones de Impacto en la Protección de Los Datos Sujetas al RGPD[15], se presentan los siguientes elementos a considerar:

Operaciones que entrañan alto riesgo de afectación a los Titulares

En primer lugar se deberá identificar en la operación objeto de evaluación, si la misma entraña un alto riesgo para el titular de los datos. Para tal efecto y entendiendo por riesgo, como aquel suceso que de llegar a materializarse generaría un perjuicio para el titular, se estima que generarían un alto grado de afectación, sin que sean los únicos, los siguientes:

1. Usurpación fraudulenta de identidad
2. No disponibilidad del dato
3. Divulgación no autorizada de datos patrimoniales
4. Divulgación no autorizada de datos de reputación
5. Divulgación no autorizada de datos genéticos o de salud
6. Acceso no autorizado de información protegida por secreto profesional
7. Reversión de seudonimización o anonimización de datos
8. Acceso no autorizado a datos de perfiles, desempeño, movilidad, hábitos, comportamiento
9. Alteración del dato

[15] Agencia Española de Protección de Datos. Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD. Disponible en línea: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

10. Gestión desactualizada del dato
11. Ilegitimidad o ilegalidad del dato

El Responsable deberá tener en cuenta que estos riesgos han de ser analizados, a propósito de definir si ha de hacerse o no una EITD, teniendo en cuenta las características de la operación misma en relación con la tipología los datos personales vinculados, entendiendo que habrá de ameritar la mencionada evaluación por esencia para los casos de tratamiento de datos sensibles y en ciertos y determinados casos para datos privados o semiprivados[16].

Adicionalmente, se requerirá que el análisis de los anteriores riesgos se cruce con los riesgos subjetivos del titular, atendiendo a sus características propias, de forma que se pueda precisar si las mismas pueden agravar la condición del riesgo. Por ejemplo, no es lo mismo la no disponibilidad del dato de un titular cualquiera en relación con sus datos financieros, que la no disponibilidad del dato de un titular menor de edad en condición de desplazamiento como beneficiario de un servicio de apoyo estatal que requiere tal información o el perfilamiento de un funcionario privado para definir sus hábitos de consumo, que el perfilamiento de un líder social o sindical enlistado en los protocolos oficiales de protección humanitaria.

Operaciones incorporadas en listas de obligatoria realización

Una vez que el Responsable lleva a cabo el análisis de riesgos y deriva del mismo la conclusión de no identificar riesgos que ameriten la realización de la EITD, ello no bastará para descartar el mencionado deber. Agotada la anterior etapa le

[16] Cote Peña, Luis Fernando. Habeas Data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001:2013. Op. Cit. Pág. 100.

corresponderá identificar si existen o no, listas de operaciones en las que la autoridad defina como obligatoria la EITD.

En España, por ejemplo, acatando las orientaciones del RGPD en general y de manera particular el mandato incorporado en el numeral 4 del artículo 35 que impuso a la autoridad de protec*ción* de datos el deber de publicar *"una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos"*, la Agencia Española de Protección de Datos– AEPD publicó la Lista de Tipos de Tratamiento de Datos que Requieren Evaluación de Impacto Relativa a Protección de Datos Personales[17].

En América Latina y especialmente en Colombia no se ha identificado la elaboración de listas similares, convirtiéndose la labor efectuada por la AEPD como referente de consulta.

Por tal razón, se sugiere en virtud del principio de precaución, soportados en la referida *Lista de Tipos de Tratamiento de Datos que Requieren Evaluación de Impacto Relativa a Protección de Datos Personales de la AEPD*, tener como operaciones que para el caso de Colombia deberían ser objeto de EITD, sin que sean las únicas, las siguientes:

1. Perfilamiento o valoración del sujeto, personalidad, comportamiento o hábitos
2. Toma de decisiones automatizadas
3. Monitoreo, supervisión o geolocalización
4. Vigilancia de zonas de acceso público
5. Captura de datos a través de redes y aplicaciones

[17] Agencia Española de Protección de Datos. Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos. Disponible en línea: www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

