Revista de Derecho

ARTÍCULO DE INVESTIGACIÓN
RESEARCH ARTICLE
https://dx.doi.org/10.14482/dere.64.325.421

Consideraciones éticas y jurídicas sobre riesgos de la divulgación de datos personales en la contratación pública colombiana

Ethical and Legal Considerations on Risks in the Disclosure of Personal Data in Colombian Public Procurement

Lizeth Paola Cortina Candanoza

Abogada. Especialista en Gestión Pública e Instituciones Administrativas. Magíster en Derecho Público. Docente-investigadora de la Universidad Pontificia Bolivariana (Colombia).
Lizeth.cortina@upb.edu.co
https://orcid.org/0000-0002-5491-2799

Carolina Montañez Uribe

Abogada. Especialista en Derecho Penal y en Derecho Constitucional. Magíster en Derecho. Docente-investigadora de la Universidad Pontificia Bolivariana (Colombia).
carolina.montanez@upb.edu.co
https://orcid.org/0009-0005-7221-888X

Diana Marcela Pedraza Díaz

Licenciada. Magíster en Semiótica. Doctoranda en Historia y Estudios Humanísticos de la Universidad Pablo de Olavide (España). Docente-investigadora de la Universidad Pontificia Bolivariana (Colombia). diana.pedraza@upb.edu.co
https://orcid.org/0000-0001-6910-7568

Resumen

La Ley 80 de 1993 regula la actividad contractual pública en Colombia, estableciendo principios como la transparencia, que obliga a divulgar toda información de procesos contractuales. Sin embargo, plataformas como SECOP II exponen datos que pueden afectar los derechos individuales de contratistas y oferentes. Esto requiere un análisis ético y legal para mitigar riesgos mientras se cumple la ley. Por tanto, este artículo propone criterios ético-jurídicos para la divulgación y protección de datos personales en la actividad contractual del Estado sin perjudicar la cultura de la transparencia. Desde un enfoque cualitativo de estudio de caso con diseño documental se evidenció la necesidad de adoptar valores y principios éticos y jurídicos en la contratación pública desde el nivel de riesgo, clasificado en niveles del 1 al 5, siendo el nivel 1 datos públicos y el nivel 5 datos críticos no regulados. La adopción principios y valores es crucial para mitigar los riesgos identificados y garantizar la transparencia sin comprometer los derechos.

PALABRAS CLAVE

Contratación estatal, transparencia, protección de datos, valores éticos, valores jurídicos.

Abstract

Law 80 of 1993 regulates public contractual activity in Colombia, establishing principles such as transparency, which mandates the disclosure of all information related to contractual processes. However, platforms like SECOP II expose data that can affect the individual rights of contractors and bidders. This necessitates an ethical and legal analysis to mitigate risks while complying with the law. Therefore, this article proposes ethical-legal criteria for the disclosure and protection of open and personal data in the State's contractual activity without undermining the culture of transparency. Using a qualitative case study approach with a documentary design, the need to adopt ethical and legal values and principles in public contracting was evidenced based on risk levels classified from 1 to 5, with level 1 being public data and level 5 being unregulated critical data. The adoption of these principles and values is crucial to mitigate identified risks and ensure transparency without compromising rights.

KEYWORDS

State contracting, transparency, data protection, ethical values, legal values.

Fecha de recepción: 2/05/2024
Fecha de aceptación: 10/02/2025

INTRODUCCIÓN

Este estudio responde a los principios rectores de la Administración pública dictados en Colombia. Al respecto, se parte de las responsabilidades establecidas en la Ley 1581 de 2012 por el Estado colombiano para quienes se involucran con el tratamiento del dato de los ciudadanos. Esto incluye las orientaciones concretas para los distintos actores involucrados en el tratamiento de datos. Además, clarifica las obligaciones que deben cumplirse en su totalidad para mitigar riesgos en todo el ciclo del dato. Sin embargo, el manejo de datos en el contexto de la contratación estatal no solo requiere cumplir con las regulaciones para el ciclo de procesamiento de la información, sino también operar dentro del marco de la ley de transparencia y acceso a la información pública.

En este sentido, los responsables y encargados de los datos en el contexto de las contrataciones estatales deben cumplir con el principio de máxima publicidad, lo que implica la divulgación de toda la información en su poder. Sin embargo, esto puede conllevar a la afectación, en ciertos casos, del derecho a la protección de datos personales, incluyendo la intimidad, dignidad y reputación de los servidores públicos y contratistas. Con el ánimo de salvaguardar la protección de los derechos fundamentales de los titulares de datos de cara al interés público, para el caso que nos ocupa, el de máxima publicidad, se hace necesario tener presente que el principio de proporcionalidad es una herramienta argumentativa, empleada para evitar o controlar que se restrinjan derechos fundamentales (Cuello y Sardoth, 2018, p.7). La Corte Constitucional indicó que en este principio se concreta una ponderación entre los bienes o principios en conflicto, teniendo en cuenta su peso abstracto, la intensidad de afectación y los efectos de tal relación (Sentencia C-022/2020).

Teniendo así que este principio permite sopesar la colisión que se presenta en estos casos, resulta necesario asegurar que la publicidad de la información no exceda lo estrictamente mandado por la ley, evitando una posible vulneración de los derechos del titular. En ese sentido, en el ejercicio de las funciones, las entidades divulgan indiscriminadamente datos de categoría semiprivada, privada e, incluso, sensible a través de plataformas de contratación pública, lo que es una riesgosa realidad para Colombia.

Dada la necesidad de dar respuesta a la tensión que se presenta frente al cómo proteger los datos abiertos y personales durante la actividad de divulgación contractual del Estado colombiano sin menoscabar la cultura de la transparencia, en este artículo se proponen unos criterios éticos y jurídicos para la divulgación y protección de datos abiertos y personales en el ejercicio de la actividad contractual del Estado colombiano. Mismos que se espera sean orientadores para generar acciones concretas por parte de las entidades y encargados del dato.

Para el desarrollo de esta investigación resultó indispensable pensar lo teórico en dos vías: por un lado, los referentes éticos alrededor del tratamiento de datos en el marco de una ética que debe actuar en mundo digitalizado y, por otro, los lineamientos legales que a nivel nacional e internacional pueden guiar el proceso. Por ello, desde una investigación ético jurídico de enfoque cualitativo, alcance propositivo y diseño documental se guió el proceso investigativo desde la identificación de documentos teóricos y jurídicos cuyo eje central fuesen las categorías ética, ética digital, ética del dato, tratamiento de dato, contratación estatal en Colombia y riesgos en el ciclo del dato.

Paso seguido, se procedió a realizar el análisis de la publicación de información digital durante la actividad contractual estatal del Estado en la plataforma SECOP II desde las categorías anteriores y a la luz de la ley de protección de datos personales y el acceso a la información pública en una cultura de la transparencia. Con los resultados de estas dos fases de estudio documental fue posible establecer unos niveles de riesgos a los que en la actualidad se expone a los contratistas en el país y proyectar unas orientaciones ético-jurídicas que pueden ayudar a construir iniciativas concretas que permitan disminuir el riesgo.

Con esta propuesta y publicación se busca fomentar las buenas prácticas en la divulgación de datos personales y datos abiertos, superando la disyuntiva planteada en esta aproximación inicial. Además, se pretende fortalecer la cultura de transparencia en el ámbito de la contratación pública dentro de las entidades gubernamentales, lo que tendrá un impacto en la sociedad y en el logro de objetivos a nivel nacional, departamental y municipal, sin perjudicar a los actores involucrados en el ciclo del dato.

EL PRINCIPIO DE TRANSPARENCIA EN LAS PLATAFORMAS ELECTRÓNICAS DE COMPRAS PÚBLICAS Y SU IMPACTO EN LA ÉTICA DEL DATO

La transparencia es un principio rector del Estado colombiano. De acuerdo con este, “toda la actividad administrativa es del dominio público, por consiguiente, toda persona puede conocer las actuaciones de la administración, salvo reserva legal” (art. 3 numeral 8 Ley 1437/2011 de 18 de enero). En virtud de esta disposición del país, las autoridades públicas deben aplicar este principio desde una noción de Estado abierto, que permite una interacción más cercana con la ciudadana y un rol más activo por parte de estas. En añadidura, la Constitución Política de Colombia de 1991 estableció el derecho de acceso a la información pública y la forma en que este derecho se desarrolla a partir de los datos abiertos, los cuales “son información pública dispuesta en formatos que permiten su uso y reutilización bajo licencia abierta y sin restricciones legales

para su aprovechamiento" (Ministerio de Tecnologías de la Información y las Comunicaciones [Mintic], 2019, p.5).

La implementación del principio de transparencia en plataformas como el SECOP II ha resultado complejo, ya que evitar riesgos relacionados con la protección de datos personales no ha sido una tarea fácil. Una de las principales problemáticas es la divulgación indiscriminada de información categorizada como datos sensibles, semiprivados y privados. Por lo que en este estudio se logró encontrar en la plataforma SECOP II información relacionada con registros fotográficos, huellas dactilares, datos bancarios, hojas de vida con información completa de residencia y domicilio, teléfonos de contacto, historias clínicas, entre otros.

Esta situación se presenta porque las instituciones del estado han priorizado el principio de publicidad máxima, sin aplicar límites frente a la clasificación y anonimización de los datos, generando así riesgos para el titular de la información como la falsificación personal, suplantación personal, hurto, fraude, afectación a la intimidad, discriminación, entre otros.

Hoy, la noción de Estado abierto se establece en el CONPES 4070/2021, documento que fija los lineamientos de la política pública para la implementación de un modelo de Estado abierto. Según este informe, en Colombia se han establecido estructuras institucionales para abordar desafíos fundamentales relacionados con el acceso a la información pública, la integridad en el servicio público, la lucha contra la corrupción, la participación ciudadana en la toma de decisiones y la inflexibilidad en las políticas públicas. De ahí que una de las principales problemáticas que busca solucionar la política pública en mención se encuentra relacionada con la ausencia de garantías en el acceso a la información pública, la necesaria consolidación de una cultura de integridad y la falta de capacidad institucional para luchar contra la corrupción, entre otras (p. 3).

