El futuro es de todos

DNP
Departamento Nacional de Planeación

Guía normativa aplicable a la explotación de datos

JUNIO DE 2020

Guía normativa aplicable a la explotación de datos

Documento final

Luis Alberto Rodríguez
Director General

Daniel Gómez Gaviria
Subdirector General Sectorial

Amparo García Montaña
Subdirector General Territorial

Diana Patricia Ríos García
Secretaria General

Iván Mauricio Durán Pabón
Directora de Desarrollo Digital

Viviana Vanegas Barrero
Subdirectora de Prospectiva Digital

Grupo de Comunicaciones
y Relaciones Públicas

Luis Segundo Gamez Daza
Coordinador

Calle 26 13-19 Bogotá, D. C.
PBX: 3815000
Junio de 2020

Este estudio ha contado con el apoyo de los asesores

Oscar Eduardo Salazar

Diana Paola Ramírez

Aportes técnicos externos:

Ministerio de las Tecnologías de la Información y las Comunicaciones

Superintendencia de Industria y Comercio

DOCUMENTO VERSIÓN FINAL: Guía normativa aplicable a la explotación de datos

Contenido

Introducción

En el marco de la Política Nacional de Explotación de datos CONPES 3920, el desarrollo de políticas públicas y marcos normativos que se adapten a los avances tecnológicos y que respondan de manera pertinente a los requerimientos de la sociedad de la información, se convierte en una necesidad para el aprovechamiento de datos. Los cuales generan beneficios para las entidades públicas en términos de transparencia, mejoras en la toma de decisiones, y en el diseño y focalización de programas y políticas públicas.

Una de las barreras que se identificó en el CONPES 3920 fue la incertidumbre que perciben las entidades públicas frente al marco normativo aplicable a la explotación de datos por dos razones. La primera asociada a la dispersión y desconocimiento del marco normativo y la segunda relacionada con la gestión de los posibles riesgos que acarrea la explotación de los datos, por ejemplo, la protección de datos personales. Algunos de los retos que se identifican en el CONPES frente al marco normativo, están relacionados con la captura de datos por parte de las entidades, el intercambio de la información para la prestación de servicios ciudadanos, la baja digitalización, la gestión documental y la publicación de la información.

En Colombia, el marco normativo asociado a la explotación de datos ha surgido con diferentes objetivos y alcances que no están directamente relacionados con el aprovechamiento del Big Data. Sin embargo, es importante reconocer que existen leyes, decretos y normativas que habilitan y respaldan la explotación de datos para la generación de valor social y económico. Por tal motivo, esta guía tiene la finalidad de presentar el marco normativo que existe en Colombia aplicable a la explotación de datos, con el propósito de orientar a las entidades para que generen procesos de explotación de datos de forma responsable y en el cumplimiento de lo estipulado por la normatividad colombiana.

El primer capítulo de esta guía tiene dos secciones: La primera tiene un recuento general de la explotación de datos y Big Data, y la segunda se describe el marco jurídico aplicable en Colombia al ciclo de vida de los datos. En el tercer capítulo se listan recomendaciones generales para las entidades en materia de protección de datos personales. En los anexos se encuentran algunas definiciones que aportan a la comprensión de las normas en materia de protección de datos y acceso a la información pública, y se hace un recuento del marco normativo en Colombia aplicable a la explotación de los datos.

1 Contexto general - Explotación de datos y Big Data

El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) y el aumento de la cobertura a Internet ha facilitado que, en los últimos años, se generen datos de manera exponencial y en diversas fuentes de información. El volumen, la velocidad y la variedad de los datos generados en este contexto inicialmente fue un reto tecnológico, pero con la aparición de nuevas técnicas y formas de almacenamiento, procesamiento, análisis y visualización se crearon las condiciones para aprovechar su potencial. Por medio de la datificación, las elecciones de consumo, las preferencias individuales y colectivos y los aspectos de la vida diaria se han transformado en datos. El reto actual para los distintos gobiernos y organizaciones privadas consiste en reducir las barreras de tipo técnico, jurídico y organizacional que disminuyen el aprovechamiento de los datos para generar valor social y económico.

En ese contexto, los datos se han convertido en uno de los activos más importantes para el sector público en la medida en que aportan beneficios para tomar decisiones informadas. La adecuada gestión de los datos a lo largo de todo su ciclo de vida, desde su recopilación o generación, clasificación, almacenamiento, uso, compartición y reutilización conllevan a extraer el valor de éstos para crear análisis descriptivo, predictivo, o prescriptivo que permitan diseñar nuevas estrategias, analizar con un enfoque más amplio problemáticas de carácter público y tomar decisiones. En el contexto actual, uno de los habilitadores para la transformación digital, es la explotación de los datos para aumentar el valor público de las entidades, de cara a la prestación de bienes y servicios para los ciudadanos.

En el sector público, la explotación de datos suele referirse al uso de fuentes de datos no tradicionales y a las innovaciones en materia de datos para que las soluciones gubernamentales tengan más capacidad de respuesta y sean más eficaces. Las entidades públicas tienen la oportunidad de aprovechar soluciones basadas en el Big Data para mejorar su productividad y reducir costos administrativos. Hoy el manejo de grandes bases de datos es una cuestión apremiante, especialmente en un momento en que muchos están preocupados por el papel de la información en las decisiones políticas. En el contexto actual, las entidades gubernamentales tienen que actuar como productoras, consumidoras y facilitadoras del Big Data (World Bank Group, 2017).

En el sector público la explotación y analítica de datos puede generar valor de diversas maneras:

- El manejo de grandes bases de datos aporta en los procesos de formulación de políticas públicas; permite la construcción de nuevos indicadores en tiempo real y proporciona información sobre los posibles beneficiarios de una política pública. Todo esto, permite tomar decisiones políticas mejor informadas y establecer políticas personalizadas y precisas.
- Puede ser utilizado para evaluar y mejorar los servicios públicos existentes o para crear nuevos servicios. La explotación de datos y Big Data ayuda a procesar la gran cantidad de información que manejan las entidades públicas, facilitando la detección de irregularidades en las operaciones gubernamentales.
- Permite a las entidades públicas involucrar a los usuarios en el diseño de servicios públicos y en la formulación de políticas. Una mejor interacción entre el gobierno y los ciudadanos promueve el compromiso ciudadano.