6. Telecomunicaciones, Servicios web, TV interactiva, aplicaciones móviles
7. Gestión de información de antecedentes penales
8. Gestión de información financiera o patrimonial
9. Uso de datos biométricos para identificar titulares
10. Uso de datos genéticos para cualquier fin
11. Uso de datos sensibles a gran escala
12. Uso de datos de sujetos vulnerables o en riesgo de exclusión social
13. Uso de datos de menores de edad
14. Uso de datos de sujetos con algún grado de discapacidad
15. Uso de datos de víctimas de violencia de género
16. Impedimento a los titulares de ejercer sus derechos, utilizar servicios o ejecutar contratos
17. Asociación o combinación de bases de datos de dos o más Responsables
18. Transferencias nacionales o internacionales de datos personales
19. Utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas

EXCEPCIONES AL DEBER DE REALIZAR EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES

Con todo lo advertido, el Responsable, una vez ha identificado dentro de sus operaciones aquellas que entrañan alto riesgo de afectación a los titulares y/o que alguna de ellas se encuentra dentro de los listados sugeridos, se le recomienda identificar si existe algún listado de operaciones que se estimen por parte de la autoridad como exceptuadas de llevar a cabo la EITD.

A propósito de ello, resulta de interés advertir que en el caso español se ha promulgado un listado “orientativo” de aquellas operaciones que no requirieren la

realización de la EITD[18], en cumplimiento de lo ordenado en el artículo 35 numeral 5 del RGPD europeo, advirtiendo que *"Por supuesto, queda excluida de esta obligación cualquier tratamiento de datos en los que estos no sean de carácter personal (…)".*

Teniendo en cuenta que en el caso colombiano no se cuenta con un listado similar, no se recomienda acudir a las exclusiones contenidas en la normativa española, pues ello genera, hasta tanto surja regulación nacional, un riesgo para los Responsables. No obstante, con base en la orientación española, se dejan planteadas las siguientes sugerencias de exclusión de cara a que las autoridades nacionales de Colombia evalúen la posibilidad de su adopción:

1. Operaciones que sean realizadas en estricto acogimiento a las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por la SIC a través de la Delegatura de Protección de Datos, siempre que el alcance, tratamiento, contexto y finalidades no hubiera sido modificado desde la expedición de las directrices o del otorgamiento de la autorización correspondiente.

2. Operaciones que se encuentren certificadas en el marco de las normas corporativas vinculantes, adoptadas según la reglamentación que conforme al artículo 27 de la Ley 1581 de 2012 expida el Gobierno Nacional, siempre y cuando se hubiere efectuado una EITD completa para validar las normas corporativas vinculantes.

[18] Agencia Española de Protección de Datos. Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.5 RGPD. Disponible en línea: www.aepd.es/sites/default/files/2019-09/ListasDPIA-35.5l.pdf

3. Operaciones realizadas por las personas jurídicas de propiedades horizontales de que trata la Ley 675 del 2001 por medio de la cual se expide el régimen de propiedad horizontal.

4. Operaciones efectuadas por micro y pequeñas empresas, con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

5. Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento datos sensibles conforme al artículo 5º de la Ley 1581 de 2012.

6. Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular profesionales de la salud o abogados, salvo que sus servicios impliquen alguna operación de las señaladas como obligatorias para la realización de una EITD.

Respecto de la excepción contenida en el numeral 7 de la lista de excepciones adoptadas por la AEPD, en la cual refiere que se tendrán por tal: *"(…)Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa",* se considera pertinente comentar que argumentar como excepción la operación ejecutada por "*obligación legal o en el ejercicio de poderes públicos conferidos al responsable"* en el caso colombiano donde, conforme al

artículo 10º literal de la Ley 1581 de 2012 solo revela al Responsable del deber de recolectar la autorización, enviaría un mensaje equivocado en virtud del cual se podría interpretar equivocadamente que estos Responsables se encuentran revelados del deber de cumplimiento los principios de *accountability* y responsabilidad proactiva, lo cual resultaría altamente riesgoso.