A su vez, señala que la cultura y aprovechamiento de datos es considerada como una de las principales barreras con que se encuentran las entidades de cara a la innovación (p. 66). En consecuencia, existe una gran preocupación por desarrollar las iniciativas de innovación alrededor del acceso, la construcción y la utilización de la información suministrada por distintas fuentes, a fin de crear mejores respuestas a los problemas públicos (Rugel y García, 2020, p. 26).

La Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (CCE) en 2023 elaboró y publicó la guía para la contratación de prestación de servicios, en la que se establecen lineamientos claros frente a la anticorrupción y la promoción del principio de transparencia en procesos contractuales. En su acápite de publicidad en la contratación pública se señalan las obligaciones que establece la Ley 1712 de 2014, de cara al principio de máxima publicidad en la ejecución de los procesos de contratación que se adelanten (art. 9 literal e, reglamentado en el

Decreto único reglamentario 1081 de 2015, artículo 2.1.1.2.1.7). También se indicó que, conforme a la circular externa de CCE, todas las entidades del país, sin importar su régimen jurídico, tienen la obligación de publicar la información en SECOP I, siendo desde 2022 obligatorio también en SECOP II (p.16). No obstante, en dicha guía no se abordan los riesgos asociados a la protección de los datos personales de servidores públicos y contratistas.

Medallo Ruiz (2017) señala que:

> El propio derecho subjetivo de acceso a los archivos y registros administrativos se ha venido reconduciendo hacia un derecho más genérico de acceso a la información pública, como derecho a saber, y no solo como solicitud rogada de acceso a la información documental en manos de sujetos públicos. (p. 177)

Es decir, lo que antes era considerada una solicitud específica para acceder a documentos en manos de entidades públicas, hoy se está transformando en un derecho más amplio y general de acceso a la información pública, que a su vez implica un derecho fundamental a estar informado, y no solo una solicitud específica. Es de aclarar que el derecho de acceso a la información pública en Colombia se encuentra contenido en el artículo 20 constitucional cuando se señala que "se garantiza a toda persona la libertad (...) de recibir información veraz e imparcial (...)".

En este contexto de transparencia y divulgación, se destaca la importancia de la protección constitucional y legal de los datos personales en Colombia. Según el artículo 3 de la Ley 1581/2012 de 18 de octubre, "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" es considerado un dato personal. A la par, en el artículo 15 de la Constitución se consagra el derecho a la intimidad personal y familiar y al buen nombre, que tienen todas las personas, con el Estado como encargado de protegerlos y respetarlos.

A nivel internacional, estos derechos están respaldados por la Carta de los Derechos Fundamentales de la Unión Europea de 1999, la Resolución 45/95 del 14 de diciembre de 1990 de Naciones Unidas y la Convención Americana de Derechos Humanos. Herrero (2023) señala que los países de América Latina están emulando fielmente al marco normativo europeo. Los países más democráticos sancionan leyes con un nivel de protección de datos mayor (p. 48).

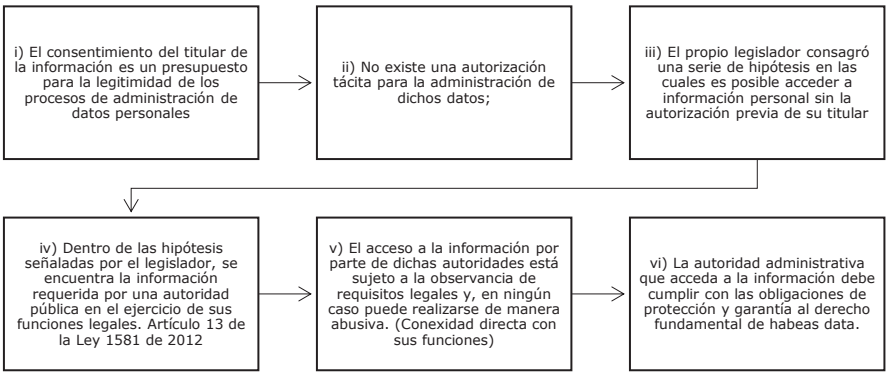
Un hito regulatorio en Colombia ocurrió en 2008 con la Ley 1266 de 2008, que desarrolló el derecho constitucional al *habeas data*, regulando la gestión de información en bases de datos personales, particularmente la que tiene que ver con información financiera, crediticia y comercial. Posteriormente, se promulgó la Ley 1581 de 2012, la cual amplió el derecho que tienen las personas a conocer, actualizar y rectificar la información recopilada sobre ellos en las bases de datos, derechos consagrados en los artículos 15 y 20 previamente mencionados.

Esta disposición de 2012 define el tratamiento de los datos, el cual supone: "cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, el almacenamiento, el uso, la circulación o supresión" (art. 3 Ley 1581/2012 de 18 de octubre). Un año después, en 2013, el Decreto 1377 reglamentó parcialmente la Ley 1581 de 2012, abordando aspectos como la autorización del titular, las políticas de tratamiento de los responsables y encargados, junto a la rendición de cuentas frente al tratamiento de datos personales. Por otra parte, el Decreto 886 de 2014 reglamentó el artículo 25 de la Ley 1581 de 2012, relacionada con la información mínima para el Registro Nacional de Bases de Datos.

Frente a la normatividad sobre los datos abiertos en Colombia, la Ley 1712 de 2014 se erige como guía fundamental. Esta regula el principio de transparencia, el derecho de acceso a la información pública y define las obligaciones de las entidades públicas frente al tema.

La jurisprudencia de la Corte Constitucional ha señalado que el deber de las entidades públicas de compartir información no implica que se permita el acceso a las bases de datos de manera ilimitada, toda vez que no puede vulnerarse el derecho fundamental de *habeas data* (p. 8). Según el artículo 10 de la Ley 1581 de 2012 y la Sentencia C-748 de 2011, al momento de publicar información bajo el principio de transparencia por parte de entidades públicas se deben tener en cuenta los aspectos que se incluyen en la figura 1:

Figura 1. Derecho fundamental de habeas data



Fuente: elaboración propia.

Por otra parte, el derecho a la intimidad o *privacy*, según Carrillo (2003), está intrínsecamente vinculado con conceptos como dignidad humana, honorabilidad, autodeterminación informativa o libre desarrollo de la personalidad (Bautista Avellaneda, 2015, p. 16). En ese sentido, no se comprende que la ciudadanía tenga acceso a información contenida en base de datos abierta sin haber pasado por un análisis de su utilización y finalidad. Al no efectuar este análisis riguroso,

pueden verse afectados los titulares en sus datos sensibles o privados, lo cual vulnera su dignidad humana, honorabilidad, buen nombre, entre otros derechos constitucionalmente protegidos.

En ese sentido, la ética emerge como un componente fundamental en la esfera pública administrativa y en el ámbito legal, actuando como elemento central capaz de orientar el proceder de los sujetos involucrados en estas nuevas dinámicas de lo digital. Como señala Adela Cortina (2013), es una "obligación ahorrar sufrimiento y gasto haciendo bien lo que sí está en nuestras manos" (p. 21). Eso es lograr que los actores involucrados en el proceso de tratamiento del dato forjen buenos hábitos, desarrollen un carácter ético en sus acciones y reconozcan las consecuencias negativas de sus decisiones en la divulgación del dato, que podrían llevarlos a actuar de manera reactiva, en lugar de preventiva, frente a los riesgos de un mundo digitalizado.

En la implementación de medidas normativas relacionadas con la transparencia y los datos abiertos en un contexto de lo digital, es necesario que las instituciones contratantes y las partes involucradas en el procesamiento del dato se convenzan de la necesidad y las implicaciones ético-jurídicas que conlleva una aplicación inadecuada de la Ley 1581. Estos principios éticos les permitirán concretar máximas para su actuación y protección, en especial en los casos en los que las medidas legales aún no llegan a menoscabar el dolor, el sufrimiento y el gasto causado por prácticas no responsables alrededor de la tecnología digital y el olvido todas estas partes de una visión basada en el "cuidado". Este camino ético debe recorrerse para abordar deficiencias que existan en aquellos lugares donde las medidas legales aún no son suficientes e, incluso, en aquellas donde se han producido avances.

En el caso de Colombia, la implementación de medidas normativas para la transparencia (Ley 1712 de 2014), la rendición de cuentas (CONPES 3654 de 2010), la participación ciudadana (Ley 1757 de 2015) y la eficiencia administrativa (art. 209 C.P.) debe estar fundamentada en la ética del cuidado. Con ello, se puede asegurar que las políticas de transparencia y rendición de cuentas no se limiten a cumplir con requisitos legales, sino que reflejen un compromiso genuino con el bienestar de la ciudadanía.

Una ética del cuidado como orientadora de las prácticas resulta relevante, ya que Colombia ha venido reconociendo perjuicios en juicios de responsabilidad del Estado por vulneración de derechos fundamentales como la intimidad personal[1]. Incluso en el reglamento de la Unión Europea GDPR se establece expresamente el derecho de todo interesado en solicitar indemnización por daños y perjuicios materiales (art. 146) relacionados con la protección inadecuada de sus

1 Al respecto, véase sentencia de reparación directa, Tribunal Administrativo de Cundinamarca, Sección Tercera, Subsección A. Rad. 11001333704420170024902 demandada la Nación- Fiscalía General de la Nación.

datos personales. No obstante, estas disposiciones taxativas no se encuentran en Argentina, Chile ni México (ADCDIGITAL, s.f., p. 33).

Por otro lado, una ética basada en el cuidado plantea que "los seres humanos necesitamos ser cuidados para sobrevivir y estamos hechos para cuidar a los cercanos, pero también tenemos la capacidad de llegar hasta los lejanos" (Cortina, 2013, p.72). En este sentido, las instituciones y los actores involucrados en el ciclo del dato deben adoptar una actitud proactiva en la implementación de prácticas éticas, que tengan como fin la protección de los bienes inherentes de las personas, como el buen nombre, su intimidad, honra y demás puntos constitucionalmente protegidos.

Colmenarejo (2017) señala que "la *business ethics* es una disciplina que lleva décadas de ventaja en la resolución del conflicto sobre si deben confiar las decisiones éticas que afectan a la empresa y al resto de sus grupos de interés" (p.1966). Indica la autora que hoy, dados los avances tecnológicos que genera la eclosión de información y el uso de los *big data*, hacen emerger conflictos éticos, toda vez que almacenar, gestionar y utilizar datos plantea problemas relacionados con la privacidad, la identidad y la confianza (p.1967).