¿Qué es la explotación de datos y Big data?

El Big Data es un fenómeno que se caracteriza por la generación de grandes volúmenes de datos, en diversas fuentes de información y a una rápida velocidad en su generación. Es un sistema sociotécnico para la explotación masiva de datos que requiere en las entidades públicas, la disponibilidad de recursos tecnológicos para enfrentar los retos de procesamiento, el diseño y ejecución de procesos que permitan la replicabilidad y la sistematización de la explotación de datos y el recurso humano para ejecutar estos procesos.

Por su parte, la explotación de datos es el proceso mediante el cual se analizan datos de diversas fuentes de información y en distintos tipos de formato para descubrir patrones y relaciones entre los datos, lo que permite extraer el valor de los datos para brindar una solución a una problemática específica.

Una adecuada explotación de datos requiere considerar su ciclo de vida. En este se visibiliza el paso a paso para su tratamiento, y facilita la definición de técnicas para gestionar el volumen con el que se generan y capturan los datos, la diversidad de las fuentes de información y la velocidad con que se gestionan. El ciclo de vida de los datos también debe incorporar el análisis de aspectos legales relacionados con la creación o captura de datos, almacenamiento, transferencia, uso y explotación, y conservación.

Una de las bases para garantizar una adecuada gestión táctica y operativa del ciclo de vida de los datos en toda la entidad, es la definición e implementación de marcos de gobernanza

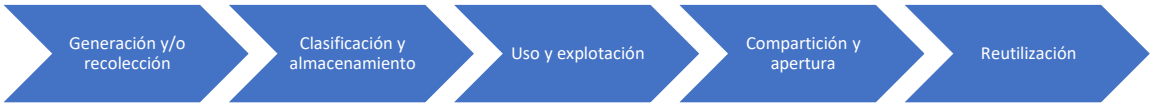
de los datos, que permitan establecer los lineamientos políticos y normativos. Es necesario que las disposiciones que adopten las entidades en materia de explotación de datos estén respaldadas por la normatividad vigente en Colombia en relación con la protección de datos personales, la transparencia y el acceso a la información pública, y el intercambio de información entre entidades públicas, ciudadanos y sector privado.

Una gobernanza de datos implementada de manera efectiva facilita el cumplimiento de la normatividad vigente en Colombia, en la medida en que se identifican roles y responsables para acceder a los datos, se clasifican, organizan y documentan los datos, se definen de manera clara mecanismos de acceso para su uso y compartición y se gestionan los riesgos relacionados con la confidencialidad y protección de la información.

2 Marco Jurídico aplicable al ciclo de vida de los datos

Para conocer el marco normativo asociado a la explotación de datos es importante definir como está constituido el ciclo de vida de los datos. Lo anterior, con la finalidad de relacionar los lineamientos jurídicos con la extracción de valor de los datos.

Figura 1. Ciclo de vida de los datos



Fuente: Elaboración propia DNP/DDD

A continuación, se hace una descripción de los procesos asociados a cada una de las fases del ciclo de vida de los datos y, adicionalmente, se relacionan con el marco normativo vigente en Colombia (ver anexo 1). En el marco jurídico se encuentran lineamientos normativos transversales a todo el ciclo de vida, por ejemplo, lo que respecta a la protección de los datos personales que se debe aplicar desde el momento de la recolección hasta la compartición y reutilización de los datos.

2.1 Generación y/o recolección

Los procesos de recolección de datos se llevan a cabo a través de cualquier operación o acto administrativo que vincule a la entidad con los ciudadanos y/o los usuarios. La recolección de datos hace parte del tratamiento de datos, y se origina cuando un ciudadano inicia un trámite administrativo, a través de una solicitud para adquirir un derecho o cumplir con una obligación, y finalizan cuando la entidad pública resuelve la solicitud, ya sea aceptándola o

denegándola. Por tanto, los datos obtenidos reúnen información de los ciudadanos del proceso asociado al trámite y de su conclusión.

En el proceso de recolección es importante que la entidad identifique de manera previa la finalidad de la recolección de los datos y qué canales y mecanismos implementa para su recolección. Adicionalmente a las actividades operativas, los datos pueden crearse a través de aplicaciones tecnológicas, dispositivos electrónicos conectados a Internet, entre otras.

El proceso de recolección implica que los datos no estén tratados, por lo cual la entidad debe generar los mecanismos esenciales para cumplir los lineamientos de protección de datos personales y, a su vez, debe garantizar que sean útiles para sus propósitos. Por tal razón, los principios asociados a la protección de los datos personales, que se encuentra en el marco normativo nacional (Ver anexo: Ley 1581 de 2012), deben ser tenidos en cuenta desde el primer momento. En esta fase de recolección es importante tener en cuenta que las personas son dueñas y titulares de sus propios datos y se deben garantizar todas las técnicas de anonimización y de seguridad de la información para reducir la posibilidad de reidentificación de las personas y el acceso a la información por parte de terceros no autorizados.

El marco jurídico en Colombia relacionado con la recolección y generación de datos se enmarca en las normativas y decretos referenciados en el siguiente recuadro:

- **Constitución Política de Colombia 1991**: Articulo 15 mediante el cual se establece el derecho que tienen las personas a conocer, actualizar y ratificar la información personal
- **Ley 1266 de 2008**: Por medio de la cual se dictan las disposiciones generales de habeas data
- **Ley 1273 de 2009**: Modifica el código penal y crea como bien jurídico tutelado la protección de la información y de los datos
- **Ley 1581 de 2012**: Principios y disposiciones que definen los derechos sobre los datos personales. Art 9. Exigencia de consentimiento previo del uso de datos personales
- **Decreto 1377 de 2012**: Reglamento aspectos relacionados con la titularidad del uso de la información para el tratamiento de sus datos personales.

