Superintendencia de Industria y Comercio

JIMÉNEZ DUARTE ASOCIADOS
Consultoría Legal y Tributaria

CIRCULAR EXTERNA No. 002 DE 2024
21 de agosto de 2024

Para: Sujetos vigilados por la Superintendencia de Industria y Comercio en su rol de Autoridad de Protección de Datos personales.

Asuntos: Lineamientos sobre el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial.

La Ley Estatutaria 1581 de 2012 estableció el régimen general de protección de Datos personales en la República de Colombia, concretizando el derecho fundamental al *Habeas Data*[1], con el propósito de establecer los lineamientos de protección del Tratamiento de Datos personales. La norma, por su parte, reconoce el derecho de los Titulares para proteger su información y el deber de los *Administradores de Datos personales*[2] en la recolección, almacenamiento, uso, circulación de la información para finalidades constitucionales en el marco del Estado Social de Derecho.

La Inteligencia Artificial (en adelante "IA") es una tecnología que tiene una dimensión tanto científica como social[3]. Su importancia está determinada por los profundos cambios sociales que produce, y en particular que para su funcionamiento se necesitan de grandes volúmenes de datos, y la mayoría de las veces de Datos personales. Así, el impacto de la IA en el derecho fundamental al *Habeas Data* es evidente.

Esta circular tiene como propósito proveer a los *Administradores de Datos personales* certidumbre sobre el Tratamiento de Datos personales para desarrollar, desplegar o usar sistemas de Inteligencia artificial ("Sistemas de IA"), y brindar a los Titulares seguridad sobre el uso de sus Datos personales en los Sistemas de IA, ya que típicamente se utilizan para tomar decisiones autónomas o para asistir a un tomador de decisiones humano a través de recomendaciones y predicciones.

---

[1] Artículo 15 de la Constitución Política de Colombia de 1991.
[2] Se entiende por *Administradores de Datos personales* a: los **Responsables del Tratamiento** (literal e) artículo 3 de la Ley Estatutaria 1581 de 2012), los **Encargados del Tratamiento** (literal d) artículo 3 de la Ley Estatutaria 1581 de 2012), las **Fuentes de información** (literal b) artículo 3 de la Ley Estatutaria 1266 de 2008), los **Operadores de información** (literal c) artículo 3 de la Ley Estatutaria 1266 de 2008) y a los **Usuarios** (literal d) artículo 3 de la Ley Estatutaria 1266 de 2008).
[3] SIERRA CADENA, Grenfieth de Jesus. Implementación de la Inteligencia Artificial en las Altas Cortes de Colombia: los casos de la Corte Constitucional y el Consejo de Estado. Revista Eurolatinoamericana de Derecho Administrativo, Santa Fe, vol. 11, n. 1, e253, ene./jul. 2024. DOI 10.14409/redoeda.v11i1.13824 "Un fenómeno científico y social que posee una doble naturaleza. Es considerada a la vez como un avance tecnológico-científico y un instrumento de transformaciones sociales. Tiene su origen en las ciencias de la computación, la informática y las matemáticas. Durante los últimos 30 años ha vivido cambios exponenciales, al punto de lograr que el desarrollo computacional se cada vez más potente, con mayor capacidad en procesamiento de datos, llegando a simular comportamientos humanos1. Como fenómeno social hace referencia a la llegada de aplicaciones, de plataformas, de redes sociales, de componentes tecnológicos que están modificando estructuralmente las relaciones humanas; determinando nuevas formas de sociedad y de gobierno."

El **CONPES** 3975[4] define la inteligencia artificial como "(...) *un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos*".

Los Estados miembros de la Organización para la Cooperación y Desarrollo Económico (**OCDE**) definieron en el 2023 un Sistema de Inteligencia Artificial como "*un sistema basado en máquinas que, con objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y adaptabilidad después de su implementación*"[5].

Las leyes estatutarias 1266 de 2008 y 1581 de 2012 son normas neutrales temática y tecnológicamente que se aplican a todo Tratamiento de Datos personales por parte de *Administradores de Datos personales*, incluyendo la recolección y/o Tratamiento de Datos personales para desarrollar, probar y monitorear Sistemas de Inteligencia Artificial o como parte de su proceso de implementación.

En ese orden de ideas, la normatividad sobre Tratamiento de Datos personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para tratar la información personal de los Titulares. Así las cosas, la ley colombiana permite el uso de tecnologías para tratar datos, pero, al mismo tiempo, exige que se haga de manera respetuosa de su ordenamiento jurídico.