En ese sentido, la ética del cuidado plantea la responsabilidad de administrar, almacenar y procesar datos conforme a los parámetros legales, éticos y políticos. Por tanto, las entidades y los actores están llamados a velar por el bienestar de aquellos a quienes afecta su gestión de la información, sean estos sus cercanos, a sí mismos y al lejano. Al incorporar esa ética del cuidado no solo como una práctica personal, sino también como un principio rector en el desarrollo y aplicación de las normativas que regulan el tratamiento de datos, se da un paso para asegurar una protección adecuada de los derechos y la dignidad de los individuos en el ámbito digital.

En el marco de las discusiones previas sobre la ética del cuidado y su relevancia en el tratamiento de datos, emerge un nuevo desafío: la necesidad de establecer una ética del cuidado del dato. Esta ética se centra en evaluar los problemas morales relacionados con los datos, los algoritmos y las prácticas, con el objetivo de formular soluciones asociadas a conductas adecuadas, valores esenciales y principios a seguir en el tratamiento del dato (Floridi y Taddeo, 2016).

En el caso de los datos, refiere pensar "la forma en que se maneja y utiliza la información en la era digital de manera responsable y ética [...] no solo alude a los datos personales, también es importante para la información que se gestiona y se transmite" (ActionsData, 2022, pp. 2-5). Esta transición de la ética del cuidado a la ética del cuidado del dato resalta la necesidad de considerar no solo el bienestar de los individuos, sino también la integridad y el uso responsable de la información en un entorno digitalizado y globalizado, caracterizado por la circulación transfronteriza y el acceso casi inmediato a los datos. En consecuencia, en los subtítulos posteriores

de este texto se presentará una serie de valores y principios rectores específicos para cada actor involucrado en el tratamiento de datos. Por lo que, a partir de ese desarrollo analítico, se invita a tener presente cada uno de los valores y principios identificados, ya que pueden servir como líneas de acción utilizables en actividades relacionadas con formación, promoción, auditorías, evaluación de impactos éticos, conformación de comités de ética, desarrollo de protocolos de actuación, entre otros. Por ejemplo, la implementación de programas de capacitación continua en la ética del cuidado y los valores que rigen su actuar, según lo propuesto en este estudio, puede fortalecer la conciencia y el compromiso de los funcionarios públicos en una cultura de transparencia (artículo 133 de la Ley 1753 de 2015 y Decreto 1499 de 2017 art. 2.2.22.2.1 numeral 5[2]).

Así las cosas, en la era digital, caracterizada por la transparencia en el uso del dato y el acceso equitativo al mismo, o lo que es lo mismo, una cultura organizacional basada en la ética del cuidado y la ética del dato, uno de los desafíos cruciales es la privacidad y la seguridad de la información. Aspectos que se han vuelto críticos y exigen garantizar que la información divulgada no contenga información íntima o confidencial que ponga en riesgo al titular del dato o genere responsabilidades jurídicas a las personas y organizaciones encargadas de los procesos, estrategias y políticas de datos.

Este aspecto engloba una ética práctica dentro del ámbito de la ética de los datos, cuyo objetivo es "definir un marco ético para dar forma a los códigos profesionales sobre la innovación, el desarrollo y el uso responsable" (Floridi y Taddeo, 2016, p. 6) sin detrimento de la cultura digital, la cultura de la transparencia y la protección de los derechos de individuos y grupos. A nivel gubernamental, en el mundo existen lineamientos, pero resultan insuficientes para abordar las problemáticas actuales de un mundo digitalizado, por lo que sigue en construcción el camino de un gobierno de los datos basado en la ética del cuidado. Así lo expresan varios autores en sus estudios. Al respecto, Sánchez (2023) señala:

> [...] El marco normativo con el que contamos, al menos en México, no es suficiente para garantizar la eficacia de la gran mayoría de los derechos humanos y particularmente, por lo que nos atañe en el presente estudio, en lo referente a los derechos a la privacidad, a la protección de los datos personales, entre otros más, recordando que los derechos humanos se encuentran conectados entre sí; más bien, lo que se está quedando como objeto de análisis es el incremento en la vulnerabilidad. (p. 11)

2 ARTÍCULO 2.2.22.2.1. Políticas de Gestión y Desempeño Institucional. Las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominarán políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes: (...) 5. Transparencia, acceso a la información pública y lucha contra la corrupción.

Por su parte, Franzke y Schafer (2021) destacan:

> El uso del llamado *Systeem Risicoindicatie* (SyRi), que utiliza una amplia gama de fuentes para detectar el fraude en prestaciones sociales suscitó numerosas críticas e investigaciones parlamentarias. En febrero de 2020, un tribunal holandés declaró ilegal este algoritmo desarrollado y utilizado por el gobierno [...] Como resultado, los gobiernos locales se han vuelto cada vez más conscientes de la necesidad de manejar los datos de manera responsable y ética. La ciudad de Zaanstad lleva a cabo "revisiones éticas"; la ciudad de Utrecht hizo obligatoria las revisiones éticas; un taller de ética de datos también fue parte del congreso anual de la Asociación de municipios holandeses en 2017 y 2019 [...] (párr.16)

En Argentina, la Ley 25326 del 2000 regula la protección de los datos personales, que si bien cumplió con su cometido, dejó por fuera situaciones que para el momento de su promulgación eran impensadas o implicaban tecnologías incipientes (ESET, 2023, párr.7).

Aunque el contexto anterior refleja una realidad en construcción alrededor de la ética de los datos y el cuidado, desde la academia se siguen generado reflexiones y propuestas como la de Sánchez Díaz (2023), en la que la falta de protección de los datos personales y la vulneración de la privacidad es una afectación a la dignidad humana y, por ende, a los derechos humanos.

Otro ejemplo claro de los desafíos éticos en el tratamiento de datos personales es el derecho al olvido, el cual ha sido objeto de regulación en varios países del mundo, pero en Colombia aún no. Este derecho cada vez resulta más crucial para dar soluciones a cuestiones éticas que pueden presentarse respecto al tratamiento de la información personal cuando su finalidad se ha agotado o ha cambiado respecto a lo expuesto originalmente a su titular.

En España, por ejemplo, en el artículo 29 se reconoce el derecho al olvido en materia de archivos de deudores en mora. En Argentina, la Ley 25.326 (República de Argentina, 2000), de Protección de Datos Personales, lo reconoce en el artículo 26. En México, se encuentra garantizado por el artículo 16 constitucional, párrafo segundo, y la Ley Federal de Protección de Datos en Posesión de Particulares (Estados Unidos Mexicanos, 2010), el cual es un derecho humano al que se puede acceder por medio de los derechos de cancelación y oposición al tratamiento de nuestros datos personales (Bautista Avellaneda, 2015, p. 29). La ausencia de regulación del derecho al olvido en Colombia destaca la necesidad de abordar estas cuestiones éticas y garantizar la protección adecuada de los datos personales en el contexto digital.

La regulación del tratamiento y divulgación de los datos en el marco de la contratación estatal debe ser abordada desde una perspectiva ética y jurídica, para garantizar que se respeten los derechos fundamentales de las personas. Además, debe ser orientada desde una perspectiva

interdisciplinaria, que tenga en cuenta tanto aspectos técnicos como éticos y legales, mediante la cual se logre equilibrar los beneficios potenciales de la digitalización del mundo físico frente a los riesgos.

RIESGOS IDENTIFICADOS EN LA CONTRATACIÓN ESTATAL DURANTE EL EJERCICIO DE DIVULGACIÓN DE DATOS PERSONALES

La contratación estatal representa una de las actividades más importantes de los estados. De acuerdo con Rousseau (como se cita en Bejarano, 2009, p. 49), este proceso implica el uso de considerables cantidades de recursos públicos para que se compren y adquieran bienes y servicios del sector privado por parte de las entidades gubernamentales. De ahí que una de las principales características de esta actividad es su sujeción con el ordenamiento jurídico, es decir, las normativas y regulaciones son fundamentales para garantizar la transparencia, la equidad y la legalidad en los procesos de contratación pública.

Santofimio Gamboa (como se cita en Lucas Ortegón, 2017, p. 18) advierte que el principio de legalidad en la contratación estatal se ve reflejado a partir de "la necesaria conformidad de los actos que deban proferirse con ocasión del contrato, con el ordenamiento jurídico general, y con el que le da la fundamentación especial". En este contexto, cualquier acto administrativo relacionado con un contrato debe estar en conformidad tanto con las leyes generales como con las normativas específicas aplicables al caso.

En Colombia, su regulación se encuentra en la Ley 80 de 1993 junto a sus modificaciones y decretos reglamentarios. Esta se encuentra enmarcada en tres principales etapas: precontractual, contractual y postcontractual. En la primera, la entidad pública despliega una serie de actividades preparatorias de cara al perfeccionamiento del contrato. Entre las actividades que se resaltan están: la realización de pliegos de condiciones, estudios del mercado y del sector, la identificación de riesgos y selección del esquema de cobertura, la selección de la modalidad de selección del contratista y de contratación de cara al objeto que la entidad quiera contratar. La fase contractual se identifica porque la entidad respeta lo realizado en la fase precontractual. Así que selecciona al contratista, eleva por escrito el contrato y perfecciona el mismo, esto es, que las partes consientan en el objeto a contratar (art. 41 Ley 80/1993 de 28 de octubre). Finalmente, la fase postcontractual guarda relación con la fase posterior a la ejecución contractual, caracterizada principalmente por la liquidación del contrato (art. 60 Ley 80/1993 de 28 de octubre).

Para el caso de nuestro país, la contratación de las entidades públicas se desarrolla en páginas de acceso abierto al público para la respectiva vigilancia y/o veeduría ciudadana. Una de las principales plataformas con este propósito es SECOP II (Sistema Electrónico de Contratación Pública),

que es una versión más avanzada que SECOP I, y permite realizar el proceso de contratación en línea. Por lo anterior, fue esta el referente de análisis de esta investigación.

En el desarrollo del análisis se tomaron en consideración las modalidades de selección de contratistas establecidas en la normativa vigente. Entre estas se revisaron los procesos de contratación de 2021 y 2022, asociados a: la licitación pública, definida en el artículo segundo número1 de la Ley 1150; la selección abreviada, definida en artículo segundo número 2 de la Ley 1150; la mínima cuantía, definida en artículo 94 de la Ley 1474; concurso de méritos, definido en artículo segundo número 3 de la Ley 1150; y la contratación directa, definida en artículo segundo número 4 de la Ley 1150.