EFECTOS DEL INCUMPLIMIENTO DEL DEBER DE REALIZAR EIPD

Para resolver el interrogante referido a las implicaciones que se derivan de no realizar la EIPD cuando se está obligado a ello conforme a las indicaciones dadas, ha de tenerse en cuenta que *"Sin necesidad de afectación de derechos del Titular, puede generarse responsabilidad administrativa para el Responsable y Encargado, cuando estos no logren demostrar ante la Superintendencia de Industria y Comercio - SIC el cumplimiento de las obligaciones que la ley les ha impuesto. Para tal propósito, la SIC, por intermedio de la Delegada para la Protección de Datos Personales, con su Grupo De Investigaciones Administrativas, verifica que las políticas adoptadas por los Responsables y Encargados garanticen una estructura acorde al desarrollo organizacional, los mecanismos internos para el desarrollo de la política (herramientas de implementación, entrenamiento y programas de educación), así como los procesos de atención a Titulares (artículo 2.2.2.25.6.2 del Decreto 1074 de 2015) para lo cual, soportada en el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, verificará que las medidas adoptadas sean apropiadas y efectivas para garantizar los derechos de los Titulares, que deben ser objeto de revisión en cada caso según las características propias de cada organización"*. (Cote Peña, Hábeas Data En Colombia, 2016, p. 145) Sumando que, desde la perspectiva de la responsabilidad proactiva hoy exigida por la SIC, "no incumplir ya no será suficiente" como lo señala el mensaje de la Agencia Española de Protección de Datos.

Por tanto, los Responsables del tratamiento de datos personales que, en el evento en que la SIC, en uso de sus facultades de inspección, vigilancia y control, identifiquen como, en relación con una operación determinada se debió ejecutar una evaluación de impacto del tratamiento dado a los datos, la misma no se efectuó, podrá estimar que se está incumplimiento del deber consagrado en el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015 en concordancia con el artículo 17 literal 1 de la Ley 1581 de 2012, al haber no haber adoptado las *"medidas apropiadas y efectivas"*, lo cual dará lugar a la imposición de las sanciones de que tarta esta ley, dentro de las cuales se han señalado las multas hasta de 2000 salarios mínimos legales mensuales vigentes, susceptibles de imponerse al Responsable y/o al administrador (gerente, director, consejo de administración, junta directiva, etc.), en este último caso por violar los deberes establecidos por la Ley 222 de 1995 en su artículo 24. En tratándose de servidores públicos, la responsabilidad será imputada por la Procuraduría General de la Nación para quien, por tratarse del incumplimiento de un deber que expone en riesgo los derechos fundamentales de los titulares de quienes se tratan los datos personales, podría derivar en destitución.

CONLUSIONES

1. "No incumplir ya no será suficiente", por tanto, en virtud del principio de responsabilidad proactiva derivado de la Ley 1581 de 2012, artículo 17, literal a, en concordancia con el artículo 2.2.2.25.6.1 del Decreto 1075 de 2015, es un deber de los Responsables realizar las EIPD en los eventos requeridos.

2. La no realización de la evaluación de impacto del tratamiento de datos personales, estando obligado a ello, se entiende como violación de los

deberes impuestos por ordenamiento jurídico y por tanto podrá conllevar las sanciones de que trata el artículo 23 de la Ley 1581 de 2012, esto es, entre otras, la imposición de mutas hasta de 2.000 salarios mínimos legales mensuales vigentes, en cabeza del Responsable y/o en cabeza de sus Administradores.

3. Si bien es cierto la EIPD se ha concebido como instrumento proactivo en la gestión segura de los datos personales en operaciones que habrán de realizarse, constituyéndose por tanto en el primero paso de las actividades de protección desde el diseño y por defecto, ello no significa que no se deba y pueda realizar en relación con aquellas operaciones que ya se encuentran en ejecución y que, previo el análisis de riesgo de las mismas, se identificado como objeto de la mencionada evaluación.