Frente a la aplicabilidad y alcance de la Ley 1581 de 2012 en el marco de la explotación de datos y Big Data, es importante tener presente la circular N° 4 de 2019 expedida por la SIC, en el que se menciona que la Ley 1581 de 2012 aplica a todo tipo de tratamiento y está al margen de las tecnologías o herramientas actuales y futuras que se utilicen para el tratamiento

de datos personales. Así mismo, esta circular menciona que los derechos de las personas frente al tratamiento de datos de carácter personal están protegidos por principios transversales que tienen que ser cumplidos en cualquier actividad que involucre tratamiento de datos y aplicable a cualquier tipo de tecnología. Así mismo, en la Resolución 38281 de 2020, en donde se establece que: *"La Ley Estatutaria 1581 de 2012 es neutral tecnológica y temáticamente. Ello significa que aplica a cualquier Tratamiento con independencia de las técnicas, procesos o tecnologías – actuales o futuras- que se utilicen para dicho efecto. Por ende, debe observarse en la recolección, uso y Tratamiento de datos personales para diversos fines (marketing, políticos, cobro de cartera, etc) mediante el uso de técnicas o herramientas como "marcadores predictivos", "robocalls", "nuisance calls" e inteligencia artificial (IA).".*

Con el fin de conocer qué tipo de datos está recolectando la entidad, es necesario que se tenga conocimiento frente a la tipología de los datos definido en la Ley 1266 de 2008, donde se definen los datos personales, públicos, semiprivados y privados y la Ley 1581 de 2012 donde se clasifican los datos privados de acuerdo con su definición. Con base en la clasificación y tipología de los datos, la entidad podrá incorporar de manera más efectiva y precisa los procesos de almacenamiento, uso y compartición de los datos.

La entidad pública en el marco de sus funciones y fines administrativos propios tiene el derecho de acceder a información de las personas siempre y cuando esta sea usada para realizar el ejercicio de sus funciones (Artículo 5 de la Ley 1266 de 2008). Sin embargo, es importante que la entidad incorpore en la recolección de datos, el aviso de privacidad donde se defina el principio de finalidad, con el fin de exponer con qué objetivo se recolectan los datos y cuál va a ser el propósito de almacenarlos y usarlos. Así mismo, tiene la obligación de presentar los derechos que tienen las personas como titulares de sus propios datos de acuerdo con lo estipulado en la Ley 1581 de 2012 y el mecanismo para acceder a la política de tratamiento de datos personales.

Otro de los aspectos más importantes de la Ley 1581 de 2012 es la definición de principios para el tratamiento de datos personales como el de confidencialidad, legalidad, libertad, calidad, veracidad, seguridad, acceso y circulación restringida. La Ley también establece el principio de responsabilidad demostrada en el cual, la entidad responsable del tratamiento de los datos personales debe tener la capacidad de evidenciar la gestión de los datos personales que ha recolectado, la aplicación de técnicas de protección de datos y la implementación de políticas que le permitan a la entidad dar cumplimiento con los principios

establecidos en la normatividad. Frente a este tema en específico, es importante mencionar que la Superintendencia de Industria y Comercio es la entidad encargada de velar por la protección de los datos personales, razón por la cual ha elaborado guías de lineamientos técnicos como, la Guía de implementación del Principio de responsabilidad demostrada , entre otras, que permite a las entidades públicas ampliar su conocimiento sobre el marco normativo aplicable a la protección de datos y adoptar lineamientos y técnicas para su cumplimiento.

2.2 Clasificación y almacenamiento

La cantidad de datos que las entidades públicas recolectan y/o generan requieren la implementación de una adecuada gestión de la información para asegurar la protección, almacenamiento y acceso de los datos. Para ello es importante que las entidades públicas consideren el diseño e implementación de una arquitectura de almacenamiento de datos, que respalde la confidencialidad, integridad y disponibilidad de éstos.

El almacenamiento de los datos se refiere al proceso mediante el cual la entidad pública guarda y archiva los datos que recopila o genera. Para ello la entidad debe establecer una arquitectura de almacenamiento mediante la cual se define la infraestructura tecnológica y los protocolos necesarios para almacenar, organizar y acceder a los datos.

El primer paso para el almacenamiento de los datos consiste en hacer un inventario de los activos de datos en la entidad, tanto internos como externos, y posteriormente hacer la clasificación de éstos de acuerdo con su tipología. Para la clasificación es importante conocer de antemano el marco normativo que define la tipología de los datos y las condiciones para su tratamiento, dado que, con base en su clasificación, se define su tratamiento, la ubicación de almacenamiento y el control de acceso. Como se mencionó anteriormente, los datos que son de carácter personal y afectan en mayor medida la privacidad de las personas están sujetos a la Ley 1581 de 2012 y su nivel de protección es mucho más alto, razón por la cual las entidades públicas deben implementar técnicas de anonimización de los datos personales para evitar los riesgos de reidentificación.

Una vez clasificados los datos, se define la infraestructura o tipo de almacenamiento que se va a adoptar para almacenar la información de manera más adecuada. Existen principalmente dos tipos de almacenamiento de datos que son el local y el almacenamiento en la nube. En el almacenamiento local los datos se preservan en un medio físico que usualmente se caracteriza por ser un disco duro, dispositivos móviles o en tarjetas de memoria. El otro tipo de almacenamiento es en la nube donde la información está almacenada en proveedores

externos que deben cumplir con los mismos criterios de seguridad de la información. La arquitectura de almacenamiento de datos debe incorporar protocolos y técnicas de gestión de la información frente a pérdidas, fugas y recuperación de los datos. Además de garantizar la infraestructura para el almacenamiento de los datos y las políticas para salvaguardar la seguridad de la información, se deben crear los mecanismos que permitan la disponibilidad de los datos de acuerdo con las necesidades de los usuarios.