Tras la revisión documental, en estas contrataciones se identificó la presencia de información digitalizada de contratistas con acceso abierto al público. Con el estudio de cada documento fue posible categorizar en diferentes niveles de confidencialidad los datos encontrados en la plataforma. Esa información expuesta en red plantea un riesgo significativo, ya que puede ser utilizada por cualquier persona con diversos propósitos, incluso con fines delictivos, pues se encuentra expuesta por la entidad pública sin implementar medidas de seguridad, permitiendo la manipulación de la información a través de la descarga o la toma de pantallazos de todo lo allí divulgado.

Así las cosas, al analizar los datos digitalizados disponibles en SECOP II, se identificaron varios tipos de datos (sensible, privado, semiprivado y público) en acceso abierto en las distintas modalidades de selección de contratistas. Los hallazgos incluyeron los aspectos indicados en la siguiente tabla:

Tabla. Datos expuestos al riesgo en plataforma abierta de contratación

Clasificación del dato	Dato al que se tiene acceso en la plataforma
Dato sensible	Examen preocupacional: valoración visiometría, osteomuscular. Sexo del paciente. Firma de médico y paciente. Restricciones laborales. Foto en cédula. Firma en cédula. Sexo del ciudadano.
Dato privado	Dirección de residencia. Teléfono celular personal. Datos bancarios (número de cuenta, banco y tipo de cuenta). Firma en cédula. Declaración de bienes y raíces. Recomendaciones y observaciones médicas en examen preocupacional. Pagos de seguridad social. Información financiera.
Dato semiprivado	Certificación bancaria. RUT. Tipo de sangre. Fecha de expedición de la cédula. Títulos profesionales y certificados de estudio. Certificado laboral. Certificado de salud. Certificado de pensión. Tipo de sangre. Fecha de expedición de la cédula.
Dato público	Número de cédula. Detalles del contrato. Registro mercantil. Correo empresarial o institucional. Dirección de lugar de trabajo. Valor del contrato. Antecedentes penales. Lugar de nacimiento. Certificado de Inhabilidades. Hoja de vida. Antecedentes disciplinarios y fiscales. RUP. NIT.

Fuente: elaboración propia.

Con este detalle se hace evidente una preocupante vulnerabilidad en la infraestructura de las páginas de datos gubernamentales, en particular en la plataforma analizada; misma que presenta de manera indiscriminada datos sensibles, privados y semiprivados que según la legislación vigente deben mantenerse en reserva y bajo medidas de seguridad adecuadas, garantizando los principios de protección de datos personales consagrados en la Ley 1581 de 2012. En este contexto, la existencia de un acceso abierto a estos datos plantea serios interrogantes sobre la integridad y confidencialidad de la información, y pone de manifiesto la necesidad urgente de revisar y fortalecer los protocolos de seguridad, junto a las políticas de acceso en el marco de la cultura de la transparencia.

Por ello, resulta necesario balancear el principio de transparencia con la protección de los derechos fundamentales de contratistas y servidores públicos, cuyos datos personales se encuentran expuestos en plataformas abiertas como SECOP II. De esta situación, uno de los interrogantes que puede surgir es, ¿cómo esto afecta la protección de datos personales y la intimidad?

La respuesta está dada desde la misma jurisprudencia de la Corte Constitucional Colombiana "no hay derechos ni libertades absolutos" (Sentencia C-046/1996). Y esto es así porque es clara la obligación de publicar todo lo que una entidad pública tiene en su poder cuando de contratación pública se trata, ya que esta obligación resulta ser de suma importancia, atendiendo a "la finalidad e importancia de publicar los contratos de la Administración es realizar una comunicación masiva que permita informar, persuadir y conseguir un comportamiento determinado de las personas que reciben la información" (Corte Constitucional, Sala Plena, Sentencia C-384 del 13 de mayo de 2003, expediente D-4312, como se cita en Duque Botero, 2021, p.16).

No obstante, existe una limitación, contenida en la norma, la cual establece: tendrán el carácter de reservado los documentos que "involucren derechos a la privacidad e intimidad de las personas" (Ley 1437/2011 art. 24 nº. 4). En materia de protección de datos, Colombia adopta una "regulación abierta a partir de principios que guían la tarea interpretativa" (Alarcón, 2021, p. 147). Esto significa que es el servidor público, y puntualmente la entidad, quien al momento de cumplir con el principio de máxima publicidad debe aplicar un procedimiento que se establezca previamente para seleccionar aquella información que tenga el carácter de pública, privada o semiprivada, siempre y cuando en esta dos últimas se cuente con autorización del titular y que dicho documento repose en los documentos que se publican en esta plataforma, siendo entonces necesario anonimizar aquella información de carácter sensible que pueda afectar la intimidad del titular.

Es por ello que se subraya la importancia crítica de la ciberseguridad, la protección de los datos sensibles, privados y semiprivados, en el contexto gubernamental de la contratación, junto al

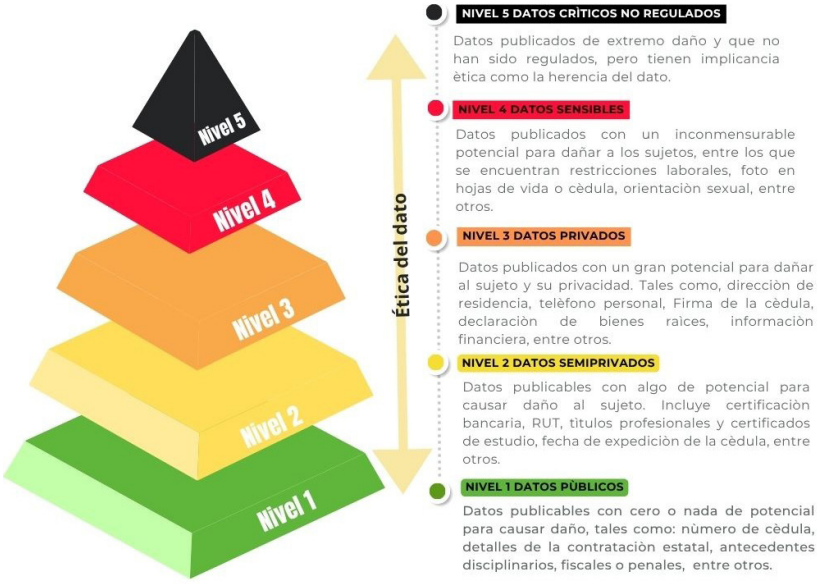
reconocimiento de los niveles de riesgo a los que se expone al titular del dato cuando se divulga información personal que jurídicamente ya se encuentra regulada. Ese análisis no desplaza la necesidad de garantizar el principio de transparencia y la garantía de la máxima publicidad a cargo de entidades públicas, sino, por el contrario, es imperativo que quienes llevan a cabo el tratamiento de esta información verifiquen y contrasten derechos y garantías protegidas en el marco de su responsabilidad. Esto es fundamental para aplicar buenas prácticas cuando se está publicando información privada y sensible del titular, a fin de evitar riesgos asociados a la vulneración de derechos como su buen nombre, honra, dignidad.

Un ejemplo concreto, encontrado en esta investigación, fue la presencia de un examen ocupacional entre los documentos publicados en la página de SECOP II y a los que se tuvo acceso sin restricción durante el este estudio. Este examen reveló detalles del estado físico del contratante, su peso, recomendaciones médicas y hasta su fotografía personal; datos que, según la normatividad colombiana, son de carácter sensible (Ley 1581/2012 art. 3 y 5) y su disposición en redes públicas representa una violación a los derechos constitucionalmente protegidos (Sentencia de unificación de la Sala Plena del Consejo de Estado de 14 de septiembre de 2011).

En la Sentencia del 14 de septiembre de 2011 se sostuvo que esta clase de afectaciones a bienes o derechos constitucionales o convencionalmente afectados deben ser reconocidos como una tercera categoría de daños inmateriales autónomos. Bajo esta óptica, se sistematizó de la siguiente manera la tipología del perjuicio inmaterial: i) perjuicio moral; ii) daño a la salud (perjuicio fisiológico o biológico); iii) cualquier otro bien, derecho o interés legítimo constitucional, jurídicamente tutelado siempre que esté acreditada en el proceso su concreción y sea preciso su resarcimiento (Consejo de Estado, Sentencia de Sala Plena del 14 de septiembre de 2011, rad. 19031 y 38222, M.P. Enrique Gil Botero).

Por ello, ante este panorama de los datos normatizados, se hace necesario reflexionar sobre la ética de los datos aún no regulados y que pueden representar un costo económico, traducido en demandas de responsabilidad contra el Estado y de sufrimiento a los distintos actores del ciclo del dato. Para proporcionar una orientación más clara sobre este asunto, en la figura 2 se presenta la pirámide de riesgos de publicación del dato, la cual tiene en cuenta los datos normatizados y aquellos que carecen en Colombia de regulación. Por ende, queda claro que el tratamiento ético del dato debe darse en todo el proceso, no solo en las prácticas no reguladas.

Figura 2. Niveles de riesgo ético y jurídico en la divulgación de datos



Fuente: elaboración propia.

Así las cosas, para el momento del estudio de la página SECOP II en el marco de las modalidades de mínima cuantía, contratación directa, licitación pública, selección abreviada y concurso de méritos, se identificó un acceso ilimitado a los datos de los contratistas y la posibilidad de descargar los adjuntos a cada información. Esto sugirió la presencia de posibles riesgos relacionados con la violación de la privacidad del ciudadano al tener acceso a direcciones privadas y datos financieros. Además, existe la preocupación por la exposición al robo de identidad, lo que podría generar fraudes financieros u otras actividades ilícitas que ponen en riesgo o lesionan los bienes jurídicos protegidos por el ordenamiento colombiano.

Existe el riesgo de que la divulgación de datos pueda llevar a acoso o *phishing* por parte de estafadores que haciéndose pasar por entidades estatales o privadas engañan al ciudadano y lleguen a robarle información adicional o dinero de manera fraudulenta. Con este retrato de los riesgos asociados a la divulgación actual de datos en la contratación estatal se genera un clima de desconfianza alrededor de los encargados del dato y los responsables del mismo; además de una percepción de baja eficacia gubernamental.