En materia de Tratamiento de Datos personales impera como regla de responsabilidad el deber de responsabilidad demostrada o "*accountability*", el cual exige a los *Administradores de Datos personales* adoptar medidas útiles, oportunas, eficientes y demostrables para acreditar el total y correcto cumplimiento de la regulación. Lo anterior, se ve materializado en el artículo 19A de la Ley Estatutaria 1266 de 2008, que establece: "*Los operadores, fuentes y usuarios de información financiera, crediticia, comercial y de servicios* ***deben ser capaces de demostrar*** *que han implementado medidas apropiadas, efectivas y verificables para cumplir con las*

[4]Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional De Planeación. Documento CONPES 3975 POLÍTICA NACIONAL PARA LA TRANSFORMACIÓN DIGITAL E NTELIGENCIA ARTIFICIA

[5] Organización para la Cooperación y Desarrollo Económico (OCDE). EXPLANATORY MEMORANDUM ON THE PDATED OECD DEFINITION OF AN AI SYSTEM. Marzo 2024. https://www.oecd-ilibrary.org/docserver/623da898-en.pdf?expires=1723212626&id=id&accname=guest&checksum=E9A3D570869087CCF8A0A929BBE2B2FF

obligaciones establecidas en la Ley 1266 de 2008" (subrayado fuera de texto). Y, a su vez, en el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Decreto 1074 de 2015, al disponer que: "*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*". (Subrayado fuera de texto).

La privacidad desde el diseño y por defecto (*Privacy by Design and by Default*), es considerada una medida proactiva para, entre otras, cumplir con el Principio de Responsabilidad Demostrada. Al introducir la privacidad desde el diseño, se garantiza el debido Tratamiento de los datos utilizados en los proyectos informáticos que involucren Tratamiento de Datos personales.

Esto implica que en el momento de hacer analítica de datos para entrenar una maquina con inteligencia artificial se deberán aplicar técnicas matemáticas que impidan identificar a la persona que proporciona la información. Con esto se busca prevenir niveles de riesgo no aceptables, por su impacto al vulnerar el consentimiento de los Titulares en su derecho fundamental a la privacidad. Así, el debido Tratamiento de la información debe ser un componente esencial del diseño y puesta en marcha de proyectos de inteligencia artificial; lo cual implica la materialización del principio de seguridad previsto tanto en el literal f) del artículo 4 de la Ley Estatutaria 1266 de 2008, como en el literal g) del artículo 5 de la Ley Estatutaria 1581 de 2012, en tanto conlleva la adopción de medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Esta Superintendencia a través de la Delegatura para la Protección de Datos personales tiene entre las funciones asignadas por la Ley Estatutaria 1581 de 2012, las de "*velar por el cumplimiento de la legislación en materia de protección de Datos personales*" e "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley*"[6].

---

6 Literales a) y e) del artículo 21 de la Ley Estatutaria 1581 de 2012.

Además de lo anterior, en Sentencia C-1011 de 2008, la Corte Constitucional de Colombia revisando la constitucionalidad del proyecto correspondiente a la hoy Ley Estatutaria 1266 de 2008, se pronunció respecto de las funciones de esta Superintendencia que:

> *"Para cumplir con esta obligación de protección y garantía de los derechos del sujeto concernido, el legislador estatutario estableció en el artículo 17 que las Superintendencias de Industria y Comercio y Financiera ejercerán la función de vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto refiere a la administración de Datos personales regulada por la normatividad objeto de estudio.* ***Estas funciones de vigilancia consisten, entre otros aspectos, en impartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones previstas por la normatividad estatutaria, relacionadas con la administración de la mencionada información, para lo cual las Superintendencias fijarán los criterios que faciliten su cumplimiento y señalarán procedimientos para su cabal aplicación****."* (Destacado fuera de texto).

A su vez, mediante Sentencia C – 748 de 2011 (de constitucionalidad del proyecto correspondiente a la Ley Estatutaria 1582 de 2012) la Corporación se refirió a las facultades de esta autoridad establecidas en el artículo 21 del citado proyecto en los siguientes términos:

> *"Esta disposición enlista las funciones que ejercerá la nueva Delegatura de protección de Datos personales. Al estudiar las funciones a ella asignadas, encuentra esta Sala que todas corresponden y despliegan los estándares internacionales establecidos sobre la autoridad de vigilancia. En efecto, desarrollan las funciones de vigilancia del cumplimiento de la normativa, de investigación y sanción por su incumplimiento, de vigilancia de la transferencia internacional de datos y de promoción de la protección de datos.*
>
> *Además, debe afirmarse que, tal como lo estableció la Corte en la Sentencia C-1011 de 2008,* ***la naturaleza de las facultades atribuidas a la Superintendencia –a través de la Delegatura-, "caen dentro del ámbito de las funciones de policía administrativa que corresponden a esos órganos técnicos adscritos al ejecutivo*** *(Art. 115 C.P.), en tanto expresión de la potestad de dirección e intervención del Estado en la economía (Art.334), y de intervención reforzada del Gobierno en las actividades financiera, bursátiles y aseguradoras (Art. 335 C.P.)."* (Destacado fuera de texto).