Otro de los aspectos que incorporan la arquitectura de almacenamiento de datos es el que tiene que ver con su gestión y su conservación. En este punto es muy importante considerar que en el marco de la explotación de datos y el Big Data, los documentos físicos se convierten en una fuente de información de importante valor, dado que es posible implementar técnicas para el aprovechamiento de documentos o archivos que anteriormente eran difícil de analizar. Por tal motivo, frente a la conservación de los archivos documentales, es importante que las entidades gestionen los documentos que han elaborado o recopilado con anterioridad los cuales precisan trazabilidad de la información. Entre estos ejemplos se encuentran las historias médicas, documentos legales, entre otros.

Respecto al tratamiento, clasificación y almacenamiento de documentos, el marco normativo instaura la Ley 594 de 2000 que tiene por objeto establecer las reglas y principios generales que regulan las funciones archivísticas del Estado. Para ello se establece que la información debe ser presentada de tal forma que se garantice como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. La Ley establece los principios que rigen la función archivística, de los cuales es importante destacar el principio de los fines de archivos, el de importancia de los archivos, el de institucionalidad e instrumentalidad, el de responsabilidad, el de administración y acceso y el de manejo y aprovechamiento de los archivos.

Los principios definidos en la ley no solo identifican la importancia de los archivos, sino que también definen las responsabilidades sobre el manejo de los archivos y la conformación de bancos de información. Al igual que en la sección anterior, los principios establecidos en la Ley 594 corresponden con el artículo 15 de la Constitución (Alshboul, Wang, & Nepali, 2015).

En el marco de la digitalización de las entidades públicas, en el Acuerdo 27 de 2006, el Archivo General de la Nación definió la digitalización como la técnica mediante la cual la información análoga (como papeles, videos, cintas de reproducción) es transformada para ser leída a través de un dispositivo digital con el fin de facilitar la gestión, consulta y respaldo de la

información. Y en el año 2012 se publicó la Circular externa AGN No.005 mediante la cual se dan las recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas en el marco de la iniciativa cero papel y se establecen los principios o elementos para adelantar un proyecto de digitalización en las entidades públicas, en el marco de la eficiencia.

2.3 Uso y explotación de los datos

Esta etapa incluye las actividades que se realizan para depurar, consolidar, integrar, visualizar, analizar los datos y generar valor agregado a partir de estos. Esta etapa tiene en consideración la identificación y análisis de las fuentes de información de donde provienen lo datos, la implementación de técnicas para evaluar la calidad de los datos, verificando el estado de completitud, disponibilidad y actualización. Posteriormente se incorporan técnicas de depuración y validación para tener datos óptimos para el análisis, se agregan y posteriormente se implementan técnicas de analítica descriptivas, predictivas o prescriptivas, con el fin de obtener resultados que permitan extraer el valor de los datos para tomar decisiones.

Las actividades que incluyen la explotación de datos deben estar respaldadas por la protección de datos personales, en caso de tratar información que vulnere la privacidad de las personas. En este punto, es preciso una vez más, que la entidad pública tenga en cuenta las consideraciones relacionadas con la Ley 1581 de 2012. A nivel de técnicas para el tratamiento de datos personales, es relevante tener en consideración las técnicas de anonimización de datos personales, los análisis de evaluación del riesgo del tratamiento de datos, y la evaluación de la utilidad de los datos una vez se han aplicado técnicas de anonimización. Por otra parte, es preciso efectuar una evaluación de impacto de la privacidad para garantizar que los datos se estén tratando conforme a la regulación existente.

Los procesos de uso sobre los datos pueden traer grandes beneficios para la entidad en términos de mejorar la toma de decisiones, aumentar la transparencia, a través de la generación de datos que contribuyan a la participación ciudadana y a facilitar procesos de auditoria tanto interna como externa sustentados en la información que genera y recolecta la entidad; mejorar el seguimiento de la población objetivo para focalizar acciones, el análisis de datos permite mejorar los procesos de caracterización de la población objetivo de la entidad, lo que promueve acciones que generen impacto positivo; aumentar innovación de las actividades de la entidad, a través de la generación de nuevos servicios o productos. (McKinsey Global Institute, 2011)

2.4 Compartición y apertura de datos

En esta etapa los datos se hacen accesibles a otros usuarios externos para su consulta, uso y reutilización. Una vez los datos son tratados y se ponen a disposición de los interesados a nivel interno de las entidades que los recaban, es necesario ponerlos a disposición de cualquier interesado con un interés legítimo, para ello, la Ley 1712 de 2014 señala a qué título los datos son de índole pública. En esta Ley es importante resaltar el principio de máxima publicidad que define que toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley. Los datos deben ser compartidos de tal manera que se cumplan los preceptos que faciliten la interoperabilidad y el intercambio, así como su apertura y anonimización cuando sea requerida, en concordancia con las normas que rigen la materia. La Ley 1712 cita las excepciones del acceso a la información pública entre las que se encuentra:

1. Defensa y seguridad nacional.
2. Seguridad pública.
3. Relaciones internacionales.
4. Prevención, investigación y persecución de delitos y faltas disciplinarias.
5. El debido proceso y la igualdad de las partes en los procesos judiciales.
6. La administración efectiva de la justicia.
7. Los derechos de la infancia y adolescencia.
8. La estabilidad macroeconómica y financiera del país.
9. La salud pública

La compartición y apertura de los datos requiere que la entidad identifique los modelos de compartición que va a aplicar de acuerdo con su rol como entidad pública. Para ello debe considerar los modelos Government to Government (G2G), Government to Citizens (GTC) o Government to Business. Así, la entidad pública podrá reconocer si la compartición de los datos será a través de datos abiertos o intercambios de colaboración entre entidades públicas o con empresas del sector privado.

Como primer paso para la compartición y apertura de datos es necesario identificar cuales conjuntos de datos se van a compartir con externos y el mecanismo para hacerlo sea a través de API, portal de datos, entre otros. Identificar también el formato en el que serán compartidos los datos, el objetivo que establece la entidad frente a la compartición de los datos con terceros y los mecanismos de actualización de los conjuntos de datos y metadatos.