Se hace urgente revisar la situación desde lo normativo y lo ético, pues según la circular externa Nº 005 del 31 de agosto de 2023 de Colombia Compra Eficiente, el uso de SECOP II se hizo obligatorio para la vigencia fiscal 2023. Por lo tanto, las entidades, en su mayoría municipios, concejos y personerías municipales de todo el territorio nacional, deberán divulgar las contrataciones que realicen a través de este medio. Sin lugar a duda, la finalidad es “que los actores del sistema de

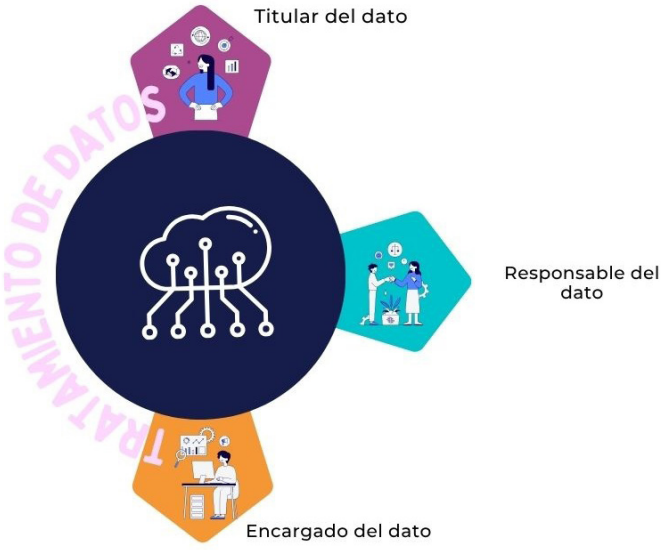
compra pública accedan, gestionen, participen y hagan seguimiento y control social a los recursos que son administrados por las entidades del Estado y los privados en cumplimiento de la normatividad aplicable" (p. 2), pero la realidad es la problemática de exposición de datos personales sin medidas de protección legal o ética.

En ese sentido, es clara la apuesta del Gobierno nacional por fortalecer los procesos de compras públicas para lograr mayor eficiencia, transparencia y optimización de los recursos públicos, y el objetivo de esta investigación, identificar los puntos críticos en esa labor, aportando caminos para seguir desde valores y principios ético-jurídicos que orienten a generar acciones concretas.

IDENTIFICACIÓN DE LOS VALORES Y PRINCIPIOS ÉTICO-JURÍDICOS POR ACTOR EN EL PROCESO DE DIVULGACIÓN DE DATOS

En el mundo de la información y la digitalización de los datos, el Comité Jurídico Interamericano (CJI, 2021) definió como actores del tratamiento de este a tres sujetos centrales (figura 3). Estos se involucran en acciones que van desde la recopilación del dato hasta su divulgación y/o transferencia. El primer actor es la persona cuyos datos se compendien, procesan, almacenan, utilizan o difunden y recibe el nombre de titular del dato. Este sujeto entrega a un encargado del dato su información; representado en una persona física o jurídica, entidad privada o entidad pública. Finalmente, se cuenta con el responsable de los datos, que se encarga del tratamiento y la protección de los datos personales; determina el contenido, las finalidades y el uso de los datos personales (CJI, 2019).

Figura 3. Sujetos involucrados en el ciclo del dato



Fuente: elaboración propia.

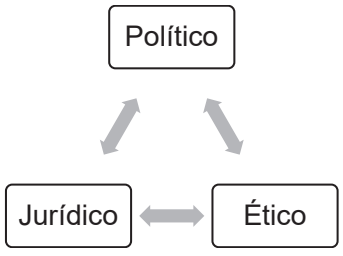
La acción de los involucrados en el ciclo del dato durante el proceso de divulgación en la contratación estatal exige identificar un conjunto de principios que orienten la conducta de los actores hacia el bien común, el cumplimiento de las normas legales existentes y la garantía de los derechos constitucionales. Esto pone de relieve la disposición de acciones orientadas desde los dos paradigmas jurídicos. El primero, el paradigma constitucional, caracterizado por el uso de principios y valores; y el segundo, el legicentrista, que se basa en el empleo de un lenguaje basado en las reglas (Estrada, 2011).

La base de la visión constitucional puede presentarse desde el campo de la filosofía ética, en la que los principios tienen por base los valores. Estos últimos son entendidos como creencias fundamentales que orientan la conducta humana, se consideran universales y permiten la derivación de principios concretados en normas, reglas o pautas más específicas para accionar. Entonces, puede definirse los valores como conceptos abstractos que guían el comportamiento humano, mientras que los principios son directrices más concretas que se derivan de esos valores y establecen normas específicas para la conducta. Por ejemplo, el valor de la honestidad puede dar lugar al principio de transparencia en la gestión pública (Ministerio de Educación Nacional [MEN], 2011, p. 6).

No obstante, desde el plano epistémico del derecho la Corte Constitucional colombiana ha definido la naturaleza y funciones de estos conceptos, valores y principios, acordes con un Estado social y constitucional de derecho. Así las cosas, para definir, diferenciar y relacionar los conceptos de principios y valores en este campo se debe partir de la presencia de un enfoque tridimensional del fenómeno jurídico presente en la divulgación de datos en medio de la contratación estatal.

Por ende, se tiene presente para su definición tres conceptos centrales (figura 4). Iniciando con lo jurídico, basado en el reconocimiento de la constitución; seguido de lo ético, relacionado con la incorporación de valores y, finalmente, lo político, encargado de la configuración del poder, su ejercicio y límites (Estrada, 2011).

Figura 4. Enfoque tridimensional del fenómeno jurídico.



Fuente: basado en Estrada (2011).

Por tanto, desde la perspectiva de la Corte Constitucional de Colombia, los valores se asocian a las normas morales, mientras que los principios se inclinan hacia la norma jurídica. Los valores se emplean de manera interpretativa (estimativa o axiología jurídicas) y no son normas jurídicas, según la Sentencia T-406 de 1992; de hecho, "los valores orientan al legislador, inspira institutos y normas, postulan reglas concretas, pero no son normas y de ellos no se puede predicar la estructura, propiedades y eficacia de aquellas" (Martínez, 2007, como se cita en Estrada, 2011, p. 5). La naturaleza de los valores se asocia a un deber ser moral; además, presenta una proyección o función en el derecho como criterio de interpretación o accionar en aquellos casos del tratamiento de datos que no se haya regulado. Señala la Corte Constitucional en Sentencia T-406 de 1992 que sobre los valores se construye el fundamento y la finalidad de la organización política. Según Duro (2021), los valores constitucionales juegan un papel fundamental como límites a la actuación de los poderes del Estado y la función pública (p. 25).

Por su parte, los principios, son normas jurídicas de aplicación inmediata que sirven para resolver situaciones concretas y presentes; a diferencia de los valores, tienen una mayor especificidad, por ende, mayor eficacia de ser aplicados de manera directa e inmediata. Los principios "no pueden ser desconocidos por otra norma legal o constitucional, tampoco por otro principio no expresamente señalado por la Constitución" (Estrada, 2011, p. 6).

Solo en los principios se encuentra una fuente que podría catalogarse de anticrisis, o, en otros términos, que nunca ha entrado en crisis (Cabrera Suarez, 2011, como se cita en Yáñez et al., 2023, p. 57). En consecuencia, los principios, como valor normativo, solo son aquellos que están en la Constitución. De hecho, de estos se derivan derechos fundamentales. Por lo anterior, las órdenes morales (valores) y jurídicas (principios), aunque mantiene contactos, no son iguales, ni equiparables.

En este marco de ideas, la acción alrededor de la práctica del tratamiento y divulgación de datos en el proceso de contratación estatal de Colombia debería tener presente los principios jurídicos, los principios éticos y los valores en el proceder de cada actor, pues todos son sujetos de derechos y responsables moral y jurídicamente de sus acciones. Por tanto, en esta toma de decisiones frente a la pirámide del riesgo divulgativo de información del contratista se hace necesario, en el actual contexto de digitalización transfronteriza de los datos, equilibrar el argumento jurídico con el argumento de naturaleza axiológica, como se propone a continuación en cada actor.

1. Titular del dato: sobre sus derechos y valores, la protección de datos personales en Colombia es un tema de creciente importancia en un mundo digitalizado. La regulación de la privacidad y la seguridad de la información personal se ha convertido en una prioridad en la legislación colombiana, en la que uno de los pilares fundamentales es la conceptualización del "titular del

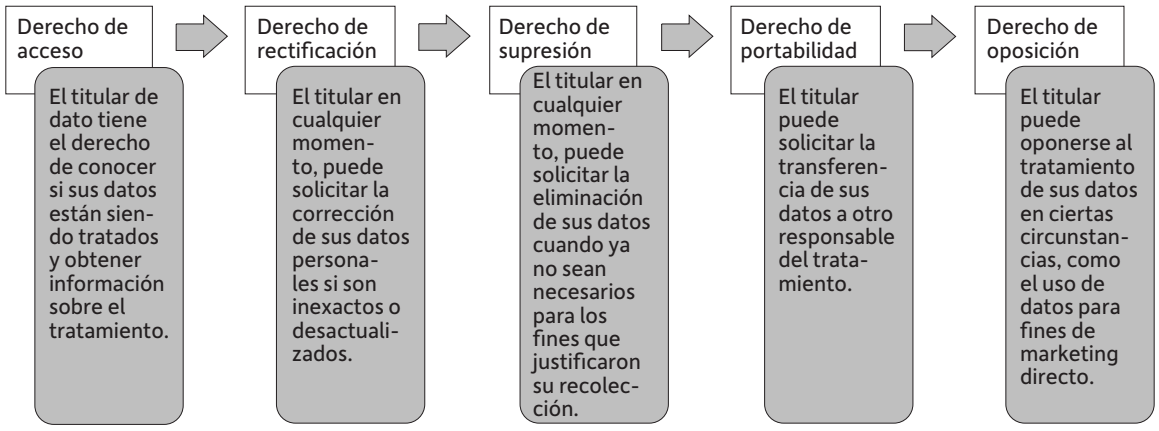
dato" como eje central de la regulación de protección. En Colombia, el titular de dato se refiere a la persona natural cuyos datos personales son objeto de tratamiento por parte de terceros, ya sean entidades públicas o privadas. En el caso objeto de estudio se hace referencia a oferentes, contratistas y servidores públicos.