Igualmente, el numeral 55 del artículo 1 del Decreto 4886 de 2011 (modificado por el Decreto 092 de 2022) señala que esta Superintendencia des competente para *"impartir instrucciones en materia de administración de Datos personales, fijar criterios que faciliten su cumplimiento y señalar los procedimientos para su cabal aplicación"*. Todo ello independientemente, de los sistemas informáticos en los cuales se estén tratando los Datos personales; tecnologías de la información y las comunicaciones.

A su vez, la Corte Constitucional en Sentencia T- 323 del 2024 reafirma la necesidad de cumplir lo establecido en la regulación sobre protección de Datos personales en el Tratamiento que se haga sobre aquellos por cualquier sistema de IA, en los siguientes términos:

> *"Ahora bien, en cuanto a la regulación del Tratamiento de datos en Colombia es importante destacar que las leyes estatutarias 1266 de 2008 y 1581 de 2012 fueron redactadas neutralmente, en el sentido que sus disposiciones aplican al Tratamiento de datos que se realice mediante cualquier herramienta manual o tecnológica. En este sentido, cualquier sistema de IA debe garantizar el cumplimiento de estas normatividades."*

En este sentido, esta Superintendencia, como Autoridad Nacional de Protección de Datos personales, instruye sobre el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial en los siguientes términos:

I. El Tratamiento de Datos personales en la IA presupone la necesidad de realizar una ponderación atendiendo cuatro criterios, destinados a salvaguardar los principios establecidos en las Leyes Estatutarias 1266 de 2008 y 1581 de 2012:
   a. Idoneidad: El Tratamiento es capaz de alcanzar el objetivo propuesto;
   b. Necesidad: No exista otra medida más moderada en cuanto al impacto de las operaciones de Tratamiento en la protección de Datos personales e igual de eficaz para conseguir tal objetivo;
   c. Razonabilidad: El Tratamiento debe estar orientado a cumplir finalidades constitucionales;
   d. Proporcionalidad en sentido estricto: Las ventajas obtenidas como consecuencia de la restricción del derecho a la protección de datos no deberán ser superadas por las desventajas de afectar el derecho al *Habeas Data.*

II. En caso de presentarse falta de certeza frente a los potenciales daños que puede causar el Tratamiento de Datos personales, y con miras a evitar que se cause un daño grave e irreversible, los *Administradores de Datos personales* deberán abstenerse de

realizar dicho Tratamiento o adoptar medidas precautorias o preventivas para proteger los derechos del Titular del dato, su dignidad y otros derechos humanos.

III. La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos esenciales del principio de responsabilidad demostrada[7]. Así, en el Tratamiento de Datos personales en la IA se requiere que los *Administradores de Datos personales* adecúen, entre otros, sistemas de administración de riesgos asociados al Tratamiento de aquella información. Lo anterior, con el objetivo de identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo que están expuestos en desarrollo del cumplimiento de las normas de protección de Datos personales.

IV. Previo al diseño y desarrollo de la IA, y en la medida en que sea probable que los productos realizados a través de dichas técnicas entrañen un alto riesgo de afectación a los Titulares de la información, será necesario efectuar y documentar un estudio de impacto de privacidad. Aquel, como mínimo, deberá contener lo siguiente:

   a. Una descripción detallada de las operaciones de Tratamiento de Datos personales.
   b. Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los Datos personales. En la evaluación de riesgos se espera, por lo menos, la identificación y clasificación estos.
   c. Las medidas previstas para evitar la materialización de los riesgos, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de Datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas que puedan eventualmente resultar afectadas.

V. Los Datos personales sujetos a Tratamiento en la IA deben ser veraces, completos, exactos, actualizados, comprobables y comprensibles. De esta manera, se prohíbe por el ordenamiento jurídico[8] el Tratamiento de Datos personales parciales, incompletos, fraccionados o que induzcan a error.

VI. Una manera para dar cumplimiento a la *privacidad desde el diseño y por defecto* por medio de técnicas matemáticas es la privacidad diferencial[9].

---

[7] Los riesgos asociados al Tratamiento de Datos personales en la IA deben estar sujetos a planificación y esfuerzos de mitigación proporcionales a la gravedad de los eventuales daños que se pueden generar. Entre las contingencias para tener en cuenta deben estar las inherentes a la operación de los algoritmos (sesgos humanos, fallas técnicas, vulnerabilidades de seguridad, fallas en la implementación), y a su diseño.