Los datos de carácter público deben estar disponibles para la consulta de la ciudadanía con el fin de que las personas puedan conocer la información de las entidades públicas y hacer uso y aprovechamiento de esos datos para el desarrollo de investigaciones, estudios o análisis. En Colombia, la Ley 1712 de 2014 señala que el acceso a la información pública tiene el propósito de aumentar la participación ciudadana, y garantizar la transparencia de la gestión pública.

En este marco, es muy importante que las entidades públicas tengan claridad de la gestión de los datos abiertos. Estos facilitan que los datos puedan ser reutilizados por otros actores, que sean de fácil acceso, y sin restricciones para su uso. La Ley 1712 de 2014 define los datos abiertos como los datos que se encuentran en formatos estándar e interoperables disponibles para su acceso y reutilización y son custodia de las entidades públicas o privadas que cumplen con funciones públicas. La finalidad de los datos abiertos es que estos puedan ser utilizados sin ninguna restricción por los usuarios, y que no requieran de procedimientos innecesarios para la compartición de los datos.

En este punto, es importante que la entidad pública tenga en cuenta una vez más, la clasificación de los datos que realizó con anterioridad con el fin de nutrir el Índice de Información Clasificada y Reservada en el que la entidad establece que información es de carácter personal, de defensa, seguridad o estabilidad de la nación. Así mismo, es importante que la entidad tenga claridad que los datos personales no son excluyentes de ser datos abiertos, en la medida en que estos pueden ser tratados para ser anonimizados y minimizar al máximo el riesgo de reidentificación. En este punto se recomienda ver la Guía de apertura de datos abiertos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2016). https://herramientas.datos.gov.co/sites/default/files/Guia de Datos Abiertos de Colombia.pdf

Frente a la publicación de datos abiertos para su reutilización, es importante que la entidad pública promueva su uso tanto al interior como al exterior de su entidad, mantenga actualizados los datos y gestione procedimientos técnicos para corroborar la calidad de la información.

Intercambio de información entre entidades del Estado Colombiano

En el artículo 147 de la Ley 1955 de 2019 por medio de la cual se expide el Plan Nacional de Desarrollo 2018-2022, el Gobierno Nacional incorporó el principio de plena interoperabilidad entre los sistemas de información públicos para garantizar el suministro e intercambio de la información, como base de la transformación digital del Estado. Así, todas las entidades

públicas deben adoptar en sus planes de acción, el componente de transformación digital y el principio de plena interoperabilidad. Lo cual contribuye a su vez con la eficiencia de la función administrativa conforme lo establecido en artículo 209 de la Constitución Política de Colombia.

En relación con la simplificación del intercambio de información entre entidades públicas, es importante mencionar la Directiva No.7 de 2019-Presidencia de la República de Colombia, por medio de la cual se dan facultades extraordinarias para simplificar, suprimir o reformar trámites, procedimientos innecesarios en la Administración pública. Esta directiva es muy relevante, dado que una de las barreras que se identifica para el intercambio de información entre las entidades públicas son los trámites administrativos que regularmente emplean las entidades públicas como mecanismo de compartición de datos.

Frente al principio de interoperabilidad y la recepción de información de datos personales por parte de las entidades públicas, es importante que estas consideren lo estipulado por la Superintendencia de Industria y Comercio, en la circular No.4 de 2019, en la cual se menciona que: El artículo 10 y 13 de la Ley 1581 de 2012 establece que las entidades públicas pueden recopilar datos personales en el marco del cumplimiento de sus funciones administrativas por lo cual no requiere una autorización especial para suministrar los datos a entidades en el marco de proyectos de interoperabilidad, y que cualquier operación de interoperabilidad debe realizarse de acuerdo con lo establecido en la Ley 1581 de 2012 y en el artículo 15 de la Constitución.

En el marco de interoperabilidad del Estado Colombiano, el Ministerio de las TIC elaboró el Marco de Interoperabilidad de los servicios ciudadanos digitales para facilitar el intercambio de datos de las entidades públicas con el fin de mejorar la prestación de servicios ciudadanos digitales (MinTIC, 2019). De acuerdo con lo establecido en el Decreto 620 de 2020, para enfocar la compartición de datos para el uso y operación de servicios ciudadanos digitales, se define:

Marco de interoperabilidad:

Es la estructura de trabajo común donde se alinean los conceptos y criterios que guían el intercambio de información. Define el conjunto de principios. recomendaciones y directrices que orientan los esfuerzos políticos, legales, organizacionales, semánticos y técnicos de las entidades, con el fin de facilitar el intercambio seguro y eficiente de información.

El marco de interoperabilidad de los servicios ciudadanos digitales del citado decreto establece los principios definidos en la Tabla 1 (Ver: Marco de Interoperabilidad para Gobierno Digital) (MinTIC, 2019):

Tabla 1. Principios del Marco de interoperabilidad de servicios ciudadanos digitales

Cobertura y proporcionalidad	La interoperabilidad deberá ser aplicada en cualquier tipo de entidad del orden nacional, departamental o municipal. También deberá ser utilizado por parte de organizaciones privadas cuando interactúen con el Estado. Así mismo, cada entidad deberá vincular los servicios de intercambio de información a los Servicios Ciudadanos Digitales mediante el servicio de interoperabilidad y su integración a la plataforma de Interoperabilidad.
Seguridad, protección y preservación de la Información	Deberán aplicarse medidas y controles que aseguren, protejan, preserven y mantengan la privacidad de la información susceptible de interoperar generando un entorno seguro y de confianza que permita transmitir a los ciudadanos un ambiente de seguridad, donde se vela por sus intereses y se cuida la privacidad de la información y se respeta plenamente la normativa aplicable cada vez que interactúan con el Estado.
Colaboración y participación	Las entidades en atención a los dispuesto en la Ley 489 de 1998, deberán estimular y participar de los esquemas de interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente.
Simplicidad	Las entidades públicas deberían racionalizar y simplificar sus trámites, servicios y otros procedimientos administrativos mediante la optimización de los mismos, evitando exigir documentos, certificaciones, constancias u otros actos administrativos que pueden ser verificados, compartidos o intercambiados a través de los servicios de intercambio de información.