Hablar de datos personales incluye cualquier información que permita identificar a una persona, desde nombres y apellidos hasta números de identificación, dirección personal, y detalles financieros, entre otros. Por lo que el titular del dato tiene el derecho de conocer, actualizar, rectificar y suprimir sus datos personales, así como el derecho a revocar el consentimiento otorgado para su tratamiento (Ley Estatutaria 1581 de 2012, el Decreto Reglamentario 1377 de 2013).

Dado que uno de los principios fundamentales de la normativa colombiana es el de tener el consentimiento informado del titular de un dato, esto significa que antes de recopilar y tratar datos personales, las organizaciones deben obtener el permiso explícito y libre del titular de datos. Además, las entidades que manejan datos personales deben garantizar la seguridad y confidencialidad de la información y adoptar medidas de protección adecuadas a la normativa fundamental que rige la protección de datos personales en Colombia, dejando de presente que la Superintendencia de Industria y Comercio (SIC) es la entidad encargada de supervisar y regular el cumplimiento de estas normas en el país. En el ejercicio desarrollado se omitió este consentimiento.

También, el ordenamiento jurídico colombiano confiere a los titulares de datos personales una serie de derechos fundamentales para proteger su privacidad y controlar el tratamiento de sus datos. Estos derechos se describen en la figura 5.

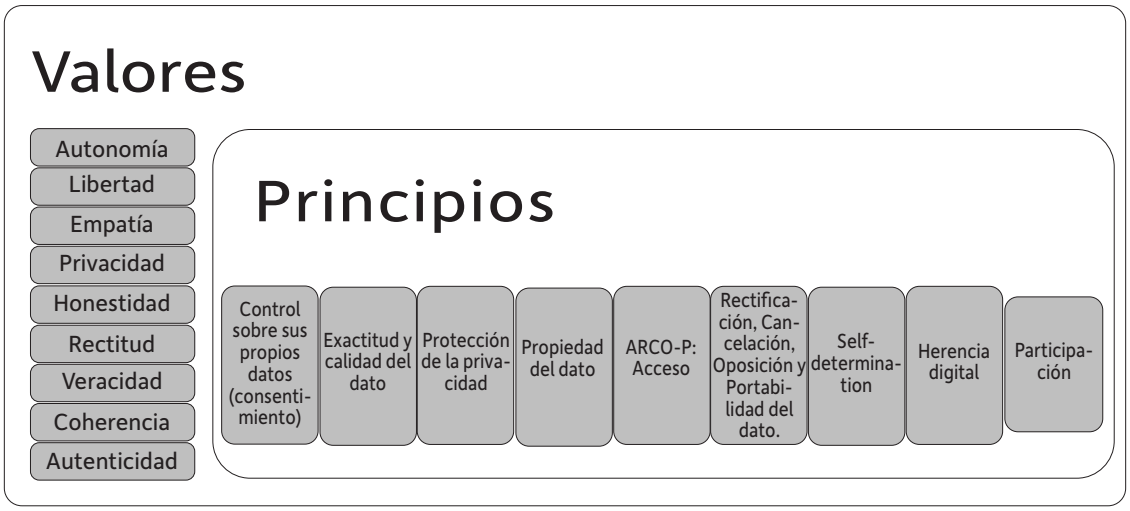
Figura 5. Derechos de los titulares de datos personales



Fuente: elaboración propia.

Por su parte, los titulares de datos tienen la responsabilidad de proporcionar información precisa y actualizada a los responsables del tratamiento. También, deben informar a las autoridades y a los responsables de cualquier cambio en su información, así como notificar cualquier violación de seguridad de datos que puedan experimentar. Los valores y principios éticos asociados al titular del dato deberían ser:

Figura 6. Valores y principios éticos asociados al titular del dato



Fuente: elaboración propia.

2. El responsable del tratamiento del dato o *data controller*: El responsable del tratamiento del dato es una figura física o jurídica, pública o privada, crucial en el ciclo del dato, pues determina los propósitos y los medios para el procesamiento de estos. Protege los datos y su privacidad, pues debe garantizar que se cumplan todas las obligaciones legales y regulaciones, además de proteger los derechos de los titulares. Para el caso de este estudio son las entidades estatales las que cumplen este rol (SIC, 2015).

La determinación de estos propósitos y medios no solo son esenciales para garantizar la transparencia en la recopilación y el uso de datos, sino que también asegura que el procesamiento se realice de manera legal y ética, que los datos solo se usen para fines legítimos y específicos, siempre en línea con las regulaciones de privacidad y protección de datos aplicables a cada situación y país.

Así las cosas, los principios jurídicos que corresponden al accionar del responsable del tratamiento del dato son cuatro. En primer lugar, el principio de seguridad, que exige manejar los datos con las medidas técnicas, humanas y administrativas que se requieran para evitar la pérdida, consulta a datos semiprivados, privados o sensibles y el acceso no autorizado e inclusive fraudulento

a la información de los titulares. En segundo lugar, el principio de finalidad, en el que se exige tener clara la finalidad legítima de la divulgación del dato en el marco la regulación de cada estado (constitucional y legislativa). En tercer lugar, el principio de responsabilidad demostrada en el que se exige que el responsable del dato demuestre de manera efectiva su cumplimiento con las leyes y regulaciones de protección de datos. Para ello, se puede tener registro de actividades de tratamiento, designación de un encargado del tratamiento, evaluación de impacto de protección de datos, entre otros. Finalmente, se debe tener en cuenta el principio de legalidad en el que se establece que una entidad o persona solo puede recopilar, almacenar, utilizar, procesar o divulgar datos personales si existe una ley, una autorización expresa del titular de los datos, o una finalidad legítima que permita realizar dicho tratamiento.

Desde el plano ético, los valores centrales que deben orientar el accionar del responsable del tratamiento del dato son: autonomía, igualdad, imparcialidad, privacidad, solidaridad, honestidad, justicia social, servicio, valor social, autoridad, valor de comunicación.

Estos valores tienen presente la dignidad humana como centro de su acción, ya que implica que cada individuo es merecedor de respeto y protección, no debe ser cosificado (Data ethik, 2018). Además, invita a este actor a actuar con transparencia, rectitud, veracidad y coherencia en sus funciones a nivel jurídico y ético, en conformidad con la obligación adquirida como representante del Estado.

Para asegurar una contribución positiva a los distintos actores del proceso, el responsable del dato puede guiarse por los siguientes principios éticos en el desempeño de sus funciones. El *primero* de ellos es *in dubio pro actione*, que se refiere a refiere a tomar decisiones que favorezcan la acción o el procedimiento en caso de duda, lo que puede ser considerado ético en la búsqueda del bien común y el avance. El *segundo*, bien común, que parte de la idea de que las acciones deben beneficiar a todos los actores involucrados en el ciclo del dato y no solo a intereses individuales. El *tercero*, conciencia social, implica que se debe ser consciente de las necesidades y demandas de los ciudadanos frente a los datos divulgados. El *cuarto*, la confidencialidad, el respeto a la confidencialidad es un principio ético fundamental en la protección de la privacidad y la confianza de las personas. El *quinto*, el compromiso social que implica que el responsable del tratamiento del dato debe estar comprometido con el bienestar de la sociedad y actuar de manera ética en su servicio a la comunidad. El *sexto*, el humanismo en el que se invita a actuar con sensibilidad y empatía hacia las necesidades y demandas del ciudadano, en especial frente al titular del dato. El *séptimo*, relacionado con la igualdad de trato y prohibición de la discriminación; estos principios éticos que promueven los valores de la justicia y la equidad. El *octavo*, la legalidad, que es un principio ético importante que implica respetar y cumplir con las leyes y regulaciones. El *noveno*, la objetividad, mediante la cual se promueve el actuar sin influencias

personales o subjetivas en el desempeño de las funciones, es un componente ético importante en la toma de decisiones justas. El *décimo*, relacionado con la tolerancia como un principio ético que promueve la comprensión y la convivencia pacífica. El *décimo primero*, utilidad pública, que implica que las acciones deben ser de utilidad para la sociedad en general.

La elección entre actuar según principios jurídicos o éticos no es una cuestión de "mejor" o "peor" camino para actuar por parte del responsable del dato en el momento de la divulgación, sino que ambos desempeñan roles importantes y a menudo se complementan, pues mientras el jurídico tiene la dirección de las leyes y regulaciones, lo ético va más allá de lo legal y se centra en considerar las implicancias de las acciones de este actor hacia la sociedad, cuando no mantiene un accionar integral.

3. El encargado del tratamiento del dato o *data processor*: Según el artículo tercero de la Ley 1581, el encargado del tratamiento es aquella "persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento", es decir, el encargado del tratamiento del dato realiza esta función por instrucción o delegación del responsable. Las obligaciones del encargado se encuentran establecidas en el artículo 17 de la Ley 1581, entre las que resaltan: "conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

Los valores éticos asociados a las actividades que realiza el encargado del dato según sus funciones deberían ser: autonomía, empatía, honestidad con el tratamiento del dato, y en la comunicación con el titular del dato, imparcialidad, orden, pluralismo, privacidad, respeto a las personas cuyos datos se van a usar, responsabilidad con la información durante todo el ciclo del dato, servicio, valor de comunicación. Estos valores permiten un correcto actuar frente a la disposición, utilización y tratamiento de los datos que, a nombre del responsable, realiza el encargado del dato.

Aunque no solo se deben observar estos valores para un desarrollo responsable de las actividades que desarrolla este actor. El principio ético de la accesibilidad, la anonimización o pseudoanonimización, la confiabilidad, la confidencialidad, la disponibilidad, la discreción, el humanismo, el cual busca un actuar con sensibilidad, y la empatía hacia las necesidades y demandas del ciudadano resultan primordiales. La igualdad de trato y de prohibición de la discriminación, la integridad, independencia frente a actividades, situaciones o terceros, la imparcialidad, la legalidad, la licitud y la lealtad, la limitación de la conservación, la minimización de datos y la objetividad.

En otras palabras, el servidor público debe tomar decisiones basadas en criterios técnicos y profesionales, sin dejarse influir por prejuicios, intereses personales o políticos, la profesionalidad, propósito legítimo y limitado, protección del dato y la privacidad, seguridad, mitigación de riesgos, transparencia y, finalmente, utilidad.