[8] Literal d) del Artículo 4 de la Ley Estatutaria 1581 de 2012.

[9] En palabras de la profesora de la Facultad de Matemáticas de la Universidad de los Andes, Valérie Gauthier "*La privacidad diferencial es un conjunto de técnicas matemáticas que permiten hacer analítica sobre datos sin revelar información de las personas que proporcionaron esos datos. En este caso se confía en una entidad central que tiene los datos, y responde preguntas sobre los datos de tal manera que no se pueda revelar información de los individuos en particular, aun cuando se combine con otro conjunto de datos.*

VII. En el Tratamiento de Datos personales en la IA debe garantizarse el derecho de los Titulares de la información a obtener de los *Administradores de Datos personales*, en cualquier momento y sin restricciones, información acerca del Tratamiento de sus Datos personales[10].

VIII. Para cumplir el principio de seguridad, en el desarrollo y despliegue de la IA, se requiere adoptar medidas tecnológicas[11], humanas, administrativas, físicas, contractuales y de cualquier otra índole para evitar:

a. El acceso indebido o no autorizado a los Datos personales.
b. La manipulación de la información.
c. La destrucción de la información.
d. El uso indebido o no autorizado de la información.
e. Circular o suministrar la información a personas no autorizadas.

Las medidas de seguridad implementadas deben ser auditables por las autoridades para su evaluación y mejoras permanentes.

IX. La información personal que es "*accesible al público*" no es, per se, información "*de naturaleza pública*"[12]. El hecho de que estén disponibles en internet no significa que cualquier persona puede tratarlos sin autorización previa, expresa e informada del Titular del Dato[13]. De esta manera, los *Administradores de Datos personales* que recolecten Datos personales privados, semiprivados o sensibles en internet no están legitimados para apropiarse de dicha información y tratarla para cualquier finalidad que consideren apropiado sin la autorización previa, expresa e informada del Titular de la información.

X. El Tratamiento de Datos personales que se realice en sistemas de IA debe prever estrategias pertinentes, eficientes y demostrables para garantizar el cumplimiento de

---

La privacidad diferencial local, tiene un mismo propósito, pero no necesita una entidad central de confianza. Cada individuo va a añadir un ruido a sus datos de tal manera que nadie conozca el valor real de sus datos, pero que no afecte la analítica de los datos globalmente.

Para ambos métodos hay que tener un presupuesto de privacidad, de tal manera que permita tener analítica de datos muy aproximados a los reales sin perder la privacidad de las personas. Ese presupuesto puede depender de la sensibilidad y del valor de los datos en cuestión".

Para más información sobre la privacidad diferencial:
Dwork, C & Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. Theoretical Computer Science. https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf
Wang, T & Jha, S. (2017). Locally Differentially Private Protocols for Frequency Estimation. USENIX Security Symposium. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-wang-tianhao.pdf

[10] Literal e) del Artículo 4 de la Ley Estatutaria 1581 de 2012.
[11] Literal g) del Artículo 4 de la Ley Estatutaria 1581 de 2012.
[12] El numeral 2 del artículo 3 del Decreto 1377 de 2013 (incorporado en el Decreto Único Reglamentario 1074 de 2015) establece que un Dato Público es "(...) *el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva*".
[13] Resolución No. 71406 del 15 de noviembre de 2023. Por la cual se imparten unas ordenes administrativas a LinkedIn.

los derechos de los Titulares de la información establecidos en las leyes estatutarias 1266 de 2008 y 1581 de 2012 y sus decretos reglamentarios[14].

Así, en armonía con las normas citadas y la jurisprudencia constitucional, el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial requiere la debida observancia de lo establecido en materia de protección de Datos personales. La ley colombiana permite el uso de tecnologías para tratar datos, pero, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico. Quienes crean, diseñan o usan "*innovaciones tecnológicas*" deben cumplir todas las normas sobre Tratamiento de Datos personales recolectados y/o tratados en Colombia.

De esa manera, estas instrucciones armonizan las anteriores normas para garantizar el fin constitucional de una efectiva protección del derecho al *Habeas Data* y el debido Tratamiento de Datos personales.

Cordialmente,

CIELO ELAINNE RUSINQUE URREGO
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Elaboró: Grenfieth Sierra/ Alejandro Londoño
Revisó: Héctor Barragán// Grenfieth Sierra
Aprobó: Grenfieth Sierra /Gabriel Turbay

[14] Téngase presente: Decreto 2952 de 2010 (incorporado en el Decreto único Reglamentario 1074 de 2015), Decreto 1377 de 2013 (incorporado en el Decreto único Reglamentario 1074 de 2015) y el Decreto 255 de 2022.