Neutralidad tecnológica y adaptabilidad	El desarrollo de servicios de intercambio de información se deberá orientar en la atención de las necesidades manifiestas de los ciudadanos y empresas; por lo tanto, la construcción de estos servicios deberá orientarse por la funcionalidad y no por la tecnología que ofrezca una herramienta o proveedor en particular.
Reutilización	Reutilizar se interpreta como la posibilidad a través del cual las entidades públicas pueden aprovechar el conocimiento previamente adquirido por ellos mismos u otras entidades, sobre soluciones tecnológicas o experiencia en la implementación de servicios de intercambio de información de una forma coordinada, de fácil acceso y adopción.
Confianza	Las entidades deben garantizar que los servicios de intercambio de información ofrecidos entregan información exacta y confiable. Adicionalmente, los datos que sean proporcionados deberán cumplir con criterios de calidad. Adicionalmente, que sus metadatos, semántica y sintaxis están disponibles para consulta y referencia.
Costo-efectividad	Las inversiones para que las entidades públicas puedan ofrecer servicios de intercambio de información deben generar beneficios que justifiquen, compensen e idealmente excedan los gastos incurridos. Las dimensiones de evaluación de los beneficios deberán estar asociadas con el aumento del bienestar de ciudadanos y empresas, y con la calidad que ellos perciben en su relación con el Estado.

Los principios propuestos por el Ministerio de las Tecnologías de la Información y las Comunicaciones definen las medidas a tener en cuenta para garantizar los procesos de interoperabilidad, de forma acertada y consciente sobre las medidas que protegen a los sistemas de información y a los usuarios. En el siguiente recuadro, se describen las normas relacionadas con el intercambio y compartición de datos de forma adecuada.

- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Art 10 y 13 establece que las entidades públicas pueden recopilar datos personales en el marco del cumplimiento de sus funciones administrativas
- Ley 1712 de 2014: Ley de transparencia y del derecho de acceso a la información pública nacional
- Ley 1955 de 2019: Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. Art 147 (principio de interoperabilidad)
- Directiva Presidencial No 7 de 2019: Por medio de la cuál se dan facultades extraordinarias para simplificar, suprimir o reformas trámites, y procedimientos innecesarios en la administración pública
- Decreto 620 de 2020: Lineamientos generales en el uso y operación de servicios ciudadanos digitales

2.5 Reutilización

Los procesos asociados al ciclo de vida de los datos tienen un carácter interactivo, en la medida en que es una sucesión fases que otorgan y garantizan el valor de los datos, e iterativo, dado que el proceso es un ciclo que se puede repetir conforme a las necesidades de la organización. Por tal razón, la entidad que ha generado o recolectado los datos puede hacer uso de la información en reiteradas ocasiones con el fin de generar nuevos usos o asegurar los principios de seguridad de la información.

Los datos recolectados o generados por una entidad pueden producir beneficios por fuera de su contexto original de producción; pueden servir para diferentes propósitos, en diversos contextos a través del tiempo. Estos datos tienen la posibilidad de ser insumo para la actividad investigativa, académica y productiva, para la toma de decisiones públicas y para la garantía de derechos. La reutilización de datos permite aprovechar conocimientos previamente adquirido como un punto de partida para nuevos proyectos. En ese sentido, los datos recolectados por una entidad suelen ser de interés para otras entidades. Es importante que los datos se hagan accesibles a otros usuarios externos a las entidades que los recaban, ya que los datos son de propósito general. Claro está, que para tal propósito habrá que tener en cuenta el nivel de publicidad y circulación de los datos, definido por las normas expedidas para la protección de derechos y la transparencia.

La reutilización de datos no solo le sirve a quien los utiliza, sino también a quien los comparte y a la comunidad en general. Por un lado, la consulta, uso y reutilización de los datos por parte de externos permite reproducir, replicar y validar investigaciones, lo cual aporta a

avanzar en los procesos investigación e innovación. Por otro lado, el reutilizamiento ayuda a fortalecer y complementar, y depurar bases de datos, lo cual es útil ya que la investigación basada en datos depende en gran medida de grandes conjuntos de datos, que no se puede producir fácilmente de forma independiente. En ese sentido, la reutilización de datos promueve la colaboración armónica entre entidades y responde a la necesidad de articulación en materia de gestión de la información. Pasar de un enfoque centrado en la publicación de datos a un enfoque de colaboración, de resolución de problemas y de determinación de objetivos es un paso necesario para el logro de la creación conjunta de valor (OCDE, 2018).

La reutilización de los datos es un proceso, más que un acto único, que requiere de Marco de interoperabilidad para su desarrollo. En ese sentido, la reutilización de datos requiere el cumplimiento de ciertos principios; la reutilización de datos demanda que en la compartición y apertura de datos se tenga en cuenta que estos deben ser comprensibles para cualquier otro investigador que desee utilizarlos, aún en el largo plazo. Los diccionarios de datos pueden contribuir a la reutilización proporcionando definiciones detalladas de los tipos de datos y las metodologías utilizadas en un estudio determinado.

3 Recomendaciones

De manera general y de acuerdo con la Superintendencia de Industria y Comercio, se recomienda a las entidades públicas en materia de protección de datos:

1. Implementar test de necesidad y proporcionalidad, en cualquier proyecto, propuesta, iniciativa de explotación de datos e inteligencia artificial, que involucre datos personales, con el fin de proteger los derechos a la protección de datos personales y privacidad de los Titulares de la Información.
2. Realizar evaluaciones de impacto relativas a la protección de datos para identificar, evaluar y gestionar los riesgos asociados al Tratamiento de los datos personales. Estas evaluaciones deben estar documentadas, con el fin de llevar su trazabilidad, y deben incluir procedimientos de auditorías, a fin de evaluar su efectividad frente al cumplimiento de la normatividad vigente.
3. Efectuar evaluaciones para determinar de manera previa si una publicación o divulgación de información de carácter personal puede vulnerar lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, especialmente, en aquellos casos relacionados con datos de niños, niñas y adolescentes, población en situación de vulnerabilidad, datos que pueden generar algún tipo de discriminación, revelación de

aspectos íntimos de las personas, datos de carácter sensible o que pueden afectar otros derechos fundamentales. Lo anterior, en concordancia con lo establecido en la Ley 1712 del 2014 y el Decreto 103 de 2015.