4. El Estado como actor relevante: Si bien dentro de los actores que plantea la normatividad colombiana respecto a la protección de datos no se encuentra directamente el Estado, bajo los hallazgos efectuados en esta investigación se considera que su rol y funciones son necesarios para implementar políticas eficaces tendientes a la correcta aplicación del tratamiento de datos personales en el sector público, especialmente en la actividad contractual que realizan las entidades. Las funciones de inspección, vigilancia, regulación, formulación de lineamientos y políticas, las desarrolla el Estado a través de entidades como la Superintendencia de Industria y Comercio, autoridad conferida a esta entidad en el artículo 19 de la Ley 1581.

Los valores éticos asociados al encargado según sus funciones son: dignidad humana, equidad, igualdad, libertad, pluralismo, respeto por los derechos humanos, responsabilidad. Ecuanimidad, que busca lograr un equilibrio en el internet que evite la creación de los monopolios tecnológicos y el control de unas minorías que concentran el poder sobre el uso y el acceso de la información.

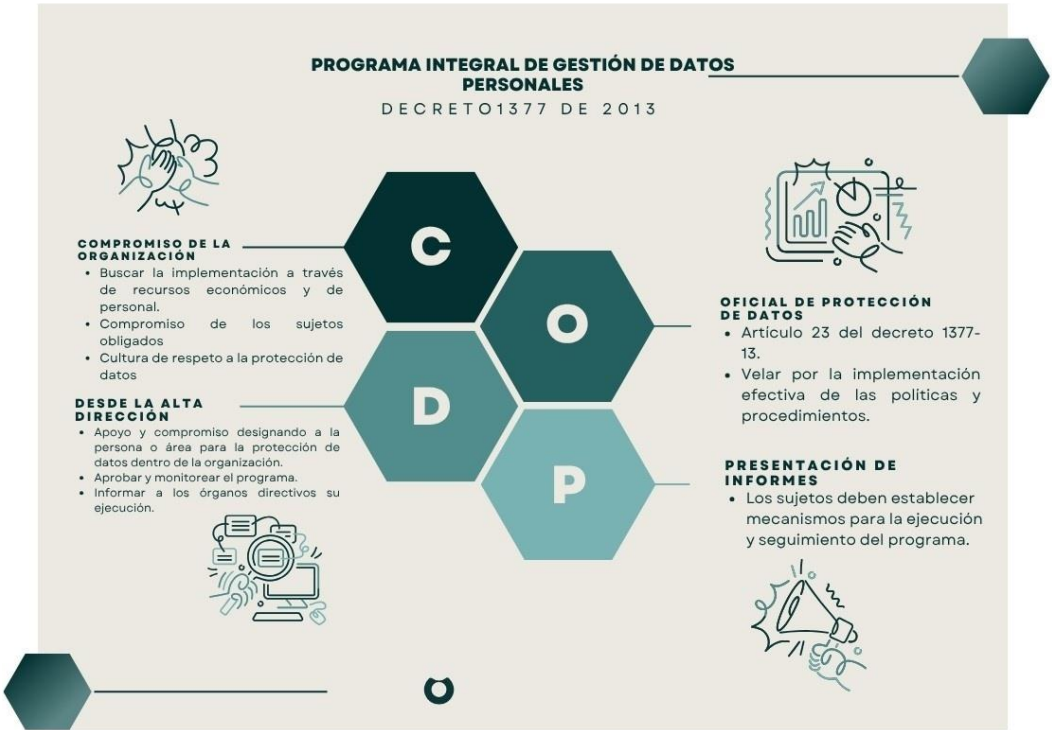
Los principios éticos que desarrollan los Estados de cara a la garantía de protección de los datos personales son: El Flujo Transfronterizo de Datos: busca la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos principios.

Hay excepciones, las cuales tendrán motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, o el interés público.

En segundo lugar, la protección por autoridades determinadas es otro principio que busca establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos principios. En tercer lugar, el principio *pro homine*, el cual se refiere a aquellas prerrogativas orientadas a la protección y promoción de los derechos humanos. En otras palabras, estos principios buscan proteger la dignidad humana y garantizar que se respeten los derechos fundamentales de todas las personas. Como cuarto principio se encuentra la democracia, para que las decisiones en materia de protección de datos tengan por finalidad el bienestar común.

La función de Inspección, Vigilancia y Control en cabeza de la Superintendencia de Industria y Comercio garantiza que las normas en materia de protección de datos se cumplan a través de medidas administrativas como la imposición de sanciones pecuniarias, las cuales deben ajustarse a ese catálogo de valores y principios mencionados. De ahí que se ha venido desarrollando el principio de responsabilidad demostrada o *accountability*, el cual busca de parte del responsable del tratamiento del dato demostrarle a la autoridad de protección de datos la implementación de un programa integral de gestión de datos personales a fin de evitar que se materialicen posibles riesgos, como los señalados en este estudio. Este programa se analiza a partir de los ejes que se muestran en la figura 7

Figura 7. Programa Integral de Gestión de Datos Personales



Fuente: elaboración propia a partir de la guía para la implementación del principio de responsabilidad demostrada, SIC.

Contar con una estructura administrativa conforme al gráfico anterior, requiere la adopción de mecanismos internos para poner en práctica tales políticas y adoptar procesos para la atención de respuesta a peticiones, reclamos respecto al tratamiento. Es así como el principio de responsabilidad demostrada permite a los responsables del tratamiento del dato demostrar a la entidad pública, en el caso de Colombia, a la Superintendencia de Industria y Comercio, que ha incorporado un programa de buenas prácticas en el ejercicio de tratamiento de datos personales,

a fin de evitar sanciones administrativa, pero también representa para la sociedad la confianza de las actividades que desarrolla la entidad, toda vez que es transparente en la forma como se trata los datos personales de los titulares.

Como puede observarse, las soluciones que se plantean desde la problemática expuesta son variadas. Entendiendo que la normatividad en materia de protección de datos en Colombia es abierta, se requiere la interpretación del responsable y encargado del dato. En este caso, las entidades estatales en los procesos de contratación estatal deben analizar, en cada caso, la aplicación política, jurídica y axiológica en relación con los datos personales que se expondrán en páginas de acceso abierto como SECOP II, junto a los derechos fundamentales de los titulares, para aplicar criterios de anonimización en los datos privados. Verbigracia, para el caso de las cédulas de ciudadanía que han sido definidas como datos complejos, toda vez que contiene datos públicos: número de cédula (Sentencia T-254/24), sexo o datos biométricos (sensibles) fecha y lugar de nacimiento (dato semiprivado), se recomienda en estos casos dejar de acceso abierto solo aquella información que no vulnere la intimidad del titular.

Así las cosas, un camino práctico que las entidades públicas puedan realizar en el ejercicio de la actividad contractual para proteger los datos que tiene a su cuidado es el uso de las guías de anonimización existentes como la publicada por el[3]. Son varias las entidades del orden nacional que han establecido protocolos de este tipo a fin de evitar la vulneración de derechos fundamentales y la protección de datos personales.

CONCLUSIONES

Cumplir con las leyes y regulaciones colombianas e internacionales aplicables a la divulgación de los datos en el proceso de contratación estatal es una prioridad absoluta, pues no cumplir con los requisitos legales puede resultar en graves consecuencias legales, financieras y de bienestar de los involucrados. Al mismo tiempo, se debe adoptar una perspectiva ética sólida al manejar datos. Esto implica considerar unos principios fundamentales, incluso y con prioridad cuando la ley no es específica al respecto. Así las cosas, es evidente la necesidad de fomentar una cultura jurídica y ética dentro del ciclo del dato. También implica capacitar al personal y tomar medidas proactivas para proteger a todos los actores.

En relación con las responsabilidades que la ley impone, resulta relevante contar con la claridad respecto del responsable, encargado del dato en el ciclo del dato. También, resulta relevan-

3 Al respecto véase: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/Guia_de_Anonimizacion-min.pdf

te identificar el rol de los estados, que, si bien no se encuentra concretamente definido como responsable en la ley, a través de las funciones de inspección y vigilancia frente al cumplimiento de las obligaciones del responsable y encargado, a través de la Superintendencia de Industria y Comercio se destaca que se incentive en el interior de las entidades políticas de responsabilidad demostrada a fin de evitar la imposición de sanciones por el manejo inadecuado de los datos personales que están obligados a tratar.

Una de las cuestiones que se identificaron en el desarrollo de este estudio fue que en el ejercicio de la actividad contractual que realizan las entidades públicas a través de la plataforma transaccional denominada SECOP II, cuyo acceso es libre, se puede conocer, descargar y disponer de datos de categoría privado, semiprivado e incluso sensible, generando afectación al titular del dato en su dignidad humana, buen nombre y demás bienes constitucionalmente protegidos. Lo que puede llevar a demandas legales y a la necesidad de indemnizar a las personas afectadas. Erosionar la confianza de los ciudadanos con las instituciones públicas y hasta afectar la reputación internacional del país.

En ese sentido, si bien la información relacionada con las compras públicas se encuentra dentro del marco del principio de máxima publicidad y están catalogados como datos abiertos, solo lo son en lo que tiene que ver con los gastos en contratación, por lo que la correcta y adecuada publicación de datos que tengan otra categoría (semiprivado, privado, sensible) debe articularse con los principios establecidos en la ley de protección de datos personales y con la vivencia de una ética del cuidado.

Los riesgos identificados se establecieron en distintos niveles, dependiendo de la gravedad en la afectación. Así, para el nivel 1, el riesgo es 0, toda vez que se obedece a datos públicos que no se requiere autorización del titular para ser publicada. El nivel 2, donde los datos a revelar son de categoría semiprivada; el nivel 3, donde los datos publicados son los datos privados; el nivel 4, donde la entidad publica datos sensibles, y el nivel 5, que se refiere a aquella información no regulada como extremo daño.

Frente a los riesgos identificados desde el nivel 2 al 5 resulta relevante adoptar acciones correctivas a través de políticas eficaces en el interior de la entidad para evitar el riesgo antijurídico de cara a la afectación de derechos fundamentales de los titulares.

Finalmente, se propone la adopción de valores y principios tanto éticos como jurídicos para que las entidades públicas identifiquen la clase de dato a publicar y con base en ello establecer los controles adecuados para evitar que los riesgos identificados se materialicen. Bajo la premisa de

que el uso poco ético de los datos no siempre es ilegal, pero puede ser considerado indeseable desde la perspectiva de ciertos valores, principios y contextos como los aquí expuestos.