4. El principio de lealtad consagrado en la Sentencia C-748 de 2011 requiere que los datos personales no se procesen de tal forma que sea perjudicial, discriminatorio, inesperado o engañoso para los ciudadanos; de esa manera el tratamiento de los datos debe corresponder con las expectativas razonables de las personas.
5. La 1581 de 2012 aplica durante todo el ciclo de vida del dato personal, es decir, desde el momento de la recolección hasta su supresión; esto salvo que la información sea anonimizada que impida vincularla a una persona natural determinada o determinable.
6. Señalar una disposición legal como la base legal para el tratamiento de datos personales no es suficiente en sí misma para satisfacer el principio de libertad. De ahí que las entidades públicas deben demostrar cómo el procesamiento de datos es necesario para el cumplimiento de la norma en cuestión.
7. El Decreto 1074 de 2015 como la Sentencia C-748 de 2011 de la Corte Constitucional consagran otros principios rectores en materia de protección de datos que es importante tener en consideración como el principios de proporcionalidad y necesidad – o minimización- (artículo 2.2.2.25.2.1.) y limitación temporal del uso de los datos (artículo 2.2.2.25.2.8.).
8. Si un tercero trata los datos por encargo de la entidad pública, por ejemplo, proveedores de servicios de computación en la nube, es importante tener en cuenta lo establecido en los artículos 2.2.2.25.5.1. y 2.2.2.25.5.2. del Decreto 1074 de 2015.

4 Marco normativo en Colombia a la explotación de datos.

El marco normativo va a describir los aspectos legales y confidenciales del proceso de transformación y explotación de los datos, destacando las leyes o decretos que se utilizan para la protección de los datos personales, los accesos a la información pública, los archivos y gestión documental, etc. Con el objetivo de proteger los sistemas de información y a los usuarios que operan en estos procesos, y poder establecer los lineamientos adecuados para la explotación de los datos.

Protección de datos personales:

- **Constitución Política de Colombia, artículo 15 (1993)**

“Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley”. (Const., 1991, pág. art 15)

- **Ley 1266 (2008)**

Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Congreso de la República de Colombia, 2008)

- **Ley 1273 (2009)**

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Congreso de la República, 2009)

- **Decreto 1727 (2009)**

Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información. (Decreto 1727 DE 2009, 2009)

- **Decreto 29 (2010)**

Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008

- **Ley 1581 (2012)**

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a

que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Congreso de la República, 2012)

- **Decreto 1377 (2013)**

Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas

Acceso a la información pública

- **Ley 1712 (2014)**

Por medio del cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública.

- **Decreto 103 (2015)**

Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional Intercambio de datos y racionalización de trámites

- **Decreto 2016 (2019)**

Por el cual se dictan las normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública

- **Artículo 209 de la Constitución Política de Colombia (1991)**

La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.

- **Circular externa N.004 de la SIC (2019)**

Tratamiento de datos personales en sistemas de información interoperables

- **Ley 962 (2005)**

Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos

- **Decreto 620 (2020)**

"Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"

Archivos y gestión documental

- **Ley 594 (2000)**

Por el cual se dicta la Ley General de Archivos y se dictan otras disposiciones

- **Acuerdo 27 (2006)**

“Por el cual se modifica el Acuerdo No. 07 del 29 de junio de 1994” EL CONSEJO DIRECTIVO DEL ARCHIVO GENERAL DE LA NACIÓN DE COLOMBIA en uso de sus facultades legales y en especial de las conferidas por la Ley 80 de 1989 y el Acuerdo 017 del 27 de febrero de 2001

- **Decreto 2758 (2012)**

Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto número 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los archivos del Estado

- **Acuerdo 5 (2013)**

Por el cual se establecen los criterios básicos paro la clasificación, ordenación y descripción de los archivos en las entidades públicas y privadas que cumplen funciones públicas y se dictan otras disposiciones.

- **Directiva presidencial 4 (2012)**

Eficiencia Administrativa y lineamientos de la política cero papel en la administración pública

- **Circular externa AGN N°5 (2012)**

Recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas en el marco de la iniciativa Cero Papel.

- **Acuerdo AGN No.002 (2014)**

Por medio del cual se establecen los criterios básicos para creación, conformación, organización, control y consulta de los expedientes de archivo y se dictan otras disposiciones

- **Acuerdo AGN No. 006 (2014)**

Por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI "Conservación de Documentos" de la Ley 594 de 2000.

Sector TIC

- **Ley 1341 (2009)**

Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- **Ley 1978 (2019)**

Por el cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

Transformación Digital:

Artículo 147 de la Ley 1955 (2019)

5 Anexos

5.1 Términos y definiciones

Dato personal: Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

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.

Dato privado: Pertenecen e interesan única y exclusivamente a la persona sobre la cual recae la información.

Dato semiprivado: Es aquel dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio.

Datos sensibles: Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (Artículo 6 Ley 1712 de 2014). Su divulgación no causa perjuicios a la Entidad, ni a la ciudadanía.

Información pública clasificada: Es toda aquella que al ser divulgada puede llegar a causar daño a algunos derechos individuales de personas naturales o jurídicas por contener información relacionada con la intimidad y privacidad de éstas. (Artículo 18 de la Ley 1712 de 2014).

Información pública reservada: Su divulgación indebida puede afectar bienes o intereses públicos. (Artículo 19 Ley 1712 de 2014). Es necesario establecer el plazo para la clasificación de la reserva, es decir el tiempo en que se considera debe limitarse el acceso a la información el cual según la Ley solo puede durar un máximo de 15 años desde la creación del documento.