REFERENCIAS

ActionsDATA. (2022). *Ética de datos: la solución para el buen uso de la información en la era digital*. Recuperado el 13 de febrero de 2022, de: https://www.actionsdata.com/blog/etica-de-datos-la-solucion-para-el-buen-uso-de-la-informacion-en-la-era-digital.

Alarcón Requejo, G. (2022). Precisiones al derecho de acceso a la información pública a partir del primer precedente del Tribunal de Transparencia y Acceso a la Información Pública del Perú. *Revista de Derecho*, *58*. doi: https://dx.doi.org/10.14482/dere.58.128.964

Argentina. Ley 25.326/2000, de 4 de octubre, Ley de Protección de los Datos Personales.

Bautista Avellaneda, M. E. (2015). *El derecho a la intimidad y su disponibilidad pública*. Universidad Católica de Colombia. Colección JUS público.

Bejarano Roncancio, J. (2009). Fundamentos de contratación pública para proyectos sociales en alimentación y nutrición [online]. Universidad Nacional de Colombia.

Buenadicha, C., Galdon Clavell, G., Hermosilla, M. P. y Loewe, D., Pombo, C. (2019). *Algoritmos y derechos humanos: una guía práctica para una evaluación de impacto*. Banco Interamericano de Desarrollo.

Colombia Compra Eficiente, Agencia Nacional de Contratación Pública. (2019). Circular externa 001/2019 de 22 de agosto. Obligatoriedad del uso de SECOP II en 2020.

Colombia Compra Eficiente, Agencia Nacional de Contratación Pública. (2021). Circular externa 001/2021, de 10 de febrero, obligatoriedad del uso de SECOP II vigencia 2021.

Colombia Compra Eficiente, Agencia Nacional de Contratación Pública. (2023). Circular externa 005/2023, de 31 de agosto. Obligatoriedad del SECOP II para la vigencia fiscal 2023.

Colombia Compra Eficiente, Agencia Nacional de Contratación Pública. (2023). Guía para la incorporación de lineamientos de integridad en la contratación de prestación de servicios. Recuperado el 11 de febrero de 2025, dehttps://www.colombiacompra.gov.co/sites/cce_public/files/cce_documents/cce-eicp-gi-23_guia_contratacion_prestacion_de_servicios_v1_11-07-2023_def_1_1.pdf

Congreso de la República de Colombia. (2015, 9 de junio). Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”..

Congreso de la República de Colombia. (2015, 6 de julio). Ley estatutaria 1757. Por la cual se dictan disposiciones en materia de promoción y protección de derecho a la participación democrática.

Congreso de la República de Colombia. (2017, 11 de septiembre). Decreto 1499. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Constitución Política de la República de Colombia, 20 de julio de 1991.

Consejo de Estado. (2014, 14 de septiembre). Sentencia de unificación, rad. 05001-23-25-000-1999-01063-01(32988), C.P. Ramiro de Jesús Pazos Guerrero. Actor: Félix Antonio Zapata González y otros. Demandado: Ministerio de Defensa - Ejercito Nacional.tros. Demandado: Ministerio de Defensa - Ejercito Nacional.

Consejo de Estado. (2021, 6 de mayo). Sentencia 2458/2021. Concepto de la sala de consulta y servicio civil. C.P. Álvaro Namén Vargas. Radicación Nº: 11001-03-06-000-2020-00234-00(2458). Actor: Ministerio de Transporte.

Corte Constitucional de Colombia (1992, 5 de junio). Sentencia T406/1992. Proceso de acción de tutela promovido por el señor José Manuel Rodríguez Rangel contra el señor Enrique Chartuny González, gerente de las Empresas Públicas de Cartagena y resuelto en primera instancia y única instancia por el Tribunal Contencioso Administrativo de Bolívar.

Corte Constitucional de Colombia. (2011, 6 de octubre). Sentencia C748/2011. Control constitucional al Proyecto de Ley Estatutaria Nº 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales".

Corte Constitucional de Colombia. (2020, 29 de enero). Sentencia C022/2020. Control constitucional al artículo 162 (parcial) de la Ley 1819 de 2016. Por medio de la cual se adopta una reforma tributaria estructural, se fortalecen los mecanismos para la lucha contra la evasión y la elusión fiscal y se dictan otras disposiciones.

Corte Constitucional de Colombia. (2024, 2 de julio). Sentencia T-254/2024. Proceso de acción de tutela promovido por Pablo y Marcela contra Colegio Privado.

Colmenarejo Fernández, R. (2017). *Una ética para big data. Introducción a la gestión ética de datos masivos*. Editorial UOC.

Comité Jurídico Interamericano Organización de los Estados Americanos. (2021). *Principios actualizados sobre la privacidad y la protección de datos personales (con anotaciones)*.

Comisión para el Acceso a la Información Pública y Protección de Datos Personales del Estado. (s.f.). Código de Ética. Recuperado el 3 de febrero de 2023, de: https://www.infomexjalisco.org.mx/sites/default/files/documentos/CodigoEtica.pdf

Cortina, A. (2013). *¿Para qué sirve realmente la Ética?* Paidós.

Cuello Quiñonez, M. M. y Sardoth Redondo, A. K. (2018). [Tesis de especialización, Universidad Santo Tomás]. Principio de proporcionalidad y test de ponderación como técnica para dar solución a derechos fundamentales en conflicto en derecho administrativo en el tiempo posmoderno. Club CDO Spain. (28 de marzo de 2019). *Debate Club CDO Spain: Poniendo el "Data" en el "Ethics"*. https://empresas.blogthinkbig.com/debate-club-cdo-spain-poniendo-el-data-2/

Departamento Nacional de Planeación (DNP). (2021). *CONPES4070. Lineamientos de política para la implementación de un modelo de estado abierto*. Bogotá, D.C.

Departamento Nacional de Planeación. (DNP). (2010, 12 de abril). CONPES 3654: "Política de rendición de cuentas de la rama ejecutiva a los ciudadanos".

Departamento Nacional de Planeación. (DNP). (2020). Documento de Análisis de información Mapeo de Iniciativas de Innovación Pública. Grupo de modernización de Estado. Equipo de innovación pública.

Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic). (2019). *Guía para para el uso y aprovechamiento de Datos Abiertos en Colombia*. Bogotá, D.C.

Duque Botero, J. (2020). Los principios de transparencia y publicidad como herramientas de lucha contra la corrupción en la contratación del Estado. *Revista Digital de Derecho Administrativo*, *24*, 79-101. doi: https://doi.org/10.18601/21452946.n24.04.

Duro Carrión, S. (2021). Los valores y principios constitucionales como límites a la actuación de los poderes del estado y la función pública. *Revista de Derecho Político*, *111*, 225-254.

Estrada Vélez, S. (2011). La noción de principios y valores en la jurisprudencia de la Corte Constitucional, *Revista de la Facultad de Derecho y Ciencias Políticas Universidad Pontificia Bolivariana*, *41* (114). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-38862011000100002. [Consultado 31-10-2023]

ESET. (2023, 13 de febrero). Panorama de la protección de datos en los países de LATAM. WeLiveSecurity. Recuperado el 13 de febrero de 2025, de: https://www.welivesecurity.com/es/privacidad/panorama-proteccion-datos-paises-latam/

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A. *Mathematical, Physical and Engineering Sciences*, *376*(2133), 1-19. http://dx.doi.org/10.1098/rsta.2016.0360

Franzke, A., Muis, I. y Schäfer, M. (2021). Data Ethics Decision Aid (DEDA): un marco dialógico para la investigación ética de proyectos de IA y datos en los Países Bajos. *Ethics and Information Technology*, *23*, 551-567. https://doi.org/10.1007/s10676-020-09577-5.

Herrero, J. (2023). *Protección de Datos Personales en América Latina y el Caribe: un Estudio Comparado* [Tesis de grado, Universidad Torcuato Di Tella]. Repositorio Digital Universidad Torcuato Di Tella. https://repositorio.utdt.edu/handle/20.500.13098/12190

IDECA. (2018). *Buenas prácticas para la publicación de datos*. http://www.ideca.gov.co

Informe del Secretario General de las Naciones Unidas. (1990). Principios rectores para la reglamentación de los ficheros computadorizados de datos personales. A/44/606. https://undocs.org/es/A/44/606

Lucas Ortegón, C. A. (2017). Actividad contractual de entidades territoriales a la luz de los principios de la contratación estatal. *Advocatus*, *28*, 215-239. doi: 10.18041/0124-0102/advocatus.28.899.

Martínez, S. (2007). *Manual de derecho Constitucional*. Tirant Lo Blanch.

Mellado Ruiz, L. (2017). *El principio de transparencia integral en la contratación del sector público*. Tirant Lo Blanch.

México. (2010, 5 de julio). Ley Federal de Protección de Datos en Posesión de Particulares. *Diario Oficial* de la Federación.

Ministerio de Educación Nacional [MEN]. (2011). *Código de Ética y Buen Gobierno*.

Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic). (2020). Resolución 1519/2020, de 24 de agosto, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Sánchez Díaz, M. F. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, vol. 10, 1- 23p. DOI: https://doi.org/10.14409/redoeda.v10i1.12626

Superintendencia de Industria y Comercio. (SIC). (2015). *Políticas de datos personales*. https://www.sic.gov.co/sites/default/files/documentos/072020/Pol%C3%ADtica%20de%20Tratamiento%20de%20Datos%20Personales%20-%20SIC.pdf

Superintendencia de Industria y Comercio. (SIC). (s.f.). *Guía para la implementación del principio de responsabilidad demostrada*. Bogotá, D.C.

Tribunal Administrativo de Cundinamarca, Sección Tercera, Subsección A. (2022, diciembre 12). *Sentencia, rad. 11001-33-37-044-2017-00249-02, medio de control de reparación directa. Actor: Nación – Fiscalía General de la Nación*.

Universidad de Castilla-La Mancha. (2019). *Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha, vol. 1,* 1- 53.

Unión Europea (2016, 27 de abril). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Yáñez, M., Ramírez, D. y Rangel, D. (2023). Configuración de la cláusula general de fuentes del derecho en Colombia: problemas y desafíos a partir de la complejidad del sistema normativo y los medios de control de la actividad de los particulares y las autoridades. *Revista de Derecho*, *60*, 140-165. doi: https://dx.doi.org/10.14482/dere.60.407.897