Tratamiento: Cualquier operación sobre los datos como la recolección, almacenamiento, uso, circulación o supresión.

5.2 Principios para el tratamiento de datos personales

La ley 1581 de 2015 establece los siguientes principios para garantizar la protección de datos personales durante su tratamiento:

Acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución.

En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

Confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Legalidad: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

Libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Seguridad: La información sujeta a Tratamiento por el responsable del tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

Transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Veracidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

5.3 Protección de datos personales y su tratamiento desde el diseño y por defecto en el entorno del Big Data.

La privacidad desde el diseño y por defecto (*Privacy by Design and by Default*), es considerada una medida proactiva para cumplir con el Principio de Responsabilidad Demostrada. Al introducir el debido tratamiento de datos personales desde el diseño, se está buscando garantizar los principios de protección de datos a lo largo de toda la vida del tratamiento.

La privacidad desde el diseño es un requisito legal que desarrolla garantías para la protección de los derechos y la libertad de los datos personales desde el momento en que se concibe el producto o servicio de datos. Para alcanzar un marco integral para la protección de los datos dentro de los procesos de diseño, operación y gestión de los sistemas, se adoptan unos principios definidos por Ann Cavoukian, para que las autoridades que protegen los datos puedan incorporar dentro de sus políticas la protección de datos en cada uno de los Estados. Es decir, estos principios (Ver Tabla 2) funcionan como una guía que va a impulsar y orientar las leyes de protección de datos personales en los distintos países. (Agencia española protección de datos, 2019)

Tabla 2 Principios de la Privacidad desde el Diseño.

Principios fundacionales de la privacidad desde el Diseño
1. Proactivo, no reactivo; Preventivo, no correctivo
2. La privacidad como configuración predeterminada
3. Privacidad incorporada en la fase de diseño
4. Funcionalidad total: pensamiento “todos ganan”
5. Aseguramiento de la privacidad en todo el ciclo de vida.
6. Visibilidad y transparencia
7. Enfoque centrado en el sujeto de los datos

Fuente: Elaboración propia, con información de la agencia española para la protección de los datos, 2019.

De acuerdo con lo expuesto en la Tabla 2 estos principios tienen como objetivo a través del aseguramiento de la privacidad, diseñar un modo de operación que permita soportar el tratamiento de los datos dentro de los modelos de negocios y sistemas de tecnología de la información. El seguimiento de estos principios implica que se utilice un enfoque orientado a la gestión del riesgo y la responsabilidad proactiva que permita establecer estrategias que se puedan incorporar en el ciclo de vida del producto.

Dentro de este ciclo se deben contemplar los procesos y prácticas de los negocios relacionados con el tratamiento de los datos para que dentro del marco regulativo se logre una gobernanza correcta de los datos por parte de las organizaciones, es en ese orden de ideas que la privacidad va a formar parte integral de la naturaleza de dicho producto o servicio, porque en el ciclo de vida se contemplan todas las etapas del producto desde su concepción hasta su finalización. (Agencia española protección de datos, 2019)

De acuerdo con la red iberoamericana de autoridades de protección de datos en su declaración relativa a la ética y protección de los datos de inteligencia artificial, se establece la existencia de un vínculo entre la operabilidad de los datos personales y el desarrollo de las áreas de inteligencia artificial, la cual, cuando los productos de estas áreas se usan permiten descubrir que los datos personales además de servir para recolectar, almacenar y analizar información, contribuye a que los fabricantes de estos productos respeten la regulación especial sobre el tema, y se establezcan unas garantías que permitan que el tratamiento de los datos se realice de forma adecuada, esto incluye, que las reglas sobre el tratamiento de los datos personales que son emitidas en los distintos países eviten la vulneración de los derechos humanos en los titulares de los datos. (Red Iberoamericana de Protección de Datos, 2019)

Ahora bien, dentro de ese vínculo la privacidad desde el diseño busca garantizar un correcto tratamiento de los datos en los procesos de inteligencia artificial, incluso antes de la materialización de los riegos. Lo anterior conduce a que se use la privacidad como un factor relevante del diseño, la arquitectura de software o el algoritmo para fomentar el uso adecuado del tratamiento de los datos, porque, la privacidad dentro de ciclo de vida del producto busca convertirse además en un modo de operación predeterminado para las organizaciones, en el que antes de recolectada la información, se puedan adoptar medidas preventivas de diversa naturaleza que eviten fallas de seguridad, vulneración en los derechos de privacidad y confidencialidad, y el uso indebido del tratamiento de datos personales.

Las medidas adoptadas para asegurar el tratamiento de los datos en la inteligencia artificial deben cumplir con los siguientes objetivos: i) Evitar los accesos no autorizados a la información, ii) Evitar la manipulación de la información, iii) evitar la destrucción de la información, iv) Evitar los usos indebidos de la información, v) evitar el suministro de información a personas no autorizadas.

Cuando las medidas siguen estos objetivos se puede establecer un tratamiento debido de los datos personales, desde cualquier perspectiva o naturaleza de los datos, porque a pesar que

dentro del desarrollo de las tecnologías, software y algoritmo del sistema de información de la inteligencia artificial se presenten unos riesgos que influyen sobre la planificación en el tratamiento de los datos o sistemas de información, por ejemplo, dentro de la operación de algoritmo, se pueden producir sesgos humanos, o fallas técnicas en la implementación, a través de estas medidas se podrán controlar y evaluar los riesgos desde la normativa para que no afecten el tratamiento de los datos y no se vulneren los derechos de los titulares de los datos y se puedan proteger los datos. (Red Iberoamericana de Protección de Datos, 2019)

Finalmente, en este contexto, las entidades públicas que buscan maximizar el uso de los datos a través de diferentes tecnologías deben ser conscientes de lo anterior desde el principio y, por tanto, asegurarse que usan ese tipo de tecnología de una manera que cumpla con la regulación en materia de protección de datos.